Eşler Arası Ağlarda Teşvik Modelleri

Serkan Çakmak, Ahmet Burak Can

***Özet*—Eşler arası ağlar, kaynak paylaşımı, yönlendirme, ve kaynak arama gibi görevlerde eşlerin katkı sağlaması ilkesine göre çalışır. Eğer eşlerin bir kesimi, sisteme bu görevlerde katkı sağlamazsa, sistem verimliliği ve etkinliği önemli zarar görür. Bu bildiri, eşler arası ağlarda eşleri teşvik ederek sisteme katkıda bulunmalarını sağlamak üzere tanımlanmış olan teşvik yaklaşımları üzerine bir literatür taraması sunmaktadır. Teşvik modellerinin neden ortaya çıktığı, bu amaçla hangi yöntemlerin uygulandığı ve bazı yaygın eşler arası uygulamalarda kullanılan teşvik modelleri anlatılacaktır.**

***Anahtar Kelimeler*—Eşler arası ağlar, teşvik modelleri, oyun teorisi, karşılıklılık, mikro para modelleri**

Incentive Models in Peer-to-Peer Networks

***Abstract*— Peer-To-Peer networks work relying on involvement of peers on tasks like resource sharing, routing, and querying of resources. If some peers do not contribute to the system, efficiency and effectiveness of the system is damaged. This paper presents a literature review about incentive approaches in peer-to-peer networks used to encourage peers to contribute to the system. Why incentive models are appeared, approaches applied for this goal, and some incentive models used by common peer-to-peer applications will be explained.**

***Index Terms*—Peer-to-peer networks, incentive models, game theory, reciprocity, micro money models**

I. GİRİŞ

Bilgisayar ağlarının gelişimine baktığımızda, son senelerde eşler arası ağlar (peer-to-peer- P2P), istemci-sunucu mimarisi yanında alternatif bir ağ modeli olarak ortaya çıkmıştır. İstemci-sunucu mimarisinde bir tane veya birkaç sunucu bulunmakta ve diğer bütün istemciler bu sunuculardan indirme işlemini gerçekleştirmektedirler. Bu durumda merkezi bir yönetim ve hataya duyarlı tek bir nokta (single point of failure) olduğu net bir biçimde görülmektedir. Ayrıca, her istemcinin indirme hızı, sunucunun paylaşılan yükleme hızı ile sınırlı kalmaktadır. Ancak P2P ağlarda ortada bir istemci ve sunucu yoktur. Her eş aynı anda istemci ve sunucu olabilir. Bir eş başkalarına hizmet sağlarken sunucu görevi görebilirken, başkalarından hizmet elde etmek için de istemci görevini üstlenir. Bu ağlardaki eşlerin, hem istemci, hem de sunucu olarak görev yapabilmesi tamamen dağıtık ağ topolojileri tanımlamaya imkan tanımaktadır. P2P sistemler, dağıtık olmaları nedeni ile dosya dağıtım sistemleri için istemci-sunucu mimarisine ciddi bir alternatif olmuşlardır.

Bu metin 15 Temmuz 2013 tarihinde gönderilmiştir.

Serkan Çakmak, Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Yüksek Lisans yapmaktadır. (e-mail: serkancakmak89@gmail.com).

Ahmet Burak Can, Hacettepe Üniversitesi, Bilgisayar Mühendsiliği Bölümü'nde görev yapmaktadır. (e-mail: abc@hacettepe.edu.tr).

P2P ağlarda, eşlerin ağ üzerinde yürütülen dağıtık işlemlerde görev alması ve sisteme kaynak sağlaması, ağın devamı açısından çok önemlidir. Bazı durumlarda eşler, ağa hiç katkı sağlamadan sistem kaynaklarını kullanmaya çalışmakta veya ağın kaynakları kullandıktan sonra ağa katkı sağlamayı bırakmaktadır [1]. Bu durum, ağın etkinliğini ciddi ölçüde etkilemekte ve bazı eşlere fazla yük binmesine sebep olabilmektedir. Bu nedenle, ağ üzerindeki bütün eşleri sistem katkı sağlamaya motive etmek ve bazen de zorlamak üzere teşvik (*incentive*) modelleri önerilmiştir. Teşvik modelleri, P2P ağlarda çeşitli yöntemler uygulayarak kaynak paylaşımını artırmayı amaçlayan modellerdir. P2P ağlarda eşleri daha fazla sisteme katkı sağlamaya teşvik etmek ve sisteme herhangi bir fayda sağlamadan sistemden yararlanan kullanıcıları engellemek teşvik modellerinin en önemli görevidir.

Bu bildiride, teşvik modelleri hakkında yapılmış çalışmalar incelenecektir. Kesim II'de teşvik modelleri üzerine yapılabilecek saldırılar irdelenecektir. Kesim III'te teşvik modelleri ve iktisat teorileri arasındaki ilişki açıklanacaktır. Kesim IV'te teşvik modellerinde kullanılan bazı temel yaklaşımlar aktarılacaktır. Kesim V'te sonuçlar ve gelecekte yapılabilecek çalışmalar özetlenecektir.

II. EŞLER ARASI PAYLAŞIM PROBLEMLERİ

P2P sistemlerin gücü, eşlerin gönüllü paylaşımından gelmektedir. P2P sistemlerinde merkezi bir otoritenin olmaması ve gücünün gönüllü paylaşımdan gelmesi teşvik modellerini kaçınılmaz olarak ortaya çıkarmıştır. Çünkü istemci-sunucu mimarisinde indirme için sunucunun kurallarına uymak zorunda olan kullanıcılar, eşler arası ağlarda yöneticinin olmaması nedeniyle rasyonel davranışlar göstererek kendi kişisel karlarını en fazla yapmaya çalışırlar. Bu rasyonel davranışa sahip kullanıcılar birçok P2P uygulamanın sorunu olmuşlardır [1]. Örneğin Gnutella ve Napster üzerinde yapılan araştırmalar göstermiştir ki, bu uygulamaları kullanan kullanıcıların %50'sinin oturum süreleri 1 saatten azdır ve çoğunluğu paylaşım yapmamaktadır [2]. Kullanıcıların kendi karlarını artırma isteğinden dolayı ortaya çıkan problemler arasında en yaygın olanları, bedavacılık (*free riding*), geçmişi silme (*white washing*) ve çoklu kimlik tanımlama (*sybil attack*) problemleridir. Şimdi bu problemleri inceleyelim.

Bedavacılık (Free Riding)

Bedavacılar sisteme hiçbir katkı yapmadan sistemden yararlanan kullanıcılara denir [1,5]. Bu davranışın temel nedeni, kullanıcıların (eşlerin) kendi karlarını artırırken, sisteme herhangi bir katkı (işlemci zamanı, disk alanı, vb.) vermeden elde etmek istedikleri kaynaklara ulaşmaya çalışmalarıdır. Bu davranış biçimi, aslında insan doğasından gelen bir davranıştır. Bir kullanıcı bir şeyi bedava elde edebiliyorsa neden para/kaynak versin ki? Bu noktada,

kullanıcıları para/katkı vermeye teşvik edecek veya hatta bazen zorlayacak bir sistem olmalıdır.

Geçmişi Silme (White Washing)

Bedavacılığı önlemeye yönelik bir yöntem kullanan sistemlerde, bazen bedavacı olan kullanıcılar (eşler) sürekli olarak sistemden ayrılıp tekrar sisteme katılırlar. Böylece geçmişlerini silerek bedavacılık cezalarından kurtulmaya çalışırlar [5,24]. Özellikle itibara dayalı güven modelleri (reputation-based trust models) [25,26] bu ataklara duyarlıdır. Bu atağın ortaya çıkma nedeni, sistemdeki kimlik alma maliyetinin az olması veya olmaması ve kullanıcıların anonim olarak sisteme katılabilmeleridir. Kullanıcıların sürekli olarak kimlik değiştirip sahte kimlikle sisteme katılabilmesi çeşitli yöntemler ve cezalarla engellenmeli veya en azından zorlaştırılmalıdır.

Çoklu Kimlik Tanımlama (Sybil Attack)

Sybil saldırısında [3], saldırıyı yapan kullanıcı (eş) büyük miktarda sahte eş ve kimlikler oluşturarak sistemdeki teşvik modelini kandırmaya çalışır. Oluşturduğu sahte kimlikteki kullanıcılara sürekli olarak kaynak sağladığını iddia ederek, teşvik modelini kandırmaya ve sistemdeki diğer eşlerin kaynaklarından daha çok yararlanmaya çalışır. Sistemde güvenilir otorite olarak görev yapan bir merkez olmadığı sürece, bu atağın her zaman olma olasılığı vardır.

III. TEŞVİK MODELLERİ VE İKTİSAT İLİŞKİSİ

P2P sistemlerde teşvik modelleri ile iktisat alanı arasında ilk başta ilişki kurmak zor görünebilir, ancak P2P teşvik modellerindeki problemler, genel kullanıcı davranışları, sistemin ve kullanıcıların kar maksimize etme davranışları, iktisattaki bazı konularla oldukça paralellik göstermektedir. Şimdi şırasıyla iktisat alanından ortak malların trajedisi, oyun teorisi, ve mahkûmlar çıkmazı konularını inceleyeceğiz.

A. Ortak Malların Trajedisi Kuramı

Ortak Malların Trajedisi Kuramı [19], isminden de anlaşılacağı gibi iktisatta kamu malları gibi ortak malların yaşadığı trajediyi anlatmaktadır. Şöyle ki, kamusal mallar herkes tarafından kullanılması serbest, herkese yarar sağlayan, buna karşılık herhangi bir gideri olmayan mallardır. Yani bir kamu malı kullanımı sonucu yarar sağlarken, herhangi bir ücret verilmez. Bu gibi durumlarda kişiler başkalarından bağımsız olarak sadece kendilerini düşünerek, rasyonel davranışlarda bulunarak kendi karlarını maksimize ederler. Ancak böyle bir durumda, kamusal mal gereğinden çok daha hızlı sürede yaşam evresini tamamlayabilir ve tükenebilir. Bu duruma, kamusal malların trajedisi denir. Kamusal malların sahipliği tek bir kişi değil birçok kişiye aittir. Bu durum aslında kamusal malları sahipsiz yapmakta ve çok daha hızlı yıpranmalarına, tükenmelerine yol açmaktadır. Örneğin bir kamu alanındaki park ile bu park ile aynı yerdeki özel bir bankayı ele alalım. Her ikisinin de içinde kişilerin oturması için banklar olduğunu düşünelim. Her iki oturma bankının da aynı kişiler tarafından kullanıldığı varsayılsa bile ufak bir tahmin ile park içindeki bankın çok daha kısa sürede işlevini yitireceği ve eskiyeceğini tahmin etmek mümkündür.

Ortak malların trajedisi kuramı, ek olarak kamusal mallardan yararlanma ücreti konusuna da değinir. Ortak malların kullanım ücretleri herkes için sıfırdır. Bu durumda ortaya çıkan sonuç, herkes herhangi bir ücret ödemeden kamusal mallardan sınırsız fayda sağlayabilmektedir. Bu durumda kamuya katkı sağlayan bir insan ile sağlamayan bir insan ayrımı yoktur. Örneğin vergi veren ve vermeyen 2 kişiyi düşünecek olursak, bu iki kişinin de sokağındaki lamba yanmaktadır. Bu durumda vergi veren ve vermeyen kişileri nasıl ayırt edip insanları vergi vermeye teşvik edebiliriz.

Yukarıda anlattığımız ortak malların trajedisi kuramı ile ilgili problemler, P2P teşvik modellerinin karşılaştığı problemler ile benzerlikler göstermektedir. P2P sistemlerde paylaşım yapan kullanıcı ile paylaşım yapmayan kullanıcının ayırt edilmesi ve ortak sistem kaynakları kullanılırken eşlerin paylaşım yapmaya teşvik edilmesi gerekmektedir.

B. Oyun Teorisi ve Nash Dengesi

Bazı problemlerde, değişkenlerin tümü kontrolümüz altında olmayıp iki ya da daha fazla tarafça kontrol edilebilir. Yani değişkenlerin bir kısmı bizim, başka bir kısmı da başkalarının kontrolü altında olabilir. Bu durumda sorunun çözümü için şu kural uygulanır:

- Kazancı maksimum yapmak
- Eğer kazanma şansı yoksa kaybı minimum yapmak

Oyun teorisinde amaç karar verme stratejisi geliştirmektir. Modern Oyun Teorisi ilk olarak John von Neumann tarafından ortaya atılmıştır [20,21]. Oyun teorisinde genel amaç karşındaki kişinin yapacağı tercihleri de göz önünde bulundurarak kendin için en yararlı veya en az zararlı tercih için bir strateji belirlemektir. John von Neumann tarafından ortaya atılan iki kişilik sıfır toplamlı oyunda, oyun sonunda oyunculardan birinin kaybı diğerinin kazancına eşittir.

İkiden fazla sayıda oyuncunun yeraldığı oyunlarda, denge durumunu modellemeyi amaçlayan Nash dengesi yaklaşımı, ilk olarak olarak Steve Nash tarafından ortaya atılmıştır [22]. Bu modele göre, oyuncuların birbirlerinden bağımsız kararlar verdiği bir oyunda (non-cooperative game), oyuncular mevcut stratejilerini değiştirerek herhangi bir kazanç sağlayamıyor ise, bu oyuncular birbirleri ile Nash dengesindedir. Klasik Nash dengesi, diğer eşlerin hangi stratejiyi uygulayacağına dair sonsuz spekülasyon ve karşı spekülasyon döngüsünden çıkış yolu gösterir. Bir eş, denge stratejilerini değiştirse bile, hiçbir eşin faydasını artıramadığı yerel optimum strateji kümesi böylece elde edilir.

P2P ağlarda da, kullanıcılar arası etkileşimler çok kullanıcılı bir oyun olarak düşünülebilmektedir. Bir teşvik modeli ile kullanıcılar bazı davranış örüntülerine yönlendirilerek bu oyunda denge sağlanmaya çalışılmaktadır. Böyle bir denge durumunda, istenen davranıştan farklı bir davranış sergileyen (örneğin kaynak paylaşmayan) eşlerin oyun genelinde zarar etmesi sağlanmaya çalışılmaktadır.

C. Mahkumlar Çıkmazı (Prisoner's Dilemma)

Mahkûmlar çıkmazı [23], iki bireyin karlarını maksimize etmek istemeleri durumunda, bireylerin kişisel karlarını maksimize etmek için seçtikleri stratejinin her zaman en iyi karı sağlamadığını göstermek için geliştirilmiş bir oyundur. Mahkûmlar çıkmazına göre iki tutuklu ayrı ayrı odalarda

sorgulanır. Her bir tutuklunun iki seçeneği vardır. İtiraf etmek, ve sessiz kalmak. Eğer iki tutuklu da sessiz kalırsa; iki tutuklu da birer yıl ceza alacaktır. Eğer bir tutuklu itiraf eder, diğer tutuklu sessiz kalırsa; itiraf eden serbest kalırken, diğer tutuklu on yıl ceza alacaktır. Eğer iki tutuklu da itiraf ederse; iki taraf da beşer yıl ceza alacaktır. Buna göre bireysel kar maksimizasyonu düşüldüğünde, iki tutuklu da en az cezayı almak için itiraf edecektir ve iki tutuklu da zarar görecektir. Aksine iki tutuklu da sessiz kalsa, en az ceza alınabilirdi.

P2P ağlardaki problemler kapsamında düşünüldüğünde, Oyun Teorisi, Nash Dengesi ve Mahkumlar Çıkmazı problemleri, teşvik modellerinde eşlerin paylaşım yapıp yapmayacaklarına, katkı sağlayıp sağlamayacaklarına karar vermede kullanılabilmektedir.

IV. TEŞVİK MODELLERİNDE TEMEL YAKLAŞIMLAR

Teşvik modelleri, yukarıda bahsettiğimiz problemlerle baş etmek ve kullanıcıları sisteme katkı sağlamaya daha fazla teşvik etmek için geliştirilmiş modellerdir. Modeller için çeşitli yaklaşımlar mevcuttur. Bu bölümde, teşvik modelleri üzerine yapılan bazı çalışmalar incelenecektir. Yaygın olarak kullanılan bazı P2P uygulamalar üzerindeki teşvik modellerine de değinilecektir.

A. Mütekabiliyet (Reciprocity) Tabanlı Yaklaşımlar

Mütekabiliyeti esas alan yaklaşımlarda, eşler diğer eşlerin geçmişi hakkında bilgi tutarlar ve bu bilgiyi paylaşım için karar vermede kullanırlar. Geçmişte bir kullanıcının sisteme sağladığı katkı bilgisi saklanarak daha sonraki hizmet alımında kendisine yarar sağlar. Bu yaklaşımlar, doğrudan ve dolaylı mütekabiliyet tabanlı olmak üzere ikiye ayrılır. Doğrudan mütekabiliyeti esas alan yaklaşımlarda, X, Y ile hangi seviyede iş birliği yapacağını, geçmişte Y'den aldığı servise göre karar verir. Yani bir eş karar aşamasında sadece kendi tuttuğu geçmişe güvenir. Doğrudan mütekabiliyet, genelde uzun süren etkileşimler içeren uygulamalar için daha uygundur. Örneğin, Bittorrent [8] uygulaması bu modeli kullanır. Deneysel ve analitik çalışmalara göre bu yaklaşım, sistemdeki işbirliğini artırdığını gösterse de, free rider problemini tam olarak çözemez [6].

Dolaylı mütekabiliyet yaklaşımında, X eşi Y eşi ile hangi seviyede iş birliği yapacağını, kendisi ve diğer eşlerin de geçmişte Y'den aldığı servise (Y'nin geçmişine) göre karar verir. Yani bir eş karar aşamasında sadece kendi tuttuğu geçmişe değil başka eşlerin tuttuğu geçmişe de güvenir. Genelde bu yaklaşım, itibara dayalı güven modelleri (reputation-based trust models) [25, 26] ile birlikte kullanılır ve doğrudan mütekabiliyet yaklaşımına göre, bedavacılık problemi için genelde daha gerçekçi sonuçlar verir. Fakat 3. parti gözleme güvenmek zorunda olduğundan geçmiş temizleme ve çoklu kimlik tanımlama saldırılarına karşı duyarlıdır.

Mütekabiliyet tabanlı bazı yaklaşımları şöyle özetleyebiliriz.

Kalıtsal Cömertlik (Inherent Generosity) [4]

James Andreoni [4] tarafından geliştirilen modelde, kullanıcı cömertliği de işin içine katılarak bedavacılık ve geçmişi silme sorunları ile başa çıkılması amaçlanmıştır. Bu modelde popülasyon dağılımına göre bedavacılık oranı bulunması amaçlanmıştır. Bu modele göre, cömertlik/popülasyon oranı, belli bir eşik değerinin altında ise, sistemin etkin bir şekilde çalışmadığı; üstünde ise sistemin sürdürebilir olduğunu söylenir. Benzer şekilde, [5]'in yazarları da bu yaklaşımın benzerini kullanan bir model geliştirmişlerdir.

BitTorrent [8]

BitTorrent [8] eşlerin, diğer eşlerden dosya indirebildiği dağıtık dosya paylaşım ve indirme sistemidir. Temel fikri dosyayı parçalara ayırır ve her bir parçayı farklı eşlerden indirebilir. Böylece eşler, işbirliği yaparak eksik parçaları tamamlamaya çalışırlar. Bu yöntem, hataya duyarlı tek bir notayı (*single point of failure*) ve tek bir sunucu üzerinden dosya indirmede karşılaşılan kısıtları ortadan kaldırırken, eşleri işbirliğine zorlar. Yani sistem tasarımcıları, eşler için bir teşvik modeli sağlamışlardır. BitTorrent bugün için çok yaygındır ve bu protokol üzerinde bir çok araştırma yapılmıştır. Bunun nedenleri şöyle sıralanabilir: Sistemin kullanıcıların kendi karlarını maksime edeceği düşünülerek tasarlanmış olması, sistem tasarımında bir teşvik modeli olması, sistemin analitik ve ekonomik deneyler için uygun olması ve çok yaygın kullanılmasıdır [10, 11].

BitTorrent'teki teşvik mekanizması tit-for-tat stratejisine veya mahkumlar çıkmazı modeline dayanan yükleme ile orantılı bir indirme mekanizmasıdır. BitTorrent'te takipçiler (*tracker*) bir dosyaya tamamen veya kısmen sahip olan eşlerin listesini tutar. Dosyanın tamamına veya bir kısmına sahip her eş, takipçi tarafından takip edilir. Yeni bir eş sisteme katıldığında takipçi ile iletişim kurup, dosyayı indirebileceği eşlerin listesini takipçiden ister. Bu eşler de, yeni katılan eşle iki taraflı TCP bağlantıları kurarlar. Bu bağlantılar yardımıyla küçük bir eş altkümesi seçilmiş olarak işaretlenir. Dosyanın tamamına veya bir kısmına sahip eşler, daha iyi işbirliği sağlayan eşleri bulmak için belli aralıklarla iyimser seçme stratejisini kullanırlar. Eşler, belli aralıklarla, sağladıkları yükleme hızına göre, işbirliği yapacağı k tane eşi seçer. Böylece yüksek yükleme hızı sağlayan eşler, daha çok seçildikleri için, daha yüksek indirme hızları ile dosya indirebilirler. Bu özelliklerine rağmen, Bittorrent geçmiş temizleme ve çoklu kimlik tanımlama saldırılarına karşı savunmasızdır.

BitTyrant [9]

Bazı durumlarda BitTorrent'in teşvik modeli alt edilebilir [9]. Tit-for-tat stratejisi, kaynak paylaşımı ile kaynak indirimini dengelese ve zamanla evrensel dengeye ulaşan bir strateji olsa dahi, pratikte yüksek kapasitedeki (bant genişliği yüksek) kullanıcılar, indirme işlemini daha erken bitirdikleri için kaynak paylaşımını da erken sonlandırma eğilimindedirler. Bu durum, tit-for-tat stratejisinin istenilen şekilde çalışmasını engeller ve yüksek kapasiteli kullanıcıların sistemi sömürmesine yol açar. BitTyrant uygulamasının ana fikri, BitTorrent'teki yükleme hızından bağımsız olarak yapılan statik yaklaşımın tersine, her eş bir tit-for-tat oturumunda belli sayıda veri gönderdiği eşleri dinamik olarak seçer.

BitTyrant sisteminde *d*, eşin sisteme sağladığı katkı ve *u*, eşin kazanması gereken mütekabiliyet oranı olmak üzere, *d/u* oranı dikkate alınarak en yüksek orana sahip eşler seçilir. Her bir döngüde eğer bir eş sisteme katkıda bulunmamış ise onun *u* değeri artırılırken, bir başka eşe veri yollamış ise onun *u* değeri azaltılır. Yapılan deneylerde BitTyrant'ın

BitTorrent e göre 3 kat daha hızlı indirme sağladığı gözlenmiştir [9]. BitTyrant'ın bu performansı şöyle açıklanabilir: a)BitTyrant uzun süreli sürekli performans sağlar, b)yüksek kapasiteli eşler için azalan marjinal fayda prensibini içerir c)düşük kapasitedeki eşlere sistemden göreli fazla fayda sağlar. Fakat BitTyrant'ın artan performansı bize bir maliyet ile döner. Yeni kullanıcıların uzun ön yükleme süreleriyle karşılaşmaları buna örnek verilebilir. Ayrıca BitTyrant, BitTorrent gibi geçmiş temizleme ve çoklu kimlik tanımlama saldırılarına karşı dirençsizdir.

Credence [7]

Credence [7] içerik kirliliğini engellemek için tasarlanmış bir dağıtık itibar sistemidir. Credence sistemi ile kullanıcı, dosyanın veya online içeriğin gerçekten iddia edilen dosya/içerik olup olmadığına karar verebilir. Kullanıcılar sistem içeriklerini oylarlar ve sistem benzer oyları ağırlıklandırır. Bir benzerlik ölçütüne (*similarty measure*) göre, doğru oyları yüksek ağırlık vererek, sahte oyları ise düşük ağırlık vererek değerlendirir. Böylece kullanıcılara doğru oy vermeleri için bir teşvik modeli sağlar. Bu sistem gnutella ağı içerisinde limeware uygulamasında uygulanmıştır. Böylece kullanıcının, sorguladığı dosyanın gerçekten aradığı şey olup olmadığına karar vermesine ve dosyaları indirmeden değerlendirmesine olanak sağlanmıştır.

Buradaki içerik kirliliği tanımında, belirtilen içeriğe sahip olmayan her şey olarak tanımlanmıştır. Bu modeli ortaya koyan yazara göre, içeriğin kirli olup olmadığını değerlendirmede en etkin yol, matematiksel ve istatiksel yöntemlere oranla dürüst kullanıcılardır. Credence yaklaşımında kullanıcı, dosyayı/içeriği indirdikten sonra tek bir oy hakkına sahip olur. Doğru dosya için pozitif, yanlış dosya için negatif oy verilir. Oylar inkar edilememe ilkesi (non-repudation) gereği ve çoklu kimlik oluşturma saldırılarına karşı sayısal olarak imzalanır. Sistem, bu imzalı oyları kullanarak dosyanın oylama sonucunu hesaplar. Uygulamada bir arama olduğunda, o dosya için geçmişte verilen oylardan belli bir miktarı rastgele seçilerek indirilir ve hesaplama sonucu kullanıcıya gösterilir. Böylece kullanıcılar, dürüstlüğe teşvik edilir. Sistemin dezavantajı olarak daha önceden uzun süre dürüst olan bir kullanıcı davranışını değiştirip yalan söylerse küçük bir küme için sonuçları etkileyebilir.

Incentive Cooperation In Peer-To-Peer Networks[16]

Bu çalışmada yazarlar, P2P sistemlerde bedavacılık problemini engelleyebilmek ve sistemin yararını artırabilmek için, evrimsel mahkumlar çıkmazı yaklaşımını kullanarak bir teşvik modeli geliştirmişlerdir. Normal, simetrik bir mahkumlar çıkmazı probleminde işbirliği için, tekrarlı işlem ve ün gerekli iken P2P sistemlerde bu varsayım pek gerçekçi olmayabilir. Çünkü büyük çaplı P2P sistemlerde aynı kullanıcı ile tekrar işlem yapma olasılığı azdır ve kullanıcıların kimlik değiştirme maliyeti sıfır olduğundan kötü ün oluşması olasılığı sıfıra yakındır. Bu nedenle yazarlar simetrik mahkumlar çıkmazı problemini, P2P sistemlerde kullanılacak şekilde genelleştirmişlerdir. Yazarların bulguları şunlardır:

- Bir eşin sadece kendisinin tuttuğu bilgiye dayalı olan teşvik modelleri, sistem büyüklüğü arttıkça çalışmaz.
- Eşlerin tuttuğu bilgileri birbirleri ile paylaştığı teşvik modelleri sistem büyüklüğünden daha az etkilenirler. Ancak dağıtık bir altyapı gerektirir ve birden fazla eşle yapılan saldırılardan etkilenirler.
- Yabancı (daha önce bilinmeyen) eşleri sisteme dahil edebilen teşvik sistemleri, tam bir işbirliği sağlarlar.

A Game Theoretic Framework For Incentives In P2P Systems [18]

Yazarlar bu makalede, eşlerin etkileşimini modellemek için en iyi aracın teorik modelleme olduğuna karar vermişler ve mütekabiliyet tabanlı bir teşvik modeli oluşturmak için Nash dengesinden ve oyun teorisinden faydalanmışlardır. P2P sistemde her eşin kendi faydasını maksime edeceği düşünülmüştür. Kullanıcının sağladıkları katkı çeşitli şekillerde tutulabilir. Örneğin sisteme sağlanan katkıyı gösteren itibar bunlardan birisi olabilir. Yazarların önerdiği fark modelinin temelini, her eşin kullandığı sistem kaynakları (benefit) ve sağladığı kaynaklar (cost) arası fark oluşturur.

B. Mikro Ekonomi Tabanlı Yaklaşımlar

Mikro ekonomi tabanlı şemalarda, kullanıcılar diğer eşlerin sağladığı servislerden faydalanmak için sanal paralar ödemek zorundadırlar. Böylece sanal bir para ekonomisi kurulmaya çalışılır. Sisteme yapılan her bir katkı için bir sanal para alınırken, sistemden yararlanmak için para ödenir. Eğer İnternet servis sağlayıcıya indirme ve yükleme için ayrı ücretler ödeniyorsa, alınan hizmet ile verilen hizmet gerçekte eşit değildir. Para şeması bunu dikkate alarak tasarlanmalıdır. Bir kere kullanılan paranın tekrar kullanılmamasını sağlamak, sahte para üretimini engellemek genelde en önemli problemlerdir. Bu problemi aşmak amacıyla eğer bir merkezi bankaya dayalı model oluşturulursa ölçeklenebilirlik zordur. Merkezi yapıdan biraz ödün vererek yönetici eşler seçilmesi veya bir eşin etrafındakiler için yönetici olması, merkezi bir bankadaki darboğazı çözmek için kullanılabilecek bazı yöntemlerdir. Mikro ekonomi yaklaşımını temel alan bazı yaklaşımları şöyle özetleyebiliriz.

KARMA [13]

Karma [13], bir sanal para şeması kullanarak, kullanıcıların sisteme katkı sağlamasını amaçlar. Genel ekonomi gibi, sistemden bir kaynak bekleyen kullanıcı sanal para ödemek zorundayken, sisteme katkı sağlayan para kazanır. KARMA, bir kullanıcının sisteme sağladığı katkıları ve sistemden aldığı yararları takip ederek bedavacılarla savaşır. Her bir kullanıcının performansı karma denilen bir para birimiyle takip edilir. Sisteme ilk katılan kullanıcılara belli bir başlangıç karması (*initial seed karma*) verilir. Bir kaynak indirmek isteyen bir kullanıcının yeterli parası yoksa, o kullanıcıya indirme için izin verilmez. Böylece kullanıcılar sisteme katkı yaparak karma kazanmaya zorlanır. KARMA sistemi, banka olarak bir otoriteye ihtiyaç duymaz. Karma'lar kullanıcının banka kümesi (*bank-set*) denilen bir grup eş tarafından tutulur. Ayrıca hata dayanıklılık için yedekleme (*replication*) ve karma değerlerinin rüşvetle el değiştirmemesi için güvenlik önlemleri kullanılır. KARMA tasarımında sistemde en az *k* eş olduğu ve bunların belli bir kesiminin dürüst (*non-malicious*) olduğu kabul edilmiştir. Banka kümesi bilgisi, her bir eşin bir banka kümesi ile eşleştirildiği bir dağıtık hash tablosu (Distributed Hash Table) [14] ile tutulur. Her bir A eşinin en yakınındaki *k* adet eş, A'nın banka kümesini (*bank A*) oluşturur. A eşinin banka kümesi olan her bir eş, A'nın gizli anahtarı ile

imzalanmış karma değerlerini tutar ve A'nın yaptığı işlemlerin geçmişini tutar. Eşlerin karmalarını kullanıp sistemi terk etme durumunda veya karmalarını artırıp sistemi terk etme durumunda oluşacak enflasyon ve denflasyon ile başa çıkmak için para ayarlamaları belli zaman aralıkları (*epoch*) ile yapılır. Karma sistemi, sisteme bir eş katıldığında onun sahip olduğu dosyaların id bilgisi ile eşin id bilgisini eşleştirir. Bir eş, bir dosyayı indirmek istediğinde o dosyaya sahip eşlerin listesini elde eder ve en düşük veya en düşük 2. açık artırma teklifini yaparak (*vickey auction*) indireceği eşi seçer. İndirilecek eş seçildikten sonra takas boyunca borç/kredi tutarsızlığını geçici olarak tolere eden ve Bizans oybirliği protokolünü kullanan KARMA takas protokolü başlatılır. Bu protokol şöyledir:

A eşi B eşine, bank A'nın B'ye istenilen ücreti ödemesini gösteren imzalanmış mesajı yollar. B eşi, bunu bank B'ye iletir ve böylece A eşinden B eşine karma transferi başlar. Eğer A eşinde yeterli bakiye varsa, ücret A'dan düşülüp B'nin hesabına aktarılır. Buradaki tüm mesajlar inkar edilememe ve diğer risklere karşı imzalanmış mesajlardır. KARMA'nin ana avantajı, her bir kullanıcıyı takip etmesi nedeniyle, kullanıcıları katkıları ile tüketimleri arasında bir denge kurmaya zorlar. Ancak her bir kullanıcının, başka bir kullanıcı için bankacı rolünü üstlenmesi gereklidir. Bunun için ise bir teşvik yoktur. Ayrıca KARMA çoklu kimlik tanımlama saldırılarına karşı dirençsizdir.

Incentive For Sharing In Peer-To-Peer Networks [15]

Bu makalede yazarlar, P2P ağlarda bedavacılık problemi ile başa çıkabilmek için formal bir oyun teorisi modeli kurmuşlar ve çeşitli mikro ekonomi modelleri altında bu kullanıcıların dengesini analiz etmişlerdir. Kurdukları modelde kullanıcıların kendi faydalarını maksimize etmek için bencil davranacaklarını varsaymışlar ve buna göre sisteme çeşitli ekonomi modelleri ekleyip kullanıcıların davranışlarını analiz etmişlerdir. Kurdukları teşvik modelinde bir ajanın yaptığı toplam indirme sayısı ve toplam paylaşım sayısını içine alan bir ücret hesaplamışlardır. Buna göre her bir eşin herhangi bir anda 2 etkinliği olabilir: paylaşım ve indirme. Bu iki olayda az, orta, veya çok olarak 3 ayrı dereceye ayrılmıştır. Ayrıca her bir eşin faydası, çeşitli parametrelere dayalı bir fonksiyon olarak yazılmış ve böylece çeşitli durumlar altındaki eşlerin tercihi parasal olarak hesaplanmaya çalışılmıştır.

Yazarlar Napster sistemini incelemiş ve herhangi bir teşvik modeli olmaması nedeniyle kendi modellerini uygulamak için bu sistemi kullanmışlardır. Napster sisteminde teşvik olarak, topluluklarda paylaşım örgütlenmiş ve öntanımlı uygulama ayarlarında paylaşım yapma ayarı kurulmuştur. Böylece sistemde fedakâr kullanıcılar olması sağlanmıştır.

Enforcing Fair Sharing of Peer-To-Peer Resources [17]

Bu çalışmada yazarların amacı, bir eşin kendi paylaşım yaptığı kadar indirme yapabilmesini sağlayan bir adil paylaşım sistemi oluşturabilmektir. Merkezi otorite durumundaki bir eş tüm işlemleri gözlemleyerek bunu sağlayabilir. Fakat bu yöntem kullanılırsa, büyük bir sistemde performans sorunu ve hataya duyarlı tek bir nokta olacağı aşikârdır.

Yazarlara göre P2P sistemlerde teşvik modelini kırmanın ve sistemden daha fazla indirme yapmanın 3 çeşit durumu vardır:

- İşbirliği Olmadan: Bir eşin, ağdan daha fazla yararlanmak için kendi kendine açıklar bulmaya çalışmasıdır. Bu durumda iş birliği yapabileceği bir eş bulamamıştır.
- Azınlık İşbirliğiyle: Bir grup eşin gizli olarak anlaşarak, kaynak paylaşımları konusunda yalan söylemeleri ve böylece sistemde daha çok paylaşım yapmış gibi görünmeleridir.
- Rüşvetle: Kötü niyetli eşlerin bazı eşleri seçerek, sistemi kandırmak üzere onları ikna etmeye çalışmasıdır.

Bu çalışmada ilk olarak işbirliği olmadan yapılan saldırılara odaklanılmıştır. Kaynak tüketimi bir çeşit parasal işlem olarak düşünülmüş ve kendi kaynağımızın dışındaki kaynaklar her zaman daha çok pahalı olarak belirlenmiştir. Böylece paylaşım yapmak her zaman daha getirili bir işlem olmuştur. Eğer iki eş kendi aralarında bir şeyler paylaşıyorsa, bu işlem için parasal ücret sıfır kabul edilmiştir.

Yazarların asıl tasarımları, eşlerin yaptıkları tüm işlemleri bir şekilde kayıt altında tutmayı sağlamaktır. Bunun için 3 çeşit tasarım önermişlerdir. Bu tasarımlarda, her eşin bir açık anahtar çifti ile sayısal imzalama yapabildiği varsayılmıştır. Ayrıca bir mesaj özeti (*hash digest*) ile dosyaların gerçekten o eş üzerinde olup olmadığının anlaşılması sağlanmıştır.

Yazarların ilk önerdikleri tasarım, akıllı kart (smart cards) kullanımıdır. Bu yöntemle eşler, istekleri için ücretleri akıllı kart ile onaylatacak ve isteğini elde edecektir. Fakat, güvenilir bir otorite olmadığı ve geçerliliğini yitirmiş kartların problem olması nedeniyle P2P sistemlerde uygulanabilir görülmemiştir.

İkinci tasarım ise kota (*quota*) yöneticilerdir. Bu yöntemde, bir eşe komşu olan bir grup eş, o eşin kota yöneticisi olarak belirlenmiştir. Her bir yönetici, yönettiği eşin ne kadar veri tükettiğini ve eşden gelen istekleri onaylamak ile görevlendirilmiştir. Azınlık işbirliğini çözmek için yönetici eşler, Bizans oybirliği protokolünü uygulayarak isteğin geçerliliğini kontrol ederler. Bu yöntemin kötü yanı, her bir istek için onay gerektiği için gecikme olması (*latency*) ve kötü niyetli eş sayısının kümenin üçte birinden az olması gerektiğidir. Ayrıca reddedilmesi gereken bir isteğe izin veren bir yönetici için hiçbir ceza olmadığından, bu yaklaşım rüşvet saldırılarına karşı savunmasızdır.

Üçüncü tasarım ise her eşin sayısal olarak imzalanmış bir kullanım dosyası tutmasıdır. Bu dosyada üç çeşit bilgi vardır: sisteme sağlanan katkı (yüklemeler), gönderilenler listesi (hangi eşe hangi dosyanın gönderildiği), indirilenler listesi (hangi dosyaların indirildiği). Gönderilenler listesi ile indirilenler listesi bir eşin alacaklarını ve borçlarını anlatır. Eğer bir eşin indirdikleri yüklediklerini aşmamış ise indirme yapabilir. Bu yaklaşımda, eşlerin yalan söylememesi için imzaya dayalı önlemler alınmıştır.

V. SONUÇ

P2P sistemler kendi kendine organize olan, merkezi olmayan, dağıtık ağlardır. Herhangi bir yönetici olmaması, kontrol olmaması, dinamik olarak büyüyüp küçülmesi, dağıtık veri depolama ve paylaşma için mükemmel imkanlar sunmaktadır. Fakat P2P sistemlerin demokratik (veya anarşik) yapısının yolaçtığı bazı zararlar da vardır. Merkezi bir otoritenin olmaması, kullanıcıların sisteme katkı yapmamasına yol açar. Paylaşım için gönüllülük esasının olması, sistem kaynaklarını değişken ve tahmin edilemez

yapar. Napster, Gnutella gibi sistemler üzerinde yapılan araştırmalara göre, kullanıcıların büyük çoğunluğu sisteme katkı sağlamamakta ve sisteme sadece tüketici olarak katılmaktadır. Bu nedenlerle, P2P sistemler üzerinde eşleri, paylaşıma zorlayacak teşvik modellerine ihtiyaç vardır.

Bu çalışmada, P2P sistemlerdeki teşvik modelleri incelenmiştir. Genelde çoğu teşvik modeli, oyun teorisini temel alarak oluşturulmaya çalışılmıştır. Oyun teorisinde temel amaç, kullanıcılar arasında bir denge fonksiyonu tanımlayabilmek ve sistemin kullanıcılarını buna uyacak şekilde modellemektir. Halihazırda, mütekabiliyet tabanlı ve mikro ekonomi tabanlı yaklaşımları kullanan teşvik modelleri göze çarpmaktadır. Mütekabiliyet tabanlı modellerde, her bir eş, kendi sakladığı geçmiş paylaşım bilgilerini veya etrafındaki diğer eşlerin sakladığı bilgileri kullanarak, indirme istemleri konusunda karar vermeye çalışmaktadır. Mikro ekonomi yaklaşımlarında ise, genelde bir para birimi oluşturulmakta ve bu para ile eşler birbirlerinden hizmet isteminde bulunmaktadırlar. Böylece sanal bir ekonomik düzen oluşturulmaya çalışılmaktadır.

Gelecekte P2P sistemlerde üzerinde bu alanda yapılabilecek çalışmalarda, itibara dayalı güven modelleri yardımıyla teşvik modelleri oluşturmak iyi sonuçlar verebilecek bir yaklaşım olarak görünmektedir. Güven modellerinin topladığı bilgilere ek olarak, paylaşım bilgilerini de toplamak ve bu bilgilerin hepsini teşvik modelinde kullanmak, eşleri sisteme katkı sağlama konusunda zorlayabilecek bir yaklaşımdır. Böylelikle günlük hayatta daha uygulanabilir, kötü niyetli kullanıcıları da engelleyen teşvik modelleri geliştirmek mümkün görünmektedir.

KAYNAKLAR

[1]. E. Adar and B. Huberman. Free riding on gnutella, 2000

[2]. S. Saroiu, P. K. Gummadi, S. D. Gribble, A Measurement Study of Peer-to-Peer File Sharing Systems, Proc. of Multimedia Computing and Networking 2002 (MMCN '02)

[3]. John R. Douceur. The sybil attack. In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pages 251–260, London, UK, 2002. Springer-Verlag.

[4]. James Andreoni. Giving with impure altruism: Applications to charity and ricardian equivalence. The Journal of Political Economy, 97(6):1447–1458, 1989.

[5]. M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica. Free-riding and whitewashing in peer-to-peer systems. Selected Areas in Communications, IEEE Journal on, 24(5):1010–1019, May 2006

[6]. Seung Jun and Mustaque Ahamad. Incentives in bittorrent induce free riding. In P2PECON '05: Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems, pages 116–121, New York, NY, USA, 2005. ACM

[7]. Kevin Walsh and Emin Gun Sirer. Experience with an object reputation system for peer-to-peer filesharing. In NSDI'06: Proceedings of the 3rd conference on 3rd Symposium on Networked Systems Design & Imple-mentation, pages 1–1, Berkeley, CA, USA, 2006. USENIX Association.

[8]. Bram Cohen. Incentives build robustness in bittorrent, 2003.

[9]. Michael Piatek, Tomas Isdal, Thomas Anderson, Arvind Krishnamurthy,and Arun Venkataramani. Do incentives build robustness in bittorrent? In NSDI'07, Cambridge, MA, April 2007.

[10]. Dongyu Qiu and R. Srikant. Modeling and performance analysis of bittorrent-like peer-to-peer networks. In SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, pages 367–378, New York, NY, USA, 2004. ACM.

[11]. Lei Guo, Songqing Chen, Zhen Xiao, Enhua Tan, Xiaoning Ding, and Xiaodong Zhang. Measurements, analysis, and modeling of bittorrent-like systems. In IMC'05: Proceedings of the Internet Measurement Conference 2005 on Internet Measurement Conference, pages 4–4, Berkeley, CA, USA, 2005. USENIX Association.

[12]. Larry Peterson, Tom Anderson, David Culler, and Timothy Roscoe. A Blueprint for Introducing Disruptive Technology into the Internet. In Proceedings of HotNets–I, Princeton, New Jersey, October 2002.

[13]. Vivek Vishnumurthy, Sangeeth C handrakumar, and Emin Gun Sirer. Karma: A secure economic framework for p2p resource sharing. In Workshop on the Economics of Peer-to-Peer Systems, Berkeley, California, 2003.

[14]. Ion Stoica, Robert Morris, David Liben-Nowell, David R. Karger, M. Frans Kaashoek, Frank Dabek, and Hari Balakrishnan. Chord: a scalable peer-to-peer lookup protocol for internet applications. IEEE/ACM Trans. Netw., 11(1):17–32, 2003

[15]. Philippe Gollel, Kevin Leyton-Brown1, Ilya Mironov1, and Mark Lillibridge, Incentives for Sharing in Peer-to-Peer Networks, Computer Science Department, Stanford University, 2001

[16]. Kevin Lai, Michal Feldman, Ion Stoica, and John Chuang, Incentives for Cooperation in Peer-to-Peer Networks, Computer Science Division U.C. Berkeley, School of Information Management and Systems U.C. Berkeley, 2003

[17]. [17] Tsuen-Wan "Johnny" Ngan, Dan S. Wallach, and Peter Druschel, Enforcing Fair Sharing of Peer-to-Peer Resources, Department of Computer Science, Rice University, 2003

[18]. Chiranjeeb Buragohain, Divyakant Agrawal, Subhash Suri, A Game Theoretic Framework for Incentives in P2P Systems, Computer Science Department University of California Santa Barbara, CA 93106, 2003

[19]. Hardin, G. (1968). "The Tragedy of the Commons". Science 162 (3859): 1243–1248.

[20]. R. J. Aumann ([1987] 2008). "game theory," Introduction, The New Palgrave Dictionary of Economics, 2nd Edition. Abstract.

[21]. Roger B. Myerson (1991). Game Theory: Analysis of Conflict, Harvard University Press, p.

[22]. Nash, John (1950), "Equilibrium points in n-person games", Proceedings of the National Academy of Sciences of the United States of America 36 (1): 48–49

[23]. Axelrod, Robert. The Evolution of Cooperation. New York: Basic Books, 1984.

[24]. E. Friedman and P. Resnick, "The social cost of cheap pseudonyms,"J. Econ. Manage. Strategy, vol. 10, no. 2, pp. 173–199, 1998. [Online].Available: citeseer.nj.nec.com/friedman98social.html

[25]. P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," Communications of ACM, vol. 43, no. 12,pp. 45–48, 2000.

[26]. S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in Proceedings of the 12th World Wide Web Conference (WWW), 2003

AES Blok Şifresinin Anahtar Genişletme Rutininin Geliştirilmesi ve Bir Blok Şifreden Bağımsız Anahtar Genişletme Rutininin Tasarımı

Fatma Büyüksaraçoğlu Sakallı, Ercan Buluş, Muharrem Tolga Sakallı, Hüseyin Vural

***Özet*—AES (Advanced Encryption Standard) blok şifresi 2001 yılında standart olmuş önemli bir simetrik şifreleme algoritmasıdır. Bununla beraber AES blok şifresinin saldırılara imkân tanıyan en önemli zaafı anahtar genişletme rutininin yavaş yayılım ve bit sızıntı problemlerine sahip olmasıdır. Bu çalışmada AES blok şifresinin anahtar genişletme rutinindeki bu problemleri gideren bir anahtar genişletme rutini geliştirilmektedir ve bu rutinden faydalanarak bir blok şifreden bağımsız anahtar genişletme rutininin nasıl tasarlanabileceği tartışılmaktadır.**

***Anahtar Kelimeler*—AES blok şifresi, blok şifreler, anahtar genişletme rutini, yeni bir anahtar genişletme mimarisi.**

***Abstract*—AES (Advanced Encryption Standard) block cipher, which has been deployed as a standard in 2001, is an important symmetric cipher. However, the key expansion routine of the AES has two important weaknesses, slow diffusion and bit leakage, which are used to execute some important attacks against AES. In the present study, a new improved key expansion routine for the AES eliminating these weaknesses is developed and how to design a key expansion routine independent from a block cipher is discussed.**

***Index Terms*— AES block cipher, block ciphers, key expansion routine, a new key expansion routine structure**

I. GİRİŞ

2001 yılında DES (Data Encryption Standard) [1] şifreleme algoritmasının yerini alan ve standart haline gelen AES (Advanced Encryption Standard) [2] blok şifresi 128-bit veri bloklarını 128-bit, 192-bit ve 256-bit anahtar seçenekleri ile şifreleyen bir blok şifreleme algoritmasıdır [1-3]. Döngü sayısı 128-bit, 192-bit ve 256-bit anahtar seçenekleri için sırasıyla 10, 12 ve 14 döngüdür. Her döngü dört adım içerir:

i) SubBytes (Byte Yerdeğiştirme),
ii) ShiftRows (Satırları Öteleme),
iii) MixColumns (Sütunları Karıştırma),
iv) AddRoundKey (Döngü Anahtarı Ekleme).

Her döngüde sırasıyla gerçekleştirilen bu adımlardan byte yer değiştirme adımında 8-bit (byte) değerleri farklı 8-bit (byte) değerleri ile yer değiştirilir (S-kutusu). Bu dönüşüm doğrusal olmayan bir dönüşümdür ve GF(2^8) sonlu cisminde ters haritalama tabanlıdır [2-5]. Satırları öteleme adımında byte değerlerinin permütasyonu ile byte değerlerinin sırası değiştirilirken, MixColumns doğrusal dönüşümde 32-bit giriş değerlerinden sabit bir matris çarpımı yardımıyla 32-bit çıkış değerleri elde edilmektedir. Diğer yandan son adım olan döngü anahtarı ekleme evresinde 128-bit anahtar seçeneği ile şifreleme yapan AES şifresi için anahtar genişletme evresinden gelen 128-bit anahtar değer ile o anki blok XOR'lama işlemine tabi tutulur. Şekil 1, tek döngülük SPN mimarisine uygun AES algoritmasını göstermektedir.

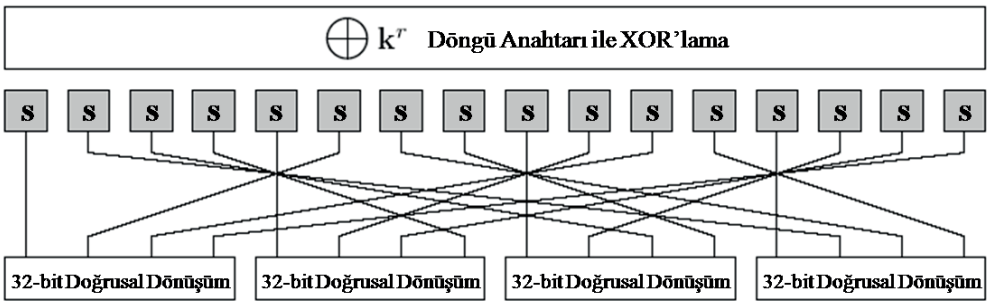
AES blok şifresinin anahtar genişletme algoritması, her ne kadar basit olsa da, bazı önemli saldırıların gerçekleştirilmesinde doğrudan etkisi olmasından dolayı döngü fonksiyonu kadar güçlü değildir. Bu saldırıların nedeni AES anahtar genişletme rutininin yavaş yayılım ve bit sızıntı problemlerine sahip olmasıdır. Yavaş yayılım problemi, AES-192 (192-bit anahtar kullanan AES blok şifresi) ve AES-256 (256-bit anahtar kullanan AES blok şifresi) için ilişkili anahtar saldırılarında kullanılmıştır [6-13]. Bit sızıntı probleminde ise saldırgan verilen bir alt anahtar bilgisi ile diğer alt anahtarları elde edilebilmektedir. Bu problem 7-döngülük AES-192 ve AES-256 için imkânsız diferansiyel saldırısında kullanılabilmektedir [14]. May vd. [15] AES blok şifresinde kullanılan anahtar genişletme rutininin güçlendirilmesi için AES döngü fonksiyonunun üç defa yürütüldüğü, her alt anahtarın birbirinden bağımsız olarak elde edildiği ve uygulama maliyeti yüksek yeni bir anahtar genişletme rutinini öne sürmüşlerdir. Bu çalışmada AES blok şifresinin anahtar genişletme rutininin orijinal yapısını bozmadan ve bahsedilen problemleri gideren yeni bir anahtar genişletme rutini önerilmektedir. Ayrıca önerilen bu yeni anahtar genişletme rutininden esinlenerek elde edilen blok şifreden bağımsız yeni bir anahtar genişletme mimarisi incelenmektedir.

Fatma Büyüksaraçoğlu Sakallı, Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne, fbuyuksaracoglu@trakya.edu.tr

Ercan Buluş, Namık Kemal Üniversitesi, Bilgisayar Mühendisliği Bölümü, Çorlu-Tekirdağ, ercanbulus@nku.edu.tr

Muharrem Tolga SAKALLI, Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne, tolga@ trakya.edu.tr

Hüseyin Vural, Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne, huseyinvural02@gmail.com



Şekil 1. Tek döngülük AES algoritması

II. AES ANAHTAR GENİŞLETME RUTİNİ

Bu bölümde AES-128 için anahtar genişletme rutini incelenmektedir. Blok şifrenin AES-192 ve AES-256 iki versiyonu için de bazı küçük değişiklikler ile birlikte rutin AES-128'inki ile aynıdır. Şekil 2 de genel şekli verilen AES-128 anahtar genişletme rutini aşağıdaki gibi ifade edilebilir:

1- İlk 4 kelime (w_0, w_1, w_2, w_3) gizli anahtardan elde edilir. Gizli anahtar k_0 dan k_{15}'e kadar 16 byte bir dizi olarak düşünülür. İlk 4 byte (k_0 dan k_3'e) w_0, ikinci 4 byte (k_4'ten k_7'ye) w_1 ve benzer şekilde diğer kelimeler w_2 ve w_3'te gizli anahtarın kelimeler şeklinde yan yana konması ile elde edilir,

2- Diğer kelimeler w_i (i = 4 den 43'e kadar) aşağıdaki şekilde elde edilir:

   a. Eğer i (mod 4) $\neq 0$ ise $w_i = w_{i-1} \oplus w_{i-4}$ şeklinde tablodan da görüldüğü gibi soldan ve üstten bir değerden elde edilir.
   b. Eğer i (mod 4) = 0 ise $w_i = t \oplus w_{i-4}$ şeklinde elde edilir. Burada t geçici bir bellek ve iki rutinin w_{i-1} üzerindeki uygulama sonucudur: SubWord ve RotWord. t'nin elde edilme süreci bir döngü sabiti RCon ile XOR lama işlemi ile sonlanır.
   Diğer bir deyişle;
   $t = SubWord(RotWord(w_{i-1})) \oplus RCon_{i/4}$.

A. Kelime Döndürme (RotWord):

Bu rutin AES şifresinde kullanılan satırları öteleme (ShiftRows) dönüşümüne benzemektedir. Ancak sadece 1 satıra uygulanır. Bu rutin bir kelimeyi 4 bytelık bir dizisi olarak alır ve her byte'ı sola dairesel olarak öteler.

B. Kelime Yer değiştirme (SubWord):

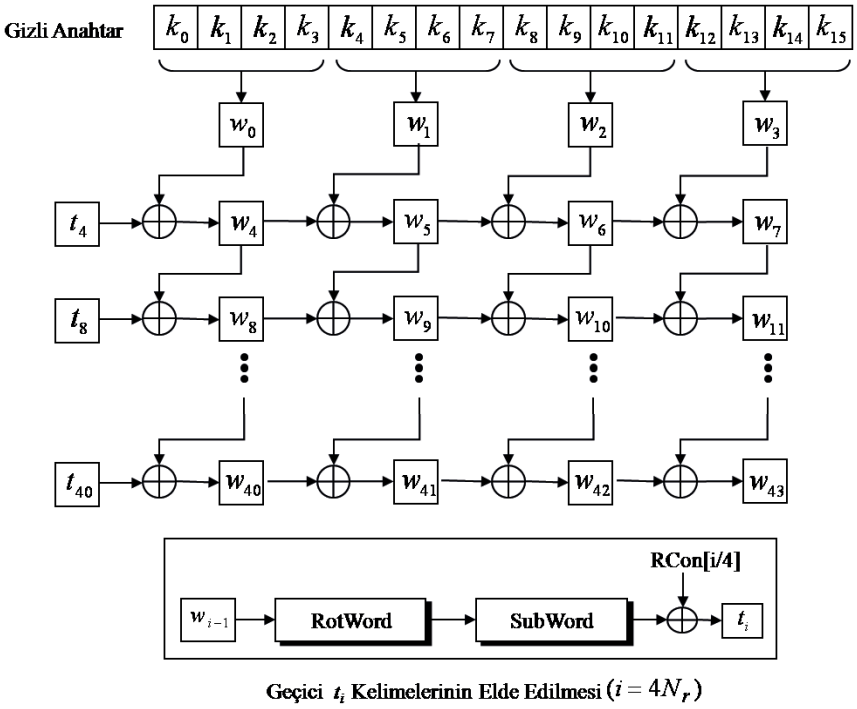
Bu rutin AES şifresinde kullanılan Byte yerdeğiştirme (SubBytes) dönüşümüne benzemektedir. Ancak sadece 4 byte'a uygulanır. Bu döngü kelimedeki her byte değerini alır ve diğer bir byte ile yerdeğiştirir.

C. Döngü Sabitleri (Round Constants):

Anahtar genişletme rutini her döngüde farklı sabit değer kullanır. Bu sabit, RCon, 4 byte değerinde ve en sağdaki 3 byte'ı 0 olan bir değerdir. AES-128 için (10 döngü için) farklı döngü sabitleri Tablo 1'de gösterilmektedir. Buna ek olarak Tablolarda kullanılan tüm ikili değerler hexadecimal (h alt simgesi ile gösterilmiştir) sayı sistemi ile temsil edilmektedir.

TABLO 1
AES-128 anahtar genişletme rutininde kullanılan döngü sabitleri

Döngü	Döngü Sabiti (RCon)	Döngü	Döngü Sabiti (RCon)
1	$(01\ 00\ 00\ 00)_h$	6	$(20\ 00\ 00\ 00)_h$
2	$(02\ 00\ 00\ 00)_h$	7	$(40\ 00\ 00\ 00)_h$
3	$(04\ 00\ 00\ 00)_h$	8	$(80\ 00\ 00\ 00)_h$
4	$(08\ 00\ 00\ 00)_h$	9	$(1B\ 00\ 00\ 00)_h$
5	$(10\ 00\ 00\ 00)_h$	10	$(36\ 00\ 00\ 00)_h$



Şekil 2. AES -128 için anahtar genişletme rutini (N_r döngü sayısını temsil etmektedir)

III. AES ANAHTAR GENİŞLETME RUTİNİNDEKİ İKİ ÖNEMLİ EKSİKLİK

Bir blok şifre daha önce de belirtildiği gibi döngülerden ve döngülerdeki aynı adımlardan oluşmaktadır. Dolayısıyla döngülerdeki simetriyi bozmak için her döngüde farklı bir anahtar materyalinin kullanılması gereklidir. Anahtar genişletme rutinleri gizli anahtardan her döngüde kullanılacak farklı anahtarların (alt anahtarların) elde edilmesini sağlayan algoritmalardır. Her blok şifrede farklı rutinler kullanılabilmektedir ve şifreleme algoritmasında kullanılan yapılar tercih edilerek bu rutinler geliştirilebilir. Lars Knudsen [16] güçlü bir anahtar genişletme rutininin özelliklerini aşağıdaki gibi vermektedir:

1- Çarpışmaya dayanıklı tek yönlü fonksiyon (one-way function) olma,
2- Tüm alt anahtarlar ve gizli anahtar arasında minimum karşılıklı ilişki bulunma,
3- Uygulama etkinliği.

Tüm alt anahtarlar ve gizli anahtar arasında minimum karşılıklı ilişki özelliği blok şifreler üzerine saldırı senaryolarının karmaşıklığını azaltarak saldırgana yardımcı olacak ilişkileri yok edecektir [15]. Bu tür ilişkilerin kullanıldığı saldırılara örnekler DES blok şifresine karşı doğrusal kriptanaliz [17], diferansiyel kriptanaliz [18] gibi saldırılar ile AES blok şifresine karşı olan ilişkili anahtar saldırısı tabanlı çeşitli saldırılar verilebilir. Yine [12] çalışmasının yazarları "Bazı saldırıların genişletilen anahtar bitleri arasındaki ilişkileri kullandıklarını ve bu ilişkilerin olamaması durumunda saldırıların daha yüksek karmaşıklık gerektireceğini" belirtmişlerdir.

Şifreleme algoritması ve anahtar genişletme algoritması güvenlik açısından olduğu kadar uygulama yönüyle de birbirlerini tamamlamalıdırlar. Bu açıdan bakıldığında anahtar genişletme algoritmasında, şifreleme algoritmasında kullanılan optimize edilen elemanların tekrar kullanılması bir avantaj olarak kabul edilebilir [15].

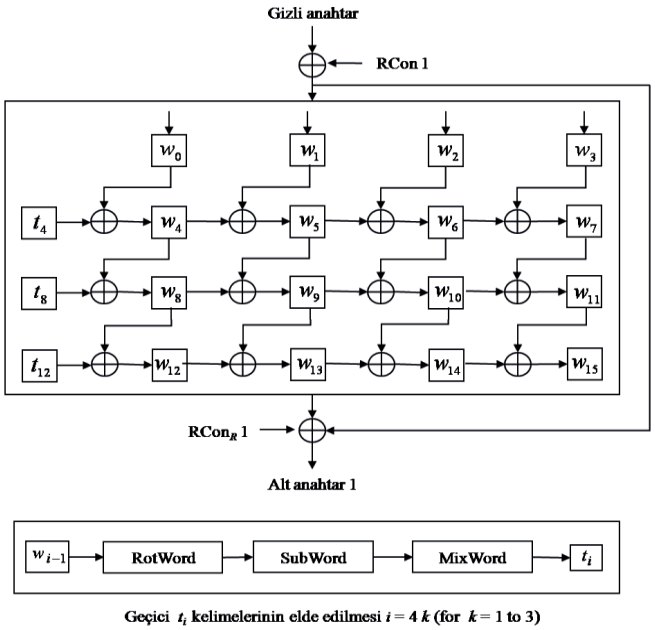
Anahtar genişletme algoritmaları ile elde edilen alt anahtarların üzerinde yürütülen iki önemli test, frekans testi ve çığ kriteri testidir. Frekans testi, bit karıştırma özelliğinin ölçülmesinde (Shannon'nın karıştırma özelliğinin ölçülmesinde temel teşkil eder) kullanılırken çığ kriteri testi, bit yayılım özelliğinin ölçülmesinde kullanılır. Bu test, giriş bloğunda bir bit değişimin çıkış bloğundaki bitlerin yarısının değişimini kontrol eder (Shannon'nın yayılım özelliğinin ölçümünü sağlar).

AES-128 blok şifresinin anahtar genişletme algoritması düşünüldüğünde, Şekil 2'de genel formu verilmiştir, yukarıda verilen özelliklerden sadece üçüncü özelliği sağladığı [15] belirtilmiştir. Bunun yanında AES'in anahtar genişletme algoritmasının kötü yayılım özelliği ilişkili anahtar saldırıları gibi bazı saldırılarda etkin olarak kullanılmaktadır. Bu tür saldırılar gerçek hayatta her ne kadar pratik olmasalar da AES-192 (192-bit anahtar kullanan AES blok şifresi) ve AES-256 (256-bit anahtar kullanan AES blok şifresi) için ilişkili anahtar saldırıların ne kadar faydalı olduğu [19,20] çalışmalarında gösterilmiştir. Bunun temel nedeni olarak AES-192 ve AES-256 versiyonlarındaki anahtar planlama algoritmasının AES-128 (128-bit anahtar kullanan AES blok şifresi) versiyonuna göre daha yavaş yayılım özelliği sağlaması olarak verilebilir. Ayrıca zaman karmaşıklığı açısından Biryukov vd. [11] 10 döngüye kadar bir AES algoritmasına pratik bir saldırıyı göstermişlerdir. Diğer yandan AES'in anahtar genişletme

algoritmasında bit sızıntısı (bit leakage) problemi bulunmaktadır. Bu problem kullanılarak çeşitli saldırılarda bir alt anahtardan faydalanarak diğer alt anahtardan parçalar elde edilebilmektedir. Örneğin [14] çalışmasında bu sızıntı problemi imkânsız diferansiyel saldırısında kullanılmıştır. Bu problemin önüne geçmek için alt anahtarların birbirinden bağımsız olarak üretilmesi bir yöntem olarak kullanılabilir.

IV. AES ANAHTAR GENİŞLETME RUTİNİNİN GÜÇLENDİRİLMESİ

Bölüm 3'te ifade edildiği gibi AES anahtar genişletme rutini iki önemli zaafa sahiptir (yavaş yayılım ve bit sızıntı). Bu zaaflardan rutindeki yavaş yayılımın giderilmesi için öncelikle geçici t_i değerleri elde edilirken bir yayılım elemanına daha ihtiyaç duyulduğu gözlenmektedir. Dolayısıyla bu eksik yayılım elemanı AES şifresinin döngü fonksiyonunda kullanılan MixColumns (Sütunları Karıştırma) dönüşümünün kullanılması ile giderilebilir. Diğer yandan Şekil 3'te verilen yeni anahtar genişletme rutininde gösterildiği gibi 3 defa orijinal AES anahtar genişletme rutininin yürütülmesi ve geçici t_i değerlerinin elde edildiği yeni yapının kullanımı ile iyi yayılım sağlayan bir rutin elde edilebilir. Alt anahtarların elde edilmesi esnasında, gizli anahtar ile XOR'lama işlemine giren döngü sabitinin sonuca eklenmesi bit sızıntı problemini de giderecektir. Yine farklı alt anahtarların elde edilmesi için kullanılan döngü sabitinin ters sırada ($RCON_R$ 1) sonuca eklenmesi ile RCON değerlerinin gizli anahtar olması durumunda bu gizli anahtarların farklı alt anahtarlar üretebilmesi sağlanacak ve oluşabilecek bir simetri giderilebilecektir. RCON 1 değeri $(r_0, r_1, \ldots, r_{15})$ şeklinde 16 byte değerini temsil ederse, $RCON_R$ 1 değeri $(r_{15}, r_{14}, \ldots, r_0)$ 16 byte değerin ters sırasını temsil eder. Sonuç olarak Şekil 3'teki verilen yeni anahtar genişletme rutininde diğer anahtarların elde edilmesi sadece farklı RCON değerlerinin bu yapıya uygulanması ile sağlanacaktır. AES-192 ve AES 256 versiyonları için anahtar genişletme rutini Şekil 3'te verilen yapı ile aynı olmakla beraber döngü sabiti değerleri sırasıyla 192-bit ve 256-bit değerlere sahip olacaktır. Buna ek olarak 3 defa uygulanan orijinal AES anahtar genişletme rutinindeki 4 kelime yerine sırasıyla 6 ve 8 kelime kullanılacaktır.



Şekil 3. AES -128 için önerilen anahtar genişletme rutini

TABLO 2
AES-128 için önerilen anahtar genişletme rutini için ilk alt anahtarın elde edilmesi

Gizli anahtar	01234567 89ABCDEF EDCBA998 76543210
RCon 1	9CC35F04 6A78F579 FC42EC14 2FCDB104
(w_0, w_1, w_2, w_3)	9DE01A63 E3D33896 1189458C 59998314
t_4	D9F3ABB2
(w_4, w_5, w_6, w_7)	4413B1D1 A7C08947 B649CCCB EFD04FDF
t_8	3605A92F
$(w_8, w_9, w_{10}, w_{11})$	721618FE D5D691B9 639F5D72 8C4F12AD
t_{12}	A2CDD003
$(w_{12}, w_{13}, w_{14}, w_{15})$	D0DBC8FD 050D5944 66920436 EADD169B
$RCon_R 1$	04B1CD2F 14EC42FC 79F5786A 045FC39C
Alt anahtar 1	498A1FB1 F232232E 0EEE39D0 B71B5613

Örnek 1. Tablo 2'de verilen 128-bit büyüklüğündeki bir gizli anahtardan blok şifre için ilk alt anahtarın elde edilmesi gösterilmektedir.

Örnek 2. Tablo 3'te verilen aralarında 1-bit değişime sahip iki gizli anahtar için alt anahtarlar arasındaki bit değişimi (B.D.) gösterilmektedir.

Örnek 3. Tablo 4'te AES-128 için önerilen anahtar genişletme rutini için her gizli anahtarın 128 farklı bit pozisyonunda 1-bit değişimi sonucu elde edilen ortalama bit değişimi verilmiştir. Ayrıca bu ortalamalar her döngü anahtarı ve farklı 20 gizli anahtar için elde edilmiştir. Sonuçlar çığ özelliği açısından iyi sonuçlar vermektedir.

TABLO 3

AES-128 için önerilen anahtar genişletme rutini ile üretilmiş bir bit değişime sahip iki gizli anahtardan elde edilen döngü anahtarları kümesinin bit değişimleri açısından karşılaştırılması

R	Döngü anahtarları kümesi 1				Döngü anahtarları kümesi 2				B.D.
-	01234567	89ABCDEF	EDCBA998	76543210	41234567	89ABCDEF	EDCBA998	76543210	1
1	498A1FB1	F232232E	0EEE39D0	B71B5613	8A4F5F2A	D75192E2	CD2B794B	D278E7DF	59
2	E6B8305E	46FAAE29	2D3E7F6A	6C96E002	EE1DE3E3	5203992C	259BACD7	386FD707	63
3	7AACD838	04288D28	28DA4722	46724914	11FCDB37	0453F371	438A442D	0609374D	59
4	0C597D7A	355C1604	29349D75	713AA8FB	7B429B6F	2C69824D	5E2F7B60	280F3CB2	63
5	A5B328CB	8604375D	B4544DCD	2CA5A72D	44F7251E	A1C6AB9F	55104018	4B673BEF	57
6	CDEB5C31	5DA9E411	CD41C2F6	AF9384F2	9A07B592	CCC39CA5	9AAD2B55	7EF9FC46	69
7	B9BCCB90	2473B523	B4A11999	31951DF4	439CCE15	B27FC4FE	4E811C1C	E7996C29	57
8	7B22245A	1AFECC32	7E4F6985	B544B21D	4E9BAB10	87AF60B3	4BF6E6CF	68151E9C	63
9	6C6AF1E8	31EA58D9	4916923E	7ECECE41	EFF2F107	76F6CF25	CA8E92D1	79D259BD	61
10	2FB5795C	9E4456B8	44878B28	E868E2F2	43967E85	568366B2	28A48CF1	60AFD2F8	53

TABLO 4

AES-128 için önerilen anahtar genişletme rutini ile 20 gizli anahtardan üretilmiş alt anahtarların 128 farklı bit pozisyonu için ortalama bit değişimleri

Gizli Anahtar	Döngü Anah.1	Döngü Anah. 2	Döngü Anah. 3	Döngü Anah. 4	Döngü Anah. 5	Döngü Anah. 6	Döngü Anah. 7	Döngü Anah. 8	Döngü Anah. 9	Döngü Anah. 10
Anah. 1	63.44	64.58	63.84	62.28	62.50	63.77	63.55	64.50	63.98	63.55
Anah. 2	64.91	64.53	65.48	63.19	63.23	63.73	64.45	64.23	64.63	64.08
Anah. 3	64.02	63.52	63.75	63.58	63.69	65.25	64.13	63.33	65.06	63.64
Anah. 4	64.02	64.25	64.20	63.53	63.09	64.75	64.06	64.81	64.72	63.89
Anah. 5	64.30	63.80	62.34	62.66	62.14	64.97	63.59	63.03	62.41	63.33
Anah. 6	64.75	63.38	64.64	63.13	64.58	64.55	64.39	64.22	64.75	64.16
Anah. 7	64.53	63.88	64.52	64.17	63.61	63.66	65.33	64.59	63.69	62.53
Anah. 8	65.00	64.13	63.42	63.38	64.06	64.00	63.44	63.03	63.55	62.69
Anah. 9	62.81	64.08	62.52	64.13	64.84	64.36	64.02	63.22	63.38	62.05
Anah.10	63.58	63.75	64.67	64.59	63.92	63.97	64.13	64.34	65.25	63.61
Anah. 11	63.91	63.97	63.88	62.00	64.36	63.91	64.36	62.13	63.13	62.45
Anah. 12	65.02	64.05	65.06	64.09	64.70	62.78	63.36	64.19	64.19	65.13
Anah. 13	62.91	65.70	62.83	64.33	64.33	62.39	63.66	63.61	63.25	62.28
Anah. 14	63.72	62.23	63.55	62.22	64.91	64.27	64.89	65.08	62.61	63.45
Anah. 15	63.73	64.59	62.72	63.91	65.89	64.50	65.11	63.38	64.72	63.61
Anah. 16	63.52	63.88	63.03	64.16	65.22	63.16	65.67	63.14	65.34	63.48
Anah. 17	63.42	64.52	64.50	64.19	62.63	64.38	64.38	63.22	63.73	62.59
Anah. 18	64.59	63.63	63.13	62.19	64.02	63.47	64.23	63.94	62.47	65.63
Anah.19	63.02	64.48	64.41	62.78	64.39	64.58	65.06	64.50	64.84	63.38
Anah. 20	65.89	63.89	63.13	63.69	65.09	63.92	63.81	64.28	63.19	63.42
Ortalama	64.05	64.04	63.78	63.41	64.06	64.02	64.28	63.79	63.94	63.45
% Ortalama	50.04	50.03	49.83	49.54	50.05	50.01	50.22	49.83	49.96	49.57

V. BİR BLOK ŞİFREDEN BAĞIMSIZ ANAHTAR GENİŞLETME RUTİNİN TASARIMI

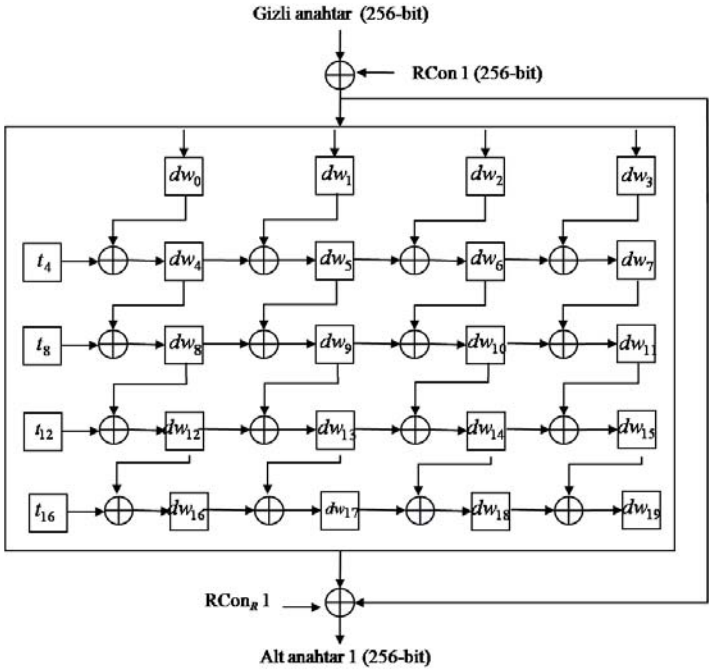
Bölüm 4'te AES blok şifresi için öne sürülen rutinden yola çıkarak bir blok şifreden bağımsız anahtar genişletme rutini mimarisi ortaya konabilir. Günümüzde kullanılan blok şifreler genellikle kendi bünyelerinde bulunan elemanları kullanan anahtar genişletme rutinlerine sahiptir. Bununla beraber bu blok şifrelerin döngü fonksiyonlarının tasarımında yer değiştirme katmanı olarak kullanılan S-kutuları 4-bit (lightweight-hafif siklet blok şifreler) ya da 8-bit boyutunda olacak şekilde tercih edilmektedir. Diğer yandan uygulama etkinliği anahtar genişletme rutinleri için önemli bir kriterdir. Şekil 3'te verilen mimaride geçici t_i değerlerinin elde edilmesi için iki farklı mimari ortaya konabilir:

1- Yayılım –Yer değiştirme – Yayılım (DSD: Diffusion-Substitution-Diffusion),
2- Yer değiştirme –Yayılım – Yer değiştirme (SDS: Substitution-Diffusion-Substitution).

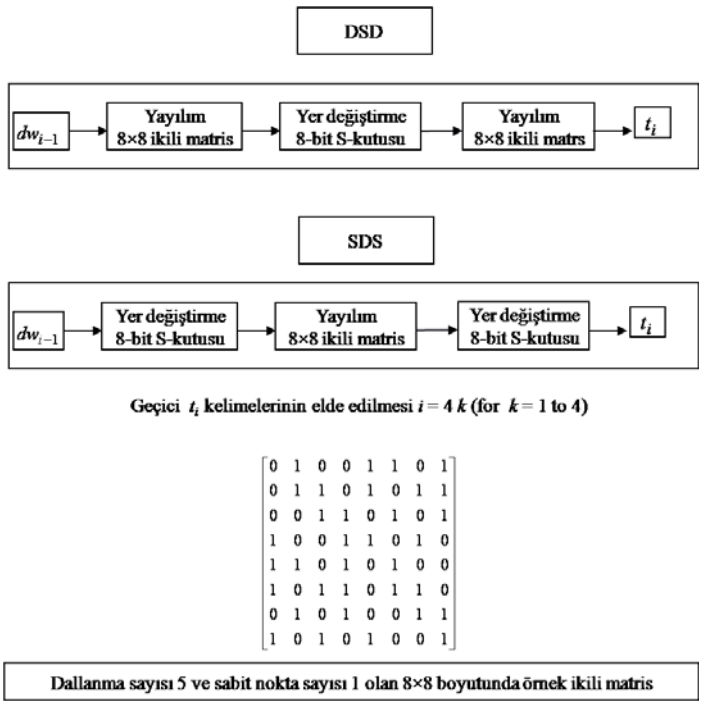
Verilen bu iki mimari de yayılım katmanının iyi uygulama özelliğine, yüksek dallanma sayısı (branch number) değerine ve olabildiğince az sabit nokta sayısına [21] sahip olması (1 sabit nokta) istenebilecek özellikler olarak karşımıza çıkacaktır. Blok şifreden bağımsız tasarlanacak anahtar genişletme rutininden farklı boyutlarda alt anahtarlar üretilebilmesi ve genişletme rutininin S-kutusunun büyüklüğünden bağımsız olabilmesi iyi bir yayılım elemanın seçimi ile sağlanabilir. Dolayısıyla bahsedilen özellikleri karşılayabilecek yayılım elemanı olarak ikili matrisler (dallanma sayısı yüksek, sabit nokta sayısı düşük ve sadece XOR işlemi tabanlı) seçilebilir. Örneğin 4×4, 5×5, 8×8 boyutunda ikili matrislerin maksimum dallanma sayıları sırasıyla 4, 4 ve 5'tir [22] ve sadece XOR işlemi tabanlı olarak uygulamaları gerçekleştirilebilir. Sahip olunan S-kutusu büyüklüğü ve üretilecek alt anahtar büyüklüğüne göre Şekil 3'te verilen yapı, geçici t_i değerlerinin elde edilmesi için iki farklı mimariden birinin seçilmesi ve uygun özelliklerde ikili matrisin kullanılması ile istenen boyutta alt anahtar üreten bir anahtar genişletme rutini haline getirilebilir.

Örnek 4. 256-bit alt anahtar üreten blok şifreden bağımsız bir anahtar genişletme rutinin tasarımı için elimizde 8-bit S-kutusu (AES S-kutusu), 8×8 boyutunda (dallanma sayısı

değeri 5 ve 1 sabit noktaya sahip [23]) ikili matris olsun. Buna ek olarak Şekil 3'te AES-128 için önerilen rutinde 32-bit geçici t_i değerleri yerine 64-bit t_i değerleri kullanılsın. Orijinal AES anahtar rutininin yürütülme sayısı 4 olarak seçilsin (Tekrar etme işleminin sayısı deneysel sonuçlarla belirlenmesi daha uygun olacaktır). Şekil 4 ve Şekil 5'te bir blok şifreden bağımsız anahtar genişletme rutini, bu rutinde kullanılacak geçici t_i değerlerinin elde edilmesinde kullanılacak iki mimari ve örnek bir 8×8 boyutunda (dallanma sayısı değeri 5 ve 1 sabit noktaya sahip) ikili matris verilmektedir.



Şekil 4. Blok şifreden bağımsız 256-bit anahtar genişletme rutini (dw: double word-64-bit değeri temsil eder)



Şekil 5. 256-bit anahtar genişletme rutininde geçici t_i değerlerinin elde edilmesinde kullanılabilecek iki mimari

VI. SONUÇLAR

Bu çalışmada AES blok şifresinde kullanılan anahtar genişletme rutini incelemiş ve bu rutindeki problemler irdelenmiştir. AES blok şifresinin anahtar genişletme rutinindeki zaafları gideren ve orijinal yapı üzerinde basit değişiklikler yapılarak elde edilen gelişmiş yeni bir anahtar genişletme rutini ortaya konmuştur. Çalışmanın son bölümünde de bu geliştirilen rutinden faydalanılarak bir blok şifreden bağımsız çeşitli büyüklüklerde alt anahtar üreten anahtar genişletme rutininin nasıl tasarımının yapılacağı tartışılarak bu tip bir anahtar genişletme rutini için örnek verilmiştir.

KAYNAKLAR

[1] US National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publications, No. 46-3, 1999.

[2] US National Institute of Standards and Technology, Advanced Encryption Standard, Federal Information Processing Standards Publications}, No. 197, 2001.

[3] B. A. Forouzan, Cryptography and Network Security, McGraw-Hill International Edition, 2008.

[4] B. Aslan, M. T. Sakallı, E. Buluş, Üs Haritalama Tabanlı Cebirsel 8-bit giriş 8-bit çıkışlı S-kutularının Sınıflandırılması, Ağ ve Bilgi Ulusal Sempozyumu 2, Girne-Kıbrıs, 2008.

[5] B. Aslan, M. T. Sakallı, E. Buluş, Classifying 8-bit to 8-bit S-boxes based on Power Mappings from the point of DDT and LAT Distributions, In Proceedings of International Workshop on the Arithmetic of Finite Fields, WAIFI 2008, Lecture Notes in Computer Science, Vol. 5130, Springer-Verlag, 2008; 123-133.

[6] G. Jakimoski, Y. Desmedt, Related-Key Differential Cryptanalysis of 192-bit Key AES Variants, In Proceedings of Selected Areas in Cryptography (SAC 2003), Lecture Notes in Computer Science, Vol. 3006, Springer-Verlag, 2004; 208-221.

[7] E. Biham, O. Dunkelman, N. Keller, Relate-Key Impossible Differential Attacks on 8-Round AES-192, In Proceedings of Topics in Cryptology-CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006, Lecture Notes in Computer Science, Vol. 3860, Springer-Verlag, 2006; 21-33.

[8] W. Zhang, W. Wu, L. Zhang, D. Feng , Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192, In Proceedings of Selected Areas in Cryptography (SAC 2006), Lecture Notes in Computer Science, Vol. 4356, Springer-Verlag, 2007; 15-27.

[9] E. Biham, O. Dunkelman, N. Keller, Related-Key Boomerang and Rectangle Attacks., In Proceedings of EUROCRYPT 2005, Lecture Notes in Computer Science, Vol. 3494, Springer-Verlag, 2005; 507-525.

[10] J. Kim, S. Hong, B. Preneel, Related-Key Rectangle Attacks on Reduced AES-192 and AES-256, In Proceedings of FSE 2007, Lecture Notes in Computer Science, Vol. 4593, Springer-Verlag, 2007; 225-241.

[11] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds, Cryptology ePrint Archive, Report 2009/374, 2009. Available at http://eprint.iacr.org/2009/374/.

[12] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, D. Whiting, Improved Cryptanalysis of Rijndael, In Proceedings of FSE 2000, Lecture Notes in Computer Science, Vol. 1978, Springer-Verlag, 2001; 213-230.

[13] E. Fleischmann, M. Gorski, S. Lucks, Attacking 9 and 10 Rounds of AES-256, In Proceedings of ACISP 2009, Lecture Notes in Computer Science, Vol. 5594, Springer-Verlag, 2009; 60-72.

[14] RC-W. Phan, Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES), Information Processing Letters, 2004; 91 (1):33-38.

[15] L. May, M. Henricksen, W. Millan, G. Carter, E. Dawson, Strengthening the Key Schedule of the AES, In Proceedings of ACISP 2002, Lecture Notes in Computer Science, Vol. 2384, Springer-Verlag, 2002; 226-240.

[16] L. Knudsen, Practically Secure Feistel Ciphers, In Proceedings of FSE 1993, Lecture Notes in Computer Science, Vol. 809, Springer-Verlag, 1993; 211-221.

[17] M. Matsui, Linear Cryptanalysis Method for DES Cipher, In Proceedings of EUROCRYPT 93, Lecture Notes in Computer Science, Vol. 765, Springer-Verlag, 1994; 386-397.

[18] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, In Proceedings of CRYPTO'90, Lecture Notes in Computer Science, Vol. 537, Springer-Verlag, 1990; 2-21.

[19] A. Biryukov, D. Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256. Cryptology ePrint Archive, Report 2009/317, 2009. Available at http://eprint.iacr.org/2009/317/.

[20] A. Biryukov, Khovratovich D. Related-key Cryptanalysis of the Full AES-192 and AES-256. In Proceedings of ASIACRYPT 2009, Lecture Notes in Computer Science, Vol. 5912, Springer-Verlag, 2009; 1-18.

[21] M.R. Z'aba, Analysis of Linear Relationships in Block Ciphers, Ph.D. Thesis, Queensland University of Technology, Brisbane, Australia, 2010.

[22] D. Kwon, S. H. Sung, J. H. Song, S. Park, Design of Block Ciphers and Coding Theory, Trends in Mathematics, 2005; 8(1):13-20.

[23] B. Aslan, M. T. Sakallı, Algebraic construction of cryptographically good binary linear transformations, Security and Communication Networks (2012) doi:10.1002/sec.556.

Ulusal Siber Güvenliğin Sağlanmasında NATO'nun Olumlu Etkilerinin Artırılması İçin Yaklaşım Modeli

Ü.Bayık, İ.Semiz, S. Sönmez, M.Durak,

***Özet*— NATO 1949 yılında üye ülkelerin, ortak savunma için yeteneklerini geliştirmek, herhangi bir üyenin toprak bütünlüğünün, siyasî bağımsızlığı ve güvenliğinin tehlikede olduğunda bir araya gelmek ve herhangi birine saldırıldığında bu saldırıya hepsine karşı yapılmış bir saldırı olarak kabul ederek ortak hareket etmek maksadıyla kurulmuştur. Günümüzde ülkelere yönelik saldırılar siber uzayda yapılmaktadır. Bu saldırılar devletlerin karşılamayacağı finansal ve fiziksel birçok sonuçlar doğurmaktadır. NATO'da üye ülkelerin siber uzaydaki tecrübe, birikim ve yeteneklerinden etkin bir şekilde faydalanmak için kurumsal olarak bu alanın yönetilmesine yönelik bir model oluşturulmuştur.**

***Terimler*— NATO, Siber savunma, siber güvenlik, Mükemmeliyet Merkezi**

***Abstract*— NATO was established in 1949 in order to develop common security capabilities, to come together and act as a one country in case of any danger in any member states boundary, political sovereignty and security and any attack to one member state. Nowadays attacks are made in cyber space. These attacks cause financial and physical results that countries can not bear themselves. In order to get NATO member states' capabilities and experiences in cyber space, a model is made to manage this space.**

***Key Words*— NATO, Cyber Defense, Cyber Security, Center of Excellence.**

I. GİRİS

BİLISIM teknolojileri, sistemleri ve usullerinin devletlerin kritik alt yapılarına girmesi ile bu altyapıları birbirlerine bağlayan iletişim ortamlarının güvenlikleri stratejik seviyede değerlendirilmesi bir gereklilik haline gelmiştir. Günümüzde akademik ortamda sayısız makale yayınlanmasıyla uluslararası ortamda siber farkındalık üst düzeye çıkmıştır. Askeri unsurların birbirleri ile haberleşmesini kolaylaştırmak maksadıyla ortaya çıkan internet sağladığı faydaların yanında ortaya çıkardığı hassasiyetlerle devletlerin kâbusu haline gelmiştir.

Ülkeler arasındaki konvansiyonel harbin günümüzde ortadan kalkması daha doğru bir ifade ile ülkeler arasında kullanılan enstrümanların değişmesi ile fiziksel dünyanın sınırları genişlemiştir. Bu harp alanının boyutlarının fiziksel dünya ile entegre olan tüm boyutlarının yeniden değerlendirilmesi, her boyutta ortaya çıkabilecek hassasiyetlere tedbirler getirilmesi devletlerinin ulusal güvenliklerinin birinci önceliği haline gelmiştir. Bu maksatla devletler siber güvenliğe yönelik gerek askeri alanda gerekse kamusal alanda teşkilatlanmalara gitmiştir. Ülkemizde ulusal boyutta Ulaştırma, Denizcilik ve Haberleşme Bakanlığının sorumluluğunda yapılanmaya gidilmiştir.

II. ULUSAL SİBER GÜVENLİĞİN DAYANDIĞI PRENSİPLER, TEŞKİLATLANMA SÜRECİ

Ülkemizde siber uzayda yaşanan savaşların (1999 Yılında Kosova Harekâtında NATO Unsurlarına yapılan Siber saldırılar, Estonya-Rusya, Gürcistan-Rusya arasındaki siber savaş) ortaya çıkardığı endişeler, akademisyenlerin, kolluk kuvvetlerinin ve askeri uzmanların bu alandaki çalışmaları ile ulusal bağlamda adımların atılmasını gerektirdiğini ortaya koymuştur. Siber güveliğin dayandığı temel unsurlara bakılacak olursa, Bunlar:



Şekil 1. Siber Güvenliğin Temel Unsurları

- Ulusal politika ve stratejinin geliştirilmesi,
- Yasal çerçevenin oluşturulması,
- Teknik tedbirlerin geliştirilmesi,
- Kurumsal yapılanmanın belirlenmesi,
- Ulusal işbirliği ve koordinasyonun sağlanması,
- Kapasitenin geliştirilmesi,

Ümit Bayık, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: murataltug@gmail.com.

İnan Semiz, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: inansemiz@gmail.com.

Selçuk Sönmez, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: selcoksonmez@gmail.com.

Melih Durak, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: melihdurak@gmail.com.

- Farkındalığın artırılması,
- Uluslararası işbirliği ve uyumun sağlanmasıdır[1].

Belirtilen temel unsurlara yönelik olarak ulusal alanda birçok adımlar atılmıştır. Gerek kamu kurum ve kuruluşlarının gerekse özel sektördeki kuruluşlarının siber güvenliğe yönelik farkındalıkları artırılmıştır. Ulusal ve uluslararası alanda birçok siber tatbikatlara icra edilmiş, özel kurum, kuruluşlar ve kamu kurum, kuruluşları tatbikata katılmıştır. Bu tatbikatlarda özellikle kritik alt yapıların korunmasına yönelik senaryolar denenmiştir. Siber güvenlik yönelik birçok çalışma ve araştırma yapılmış ve yapılmaya devam edilmekle birlikte daha atılacak birçok adım bulunmaktadır. Yapılan çalışmalar aşağıdaki başlıklar altında toplanmaktadır.

- Yasal çalışmalar,
- Ulusal bilgi güvenliği kapısı,
- TR-BOME Bilgisayar Olaylarına Müdahale Ekibi,
- Bilgi Toplumu Stratejisi Eylem Planı (2006 - 2010),
- Kişisel Verilerin Korunması Kanunu Tasarısı,
- Ulusal Sanal Ortam Güvenlik Politikasının oluşturulması,
- Siber Güvenlik Tatbikatları,
- Siber Güvenlik Çalıştay ve Konferansları,
- TSK'nın Yürüttüğü Faaliyetler.

Türkiye'de siber güvenlik kapsamında ele alınacak olan bilgi toplumuna dönüşüm çalışmaları 2000'li yılların başlarında başlamıştır. Ülkemizdeki siber güvenlik tatbikatlarının ilki olan BOME 2008 Tatbikatı TÜBİTAK UEKAE bünyesinde faaliyet gösteren TR-BOME koordinatörlüğünde, 20-21 Kasım 2008 tarihlerinde icra edilmiştir.

Daha geniş katılımlı ikinci tatbikat Ulusal Siber Güvenlik Tatbikatı 2011, TÜBİTAK BİLGEM ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) koordinatörlüğünde Ocak 2011'de düzenlenmiş, 41 kamu ve özel sektör kurum ve kuruluşunun katıldığı tatbikat gerçek saldırılar ve gerçekçi senaryolar denenmiştir. [2]

Ocak 2013'te Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinatörlüğünde Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı yayımlanmıştır. Eylem planının temel amacı; Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan hizmet, işlem ve bunların sunumlarında kullanılan sistemlerin güvenliğinin sağlanması, kritik altyapılara ait bilişim sistemlerinin güvenliklerinin sağlanması olarak belirlenmiştir. Siber güvenliğe ait riskler ortaya konulmuş ve bu risklerin etkin bir risk yönetimi ile ortadan kaldırılması hedeflenmiştir [3].

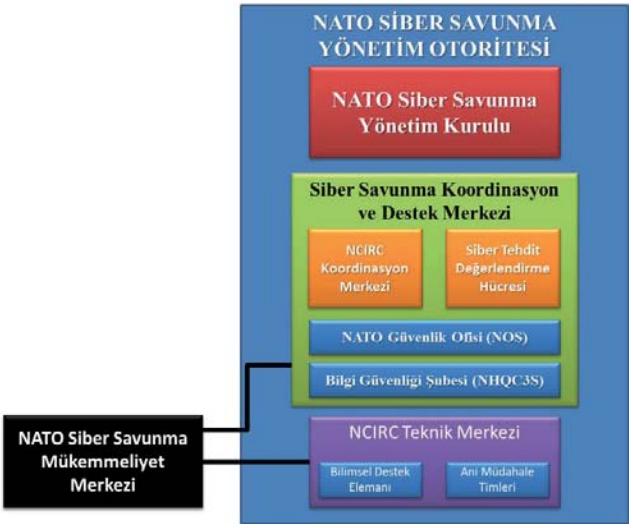
2013-2014 dönemi içerisinde yedi başlık altında hedef belirlenmiştir. Her belirlenen hedef yapbozun parçaları gibi eş güdüm halinde yürütüldüğünde bir anlam ifade etmektedir. Bu hedeflerden; yasal mevzuatın oluşturulması, Ulusal Siber Olaylara Müdahale Merkezi oluşturulması, altyapının güçlendirilmesi, siber güvenlik alanında insan kaynağının yetiştirilmesi öne çıkmaktadır. Tüm belirlenen bu hedefler stratejik seviyede farkındalığın artığını ve operatif seviyede icraya geçildiğinin bir göstergesidir.

III. NATO'NUN SİBER GÜVENLİĞE YÖNELİK ATTIĞI ADIMLAR VE HİZMETLERİ

NATO 1949 yılında üyelerinin savunma yeteneklerini geliştirmek ve doğu bloğuna karşı bir caydırıcılık sağlamak maksadıyla kurulmuştur. 21'inci yüzyılda güvenlik parametreleri soğuk savaştan sonra değişmiş üyelerinin öncelikle enerji güvenlikleri, kritik altyapılarının iletişim alt yapıları ile birbirlerine bağlanması ile bu alt yapıların oluşturduğu siber alanın güvenliği birinci önceliği haline gelmiştir. Bu küresel tehditlere karşı özellikle 2007 yazında Rusya tarafından Estonya'ya yapılan siber saldırılardan sonra yeni savunma stratejileri geliştirilmesi gerektiğinin bir delili olmuştur. Kamu güvenliği ve devletlerin istikrarı karşısındaki giderek büyüyen bu tehdit NATO'nun elektronik iletişime bağımlı üyelerinin siber cephede son derece zayıf olduklarını ortaya çıkarmıştır [4].

NATO Estonya'ya yapılan bu saldırılardan sonra Estonya'da Siber Savunma Mükemmeliyet Merkezi kurmuştur. NATO'nun 2010 stratejik konseptinde Siber Güvenliğe yönelik olarak " … siber saldırılara karşı yeteneğimizi geliştirerek saldırıları tespit etme, koruma ve engelleme alanlarında çalışmalar yapma…" ifadeleri yer almıştır. Bu stratejik vizyonla 8 Haziran 2011 tarihinde NATO Savunma Bakanlarının onayı ile Siber Savunma Politikası yürürlüğe girmiştir [5].

NATO Siber Savunma Teşkilatı, Siber Savunma Yönetim Otoritesine bağlı olarak çalışan Siber Savunma Yönetim Kurulu, Siber Savunma Koordinasyon ve Destek Merkezi ve Bilgisayar Olaylarına Müdahale Yeteneği (NCIRC) Teknik Merkezinden oluşmaktadır. Ayrıca, NATO çapında siber güvenliğe ilişkin farkındalık sağlamak ve standart oluşturmak maksadıyla Estonya'da teşkil edilen Siber Savunma Mükemmeliyet merkezi ile koordineli olarak bu alanda birçok eğitim faaliyeti icra edilmektedir.



Şekil 2. NATO Siber Savunma Yönetim Otoritesi

Bu teşkilatın bağlılarına ilişkin detaylı bilgiler aşağıdadır [6].

A. NATO Siber Savunma Yönetim Sistemi:

NATO çapında siber savunma olaylarının yönetimi ile ilgili tek otoritedir. İhtiyaç olduğunda, süratli ve etkili bir siber savunma için her türlü faaliyetin başlatılması ve koordinasyonun yapılmasından, ittifakın kendisinin veya İttifak üyesi bir ülkenin, siber saldırıya maruz kalması durumunda, talep edilmesi hâlinde yardım sağlanmasından sorumludur.

B. NATO Siber Savunma Yönetim Kurulu:

Üst düzey yönetim ve karar organıdır. NATO Siber Savunma Politikasının hayata geçirilmesi ve NATO ve/veya NATO ülkelerinden herhangi birine ciddi bir siber saldırı yapılması veya siber saldırı tehdidinin ortaya çıkması durumunda, uygun önlemlerin alınmasından sorumludur.

C. NATO Siber Savunma Koordinasyon ve Destek Merkezi:

Üye ülkeler ve haricî organizasyonlar ile birlikte NATO'nun siber savunma faaliyetlerinin koordinasyonu bu merkezde yerine getirilir. Kriz yönetimi ve acil müdahale konularında bilgi değişimini sağlamaktan ve gerekli bağlantıları kurmaktan sorumludur.

Ç. NATO Bilgisayar Olaylarına Müdahale Yeteneği (NCIRC) Teknik Merkezi:

NATO çapında siber savunma hizmetlerinin geliştirilmesi, uygulanması ve idamesinin sağlanmasından sorumludur. Uygulamada Bilgisayar Olaylarına Müdahale Ekibi (BOME) (Computer Events Response Team, CERT®) fonksiyonunu yerine getirir.

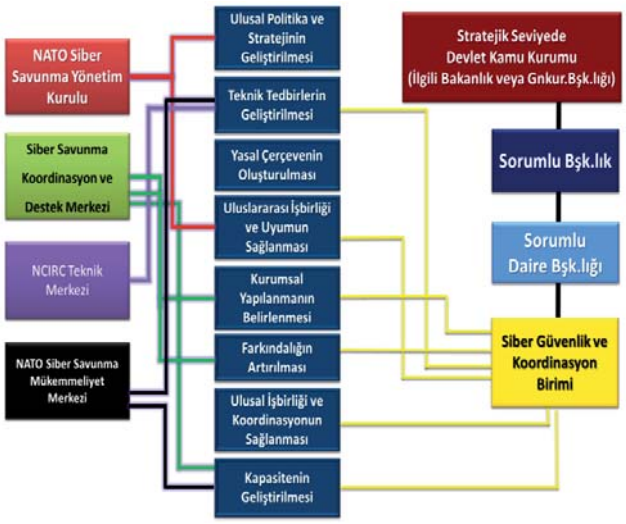
D. NATO Siber Savunma Mükemmeliyet Merkezi:

Üye ülkelerden çalışanların oluşturduğu bu merkez bir ARGE alanı gibi faaliyet göstermektedir. Gerek Siber Savunma Koordinasyon ve Destek Merkezi gerekse Bilgisayar Olaylarına Müdahale Yeteneği ve Teknik Merkezi ile koordinasyon halinde çalışmaktadır. Yeni siber savunma konseptlerin ve yeteneklerin geliştirileceği bir merkezdir.

NATO'da siber güvenliğe yönelik olarak yaklaşımlar pro-aktif bir tutumdan ziyade re-aktif bir tutum izlemektedir. Tehditlerin belirmesine müteakip tedbirler geliştirilmektedir. BU hassasiyet oluşturulan yapının en zayıf alanı olarak görülmektedir. Bu hassasiyettin giderilmesi için her yıl icra edilen Siber Tatbikatlar önem arz etmektedir.

IV. NATO'DAN ULUSAL OLARAK YARARLANILACAK SİBER GÜVENLİK UNSURLARI VE YAKLAŞIM MODELİ

NATO yukarıda da ifade edildiği gibi üyelerin güvenliklerini sağlamak maksadıyla kurulmuştur. Uluslararası alanda siber güvenlik bağlamında tecrübe kazanmış bir örgüttür. Burada kazılan yeteneklerin, tecrübelerin, üye ülkelerin yetenek ve tecrübelerinin uzman bir bakış açısı ile yönetilmesi gerekmektedir. Akademik alanda siber güvenliğe yönelik belirlenen temel unsurların NATO'da oluşturulan teşkilatın içerisinde hangi birimler tarafından yönetildiği Şekil-3'te belirtilmiştir.



Şekil 3. NATO'dan Ulusal Olarak Yararlanılacak Siber Güvenlik Unsurları ve Yaklaşım Modeli

V. SONUÇ

Olası bir siber savaşta etkin savunma yapılabilmesi için siber güvenlik konusunun iyi kavranması ve değerlendirilmesi gerekmektedir. Bu bağlamda Ulusal Siber güvenlik Strateji ve 2013-2014 Eylem planında da belirtildiği gibi yasal düzenlemelerin yapılması, uluslararası hukuktan kaynaklanan hakların kullanılabilmesi için hazırlık yapılması, ulusal bilgisayar olaylarına müdahale organizasyonunun oluşturulması, ulusal siber güvenlik altyapısının güçlendirilmesi, siber güvenlik alanında insan kaynağı yetiştirilmesi ve milli teknolojilerin kullanılması hayati öneme sahiptir [7].

Siber güvenlikte uluslararası alanda oluşturulacak işbirliği ve koordinasyon devletlerin kendi güvenliklerini sağlanmasında öncelikli alması gereken tedbirlerdendir. Bu bağlamda siber alandaki güvenliğini en üst seviyeye çıkarmak için üye ülkelerin yetenek, kabiliyet ve tecrübelerinin, yönetim alanında deneyim kazanmış personel ve teşkilatla yürütülmesi ulusal siber güvenliğimize daha fazla katkı sağlayacaktır. Söz konusu koordinasyon biriminin yetenekleri geliştirilerek özel sektördeki kurum ve kuruluşlara etkin deneyim ve bilgi paylaşımı yapabilecektir. Söz konusu yaklaşım modeli ile aşağıda belirtilen faydaların sağlanacağı değerlendirilmektedir.

- Uluslararası geliştirilen politikalar ile ulusal politika dinamik bir yapıta tutulacak, yaşayan bir siber güvenlik politikası izlenebilecek,

- NATO bünyesinde icra edilen tatbikatlardan elde edilen tecrübeler ve bilgi birikimleri ile gerek özel gerekse kamu kurum ve kuruluşlarına yol gösterilerek sistemlerinin güvenlikleri bir canlı haline gelecek,

- Bu tatbikatlardan elde edilen tecrübeler ile ulusal olarak icra edilecek tatbikatlar hedefleri gerçekçi, güncel tehditlerin değerlendirildiği, siber saldırı imkân ve kabiliyetlerinin nasıl olabileceğinin kıymetlendirildiği tatbikatlar icra edebilecek,

- Siber güvenlik, siber savunma ve gelecekte ortaya çıkması muhtemel tehditlere karşı düzenlenen akademik

çalışmalarda rol almasın için personel teşvik edilecek ve kurumsal olarak siber dünyaya yönelik akademik bir birikim oluşturulabilecek,

- Üye ülkeler tarafından siber güvenliğe yönelik izlenen politika, teknoloji ve yasal mevzuattan istifade ile ulusal alanda düzenlemeler yapılabilecek,

- Kamu kurum, kuruluşları ile özel kurum ve kuruluşların siber tehdit ve saldırılar ile güvenlik önlemleri konusunda sürekli bilgilendirici ve bilinçlendirici mekanizma tesis edileceği değerlendirilmiştir.

KAYNAKLAR

[1] Mustafa ÜNVER, Cafer CANBAY, Ayşe Gül MİRZAOĞLU "Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri" Konulu makale 2009, S. 10

[2] Bilim ve Teknik Dergisi, Emre BAKIR "Türkiye'de Siber Güvenlik" konulu makale Kasım 2012, S. 12

[3] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" konulu çalışma, Ocak 2013, S. 14-19

[4] http://www.nato.int/docu/review/2011/11-september/Cyber-threads/TR/, Yeni Tehditler; Siber Boyut, Erişim Tarihi: 10 Temmuz 2013

[5] İstanbul Bilgi Üniversitesi, Bilişim ve Teknoloji Enstitüsü "Siber Güvenlik Raporu" konulu çalışma Mayıs 2012, S. 43

[6] Rex Huges, "NATO and Cyber Defence" NATO Review, April 2009 S. 2

[7] Bilim ve Teknik Dergisi, Emre BAKIR "Türkiye'de Siber Güvenlik" konulu makale Kasım 2012, S. 15

A Secure System Development Framework for SaaS Applications in Cloud Computing

Eren TATAR, Emrah TOMUR

***Abstract*—The adoption of cloud computing is ever increasing through its economical and operational benefits. However, it also contains potential security issues in itself. Hence, while using cloud-based solutions, organizations need to be aware of these concerns and develop their solutions in a way that they include the information security management practices as a whole. In order to do that, a systematic development approach would be the most effective way to provide the necessary security controls at the beginning of the development life cycle. To handle with the security issues in the cloud computing and provide organizations a systematic way of integrating SaaS applications into their existing IT infrastructure, a secure system development framework will be developed and proposed within the scope of this study.**

***Index Terms*—Cloud Computing, SaaS, System Development Life Cycle, Secure System Development Framework**

I. Introduction

CLOUD computing has been defined several times differently by many leading experts working in IT sector. There is no just one description to be able to define all its characteristics, functionalities and architectural concept. However, all those interested in cloud computing somehow accept the definition of NIST: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." [1]. In general, cloud computing, or just 'cloud', presents a paradigm shift in the whole traditional IT environment. With its service-oriented architecture, applications, system, and network, all of which can be offered as an on-demand self-service based on pay-per-use model. Hence, organizations can take advantage of both its economical and operational benefits. However, cloud also brings some security, privacy and trust issues up for discussion due to its unique aspects. Although most of these issues are not new, already exist in traditional IT environment, they need more consideration because of the dynamic nature of cloud computing platform. Depending upon literature and some private companies' surveys on cloud, security and privacy issues are thought as the key to adoption of cloud according to IT executives. Under these circumstances, before utilizing cloud-services, organizations should ensure that they understand the security and privacy risks in the cloud environment and their security and privacy requirements based on their business requirements are satisfied by the cloud service providers (CSPs).

Manuscript received July 15, 2013.

E. Tatar is with the department of Information Systems, Informatics Institute, Middle East Technical University, Ankara, TURKEY (e-mail: eren.tatar@metu.edu.tr).

E. Tomur is with the department of Information Systems, Informatics Institute, Middle East Technical University, Ankara, TURKEY (e-mail: emrah.tomur@gmail.com).

II. Cloud Service Models

The clear understanding of cloud architecture and features ,which are usually addressed under the title of deployment models, service models and service attributes, will help us better understand the security concerns in the cloud environment. The details of service models are given below:

Software as a Service (SaaS)

SaaS is described as publicly available services and applications on an on-demand basis. The customer's responsibility begins and ends with entering system and managing its data. Everything from application level down to the infrastructure level is under the responsibility of the provider.

Platform as a Service (PaaS)

PaaS is described as middleware which provides virtual machines, operating systems, applications, services, development frameworks. The customer is responsible for installing and managing the application that is being deployed. The service provider manages the cloud infrastructure, and operating system.

Infrastructure as a Service (IaaS)

IaaS is all the infrastructures that are offered to and can be provisioned by customers. It includes virtual machines, virtual storage, other virtual infrastructures, and other hardware assets. While the service provider manages all the infrastructure, the customer is responsible for all other aspects of the deployment.

III. Security Concerns in Cloud

With the advances in cloud computing, it continues to be significant changes in business manner and technology infrastructure of organizations. Its service-oriented

architecture changes the structure of applications and systems in terms of design, development and deploy. However, these advances also brings the existing traditional security issues and also new issues into question again. According to the CSA research [8], the cloud computing top nine threats in 2013 respectively are:

- Data Breaches
- Data Loss
- Account or Service Traffic Hijacking
- Insecure Interfaces and APIs
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Vulnerabilities

These issues continue to be discussed today because of the highly dynamic nature of cloud computing. To deal with these security challenges precisely and properly, there needs to be a systematic approach covering all the information security management practices in order to provide essential security measures in each phases of a cloud-based solution development. Information security management can be defined as processes that enable organizations protect their IT operations and assets from unauthorized access, use, disclosure, disruption, modification, and destruction. It is not only a technical issue, but also a management issue. Hence, it is the responsibility of every member of the organization from the top to bottom. As cloud adoption increases, more confidentiality, integrity and availability, called as CIA triad, which forms the core of the information security, are demanded by cloud customers. Moreover, data security and system availability are considered the two most important service level agreement (SLA) parameters [9]. In order to respond all these issues properly, organizations should have a systematic way of integrating security practices into their development life cycle. Hence, it is possible with a security integrated system development life cycle.

IV. SYSTEM DEVELOPMENT LIFE CYCLE

The system development life cycle (SDLC) is a conceptual model including a sequence of processes followed to develop information systems. A typical SDLC phases are initiation, acquisition and development, implementation and assessment, operations and maintenance, and disposal. Although there are many SDLC models and methodologies such as the waterfall model, rapid application development (RAD), joint application development (JAD), spiral model, synchronize and stabilize, generally each of them consists of a series of defined steps or phases. Hence, integrating security activities into each phases of SDLC is an effective way to provide an appropriate level of security to protect critical assets in information systems development. Such an integration enables security to be planned, acquired, built in, and deployed as an integral part of a project or system [5]. It is also important to handle security practices in early stages of the SDLC. It plays a significant role in measuring and enforcing security requirements throughout the all phases of the life cycle. Also, the most effective way of integrating security into the SDLC is to plan and implement a detailed risk management program [5]. This will lead to identify, control, and minimize the security risks in information system by dealing with them in each phase of SDLC. Hence, an early attempt to control the risks can be accomplished in that way. The benefits of integrating security into an established SDLC are [5]:

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation,
- Awareness of potential engineering challenges caused by mandatory security controls,
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques,
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner,
- Documentation of important security decisions made during development, ensuring management that security was fully considered during all phases,
- Improved organization and customer confidence to facilitate adoption and usage as well as governmental confidence to promote continued investment, and
- Improved systems interoperability and integration that would otherwise be hampered by securing systems at various system levels.

V. LITERATURE REVIEW

There are several studies on secure system development life cycle for cloud platform. These studies focus on addressing security and privacy risks in cloud and studying on taking precautions by integrating information security practices into each SDLC phases, generally including initiation, development or acquisition, implementation or assessment, operation or maintenance and disposal.

In order to develop a secure SDLC framework for integrating SaaS applications to built-in IT systems in organizations, the articles examined can be found below:

A. Secure System Development for Integrated Cloud Applications

The article [2] describes that integrating a SaaS application



Figure 1. Orange Model

into an existing IT infrastructure poses serious risks in terms of data and system security. According to the researchers, security issues related with integrating SaaS systems often occurs at individual integration or customization. To solve this problem, security enhancement controls are presented from the technical point of view. Besides, a model is proposed to help enterprises securely adopting a SaaS solution from the management point of view. The importance of enhancing the security controls before integrating the SaaS solutions into existing IT infrastructure is emphasized. Otherwise, it is claimed that systems will be vulnerable against high level of risks posed. In the article, SaaS solutions are classified into three categories which are stand-alone application, web based integration, and server based integration. Then, particular risks to those categories are defined in order to provide effective security controls against risks for secure integration of SaaS solutions. Afterwards, the secure integration of SaaS solutions is discussed and suggestions are offered for the defined three different types of SaaS solutions. According to the writer, in the field of IT process research, although there are many system development models, models focusing on SaaS integration security are rare. For example, SCoM [3] is shown as an example of one of those models addressing data security framework. However, its shortcoming is that it only focuses on stand-alone applications, one of the three types of SaaS solutions defined in the article. Hence, in order to help organizations enhance their security capabilities when using SaaS applications, a secure life cycle model called the Orange Model which is shown in Figure 1, is proposed. Orange Model created with reinforcing the SCoM model uses an incremental and iterative development approach. It is composed of a number of parts which are a core, pith, flesh, inner ring, peel and seeds. Each of them has its own specific meaning and function. For instance, the flesh of the model consists of eight parts representing the phases of SDLC. In the each those phases, the processes needed to be carried out, outputs of the process, and person in charge of the process are defined in detail. Business goals and risks

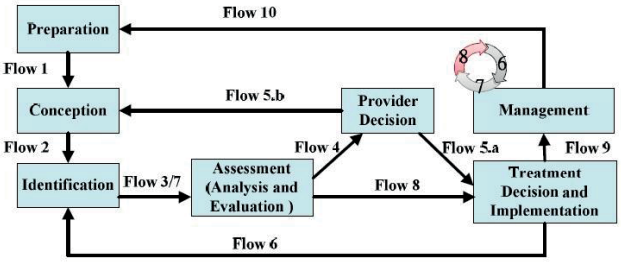


Figure 2. SCoRiM Framework

management forms the core of the Orange Model. The pith of the model covers all the phases existing in the flesh and its continuous policy improvement function and good communication with business and IT units function are defined as the key for success of secure management of the SaaS systems.

B. Enforcing Confidentiality in a SaaS Cloud Environment

The article [3] discusses that the top barriers to adoption of public cloud services (SaaS) in enterprises are losing control of systems, confidentiality issues, and rigid service level agreements (SLAs). To deal with confidentiality issues, on the basis of the idea of considering confidentiality in each phases of IT projects, a SaaS Confidentiality Risk Management Framework (SCoRiM) which is shown in Figure 2 is proposed. The framework consists of initiation, development and acquisition, implementation, operations and maintenance, disposition phases. It especially focuses on protecting critical data of small and medium sized enterprises (SMEs). Hence, it is claimed that framework enhances the client side confidentiality management on SMEs. It aims to enable SMEs gain capability of confidentiality risk analysis to determine which SaaS provider best suits their confidentiality needs. Also, the aim of the SCoRiM is cited as to enhance the data confidentiality with and without support from the service providers. However, there is no practical way offered in the article to implement confidentiality risk analysis. Without any checklist, it is quite difficult for SMEs to evaluate SaaS providers properly. In the article, SaaS applications are classified into two categories. The first one is complete applications like ERP, and CRM and the latter is custom applications like banking or customer tracking. Even if SCoRiM covers management of risks related with confidentiality issues in both categories, it especially focuses on the latter one.

C. Cloud SSDLC: Cloud Security Governance Deployment Framework in Secure System Development Life Cycle

The article [4] focuses to discuss the legal issues regarding protecting information and computer systems, laws and regulatory requirements. By its architecture, cloud computing centralizes the data storage in SaaS applications, thus, it causes data privacy and protection issues. This is why a cloud security self-governance deployment framework (Cloud SSDLC) which



Figure 3. Cloud SSDLC

is shown in Figure 3 is proposed in this article, especially from government and industry point of view. There are five main phases in proposed framework which are initiation, development, implementation, operation and destruction. Framework integrates SSDLC, cloud security domain guidelines and risk considerations. When it does that, the corresponding risks are integrated into each phase. The benefit of the model in practice is also supported by different cases from industry and government perspectives. The basic contribution of the framework is summarized as follows:

- Enhancing security in the cloud applications by integrating SSDLC and cloud,
- Identifying critical security issues in each system development life cycle phase,
- Being developed by working on a real case in a government cloud information system.

D.SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environment

In this article [7], it is described that security mechanisms are required in order to ensure the secure adoption of cloud computing since cloud gives rise to various security concerns including outsourcing, shared responsibility, virtualization, multi-tenancy, service level agreements, and heterogeneity. Consequently, a security framework for cloud computing environments is proposed to deal with different security challenges. The proposed framework consists of different modules to handle security and trust issues such as identity management, access control, policy integration among multiple clouds, trust management, secure services composition and integration. In fact, framework is based on multi-domain policy integration and secure service composition. While building the framework, security, policy and trust issues are being handled within the specified modules, not in the phases of SDLC as in the other frameworks discussed before.

E. Security Considerations in the System Development Life Cycle

The purpose of this guideline [5] is to help agencies in integrating security into their established IT system development life cycle. The guideline focuses on the information security components, not the implementation and development of SDLC. The base methodology is the waterfall SDLC in the document. For the successful integration of security into SDLC and for viability of it, the key security roles and responsibilities in SDLC are depicted. Each security activity in each phases of SDLC is defined by its description, its expected outputs including suggestions and further information for integration of other security activities, its synchronization to ensure its proper adaptation and its interdependencies with other tasks.

VI. FUTURE WORK

In order to provide such guarantees for requirements, organizations have relied on standards, guidelines and SLAs provided by cloud providers. There are some commonly accepted information security standards like ISO 27001-27006, 29361, 29362, 29363. However, although these standards are applicable to cloud [6], they should be reviewed and progressively developed for the cloud environment based on varying cloud security requirements. Moreover, the research and studies show that there are not any commonly accepted cloud standard. As well the developed models or frameworks do not present a comprehensive solution on how organizations will securely utilize application software offered as a service in their established IT system. The proposed models generally focus on a specific field of SaaS by categorizing SaaS solutions, and do not cover all core information security management practices. Currently, there are also variations in each element of the life cycle because there are no commonly accepted cloud standards. Hence, it is important to emphasize that standardization is required in order to make contribution to future development of cloud computing. Hence, we are planning to develop a comprehensive framework for organizations' system development life cycle to help them take the essential IT security issues regarding cloud computing into consideration when utilizing SaaS applications in their IT systems.

REFERENCES

[1] P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, Special Publication 800-145, September, 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Y. Chou, J. Oetting, *Secure System Development for Integrated Cloud Applications*, 2012 Second Symposium on Network Cloud Computing and Applications, IEEE, 2012.

[3] Y. Chou, J. Oetting, *Enforcing Confidentiality in a SaaS Cloud Environment*, 19th Telecommunications forum TELFOR 2011, Serbia, Belgrade, November 22-24, 2011, IEEE.

[4] T. Kao, C. Mao, C. Chang, K. Chang, *Cloud SSDLC: Cloud Security Governance Deployment Framework in Secure System Development Life Cycle*, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[5] R. Kissel, K. Stine, M. Scholl, H. Rossman, J. Fahlsing, J. Gulick, *Security Considerations in the System Development Life Cycle*, NIST, SP 800-64 Rev. 2, 2008.

[6] R. L. Krutz, R. D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley Publising, Inc. ,2010.

[7] H. Takabi, J. B. D. Joshi, G. Ahn, *SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments*, 34th Annual IEEE Computer Software and Applications Conference Workshops, 2010.

[8] *CSA, The Notorious Nine: Cloud Computing Top Threats in 2013*, Top Threats Working Group, CSA, 2013. Available: https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/

[9] Breaking through the cloud adoption barriers, KPMG Cloud Providers Survey, KPMG International, 2013. Available: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/cloud-service-providers-survey/Documents/cloud-service-providers-survey.pdf

Özgün Bir Şifreleme Algoritması Kullanan Güvenli E-Posta Uygulaması

Muhammet Serkan Çinar, Işıl Çinar, Hasan Şakir Bilge

***Özet*—Bu çalışma ile her geçen gün yaygınlaşmakta olan yüksek kapasiteli ve ücretsiz olarak dağıtılan e-posta hizmetlerinin daha güvenilir kılınması amaçlanmıştır. E-posta işlemleri için bilinen ve yaygın kullanılan şifreleme algoritmalarının dışında yeni bir şifreleme algoritması tasarlanmıştır. Tasarlanan şifreleme algoritmasıyla geliştirilen e-posta uygulaması, güvenlik konusunda getireceği avantajların yanında, ücretsiz e-posta servis sağlayıcılarının izin verdiği ölçüde sunuculara erişmekte ve yapılan konfigürasyonlara göre istenilen hesabın tüm e-posta verilerini kendi veritabanına yükleyebilmektedir. Ayrıca şifreleme algoritması MS Outlook programına eklenti olarak geliştirilen başka bir uygulamaya da entegre edilerek kurumsal e-posta iletiminde de güvenli e-posta gönderilmesi sağlanmıştır. Her iki uygulamada da şifreleme algoritması başarılı bir şekilde gerçekleştirilmiştir.**

***Anahtar Kelimeler*— E-posta Güvenliği, POP3 ve SMTP Protokolleri, Simetrik Şifreleme.**

Secure Email Application Using an Original Encryption Algorithm

***Abstract*—In this study, email services which are distributed free with high storage capacity and which become widespread every day is intended to made more reliable. A new encryption algorithm is designed for email operations which is out of the known and widely used email encryption algorithms. Besides the advantages of security issues of the email application that is developed with proposed encryption algorithm, mail application can access to the email servers to the extent permitted by free email service providers and all of the data in desired email account can be downloaded into application database according to configurations. Furthermore, the encryption algorithm has been integrated into the add-in application developed for MS Outlook program and by this way the secure message sending is provided for organizational email transmissions. The encryption algorithm was implemented successfully for both applications.**

***Keywords*— Email Security, POP3 and SMTP Protocols, Symmetric Encryption.**

I. GİRİŞ

Sürekli artmaya devam eden bilgi ve beraberinde getirdiği bilgi değişimi iş sürekliliğinde ve kurumların gelişmesinde büyük rol oynamaktadır. Bilgi değişiminde birçok metot bulunmasına rağmen; e-posta tüm kurumlar için iletişim araçları arasında ilk sırada gelmektedir [1].

Günümüzde e-postalar kurumsal iletişimin yanında bireysel iletişim için de vazgeçilemeyecek derecede önemli bir haberleşme aracıdır. İletişimin yüksek oranlarda e-postalar aracılığıyla yapılması, bu iletişim üzerinden yapılan saldırıların da artmasına sebep olmuştur. Kurumların, şirketlerin, bireysel kullanıcıların e-posta güvenliği konusunda önlem almaları ihtiyaç haline gelmiştir [2].

İncelenen çalışmalarda e-posta sistemleri güvenliği konusu genel olarak işletim sistemi seviyesinde, e-posta uygulaması seviyesinde ve ağ altyapısı seviyesinde ele alınmakla birlikte; e-posta sunucusu ve istemci arasındaki iletişimin güvenliği, güvenli oturum yönetimi, basit ve kriptografik anahtarlar, onay mesajları ile e-posta takibi, spam mesajların elenmesi, zararlı e-posta takibi gibi güvenlikle ilgili çok farklı konularda çalışmalar yapıldığı görülmüştür [3,4,5,6].

Yapılan bu çalışmada, e-posta sistemlerinin uygulama seviyesindeki güvenliği dikkate alınarak özgün bir algoritma ile şifreleme işlemi gerçekleştirilmektedir.

Bu çalışmada özellikle literatürde karşılaşılan [7, 8] saldırganın gönderici ile alıcı arasında mesaj trafiğini dinleyebiliyor olması ve mesajı değiştirebilmesi, e-postaların şifresiz olarak sunucu ve bilgisayarlarda tutuluyor olması ve genel olarak kullanıcı hataları ile donanım/yazılım açıklıkları gibi tehditlerin engellenmesi hedeflenmiştir.

Bulut bilişim ile kullanıcı verilerinin büyük bir kısmının bulut üzerinde olacağı öngörülmekle birlikte, yüksek kapasiteli ücretsiz e-posta sağlayıcılar da kullanıcıları için bir bulut ortamı sağlamaktadırlar. Bulut bilişim servis modellerinden servis olarak sunulan yazılım (Software as a Service) yaklaşımında kullanıcıların servis sağlayıcıların bulut altyapısını kullanarak web tabanlı e-posta uygulamalarına farklı cihazlardan, farklı arayüzlerle erişebilmeleri mümkün kılınmaktadır. Bu yaklaşımda, kullanıcıya özgü sınırlı konfigürasyon ayarlamaları yapılabilmekte olup kullanıcının depolama ortamını, işletim sistemlerini ve ağ altyapısını kontrol etmesi veya yönetmesi mümkün olmamaktadır [9].

Kullanıcılar tüm e-posta verilerini bulut üzerine taşıdıklarında bazı özel gizlilik dereceli verilerinin şifreli olarak bu e-posta servis sağlayıcılarında tutulmasını isteyebileceklerdir. Ücretsiz olarak sağlanan bu yüksek kapasiteli ve hizmet devamlılığı olan e-posta hizmet sağlayıcıları bu bilgileri bağlı bulundukları devletin güvenlik birimleri veya üçüncü şahıslar ile paylaşabileceklerini belirtmekle beraber istedikleri zaman kullanıcılarının hesaplarını kapatabileceklerini kullanıcı sözleşmelerinde ifade etmektedirler. Bu açılardan bakıldığında son kullanıcılar için bu ücretsiz e-posta servis sağlayıcılarının sunucularında e-posta verilerinin şifreli tutulması ve yalnızca anahtarlarını paylaştıkları kişilerle şifreli e-posta iletimlerini gerçekleştirmeleri, kişisel bilgilerinin

M.S.Çinar,Hacettepe Üniv.Bilg.Müh., e-posta:(mscinar@hacettepe.edu.tr).
I.Çinar Gazi Üniv.Bilg.Müh., e-posta: (isil.cinar@gazi.edu.tr).
H.Ş.Bilge,Doç.Dr.,Gazi Üniv.Bilg.Müh.,e-posta:(bilge@gazi.edu.tr).

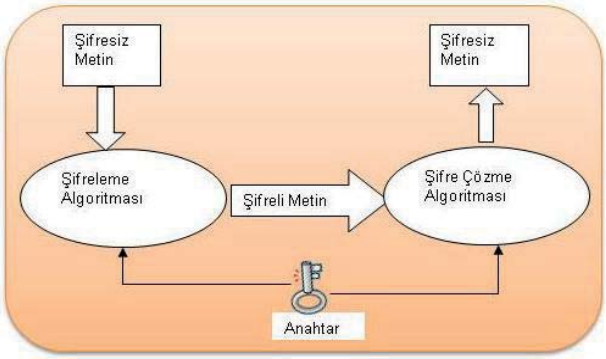
mahremiyetinin korunması hususunda önemli bir güvenlik mekanizması sağlayacaktır.

Çalışmada önerilen yaklaşım uçtan uca her seviyede güvenliği sağlamaya yönelik olarak önerilmiş bir çözüm olmamakla beraber, e-posta mesajları şifrelemesinin yaygın olarak kullanılan şifreleme algoritmaları dışında farklı bir algoritma ile sağlanmasını hedeflemiştir. Literatürde yapılan araştırmalarda simetrik şifrelemede DES, 3DES, AES ve Blowfish [10,11,12] algoritmalarının yaygın olarak kullanıldığı görülmüştür. E-posta güvenliğine yönelik simetrik şifreleme algoritmaları kullanarak yapılan çalışmalarda ise genellikle bahsedilen simetrik şifreleme algoritmaları kullanıldığı gözlemlenmiştir. Bu çalışmada ise farklı şifreleme teknikleri algoritmanın farklı adımlarında uygulanarak özgün bir simetrik şifreleme algoritması geliştirilmiştir.

Çalışmanın ikinci bölümünde geliştirilen simetrik şifreleme algoritmasından bahsedilmekte, üçüncü bölümde e-posta gönderme ve alma için gerekli protokollerin açıklaması yapılmakta ve bir sonraki bölümde de geliştirilen e-posta uygulamaları anlatılmaktadır. Beşinci bölümde gelecekte yapılması planlanan çalışmalar özetlenmektedir. Son olarak çalışmadan elde edilen kazanımlar ve sonuçlar sunulmuştur.

II. E-Posta İçerik Şifreleme Algoritması

Şifreleme algoritmasında gizli anahtarlı şifreleme yöntemi kullanılmıştır. Gizli anahtarlı şifreleme yönteminde, hem şifreleme hem de şifre çözme işlemi için aynı anahtar kullanılmaktadır. Bu yöntem simetrik şifreleme olarak da adlandırılmaktadır. Simetrik şifrelemede anahtarın alıcı tarafına güvenli bir şekilde iletilmesi önemlidir. Anahtar olmadığı sürece şifrelenmiş metin ele geçirilse de asıl metnin elde edilmesi mümkün değildir [13]. Şekil 1'de simetrik şifreleme algoritmalarının çalışma yapısı ana hatlarıyla gösterilmektedir.

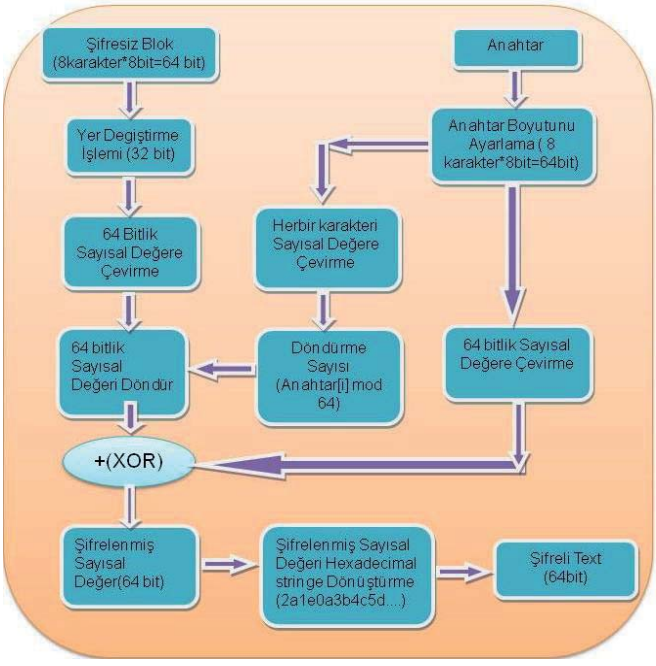


Şekil 1. Simetrik şifreleme algoritması çalışma yapısı

A. *Şifreleme Algoritması*

Çalışmanın bu bölümünde geliştirilen algoritmada uygulanan şifreleme adımları ele alınmış olup şifreleme algoritması Şekil 2'de akış diyagramı olarak sunulmuştur.

1) Şifreleme algoritması her bir 8 karakterin blok olarak alınıp, 8 karakterlik dizinin 64 bitlik sayısal değere dönüştürülmesi ve bu değerin bit seviyesinde çeşitli fonksiyonlardan geçirilmesini kapsamaktadır.
2) Şifreleme işlemine gelen 8 karakterlik dizi ilk olarak yer değiştirme işlemine tabi tutulur. İlk 4 karakter ve son 4 karakter yer değiştirir.
3) Yer değiştirme işleminden sonra 8 karakterlik blok 64 bitlik sayısal bir değişkene aktarılır. İlk karakter 64 bitin ilk 8 bitini temsil eder. Bu sayısal değer anahtar dizesinin her bir karakterinden elde edilen sayısal değer kadar döndürme işlemine tutulur.
4) Döndürme işleminin kaç kez yapılacağı anahtar dizesindeki her bir karakterin sayısal değerinin 64 ile bölünmesinden kalan değer ile belirlenir.
5) Döndürme işleminden sonra elde edilen veri ile 64 bitlik sayısal değere atanan anahtar arasında XOR işlemi gerçekleştirilir.
6) Şifrelenmiş sayısal değer onaltılık sayı tabanında string dizesine dönüştürülür. Dönüştürme işlemi sonrası şifreli blok elde edilmiş olur.
7) Diğer 8 karakterlik bloklar için aynı işlemler tekrar edilir.
8) Son kalan blok 8 karakterden daha az ise gerektiği kadar "*" karakteri yerleştirilerek 8 karaktere tamamlanır.



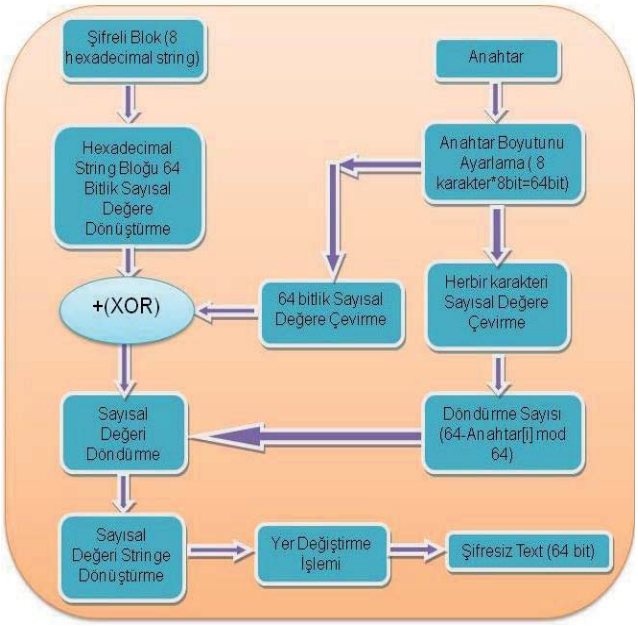
Şekil 2.Şifreleme algoritması akış diyagramı

B. *Şifre Çözme Algoritması*

Çalışmanın bu bölümünde ise geliştirilen algoritmada uygulanan şifre çözme adımları ele alınmış olup şifre çözme algoritması Şekil 3'de akış diyagramı olarak sunulmuştur.

1) Şifre çözme algoritması şifreleme algoritmasında izlenen yolun tersidir. Her bir onaltılık sistemdeki 8 değer blok olarak alınıp, 64 bitlik sayısal değere dönüştürülerek bit seviyesinde çeşitli fonksiyonlardan geçirilir.

2) Şifre çözme işlemine gelen 16 karakter (onaltılık sistemdeki 8 değer) 64 bitlik sayısal değere dönüştürülür.
3) Elde edilen sayısal değer ile 64 bitlik sayısal değere atanan anahtar arasında XOR işlemi gerçekleştirilir. Bu sayısal değer anahtar dizesinin her bir karakterinden elde edilen sayısal değer kadar döndürme işlemine tabi tutulur.
4) Döndürme işleminin kaç kez yapılacağı, anahtar dizesindeki her bir karakterin sayısal değerinin 64 ile bölünmesinden elde edilen kalan değerin, 64 sayısından çıkarılmasıyla belirlenir.
5) Döndürme işlemi sonucu elde edilen sayısal değer stringe dönüştürülür. String dizesi 32 bitlik yer değiştirme işlemine (ilk 4 karakter ve son 4 karakter yer değiştirir) tabi tutularak şifresiz blok elde edilir.
6) Geriye kalan bloklar için de aynı işlemler gerçekleştirilerek şifresiz metin elde edilir.



Şekil 3.Şifre çözme algoritması akış diyagramı

III. E-POSTA PROTOKOLLERİ

POP (Post Office Protokol) protokolü elektronik posta almak için son kullanıcılar tarafından kullanılmaktadır. POP protokolü sayesinde kullanılan e-posta sunucusunda bulunan postalar yerel diske indirilebilmektedir [14].

Elektronik posta gönderme protokolü (Simple Mail Transfer Protocol), bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür. Sadece e-posta göndermek için kullanılan bu protokolde; istemci bilgisayar SMTP sunucusuna bağlanarak gerekli kimlik bilgilerini göndermekte, sunucunun onay vermesi halinde gerekli e-postayı sunucuya iletmekte ve bağlantıyı sonlandırmaktadır [15].

A. Telnet ile POP3 ve SMTP Sunucularına Bağlanma

Herhangi bir e-posta sunucuya bağlanırken normal bir TCP/IP bağlantısı yapılmaktadır. POP3 ile ilgili gerekli ayarları yapmak ve gelen e-postaları almak için gerekli işlemleri yapmak amacıyla telnet kullanılmıştır.

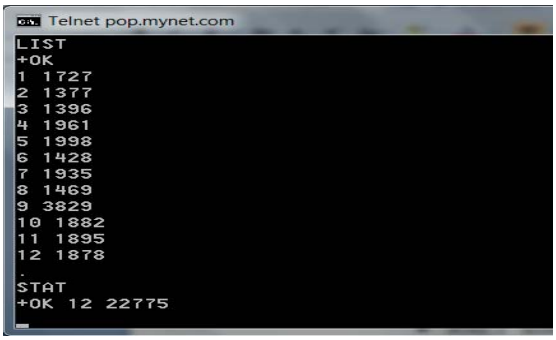
Telnetle bir sunucuya bağlanmak için öncelikle sunucunun adresi ve çalıştığı portu girmek gerekmektedir. Genellikle port için varsayılan değer 110'dur. Bu işlemin sonunda sunucu helo mesajı göndermekte ve bağlantının hazır olduğunu belirtmektedir. Yapılan işlemler doğru olduğu sürece +OK ile cevap alınmaktadır.

Bağlantı sağlandıktan sonra "USER" komutuyla kullanıcı kodu ve "PASS" komutuyla şifre girilerek sunucuya erişim sağlanmaktadır.

Bu aşamadan sonra çalışma sırasında kullanılan önemli komutlar ve görevleri aşağıda belirtilmiştir [16]:

STAT: Gelen kutusunda kaç adet e-posta olduğunu göstermektedir. STAT komutu kullanılarak gelen kutusunda e-posta olup olmadığı ve kaç yeni e-posta geldiğinin kontrolü yapılmıştır (Şekil 4).

LIST: Gelen kutusundaki e-postaların sırasını ve her birinin boyutlarını göstermektedir (Şekil 4).

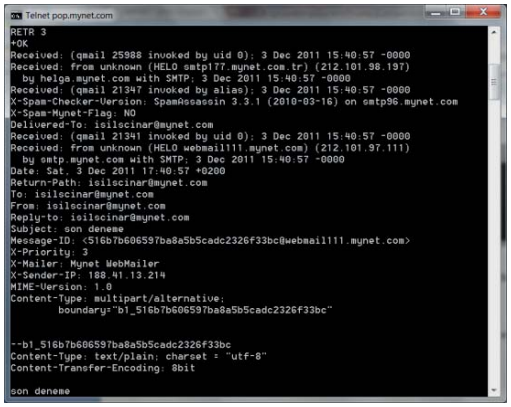


Şekil 4. LIST ve STAT komutlarının çalıştırılması ve örnek sonuçlar

QUIT: POP3 bağlantısını sonlandırmak için kullanılmaktadır.

TOP: E-posta içeriğinin istenilen satıra kadar görülmesini sağlamaktadır. "TOP 2 5" ifadesi, 2 numaralı e-postanın 5.satırına kadar görüntülenmesini sağlamaktadır.

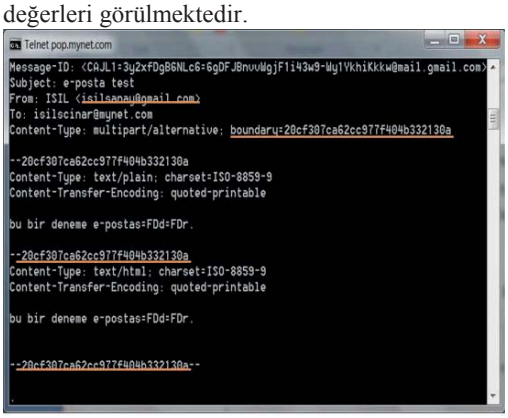
RETR: Bu komutla Şekil 5'te görüldüğü gibi gelen kutusundan istenilen e-postanın sıra numarası yazılarak detaylı olarak içerik bilgileri alınabilmektedir. Buradaki içerik standart e-postaların içeriğine benzememektedir. Buradaki bilgiler e-postanın orjinal halini göstermektedir.



Şekil 5.RETR komutunun çalıştırılması ve örnek sonuçlar

E-posta içeriğinin başlama ve bitişini belirten sınır (Boundary) değeri eğer içerikte varsa string olarak alınır ve

bundan sonraki 2. ve 3. sınır değerleri arasında kalan alan mesajın metninin verildiği alandır. Şekil 6'da Mynet e-posta sunucusuna gönderilen Gmail e-posta içeriği için örnek sınır değerleri görülmektedir.



Şekil 6. Gmail e-posta içeriği için örnek sınır değerleri

Uygulamada SMTP sunucusu olarak Gmail'in e-posta sunucusu kullanılmıştır.

B. *Ücretsiz E-Posta Servis Sağlayıcı İstemci Ayarları*

E-posta işlemleri için kullanılmakta olan Gmail, Yahoo, Mynet, Hotmail gibi ücretsiz e-posta servis sağlayıcılarının bir kısmı SMTP sunucularına erişimi engellerken bir kısmı da POP3 sunucusuna erişimi engellemiş durumdadır. Uygun sunucuların bulunması için TELNET ile bağlantı yapılarak gerekli testlerin yapılması önemlidir.

Tablo 1'de Gmail, Mynet, Yahoo ve Hotmail gibi e-posta hizmet sağlayıcılarının POP3 ve SMTP protokolleri için yapılandırma ayarları yer almaktadır. Yahoo e-posta servisinde POP3 sunucularına erişimi ücretli e-posta hesaplarına sağlamakta iken diğer e-posta servis sağlayıcılar ücretsiz olarak her iki protokolü de hizmete sunmaktadırlar. Ancak servis sağlayıcıların POP3 sunucularından e-posta verilerini alabilmek için web sayfaları üzerindeki e-posta yapılandırma ayarlarından e-posta hesaplarına erişim izninin verilmesi gerekmektedir.

TABLO I
ÜCRETSİZ E-POSTA SERVİSİ SAĞLAYICILARI PROTOKOL YAPILANDIRMA BİLGİLERİ

	Gelen E-Posta Sunucusu(POP3)	POP3 Portu	Giden E-Posta Sunucusu(SMTP)	SMTP Portu
Gmail	pop.gmail.com	995	smtp.gmail.com	587
Mynet	pop.mynet.com	110	pop.mynet.com	587
Yahoo	Yalnızca Ücretli Hesaplara Açık	-	smtp.mail.yahoo.com	587
Hotmail	pop3.live.com	995	smtp.live.com	587

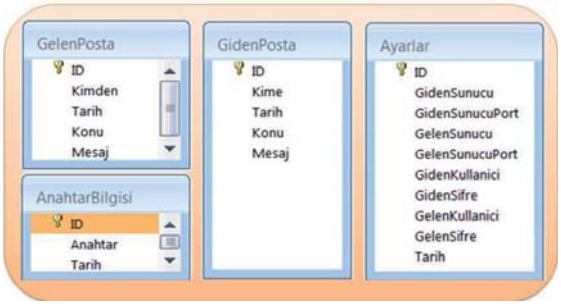
IV. GELİŞTİRİLEN E-POSTA UYGULAMALARI

A. *E-posta Kontrol Uygulaması*

E-posta kontrol uygulaması .NET 2008 platformu üzerinde C# programlama dili ile geliştirilmiş olup e-posta verilerinin tutulacağı veritabanı için MS Access 2007 kullanılmıştır.

Uygulamada temel e-posta gönderme ve alma işlemleri önceki bölümde bahsedilmiş olan Telnet komutları kullanılarak gerçekleştirilmiştir.

Veritabanında bulunan Gelen/Giden e-posta bilgilerinin tutulduğu tablolar, şifreleme işlemi için kullanılan anahtarların tutulduğu AnahtarBilgisi tablosu ve e-posta gönderme/alma işlemlerinde kullanılan sunucu ayarlarının tutulduğu Ayarlar tablosu en basit şekilde Şekil 7'de görülmektedir.



Şekil 7. E-posta kontrol uygulaması veritabanı şeması

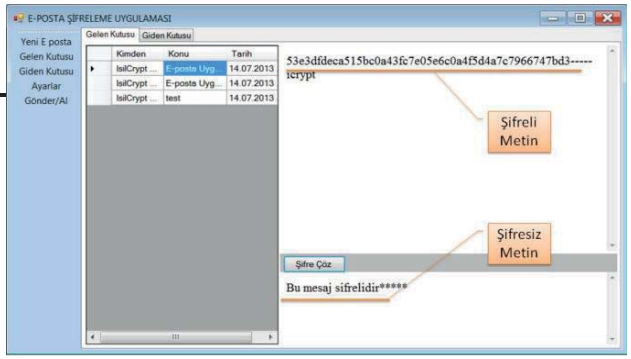
POP3 sunucusundan çekilen e-postalarla ilgili bilgiler gerekli düzenlemelerden geçirilip parçalandıktan sonra gelen posta tablosuna kaydedilmiştir.

Giden e-posta tablosunda uygulamadan gönderilen postaların bilgileri, anahtar bilgisi tablosunda şifreleme algoritmasında kullanılacak anahtar ve anahtarın kaydedildiği tarih bilgisi, ayarlar tablosunda posta gönderme ve alma işlemleri için kullanılan sunucuların bilgileri ve sunucularda yetkili olacak kullanıcının hesap bilgileri ve tarih bilgisi yer almaktadır.

Temel E-Posta İşlemlerinin Gerçekleştirilmesi

Yeni e-posta göndermek için Şekil 8'deki ana menüde "Yeni e-posta" seçeneği seçilerek e-postanın isteğe göre şifrelenmeden veya şifrelenerek gönderilebilmesi sağlanmaktadır. Şifrelenmiş olan e-postaların sonuna uygulamaya özgü bir ifade olan "-----icrypt" ifadesi eklenmektedir.

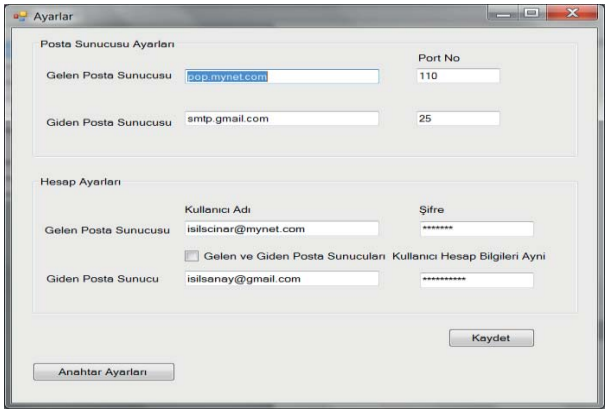
Uygulama gelen e-postanın şifreli veya şifrelenmeden gelmiş olma durumlarını şifrelenmiş olan mesajların sonunda "-----icrypt" ifadesinin bulunup bulunmadığını kontrol ederek yapmaktadır. Böylece e-postanın uygulama içerisindeki algoritmayla şifrelenip şifrelenmediği test edilmektedir. Eğer e-posta şifrelenerek gönderilmişse e-posta alanının altındaki "şifre çöz" butonuna tıklandığında aşağıdaki bölmeye şifrelenmiş mesajın şifresi çözülmüş, orjinal hali yüklenmektedir.



Şekil 8.E-Posta kontrol uygulaması gelen e-posta kutusu

Konfigürasyon İşlemleri

Uygulama içerisindeki ayarlar penceresinden e-posta sunucusu ayarları yapılmaktadır. Bu ayarlar, POP3 sunucusuna bağlanmak için gerekli olan gelen posta sunucusu, port numarası ve SMTP sunucusuna bağlanmak için gerekli olan giden posta sunucusu, port numarası ve her iki sunucu için de kullanıcı hesabı bilgilerini kapsamaktadır. Şekil 9'da örnek konfigürasyon bilgileri sunulmaktadır.



Şekil 9. E-Posta kontrol uygulaması e-posta sunucu, hesap ve anahtar ayarları

Anahtar Ayarları

Anahtar dağıtım sorunu iletişimde bulunan iki tarafın ortak bir şifreleme anahtarı üzerinde anlaşmaları sorunudur. Şifreleme anahtarı ile şifreyi çözme anahtarının aynı olduğu klasik şifreleme algoritmaları kullanan sistemlerde, anahtar dağıtım sorunu ya önceden elden ele anahtarı vererek, ya özel ve güvenli bir kanal vasıtasıyla, ya da güvenli anahtar dağıtım sunucuları kullanarak çözülmektedir [8].

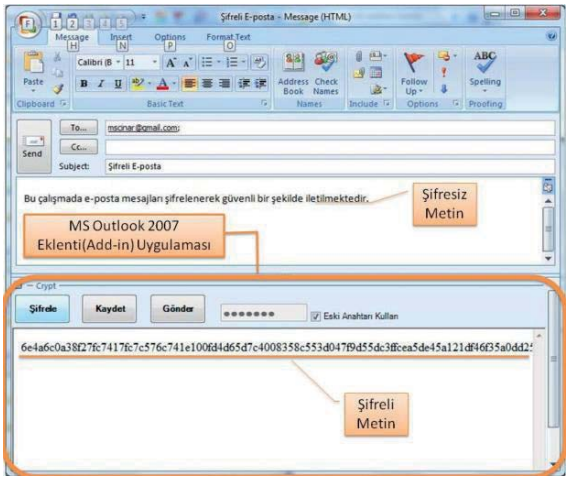
Yapılan çalışmada anahtar paylaşımının özel ve güvenilir bir kanal vasıtasıyla veya güvenli anahtar dağıtım sunucuları kullanılarak gerçekleştirildiği varsayılmıştır. Şifreleme algoritmasında kullanılmış olan ve hem gönderici hem de alıcının bilmesi gereken şifreleme anahtarı Şekil 9'daki anahtar ayarları bağlantısından sisteme kaydedilmektedir.

B. MS Outlook E-Posta Şifreleme Eklenti Uygulaması

Bu çalışma kapsamında geliştirilen ikinci uygulama, MS Outlook programına eklenti olarak (add-in) .NET 2008 platformu üzerinde C# programlama dili ile geliştirilmiştir.

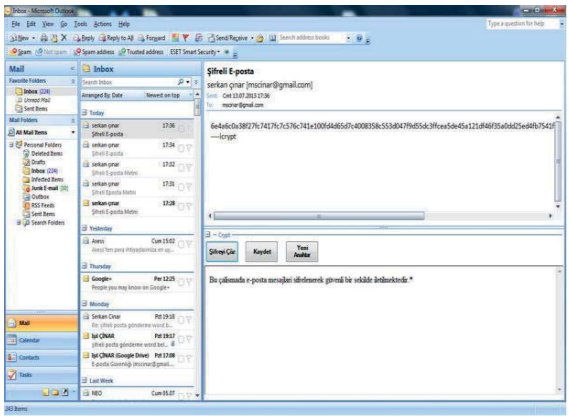
Eklenti uygulamaları programların yeteneklerini artırmak için geliştirilen ve programlara entegre edilebilen küçük programcıklardır [17].

Geliştirilen eklenti uygulaması ile şifreli e-posta gönderme ve alma işlemleri başarılı bir şekilde gerçekleştirilmiştir. Şekil 10'da şifreli e-posta gönderimine ilişkin MS Outlook programının ekran görüntüsü sunulmaktadır.



Şekil 10. MS Outlook 2007 eklentisi şifreli e-posta gönderme ekranı

Şekil 11'de ise gelen şifreli e-postanın geliştirilen outlook eklentisi ile çözülmesi işlemi gösterilmektedir.



Şekil 11. MS Outlook 2007 eklentisi gelen kutusu şifre çözme ekranı

V. GELECEKTE YAPILACAK ÇALIŞMALAR

Gerçekleştirilecek sonraki çalışmalarda, e-posta kontrol uygulaması ve MS Outlook e-posta şifreleme eklenti uygulamasında, e-posta içeriklerinde yer alan farklı türlerdeki dosya eklerinin hızlı ve etkin şifrelenmesi için tasarlanan algoritmanın geliştirilmesi planlanmaktadır. Algoritma, şifrelemede uygulanan; blok bazında yer değiştirme, bit bazında döndürme ve anahtar değeri ile şifreleme fonksiyonundan geçirme işlemleri ile şifre kırma saldırılarına karşı dirençli olmasına rağmen, tüm anahtarların denendiği kaba kuvvet (brute force) saldırılarında, gerekli hesaplama gücü anahtarın uzunluğu ile doğru orantılı olarak artacağından şifrenin kırılmaya karşı güçlendirilmesi için sonraki çalışmalarda anahtar boyutu arttırılarak şifreleme 128 ve 256 bit olarak gerçekleştirilecektir.

Ayrıca çalışmada tasarlanan şifreleme algoritması asimetrik şifreleme algoritmaları ile güçlendirilerek hibrid bir şifreleme algoritması geliştirilmesi planlanmaktadır. Geliştirilecek hibrid algoritma ile anahtar paylaşımında kullanılan açık anahtar altyapıları çalışmada yer alan uygulamalara entegre edilebilecektir.

VI. SONUÇ VE KAZANIMLAR

Bu çalışmayla her geçen gün daha da yaygınlaşmakta olan e-posta kullanımının daha güvenilir olması sağlanmıştır. Çalışmada bilinen yaygın kullanılan şifreleme algoritmaları dışında yeni bir algoritma geliştirilmiştir. DES, AES ve Blowfish gibi simetrik şifreleme algoritmaları yaygın kullanılan ve bilinen algoritmalar olması sebebiyle internet ortamında bu algoritmaların kırılmalarına yönelik çeşitli araçlar ve çalışmalar bulunmaktadır. Bu çalışmada geliştirilen şifreleme algoritmasının özgün olması, en azından programlama bilgisi olmadan hazır araçları kullanarak zaman zaman şifre kırma konusunda başarılı olan kötü niyetli kişilerin hedefi olmaktan kurtarmaktadır.

Uygulama şifreleme özelliği sayesinde güvenlik konusunda getireceği avantajlara ek olarak, ücretsiz e-posta servis sağlayıcılarının izin verdiği ölçüde sunuculara erişmekte ve yapılan konfigürasyonlara göre istenilen hesabın tüm e-postalarını uygulama kendi veritabanına yükleyebilmektedir.

Gmail, Yahoo, Hotmail gibi ücretsiz e-posta servis sağlayıcıların kullanım sözleşmesinde belirttiği üzere; kullanıcı e-postaları bu servis sağlayıcılar tarafından istenildiğinde silinebilmekte veya üçüncü kişilerle paylaşılabilmektedir. Bu çalışma sayesinde e-postalar servis sağlayıcılar tarafından silinme durumuna karşın koruma altına alınmış olmaktadır. Ayrıca e-postalar istenildiğinde şifrelenerek gönderme işlemine tabi tutulduğu için bilgiler üçüncü kişilerin eline geçse dahi gönderilen e-posta içeriği anlaşılmamaktadır.

REFERANSLAR

[1] D. Choukse, U.K. Singh, L. Laddhani ve R. Shahapurkar, "Designing secure email infrastructure," *Wireless and Optical Communications Networks (WOCN)*, 1964, pp. 1–9, 2012.

[2] Ş. Bayzan, "E-Posta Güvenliği Neden Önemlidir?", http://www.guvenliweb.org.tr/guvenlik/node/40, (Erişim: 08.07.2013).

[3] A.M.M.Rao, "Policy Specification and Enforcement for Detection of Security Violations in a Mail Service ," *9th International Conference on Information Technology* , pp. 172–175, 2006.

[4] A. Ghafoor, S. Muftic ve G. Schmölzer," CryptoNET: Design and implementation of the Secure Email System", *2009 Proceedings of the 1st International Workshop on Security and Communication Networks (IWSCN)*, pp. 1–6, 2009.

[5] S.J. Stolfo, S. Hershkop, Ke Wang ve O. Nimeskern," EMT/MET: systems for modeling and detecting errant email", *DARPA Information Survivability Conference and Exposition*, vol. 2, pp. 290–295, 2003.

[6] M. Takesue, "E-mail Sender Identification through Trusted Local Deposit-Agents", *IEEE Conf, 2011 14th International Conference on Network-Based Information Systems (NBiS)*, pp. 84–91, 2011.

[7] G.Bahadur, Chan ve W.Weber, "Privacy Defended: Protecting Yourself Online", *Que, Chapter 8*, 2002.

[8] A. Levi ve M.U. Caglayan, "Elektronik Posta Güvenliği ve Açık Anahtar Sunucuları", *Bilişim 97, TBD 14. Bilişim Kurultayı*, pp. 114-117, 1997.

[9] D. Zissis, ve D. Lekkas, "Addressing cloud computing security issues", *Future Generation Computer Systems*, pp.583-592, 2012.

[10] TropSoft,"DES Overview", http://www.tropsoft.com/strongenc/des.htm. Erişim: 01.06.2013.

[11] A. Nadeem, "A Performance Comparison of Data Encryption Algorithms", *IEEE*, 2005.

[12] J. Thakur, ve K. Nagesh, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis.", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 1, pp. 6-12, 2011.

[13] Vikipedi, "Gizli Anahtarlı Şifreleme", http://tr.wikipedia.org/wiki/Gizli_anahtarl%C4%B1_%C5%9Fifreleme, (Erişim: 08.05.2013).

[14] R. Sureswaran ve ark., "Active E-mail system protocols monitoring algorithm", *TENCON 2009 - 2009 IEEE Region 10 Conference*, 2010.

[15] Vikipedi, http://tr.wikipedia.org/wiki/SMTP, Erişim: 12.06.2013.

[16] ProgramlamaTv, "Telnet ile Pop3 Sunucuya Bağlanma ve Mail İşlemleri", http://www.programlamatv.com/ders/bilisim/telnet-ile-pop3-sunucuya-baglanma-ve-mail-islemleri/, (Erişim: 08.07.2012).

[17] J. Boyce, B. Sheresh ve D. Sheresh, "Microsoft® Office Outlook® 2007", *O'Reilly Media, Inc*., 2009.

Muhammet Serkan Çinar, 2011 yılında Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği bölümünden yüksek lisans derecesi almıştır. Şu anda Hacettepe Üniversitesi Bilgisayar Mühendisliği bölümünde doktora öğrencisidir. IPTV tabanlı uzaktan eğitim, yazılım mühendisliği, bilişim güvenliği ve semantik web alanlarında çalışmalar yapmaktadır.

Işıl Çinar, Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde yüksek lisans yapmaktadır. Bilişim güvenliği, veri madenciliği, insan bilgisayar etkileşimi alanlarına ilgi duymaktadır.

Hasan Şakir Bilge, 1992 yılında Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği bölümünden mezun oldu. 1997 yılında Kırıkkale Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda yüksek lisansını, 2003 yılında Başkent Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda doktorasını tamamladı. Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde 2003 yılında yardımcı doçent unvanını ve 2012 yılında doçent unvanını aldı.

Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi

Seda YILMAZ ve Şeref SAĞIROĞLU

***Özet*—Siber güvenlik, bireysel, kurumsal ve ulusal yapılar için önemli bir husustur. Siber tehditler sadece bireylerin kişisel verilerinin güvenliğini değil aynı zamanda ülkelerin bütünlüğünü de tehdit eder bir noktaya gelmiştir. Bu çalışmada tehditlerin yöneldiği popüler hedefler, dünya üzerindeki siber saldırı ve hatta savaş denemeleri ile ülkemizde siber güvenlik konusundaki yaklaşımların neler olduğu üzerinde durulmuş, diğer ülkelerin siber güvenlik faaliyetlerinden örnekler verilmiştir. Sonuç olarak ülkemizin siber güvenlik stratejisi değerlendirilmiştir.**

***Anahtar Kelimeler*— Siber güvenlik, hedef, siberstrateji, Türkiye**

***Abstract*—Cyber security, individual, corporate and national structures is an important consideration. Cyber +threats to the security of the personal data of individuals only, but also threatens the integrity of the countries has a point. In this study, directed the popular targets of threats, cyber attacks, and even warfare experiments in the world with what is happening in our country focuses on the approaches of other countries on cyber security and cyber security are examples of activities. As a result, our country's cyber security strategy were evaluated.**

***Index Terms*— Cyber security, target, cyber strategy,Turkey**

I. GİRİŞ

Siber güvenlik ITU tarafından "siber çevre, organizasyonlar ve kullanıcının varlıklarını korumak için kullanılabilir araçlar, politikalar, güvenlik konseptleri, güvenlik önlemleri, kurallar, risk yönetimi, eylemler,eğitimler,uygulamalar ile teknolojiler bütünü" olarak tanımlanmıştır [21].

Siber tehditler her gün başka bir alanda kendini göstermekte ve siber güvenlik kavramı gün geçtikçe önem kazanarak daha çok hayatımıza dahil olmaktadır. Ülkelerin bütünlüğünü ve güvenliğini bile tehdit eden bu kavram, devletlerin vatandaşlarını korumak için tedbir almalarının zorunlu hale getirmiştir. Artık siber dünya birkaç bilgisayar korsanının oyun alanından çıkıp popular hedeflerin olduğu, amaçlı, planlı, disiplinli saldırıların gerçekleştirildiği ve hatta ülkelerin birbirlerine güç gösterisinde bulunduğu bir yer haline gelmeye başlamıştır.

Son yıllarda ülkeler bu konunun önemini dikkate alarak ulusal stratejilerini geliştirmişler ve bu konuda gerek maddi olarak gerekse insan gücü, altyapı ve yeteneklerini arttırıcı tedbirler almaya başlamışlardır. Bu çalışmada ikinci bölümde siber güvenlikte popular hedefler, üçüncü bölümde siber savaş denemeleri, dördüncü bölümde Türkiye'de siber güvenlik, beşinci bölümde Türkiye'nin siber güvenlik stratejisi konuları tartışılmış ve altıncı bölümde Dünya'dan siber güvenlik faaliyeti örnekleri verilerek sonuç ve öneriler sunulmuştur.

II. SİBER GÜVENLİKTE POPÜLER HEDEFLER

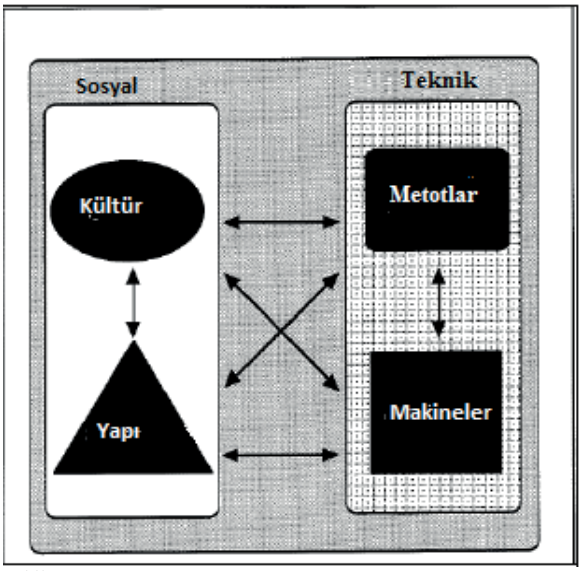
Günümüzde siber güvenlik ve savunma yaklaşımları hemen hemen her alana nüfuz etmiştir. Bu çalışmada siber güvenlik ihlallerinin en fazla olduğu ortamlar farklı başlıklar altında incelenmiştir.

A. Sosyal Ağlar

Sosyal ağlar bugün en büyük fenomendir. İnsanlar yoğun yaşam şartları içinde her yere ve her şeye yetişmek için acele edip koşuştururken en büyük insani ihtiyaç olan paylaşım ihtiyacını maalesef yeterince karşılayamamaktadır. Günlük hayatta çok şey yaşıyor, çok şey görüyor ve çok şey biriktiriyoruz. Sosyal ağlar bu konuda büyük fırsatlar sunmaktadır. Sosyal ağ uygulamaları ile paylaşımda bulunabiliyor, biriktirdiklerimizi anlatabiliyor, arkadaşlarımızla sohbet edebiliyor, fotoğraflarımızı/videolarımızı paylaşabiliyor, eski arkadaşlarımıza ulaşabiliyor, ürün tanıtımlarını yapabiliyor hatta ve hatta bir iş yeri sahibiysek işe alacağımız personel hakkında ön araştırma bile yapabiliyoruz. Çoğu zaman hayatımızı neredeyse tamamen sosyal ağ üzerinden yaşıyoruz.

Bu kadar etkin kullanılan bir sistem tabikî toplum hakkında bir takım sonuçlara ulaşılmasına da imkân sağlayacaktır. Ağa katılan farklı bireylerin üstlendikleri rolleri, davranış kalıplarını ve gizli özelliklerini ayıklamak amacıyla uygulanan analiz tekniğine Sosyal Ağ Analizi (SAA) denilmektedir. SAA iletişim, paylaşım, organizasyon, istihbarat, güvenlik gibi birçok alanda etkin olarak kullanılmakta olup bireysel analiz ve toplumsal analiz olmak üzere iki türü bulunmaktadır [2].

Kültür-Risk Teorisine göre her birey risk kavramını kendi toplumsal yapısı ve kültürünün etkisinde algılamaktadır [4]. Bireyleri, algıladıkları risklere göre analiz ederek bireysel, eşitlikçi, hiyerarşik ve kaderci olarak gruplandırmak mümkündür. Bireysel grup içine dâhil edilenler dünyayı iyimser bir yaklaşımla görmektedir. Riskin onu arayanlar için var olduğuna inanırlar. Eşitlikçi gruba dâhil olanlar çevrelerindeki olguları geçici olarak algılarlar ve risk almaktan hoşlanmazlar. Hiyerarşik olarak nitelendirilenler dünyayı hoşgörü içinde algılarlar ve belli bir limite kadar riskleri kabul ederler. Kaderci gruba dâhil olan insan profili ise olayları kaprisli bir bakış açısıyla değerlendirirler. Bu kategoriler temel alınarak ve insanların davranış özellikleri incelenerek 1990'lı yıllarda Kowalski tarafından kültür/yapı ile metot/makine incelemesinin birlikte incelendiği sosyo-teknik değerlendir-menin bilgi güvenliği için kullanılabilir bir teknik olduğu ileri sürülmüştür [4]. Sosyal ağlar üzerinden bilgi güvenliğinin sağlanmasında ve bireylerin analiz edilmesinde anlatılan teknikler temel teşkil etmektedir. Zira Amerika Ulusal Güvenlik Ajansı tarafından geliştirilen ve kabul gören 'Derin Savunma' stratejisine göre güvenliği sağlamada temel yapı taşı kullanıcıların olayları değerlendirmeleri ve davranış hareketleridir [4].



Şekil 1. Sosyo-Teknik Sistem [4].

Sosyal ağlar, kişiye ait her türlü bilginin kişinin rızası ile paylaştığı ortamlar oldukları için yemleme, önemsiz e-posta, kişinin verilerine erişim sağlamak amacıyla düzenlenen kullanıcı hesaplarının ele geçirilmesi gibi pek çok siber saldırının doğal hedefleri haline gelmişlerdir [3]. Sosyal ağlara yönelik tespit edilen ilk tehdit Şubat 2011'de kullanıcı ile sosyal ağ servis sağlayıcı arasındaki iletişimin dinlendiği PIMA saldırısı olmuştur [3].

Sosyal ağlarda kullanıcı tarafından doğrulanan bilgilerin kaydedildiği çerezlerin, korumalı olarak servis sağlayıcıya iletildiği https protokolü yerine şifresiz ve korumasız olarak iletimi gerçekleştiren http protokolünün tercih edilmesi ciddi bir tehdit oluşturmaktadır. Bu tehdit Mayıs 2011'de Windows İşletim sistemi kullanan bir makine üzerindeki IE (Internet Explorer) ile yapılan sosyal ağ servisine erişim sırasında kullanılmıştır. Bilgilerin tutulduğu çerezler, sıfır-gün açığı kullanılarak tanımlanan özel bir güvenlik bölgesine yönlendirilirken kullanıcıya da "Erişim Engellendi" mesajı döndürülmektedir. Bu şekilde istenilen bilgi elde edilmektedir. Aynı dönemde Rishi Narang'un blogunda yayınlanan bir bilgiye göre her giriş işleminden sonra bilgisayarda oluşan dosyalar ve çerezler 1 yıl kadar aktifliklerini koruyabilmekte dolayısıyla kullanıcı profillerini saklayabilmektedirler [3]. Tehlikelerin tespitinin ardından konuyla ilgili çalışmalar hızlandırılmıştır. Çalışmalar özellikle https tabanlı bağlantı protokolleri geliştirilmesi üzerinde yoğunlaşmaktadır [3].

Sosyal ağlar üzerindeki en vahim tehdit ise siber-zorbalık olarak nitelendirilen ve özellikle çocuklar ile gençleri hedef alan her türlü taciz, şiddet, sosyal manipülasyonu, dışlanma ve tehdit içerikli davranışlardır [5]. Bu davranışların tespitinde sosyo-teknik, bireysel ve toplumsal analiz yöntemleri uygulanabilir [5]. 2011'de Silva tarafından tanımlanan siber zorbalık, görsel ve metinsel iletişime dayalı sanal dışlama faaliyetleri olarak ifade edilebilir. Bu faaliyetler kimi zaman sanal şiddet boyutlarına varan sonuçlar doğurmaktadır. Bir başka çalışmaya göre de uygulanan sosyal, fiziksel, sözel ve psikolojik baskılar ile şiddet, toplumda şiddete eğilimli bir yaklaşımın yaygınlaşma tehlikesini açığa çıkarmaktadır [5].

Çocuk ve gençlerin kendilerini ispat etme,bir yere/gruba dahil olma gibi ihtiyaçları üzerinden beslenen siber-zorbalık yaklaşımında görmezden gelme, dışlama, hakaret etme, istemediği davranışlara zorlama gibi yöntemlerle bireyler üzerinde baskı oluşturulmaktadır. Bu baskı karşısında bireydeki şiddet eğilimi beslenmektedir. Ayrıca sanal dünya üzerinden kurulan yakın arkadaşlıklarla olumsuz fiziksel ve psikolojik sonuçlar doğuran tacizlerin yapılıyor olması da başka bir tehdit olarak varlığını sürdürmektedir [5].

Kişiler üzerinde maddi fiziksel ve psikolojik etkileri olan kimlik hırsızlığı sonucu karşı karşıya kalınan dolandırıcılık, kredi kartı hırsızlığı, sahte vergi işlemleri gibi uygulamalar da siber zorbalık yöntemlerine örnek gösterilebilir [5].

Sanal dünyadaki tehditlerle mücadele yöntemleri olarak; bireysel eğitime özellikle okullarda ağırlık verilmesi, teknik açıdan bireysel analiz yöntemleri geliştirilerek sosyal ağ üzerindeki davranışların takip ve analiz edilmesi, bunun yanı sıra web-metin madenciliği uygulamaları ile olası siber zorbalık içeriklerinin tespit ve takip edilmesi gibi önlemler önerilebilir [5].

B. *Akıllı Şebekeler*

Enerji, telekomünikasyon, ulaşım, kanalizasyon ve su sistemleri gibi kritik altyapı sistemleri bilgi sistem otomasyonu ile idameedilmektedir. Bu sistemlerin bir ülke için stratejik öneme sahip olduğu düşünüldüğünde doğal hedefler haline dönüşmeleri kabul edilebilir bir durumdur. Zira bir ülkeye zarar vermek, kaos yaratmak ya da ekonomisini alt üst etmek için sistemlere gerçekleştirilecek bir siber saldırı yeterli olacaktır.

En ciddi hedef, bütün sistemlerin besleyici ünitesi olan enerji sistemleridir. İşlem tabanlı bir mimarisi olan bu sistemlere saldırı düzenlemek için sadece bilgi teknolojilerine (BT) uzaktan erişim sağlamak yeterli olmayacak, sistemlerin farklı coğrafyalarda bulunması muhtemel ünitelerine erişebilmek için içerden alınacak bir desteğe de ihtiyaç duyulacaktır. Bu durum saldırıyı daha organize bir hale getirmektedir [6].

Akıllı şebekeler smart-grid adı verilen yapılar ile yönetilmektedirler. Bir akıllı şebeke tasarlanırken, iki yönlü iletişim, gelişmiş kontrol sistemleri, gelişmiş donanım bileşenleri, akıllı algılama teknolojileri ve BT uygulamaları gibi farklı teknolojilerin bir arada kullanılması verimliliği, güvenilirliği ve temiz enerji dağılımını arttırırken aynı zamanda güvenliğin sağlanması için kritik bir durum oluşturmaktadır[14].

Akıllı şebekelerin sertifika güvenlik protokolleri gerçekleştirilirken ISO / IEC 27000 serisi standartları baz alınmalıdır. Ayrıca tehdit modellemesini yapmak, saldırıları aza indirgemek için segmentasyon kullanmak, güvenlik duvarlarını aktifleştirmek, zorunlu olarak aygıt yazılımlarında imza kullanmak, hassas verileri korumak için şifreleme algoritmaları kullanmak, güvenlik açıklarını yönetmek için kontrol merkezini kullanmak, penetrasyon testlerini yapmak, güçlü kimlik doğrulama algoritmalarının kullanılmasını sağlamak ve log takiplerinin yapılmasına önem vermek güvenliğin sağlanması için alınabilecek önlemler arasındadır [14].



Şekil 2. Enerji Değer Zinciri [6].

Şekil 2'de görüldüğü gibi akıllı sistemlerle yönetilen bir altyapı olan enerjinin kullanıcılara ulaşması üretim, iletim, dağıtım ve yükleme olarak dört aşamalı bir sistemden oluşmaktadır [6]. Bu aşamalarının her birinin birbirini takip ettiği düşünüldüğünde sistemin bütününün güvenliğinin sağlanmasının her bir aşamanın bilişim sistemleri ve fiziksel erişim anlamında ayrı ayrı güvenliğinin sağlanması demek olduğu açıktır [6].

Enerji üretimi farklı coğrafi bölgelerde yapılıyor olabilir. Bu durumda bilişim sistemlerinin yanında tesislere fiziksel erişimin de kontrol altında tutulması gerekir. Üretim, iletim ve dağıtım aşamaları ağ üzerinden bilgi teknolojileri ile gerçekleştirip kontrol edildiğinden herhangi bir saldırıya maruz kalınmasının önüne geçmek adına erişim kontrollerinin yapılması, sisteme girişte kimlik bilgilerini kontrol edilmesi, donanımsal olarak zararlı içeriklerin varlığının kontrol edilmesi, yazılım güncellemelerinin yapılması, yazılımların kötü amaçlı erişimlere karşı kontrol edilmesi, güçlü bir anahtarlama ve şifreleme tekniğinin kullanılması, güvenlik protokollerinin kontrol edilmesi ve kullanıcıların güvenli şifreleme algoritmaları ile düzenlenmiş akıllı sayaçlar kullanmalarının teşvik edilmesi gereklidir. Sisteme erişimin son kullanıcılar üzerinden de gerçekleşebileceği göz önünde bulundurulmalıdır. Bu bakımdan konu değerlendirildiğinde son yıllarda popüler olan akıllı ev sistemlerinin ne kadar güvenli olduğu gelecek çalışmalar için bir inceleme konusu olarak önerilebilir [6].

C. Kapalı Devre Sistemler

Uzun yıllar kapalı devre sistemlerin internet ile bağlantısının olmaması nedeniyle daha güvenli olduğu ve virüs saldırılarına maruz kalmayacağı kanısı yaygındı. Stuxnet ile bunun aslında doğru bir kanı olmadığı gösterilmiştir. Bu sistemlerin dış ortamdaki ağ ile direk bir bağlantıları olmadığı için sistemin güvenliği erişim izni olan personel tarafından sağlanmakta ve yine güvenlik döngüsünün bu en zayıf halkası tarafından tehlikeye atılmaktadır. Bunun için "Siber Güvenlik Yönetimi Yaşam Döngüsü" modelinin kullanılması tavsiye edilmektedir [1].



Şekil 3. Siber Güvenlik Yaşam Döngüsü [1].

Şekil 3'de görüldüğü gibi siber güvenlik yaşam döngüsü birbirini takip eden aşamalardan oluşmaktadır. **Felsefe** aşamasında ilgili yapıya göre belirlenmiş bir siber güvenlik politikasının belgelendirilmesi gerçekleştirilir. **Tanımlama** aşaması bilgi varlıklarının ve potansiyel risklerinin belirlendiği aşamadır. **Rasyonelleştirme** aşamasında sistemin bütünlük içinde kullanılabilirliği için gerekli gereksinimler belirlenir. **Ayrıntılı tasarımda**, güvenlik duvarı, router, anahtarlar ve rasyonelleştirme aşamasında belirlenen gereksinimleri içeren bir mimari tasarım süreci gerçekleştirilir. **Uygulama** aşamasında aygıtlar ve bu aygıtların ayarları gerçekleştirilir. **İşlemde** ise güvenlik cihazlarının ve tüm ek fonksiyonların işlevlerini yerine getirip getirmediği kontrol edilir. **Bakım** aşamasında sistemin aksaklıkları giderilir ve idamesi sağlanır. **Değerlendirme** aşamasında sistemdeki açıklar değerlendirilir. **Değişim yönetiminde** ise siber güvenlik ayarlarının yönetimi ve ilgili değişikliklerin yapılması sağlanır [1].

Bazı kapalı devre sistemlerin ağ üzerinden dış ortamla bağlantısının olması ve/veya diğer kapalı sistemler ile iletişime geçmesi gerekebilir. Bu durumda hassasiyetle alınması gereken bazı önlemler aşağıda belirtilmiştir [1]:

- Kapalı devre sisteminin dış ağ ile bağlantısını sağlayan yapı mutlaka güvenlik duvarları, anti-virüs yazılımları ve paket filtreleme programları ile desteklemelidir.
- USB portları kapalı tutulmalıdır. Kullanılmasının zorunlu olduğu durumlarda öncelikle takılı aygıt mutlaka taramadan geçirilmelidir.
- Sistemler kabin ile korunabiliyorsa sistem odasına girilmeden gözle kontrollerin yapılabilmesi için şeffaf kapaklı modüller seçilmeli, sistemler mutlaka kilitli kapılar ardına alınmalı ve yetki kontrolü ile erişim sağlanmalıdır.
- Kapalı devre sisteminin güvenliğinin sağlanması için düzenli olarak virüs taraması yapılmalıdır.
- Tesis içi güvenlik açılarının değerlendirilebilmesi için güvenlik tarayıcı uygulamalar edinilmelidir (Örn.: Otomasyon Güvenlik 2000 (AS2000)).
- Düzenli olarak penetrasyon testileri uygulanmalıdır.

D. Acil Yardım Sistemleri

Hızla artan dünya nüfusu kaynakların yönetimini her alanda zorlaştırmaktadır. Afetler sonrası afet yönetimi, acil yardım kaynaklarının yönetimi ve hatta mevcut acil durum yardımı isteklerinin cevaplanması bile giderek zor bir hale gelmektedir. Kaynak darboğazının yaşanmaması ve en kısa sürede en iyi hizmetin ulaştırılması amacıyla acil durum (AD) yönetimine önem verilmeye başlanmıştır. Organizasyonun kolaylaştırılmasını hedefleyen acil durum yönetiminin (ADY) tasarlanmasında dikkat edilmesi gereken bazı ilkeler aşağıda özetlenmiştir [7].

- Oluşabilecek bütün acil durumlar dikkate alınarak bir planlamanın yapılması, AD (Acil Durum) görevleri ve ilgili oluşumların belirlenmesi gereklidir.
- Oluşabilecek acil ya da afet durumları için hazırlık tedbirleri belirlenmeli, müdahale edebilecek esnek gruplar tahsis edilmelidir.
- Önceliği personel ve kaynak yönetimi olan acil durum ve afet yönetim modelleri oluşturulmalıdır.
- AD gruplarınının oluşturulmasında kurum içi ve sivil vatandaşlardan oluşan karma bir topluluk seçilmelidir.

- Uygulama yapılabilecek gerçek planlar belirlenmelidir.
- Farklı gruplar arasında eşzamanlı iletişim ve hareket sağlanmalıdır.
- Planlar, değişen ve gelişen çevre koşullarına uyum sağlayabilmelidir.
- Ortak değerleri ve etik kuralları önde tutan teknolojik gelişmelere yatkın profesyonel gruplar oluşturulmasına dikkat edilmelidir.

Bilgi teknolojiler kullanılarak acil durumların planlanması, kaynakların etkin kullanımı, personel dağılımı ve koordinasyonu gibi yüksek miktardaki bilgi işlenmekte ve saklanabilmektedir. Sistemin bilgi teknolojileri ile yönetilebilir olmasının doğal sonucu olarak siber tehditler gündeme gelmiştir. Acil yardım sistemlerinin hedef alınması ile ülkeye kendi içinde ve uluslar arası platformda çok ciddi zararlar verilebilmektedir. Örneğin 2009 yılında İngiltere'nin savunma sanayisini ve acil yardım yönetimini hedef alan bir yazılım saldırısı gerçekleştirilmiş ve 2 hafta süreyle İngiliz Kraliyet Donanmasının personeli sistemler üzerine kişisel erişimlerini sağlayamamıştır. Yine aynı dönemde birçok hastanede ağ bağlantısı kesilerek hasta bilgilerine erişim engellenmiştir. Benzer bir saldırı Houston il mahkemesine yapılmış ve bu saldırı davaların sekteye uğramasına neden olmuştur [7].

E. Web Sayfaları

Yapılan çalışmalar siber saldırıların %75'inin web sayfalarını hedef alan saldırılar olduğunu göstermiştir. Bu saldırıların amaçları siteye ve servis sağlayıcıya zarar vermek, bilgilere erişmek olabileceği gibi web sayfasını bir köle sistem gibi kullanarak sayfayı ziyaret eden kullanıcıların bilgisayarlarına erişim sağlamak da olabilmektedir. Fakat bu saldırıların birçoğu maalesef çok kolay tespit edilememektedir. Saldırıların tespit edilememesinin başlıca nedenleri olarak kodlama yapılırken güvenli kodlama tekniklerinin kullanılmaması, servis sağlayıcı platformlarında bulunan güvenlik açıkları, web uygulamasının mantıksal akışındaki yanlış tasarım, sistemdeki güvenlik açıkları ya da işletme sorunları gösterilebilir. Saldırıların önlenmesi amacıyla geliştirme aşamasında kod incelenmesi, beyaz kutu testleri ile uygulamanın, sistemin ve güvenlik açıklarının taranması gibi tedbirlerin alınması gereklidir. Ayrıca güvenlik duvarlarının yerleştirilmesi ve/veya iyileştirilmesi de gerekli olan bir diğer önlemdir [8].

Web sayfalarına gerçekleştirilen saldırılar daha çok SQL enjeksiyonu, Cross-site scripting (XSS) ve Cross-Site İstek Sahteciliği (CSRF) saldırılarıdır [8].

XSS'den korunmak için veriler sayfaya yüklenme aşamasında değil veri tabanına gönderilirken ya da veri tabanından çekilirken bir filtrelemeden geçirilmelidirler. Gerekli görüldüğünde katmanlı güvenlik duvarı mimarisi de uygulanmalıdır [23,24].

Sql enjeksiyonu önlemek için girdilerin veri tabanına iletilmeden önce derlendiği parametreli "store procedure" tekniğinin kullanılması, veri tabanında salt okuma yetkisinin verilmesi, oluşan hatalarla ilgili mesajların veri tabanına dair bilgi içermeyecek şekilde düzenlemesi gibi önlemler tercih edilmelidir [9].

Saldırılardan korunmak için güncel saldırı ve güvenlik uyarıları takip edilmeli, yamaların güncellikleri kontrol edilmeli ve sunuculara mutlaka filtreleme mekanizması eklenmelidir [8].

III. SİBER SAVAŞ DENEMELERİ

Daha önceki yıllarda küçük çaplı denemeler yapılmış ise de önemli siber savaş denemeleri aşağıda kısaca açıklanmıştır.

1999:NATO'nun bilgi sistem kaynaklarına ilk saldırı gerçekleştirildi. Kosova krizi sırasında taraf olan ülkelerin NATO e-posta hesaplarına gerçekleştirilen DDOS saldırıları ile haftalarca erişim engellendi [16].

2001:ABD, Dünya Ticaret Merkezi başta olmak üzere birden çok noktaya yapılan saldırılarla binlerce insanını kaybetmiştir. Eylemin planları, koordinasyonu ve hatta eğitimleri siber dünya üzerinden yapılmış fakat ABD istihbarat örgütleri tarafından fark edilememiştir. ABD tarafından asla itiraf edilmemiş olmasına rağmen Pentagon'a kadar yaklaşan uçakların radar sistemlerinde de izlenemediği ve ABD'nin tamamen hazırlıksız yakalandığı bilinmektedir. Bu olay ABD için tam bir siber savunma zafiyeti olarak değerlendirilirken dünya üzerinde siber güvenlik ve siber savaş kavramları için dönüm noktası olmuştur [16].

2003:ABD'e karşı bilinen ilk saldırılardan biri Slammer adındaki virüs tarafından Ohio kentindeki nükleer santrale gerçekleştirilmiştir. Kapalı devre olarak çalışan sisteme kontrolsüz bir bilgisayar tarafından sızdırılan virüs yaklaşık 5 saat boyunca güvenlik izleme sistemini devre dışı bırakarak sistemi duraksatmış ve büyük bir hasara neden olmuştur. Bu saldırı işlem tabanlı sistemlerdeki güvenlik açıkları için bir erken uyarı görevini görmüştür [6].

2006: Malezya hafif raylı sistemlerini hedef alan saldırıda raylı sistem bilgi sistemi hasar görmüş ve uzun süreli servis kesintisi yaşanmıştır. Yolcuların saatlerce mahsur kaldığısaldırı sonucu yapılan açıklamada durumun teknik bir arıza olduğu ifade edilmiştir [13].

2007: Estonya ile Rusya arasında yaşanan gerginlikte Rus korsanlarının Estonya devlet kurumlarına düzenlediği DDOS saldırıları Estonya tarafından üyesi olduğu NATO'ya taşınmış ve dünya bir savaşın eşiğine getirilmiştir [15]. NATO bu olayın ardından Ocak 2008'de Siber Savunma Politikasını hazırlayarak yayınlamıştır [16].

2008:ABD'de bilgisayar korsanları tarafından elektrik nakil sistemine yapılan saldırıda birçok şehir uzun süre elektrik kesintisi yaşamıştır. Bu olay gizli tutulmuş ayrıntılara yer verilmemiştir [6].

Malezya'da borsa sistemi arızalanmış ve bütün gün işlem yapılamamıştır. Büyük maddi zarara neden olan bu durum Malezya'nın Dünya çapındaki kredibilitesini de düşürmüştür [13].

Rusya ile Gürcistan arasındaki Güney Osetya bölgesi için yaşanan savaşların bir uzantısı olarak Rus korsanlarca yapılan DDOS saldırıları sonucunda Gürcistan devlet kurumlarının bilgi varlıklarına ciddi zararlar verilmiştir [15].

2009:ABD'de Kaliforniya kentinde bir firmaya yapılan saldırıda yağ sızıntısı ihbarı verilmiş ihbar sahte olmasına rağmen müdahale sistemlerini tetiklemesi nedeniyle binlerce dolarlık hasara neden olmuştur [6].

Temmuz 2009'da Kore ana hükümet oluşumları ile sivil web sitelerini ve aynı anda ABD'de beyaz sarayın web

sayfasını hedefleyen DOS saldırıları ile büyük bir hasar verilmiş ve ülkelerin saygınlıklarının kaybına nedenolunmuştur [10].

Kasım 2009'da Çinli korsanlar tarafından sosyal mühendislik atakları, uzaktan izleme ve erişim uygulamaları ile MS Windows a ait açıklardan faydalanılarak enerji sistemlerini hedef alan bir saldırı gerçekleştirilmiştir. Bu saldırı kendini McAfee programından saklamış ve hasara neden olmuştur [6].

2010: Bilinen en büyük ve en uzun soluklu saldırı İran'ın nükleer tesislerini hedef alan Stuxnet adlı virüs saldırısıdır. Bu virüs diğerlerinden farklı olarak belirli bir endüstriyel donanım için belirli bir faaliyeti durdurmak ve üzerinde değişiklik yapmayı hedefleyerek üretilmiştir. Faaliyete geçmeden önce yaklaşık bir yıl kendini gizli tuttuğu sanılmaktadır. Virüsün ağ üzerinden kendini çoğaltığı ve birden çok bilgisayara entegre olduğu saplanmıştır. İran tarafından net bir açıklama yapılmaması nedeniyle hasarın boyutları tam olarak bilinememeklebirlikte nükleer programa büyük zarar verdiği tahmin edilmektedir. Yapısı incelendiğinde Symantec tarafından büyük bir altyapı desteği ile geliştirilmiş olması gerektiği sonucuna varılmış ve bu durum virüsün bir ülke tarafından finanse edildiği kanısının oluşmasına neden olmuştur [6].

28 Kasımda yayınladığı belgelerle dünya kamuoyunu alt üst eden Wikileaks aslında ABD'nin bir siber savaş denemesi olarak değerlendirilmektedir. ABD Dış İşleri Bakanlığı'nın gizli dosyalarına sözde yasadışı yollarla ulaşan Wikileaks elemanlarının yayınladığı belgeler dünyadaki dengeleri altüstetmiştir. Bu belgelerin tetiklediği çok sayıda isyan ile Kuzey Afrika'daki birçok ülkenin yönetimi değişmiştir. Birçok lider imaj, para ve hatta yönetimi kaybetmiştir. Hâlihazırda belgelerin etkileri devam etmekte ve dış kaynaklı silahlı bir müdahaleye gerek kalmadan dünyanın bir çok yerinde köklü rejim değişiklikleri yaşanmaktadır [13].

2011: Malezya'da hükümetin bazı web sitelerine saldırılar düzenlenmiştir. Küçük çaplı bu saldırılar sistemin açıklarının tahmin edilmesi ve gelecek saldırıların zemini olarak yorumlanmıştır [13].

IV. DÜNYA'DAN SİBER GÜVENLİK FAALİYETİ ÖRNEKLERİ

Bu başlık altında bazı ülkelerdeki siber güvenlik faaliyetleri incelenmiştir.

Amerika Birleşik Devletleri:

ABD, siber savunma konusunda en ileri bilgi ile teknoloji olanaklarına sahip olan ve bu konuda örnek alınan ülkelerin başında gelmektedir. Özellikle 2001 yılındaki olaylardan sonra siber güvenlik konusu devlet politikası olarak görülmekte, tam bir kurumsal koordinasyon ile çalışmalar yürütülmektedir [20]. Şubat 2003'de Ulusal Siber Güvenlik Politikasını yayınlayan ABD, siber güvenlik konusunda devlet, özel sektör ve vatandaşların birlikte hareket etmesinin önemini vurgulamıştır [21]. Beyaz saray bünyesinde bulunan ve ulusal siber güvenlik faaliyetlerini yürüten Siber Güvenlik Ofisi direk olarak ABD Başkanı'na bağlıdır. Bu ofis koordinasyonunda çalışan gruplardan biri olan Ulusal Siber Tepki Koordinasyon Grubu siber saldırılar karşısında federal birimler arasındaki koordinasyonu sağlamakla görevlidir. Ulusal Güvenlik ajansı ve bağlı kuruluşları izleme ve istihbarat faaliyetlerini yürütmektedir. Karşı atak ve ordu ağı savunma hizmetleri Savunma Departmanı tarafından, soruşturma süreci ise Adalet Departmanı tarafından yürütülmektedir. Bu birimlerin yanı sıra ülkenin siber güvenliğini sağlanmasında ağların trafini izlemek için kullanılan EINSTEIN programı, federal kurumların dış dünyaya açılan ağ sayısını azaltan Güvenli İnternet Bağlantıları programı ve karşı saldırı ile ilgili bilgileri içerdiği düşünülen Gizli programlardan da destek alınmaktadır [20].

Hindistan:

Siber güvenlik kavramına en çok önem veren ülkelerden birisidir. 1990'lı yıllardan beri sürdürülen çalışmalar kapsamında devlete ait alt yapıların ve kiritik sistemlerin korunmasına yönelik olarak politikalar ve kanunlar oluşturulmaktadır. Ülke genelinde Bilgi Güvenliği Farkındalığı ve Eğitimi kampanyası yürütülerek bilinç düzeyinin arttırılmasına çalışılmaktadır. Hindistan Ulusal Güvenlik Konseyi bünyesindeki oluşumlar ile 7/24 esasına dayalı olarak siber saldırı ataklarının analiz edilmesi ve erken saldırı tespitine yönelik çalışmalar yapıldığı bilinmektedir. Ülkede bilişim ve telekominikasyon alanında faaliyet gösteren ve/veya bilişim sistemlerini yoğun olarak kullanan kurum/kuruluşların ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standartları Uygunluk Sertifikasına sahip olma zorunluğu bulunmakta olup halen 250 den fazla firma bu sertifikaya sahiptir. Bunların yanı sıra ülkede acil durumlara müdahale edebilecek ya da ihtiyaç halinde ulaşılabilecek kendi alanlarında uzman personelin bilgilerini tutulduğu Ulusal Veri Tabanı ve Acil Durum Müdahale Ekipleri bulunmaktadır [20].

Çin Halk Cumhuriyeti:

Çin'de siber güvenlik faaliyetleri Çin Ordusu tarafından yürütülmektedir. Bu alanda yoğun faaliyetler yürüttüğü bilinen ordunun elinde kapsamlı bir güç olduğu tahmin edilmektedir. Ayrıca ARGE faaliyetleri kapsamında süper bilgisayarların üretildiği ve bu bilgisayarlar sayesinde birçok ülkenin şifreleme yapısının çözülebildiği iddaa edilmektedir. Ordu bünyesinde siber savunma ve saldırı konularına çalışan uzmanlardan oluşan iki ayrı grup ve sadece siber güvenlik üzerine faaliyet gösteren bir ARGE yapısı bulunmaktadır. Bazı ülkeler tarafından siber suçları desteklediği düşünülse de siber suçlarla mücadele konusunda ciddi çalışmalar yürütülmektedir. Ayrıca "Altın Kalkan" adı verilen güvenlik duvarı yapısına sahip olan ülkenin siber saldırılara karşı elinin güçlü olduğu bilinmektedir [20].

Almanya:

Almanya Federal Hükümeti tarafından etkin önlemler alınmaya başlanmıştır. Çin'de olduğu gibi Almaya'da da siber savunma faaliyetleri Ulusal Siber Güvenlik Konseyinin koordinasyonunda Alman Ordusunun sorumluluğunda yürütülmektedir [20].

İsrail:

Siber tehditler konusunda İsrail en hazırlıklı ülkeler-dendir. Siber savunma ve saldırılar konusunda ciddi yatırımlar yaptığı bilinen ülkede siber güvenlik, hükümet ve vatandaşların ortak bir faaliyeti olarak kabul edilmekte ve çalışmaların büyük kısmı ordu tarafından yürütülmektedir. İsrail ordusu emekli mensupları, BT uzmanları ve emekli MOSSAD ajanlarından oluşan "Birim 8200" isimli birim ülkenin siber gücünü oluşturmaktadır. Bu birim aynı zamanda konuda uzman personelin yetiştirilmesi için akademik bir rol de üstlenmiştir. Sahip olduğu teknoloji merkezinde ileri düzey ekipmanlar ile dünya üzerinde ağ trağini izleme ve istihbarat faaliyetlerini yürütme olanağına

sahip olduğu bilinmektedir. İnter ağını büyük çoğunlukla izleme gücüne sahip olan ülke, buna rağmen kritik işlemlerin yürütüldüğü ve bilgilerin işlendiği sistemlerini internetten bağımsız olarak kendi ağı içinde devam ettirerek bilgi güvenliğini sağlamaktadır [20].

İngiltere:

İngiltere hükümeti 2010 yılında yayınladığı Siber Güvenlik Raporu ve 2011 yılında yürürlüğe koyduğu Ulusal Siber Güvenlik Stratejisi ile bu konuda önemli adımlar atmıştır. Siber tehditlerin ülkenin güvenliğini riske atan birinci öncelikli tehditler kapsamına yerleştirmiş ayrıca bütçesinin çok büyük bir kısmını da siber savunmaya ayırmıştır. Ulusal Siber Güvenlik Programı, Hükümet Kabine Ofisi bünyesinde yürütülmektedir.Savunma Bakanlığı tarafından siber savunma faaliyetleri yürütülmektedir. Bakanlık bünyesinde oluşturulan birimler arasında bu alanda operasyonel taktik ve teknik geliştirmekle sorumlu birimler de yer almaktadır. 2013 'ün başlarında kurulum çalışmaları başlayan ve yapısal oluşumu devam eden National Crime Agency isimli teşkilat ile siber suçlarla mücadelede daha etkin bir hale gelmeyi hedeflemektedir. Ayrıca eğitim giderleri ve etik bilgisayar korsanlarının yetiştirilmesi için de ciddi bir bütçe ayrılmıştır [20].

Singapur:

E-devlet projelerini büyük oranda hayata geçirmiş olan Singapur dünyanın en etkin ve gelişmiş internet ağlarından birine sahiptir. Ülkede erken uyarı sistemlerinin geliştirilmesi, ulusal düzeyde bilincin arttılması, önlemlerin alınmasının sağlanması ve kurumlar ile özel sektör arasındaki bilgi paylaşımının/koordinasyonun arttırılması çalışmaları öncelikli olarak yürütülmektedir [20].

NATO:

NATO bünyesinde üye ülkelere yönelik siber saldırılara karşı önlemler alınması ve müttefik ülkelerin birlikte hareket etmelerinini sağlamak amaçlı çalışmalar yürütmektedir. Bu kapsamda Uluslarası Siber Savunma Politikası hazırlanmıştır. Politikanın temelinde üye ülkeler arasındaki temel ve kritik iletişimin sürdürülmesinin korunması yer almaktadır. Üye ülkelerle arasında tam bir haberleşme ve koordinasyon imkanını sağlayan kendi iletişim ağı bulunmakta olup bu yapı üzerinden gerektiğinde müdahale edebilme yeteneğine sahiptir. Bunun yanı sıra erken uyarı sistemleri, bilgi paylaşımı ve farkındalık oluşturma ağları ile de üye ülkelere destek vermektedir. Bünyesinde bulunan hızlı müdahale ekipleri, talep eden ülkeye yönelik siber saldırılara yerinde müdahale edebilmektedir. NATO, siber savunma ve müdahale konusunda gelişmiş bir teknolojiye ve sağlam bir altyapıya sahiptir [20].

Avrupa Birliği:

Üye ülkelerin maruz kaldığı ve kalabileceği siber tehditler karşısında önlem almayı hedefleyen AB, 2005'de Avrupa Ağ ve Bilgi Güvenliği Ajansını (ENISA), 2007'de siber terörizmi gözlemlemek amacıyla Avrupa Polis Ofisini(Europol) oluşturmuştur. Bu birimler hem üye ülkelere siber tehditlere karşı destek vermekte hem de ülkeler arasında koordinasyonu sağlamakla ilgili çalışmalar yürütmektedirler. Özellikle siber suçlar, internet korsanlığı, siber terörizm ve çocuk pornografisi konularında yoğun çalışmalar yürütmektedirler. AB tarafından acil durum takımlarının oluşturulması ile yasal yaptırımların belirlenmesi konusunda halen çalışmalar devam etmektedir [20].

Uluslar Arası Telekomünikasyon Birliği (ITU):

İnternet üzerinden yapılan siber saldırıların giderek yaygınlaşması bu konuda ortak bir mücadele biriminin kurulmasını zorunlu hale getirmiştir. 2003-2005 yıllarında faaliyetine başlayan ITU siber tehditlerle mücadele için ortak bir plartform oluşturmayı ve standartları belirlemeyi hedeflemektedir. Özellikle gelişmekte olan ülkeleri hedef kitlesi olarak gören kuruluş Radyo-iletişim, Standartlar ve Telekonimükasyon Geliştirme sektörlerinde faaliyet göstermektedir. 2007'de yayınladığı Global Cybersecurity Agenda(GCA) ile hukuki tedbirler, teknik/prosedürel tedbirler, siber güvenlik araçları, ulusal siber güvenlik politikalarının temelleri üzerine ortak standartlar belirlemiştir. ITU halen üye ülkelere bu konularda destek olmakta ve talep gelmesi halinde siber güvenlik tedbirleri kapsamında denetlemeler yaparak sertifikasyon uygulamaları gerçekleştirmektedir [20].

V. TÜRKİYE'DE SİBER GÜVENLİK

Siber saldırılarla mücadelede en önemli unsurlardan biri stratejik hedefler olan kritik altyapıların korunmasıdır. AB konseyi tarafından kritik altyapılar *"... insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güven-liklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları"*şeklinde ifade edilmiş ve aşağıda belirtilen unsurlar kritik altyapı olarak nitelendirilmiştir [12].

- Enerji (örn. Elektrik, gaz, rafineriler, aktarım ve dağıtım sistemleri)
- Bilgi ve İletişim (örn. Telekomünikasyon, yayıncılık, yazılım, donanım, Internet)
- Finans (örn. Bankacılık, yatırım)
- Sağlık (örn. Hastaneler, laboratuarlar)
- Gıda (örn. Güvenlik, üretim, gıda endüstrisi)
- Su (örn. Barajlar, depolama, dağıtım)
- Ulaşım (örn. Havaalanları, demir yolları, trafik kontrol sistemleri)
- Nükleer, Biyolojik, Kimyasal ve Radyoaktif madde endüstrileri
- Uzay araştırmaları
- Kamu düzeni ve güvenliği
- Sivil yönetimler

Türkiye'de siber suçlarla mücadele 2012 yılına kadarTC.Bilim, Sanayi ve Teknoloji Bakanlığı'nın koordina-törlüğünde Bilgi Teknolojileri Kurumu (BTK) tarafından sivil toplum kuruluşları ve kurumları ile birlikte yürütülmüştür. Siber saldırıların önlenmesi ve gerekli tedbirlerin alınması için ülke unsurlarının birlikte hareket etmesinin zorunluluğu prensibine dayanılarak 2002–2010 yıllarını kapsayan süreçte kritik altyapı sistemleri ve durumlarının tespiti, kurumların farkındalığının arttırılması ve siber güvenlik için bir stratejinin oluşturulmasına yönelik çalışmalar yapılmıştır [11].

Bu kapsamda 2005-2010 yılları arasında BTK tarafından gerçekleştirilen başlıca çalışmalardan bazıları aşağıda belirtilmeye çalışılmıştır [11,21]:

- Kimlik doğrulama, inkâr edilememe, gizlilik ve bütünlük ilkelerinin kullanılmasını sağlayan e-imza uygulamasına geçilmesi ve ilgili yasal mevzuatın (TCK 5070) hayata geçirilmesi.
- Haberleşme sektöründe faaliyet gösteren firmaların

varlıklarının belirlenmesi, ilgili tehdit ve zafiyetlerin belirlenmesi, fiziksel güvenliğin unsurları, donanım-yazılım ve personel güvenliği gibi unsurlar için alınması zorunlu tedbirleri içeren Elektronik Haberleşme Güvenliği Yönetmeliğinin (TCK 5809) yayınlanması.

- İnternet üzerinden işlenen şuçlarla mücadele edilmesi amacıyla İnternet ve Yapılan Yayınlar Yoluyla İşlenen Suçlarla Mücadele Yönetmeliğinin yürürlüğe girmesi (TCK 5651)
- Kişisel veri, kişisel verinin kapsamı, gizliliğinin korunması ile ilgili usul ve şartları içeren Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin yayınlanması.
- Farkındalığın arttırılması kapsamında çeşitli raporların hazırlanması ve kamuoyu ile paylaşılması
- Siber güvenlik ve bilgi güvenliği konulu konferans ve çalıştayların gerçekleştirilmesine öncülük etmek ve katkıda bulunmak
- Yığın e-postalarının önüne geçilmesi için hazırlanan projeye koordinatörlük etmek

BTK'nun yanı sıra bilgi güvenliği konusunda etkin çalışma gösteren kurumlardan birisi de Devlet Planlama Teşkilatı(DPT)'dır. DPT, "e-Türkiye girişimi Eylem Planı 2002," ,"e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003-200)", "e-Dönüşüm Türkiye Porjesi 2005 Eylem Planı", "Bilgi Toplumu Stretejisi (2006-2010)" ve "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)" belgeleri ile konu hakkında aktif çalışma göstermiştir. Bu belgeleri temel alan, bilgi güvenliği kapsamında önem arzeden düzenlemeleri içeren ve çalışmaların işlem makamlarını belirleyen "Bilgi Toplumu Stratejisi ve Ek'i Eylem Planı" 2006 da resmi gazeteyayınlanmıştır. Bu plandaki en önemli noktalardan biri Kişisel Verilerin Korunması Taslağınınhazırlanarak yasalaştırılmasından bahsediliyor olmasıdır [21].

Diğer kurumlarmızdan bir çoğunda siber güvenlik ve bilgi güvenliğine yönelik bilinen çalışmaların nispeten daha az olması ve yıllık strateji planlarında siber güvenliği içeren maddelerin 2010 yılından sonra yer almaya başlamış olması durumun öneminin kavranması konusunda endişe verici olsa da yapılan çalışmaların umut verici olduğunu da belirtmek gerekmektedir. Özellikle Milli Eğitim Bakanlığı tarafından öğrencilerin ve velilerin bilinçlendirilmesine yönelik uygulamalar yürütülüyor olması toplumsal bilincin arttırılması açısında önem arzetmektedir.

Siber güvenliğin ülke güvenliğinin bir unsuru olduğu gözönüne alındığında özellikle güvenlik güçlerinin de konu üzerine yapılan çalışmalarda aktif olarak yer alması önem arzetmektedir. Bir çok ülkede uzun yıllardır siber güvenlik çalışmaları orduların bünyesinde öncelikli olarak yürütülmektedir. Bu bakımdan Genel Kurmay Başkanlığı Muhabere ve Siber Savunma Komutanlığı' nın kurulmuş olması ve tatbikatlara katılması önemli bir gelişmedir. Ayrıca Emniyet Genel Müdürlüğü'nün siber suçlar konusundaki çalışmaları son yıllarda yoğunlaşmış ve başarılı sonuçlar vermektedir.

Konunun AR-GE ayağında ise etkin çalışmalar TUBİTAK başlamış ve ULAK-CSIRT adındaki oluşum ile araştırma ve eğitim çalışmalarını sürdürmektedir. Bunun yanı sıra hükümet tarafından hayata geçirilen Bilgisayar Olaylarına Acil Mudahale Ekipleri (TR-BOME) 2007 yılından beri etkin olarak NATO ile işbirliği içinde bulunmakta ve NATO tarafından yürütülen Uluslar arası Siber Savunma Çalıştaylarına aktif katılım göstermektedir. Bu kapsamda 2007'de NATO NCIRC (NATO Computer Incident Response Capability) ile TR-BOME arasında personel değişimi, tatbikatlara katılım, NCIRC gizli ağına erişim, teknik veritabanı paylaşımı ve alarm-uyarı sistemlerine erişim konularını kapsayan bir anlaşma imzalanmıştır. Bu anlaşma içeriğine uygun olarak 2008 ve 2009 yılında düzenlenen tatbikatlarda temsil ve katılım gerçekleştirilmiştir [21].

2012 yılında alınan Bakanlar Kurulu'nun 11/06/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin kararı ile ülkemizde siber güvenliğin sağlanması, ilgili politikaların geliştirilmesi ve ulusal siber güvenlik stratejisinin belirlenmesi görevi TC.Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na devredilmiş ve o tarihten itibaren de ilgili bakanlıkça yürütülmektedir [19].

VI. TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİSİ

Yapılan çalışmalar sonucunda siber güvenlik konusu ciddi bir tehdit olarak algılanmaya başlanmıştır. Kimlik hırsızlığı, dolandırıcılık gibi siber suçlar yönünden mağdur olan vatandaşlarımızın ne mağduriyetleri ne de suçlulukların yakalanıp yakalanmadığı malesef konunun magazin değerinin olmaması nedeniyle medyada yeterince yer almamaktadır. Bunun yanı sıra kurumlarımız kendilerine yapılan saldırıları ve kaybettikleri verilerin miktarını gerek itibar kaybı endişesi gerekse özel nedenlerle gizlemek konusunda çok kararlıdır. Yani siber saldırılar konusunda kim ne yaşıyor maalesef tam olarak bilinememektedir [17]. Ulusal siber güvenliğin sağlanması bu belirsizliğin ortadan kaldırılması, toplumun birey ve kurum bazında bilinçlendirilmesi ile mümkün olacaktır.

TC.Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın sorumluluğunda gerçekleştirilen çalışmalar sonucunda kurum ve kuruluşlarca sağlanan her türlü bilgi teknolojileri temelli hizmetlerinin korunması, kritik altyapıların korunması ve olası siber saldırılar sonrasında sistemlerin en kısa sürede eski performanslarına dönmeleri ile saldırıların soruşturulmasında daha etkin imkanlar sağlamak için altyapı oluşturmak amacıyla "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" hazırlanarak yürürlüğe girmiştir. Eylem Planında siber risklerin neler olduğu, kurumlar arası işbirliği ile öngörülen dönemde yapılması ve daha sonraki yıllarda devamının sağlanması hedeflenen adımlar belirlenmiş ve uygulamaya koyulmuştur [19].

Ulusal Siber Güvenlik Stratejisi'ne göre güvenlik anlamında orta ve uzun vadede öncelikle dikkate alınması gereken bazı konular ve atılması gereken adımlar vardır. Bu konular aşağıda genel başlıkları ile belirtilmiştir [18].

1) Uluslar Arası İşbirliği: İnternetin sayesinde dünyanın her yerinden herhangi bir kuruma ya da ülkeye kolaylıkla saldırı gerçekleştirilebiliyor olması ülkeler arasındaki işbirliğini zorunlu bir hale getirmiştir. Ülkemizin müttefik ülkelerle dil birliğini azami seviyede tutmak, BM, AB, OECD ve NATO gibi örgütler bünyesindeki çalışmalara destek vermek ve katılmak, bölgesel ve küresel anlaşmalara taraf olmak, yapılan konferans, çalıştay, seminer gibiuluslar arası aktivitelere katılmak gerekliliği önem arz

etmektedir [18].

2) Siber Güvenlik Kültürünün Oluşturulması: Özellikle kritik altyapı sistemlerinden başlayarak kamu kurum ve kuruluşlarının yönetici, personelleri ve teknik hizmet personelleri siber güvenlik, tehdit/saldırılar konusunda eğitilmeli ve bilinçlendirilmelidir [18].

3) Yasal Düzenlemeler: Uluslar arası hukuk kuralları, kamu yararı, kritik altyapı sistemlerinin korunması ve kişisel veri güvenliğinin sağlanması amacıyla siber suçlarla mücadele kapsamında caydırıcı yasal yükümlülükler getirilmeli ve uygulanmalıdır. Yasal düzenlemeler yapılırken kişisel verilerin korunması, herkesin bilgi edinme hakkının korunması, haberleşmenin gizliliği esasının korunması ve bilgi güvenliği unsurları kapsamında gerekli tedbirlerin alınmasının önemi gibi kritik konular da göz önünde bulundurulmalıdır [18].

4) Kurumsal Yapılanma: Mücadelenin ve savunmanın koordineli bir şekilde yapılması için bir takım kurumsal yapılanmaların oluşturulmasına önem verilmedir. Ulusal siber güvenlik merkezi, müdahale merkezi strateji belirleme kurumu gibi yapılar oluşturularak hükümet, devlet kurumları ve sivil oluşumlar arasında iş birliği ve koordinasyon sağlanmalıdır [18].

5) Eğitim: Siber güvenlikte en önemli ve en zayıf halka olan bireylerin siber güvenlik konusunda eğitilmesi gereklidir. Teknik personelin yetiştirilmesi için gerekli lisans ve lisansüstü eğitim programları açılmalı ve personel bu konuda teşfik edilmelidir [18].

6) Kamu, Üniversite ve Özel Sektör İşbirliği: Ar-Ge çalışmalarının yapılması, sektörler arası iş birliğinin arttırılması ve akademik programların yaygınlaştırılmasının yanı sıra kamu-özel sektör, kamu-üniversite ile üniversite-özel sektör arasındaki iş birliğinin teşvik edilmesi ve çalışma ortamlarının sağlanması gereklidir [18].

7) Milli Teknoloji Geliştirme: Bilgi teknolojilerinde özellikle siber güvenlik alanında kullanılacak yazılım ve donanımların uluslar arası standartlara uygun olarak milli sermaye ve iş gücüyle üretilmesini teşvik etmek ve milli ürünlerin kullanımı tercih etmek önem arz etmektedir [18].

8) Belgelendirme: Bilgi teknolojileri üreten/kullanan kurum ve kuruluşların uluslar arası güvenlik sertifikaları ile belgelendirilmiş olmasına özen gösterilmelidir. Kamu kurumlarının belgelendirme konusundaki eksiklikleri giderilmelidir [18].

Ülkemizin ilk resmi siber güvenlik eylem planında gerçekleştirilmesi hedeflenen adımlar aşağıda özetlenmiştir [19]:

- Kurum ve kuruluşların yetki ve sorumluluklarının belirlenmesi ile hukuki anlamdaki düzenlemelerin yapılması
- Ulusal ve uluslar arası mevcut mevzuatın incelenmesi ve gerekli iyileştirmelerin yapılması
- Ortak terminoloji oluşturulma çalışmalarının yapılması
- Saldırıların tespiti ve gerekli delillerin temini için sistemin desteklenmesi
- Delillendirmede görevli kurum/kuruluşların en son teknoloji ürünlerinin temini ve devamlılığının sağlanması konusunda desteklenmesi
- Ulusal Siber Olaylarla Mücadele Merkezi'nin (USOM) ve Siber Olaylara Müdahale Ekipleri'nin (SOME) kurulması
- USOM ile koordineli çalışacak olan kurum SOME'lerinin kurulması
- Öncelikle kritik kurum/kuruluşlar olmak üzere bütün organların risk analizlerinin yapılması
- Acil eylem planlarının sektörel olarak oluşturulması ve hayata geçirilmesinin sağlanması
- Bilişim sistemlerinin, özellikle kritik altyapı sistemlerinin güçlendirilmesine öncelik verilmesi
- Kamu kurum/kuruluşlarına yönelik zorunlu denetim uygulamalarının geliştirilmesi
- Yetkili ve etkin teknik personel yetiştirilmesi için gerekli düzenlemelerin yapılması
- Teknik personele yönelik sertifikasyon ve akademik eğitim çalışmalarının uygulanması
- Yerli teknolojilerin geliştirilmesinin desteklenmesi
- Siber güvenlik tatbikat ve çalıştaylarına önem verilmesi
- Siber güvenlik tatbikatlarına ulusal ve uluslar arası düzeyde yüksek oranda katılımın sağlanması
- Tehditlerin belirlenmesine yönelik tehdit analiz ve trafik izleme başta olmak gerekli tespit mekanizmalarının kurulması
- Bilgi sistem hizmet sağlayıcılarının belgelendirilmesi
- İnternet sitesi servis sağlayıcıları ile veri kaynağı saklayıcılarında yerli sermayenin desteklenmesi ve kamu kurumlarının bu servislerden faydalanmasının sağlanması
- Açık kaynak kodlu ürünlerin kullanımının teşvik edilmesi
- Ar-Ge çalışmalarının desteklenmesi
- Siber güvenlikten sorumlu kurumların etki alanının ulusal ve uluslar arası platformda genişletilmesi

Eylem planında kurumların sorumluluklarının belirtilmesi önemli olmakla beraber kurumlar arasında tam bir işbirliğinin temel alınıyor olması planın gerçekleştirilebilirliğini arttırmaktadır. Sistemin tam güvenliğinin sağlanması sistem içindeki mekanizmaların ve alt sistemlerin her birinin güvenliğinin sağlanmasına bağlıdır. Bunun yanı sıra işbirliği, genel bilgi birikiminin ve kalitenin de artmasını sağlayacaktır.

VII. SONUÇ VE ÖNERİLER

Siber dünyanın etkinliğinin artması ve bilgiye erişimin birden çok yolla gerçekleşebiliyor olması aslında karşılaşılması muhtemel senaryoların hiç de uzakta olmadığının bir göstergesidir. Bireylerin bilgileri yasadışı yollarla ele geçirilebilir, bu bilgilerle dolandırıcılık, sahtecilik gibi bireylere zarar verecek işlemler yapılabilir, kurumların bilgi varlıklarına, kritik altyapıları etkileyecek saldırılarla ülkenin enerji kaynaklarına, hatta ve hatta ülkenin güvenlik unsurlarına zarar verilebilir. Anlaşılacağı üzere siber güvenlik kavramı bireyler, kurumlar ve ülkeler için dikkate alınması gereken bir kavramdır. Toplumun bütün grupları arasında koordinasyon ile tam iş birliğinin yapılması zorunludur.

Yapılan incelemede görülmüştür ki ülkemizde yapılan çalışmalarla var olan tehlikenin farkında olunduğu fakat alınabilecek önlemler konusunda daha çok çaba sarfedilmesinin ve özellikle kurumların bilinç düzeyinin arttırılmasının gerekliliği ön plana çıkmıştır. Bu bağlamda Ulusal Siber .Güvenlik Stratejisinin yayınlaması ve 2013-2014 Eylem Planın uygulama koyulması önemli ve umut vadeden bir adımdır. Stratejinin etkinliğini arttırmak için okullardan başlamak üzere medyanında desteğini alarak bütün toplumu hedef alan bir bilinçlendirme programının başlatılması, siber güvenlik tatbikatlarına ağırlık verilerek özellikle kritik altyapı sistemlerinin ve ulusal güvenlik unsurlarının zaafiyetlerinin belirlenmesine ve giderilmesine öncelik verilmesi, kamu kurum ve kuruluşlarında farkındalığı arttırmak ve tehlikeye dikkat çekmek için habersiz saldırılarla sistemlerin kontrol edilmesi gibi uygulamalar önerilebilir. Kritik öneme haiz olan verilerin bulunduğu ve işlemlerin yapıldığı sistemlerin internet ortamından bağımsız olarak oluşturulacak yerel bir ağ ile yürütülmesi de önerilebilecek başka bir yöntemdir. Bunların yanı sıra oluşturulacak siber güvenlik merkezlerinin kamu kurum ve kuruluşlarındaki teknik personel, özel sektör, üniversite ve sivil toplum kuruluşları temsilcileri ile güvenlik güçleri ve beyaz şapkalı bilgisayar korsanlarının da aralarında bulunduğu geniş bir kitle ile teşkil edilmesinin siber güvenlik kavramına daha geniş bir pencereden bakılmasına olanak sağlayacağı, oluşturulacak siber güvenlik merkezlerinin yanı sıra siber saldırılar karşısında acil müdahale ekiplerinin bulundurulmasının güvenlik konusundaki etkinliği artıracağı değerlendirilmektedir.

KAYNAKLAR

[1] KITAI T. TAKAI T. ,UCHIDA H. "Multiple and Independent Protection Layer Concept for Plant Cyber Security", SICE Annual Conference (SICE), 2012 Proceedings of, Agustos 2012, (963 – 966)EMRE Bâkır, "Siber Savaşlar – Başlangıç", http://www.siberguvenlik.org.tr/ makaleler/siber-savaslar-i/, Aralık 2012

[2] HEWETT Rattikorn," Toward Identification of Key Breakers in Social Cyber-Physical Networks", Systems, Man, and Cybernetics (SMC), Ocak 2011,(2731 - 2736)

[3] CASHİON Jeffrey, BASSİOUNİ Mostafa,"Protocol for Mitigating the Risk of Hijacking Social Networking Sites", Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Ocak 2011, (324 – 331)

[4] SABBAGH Bilal Al, KOWALSKİ Stewart," ST(CS)2 - Featuring socio-technical cyber security warning systems ", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, Haziran 2012,(312 – 316)

[5] OCHOA A. ,PONCE J. ,JARAMILLO R. ,ORNELAS F. ,HERNANDEZ A. ,AZPEITIA D. ,ELIAS A. , HERNANDEZ A.,"Analysis of Cyber-Bullying in a Virtual Social Networking", Hybrid Intelligent Systems (HIS), 2011 11th International Conference on, Aralık 2011, (229 – 234)

[6] LİNE Maria B., TØNDEL Inger Anne, JAATUN Martin G., "Cyber Security Challenges in Smart Grids", Innovative Smart Grid Technologies (ISGT Europe),Aralık 2011,(1 – 8)

[7] WALKER Jessie, WİLLİAMS Byron J., SKELTON Gordon W., "Cyber Security for Emergency Management", Technologies for Homeland Security (HST), 2010 IEEE International Conference on, 2010 ,(476 - 480)

[8] DWEN-REN Tsai; CHANG A.Y., PEİCHİ Liu, HSUAN-CHANG Chen, "Optimum Tuning of Defense Settings for Common Attacks on the Web Applications", Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on ,Ocak 2009, (89 – 94)

[9] OWASP "Reviewing Code for SQL Injection", https://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection, 2010

[10] PARK Won Hyung," A Study on Risk Analysis and Assessment of Damages to Cyber Attack", Information Science and Applications (ICISA), 2010 International Conference on, Nisan 2010(1 - 6)

[11] ÜNVER Mustafa, CANBAY Cafer , "Ulusal ve Uluslar Arası Boyutlarıyla Siber Güvenlik",EMO- elektrik mühendisliği, Mart 2010, (94-103)

[12] ÜNVER Mustafa, CANBAY Cafer , ÖZKAN Hüseyin Burhan," Kritik Altyapıların Korunması", Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Mayıs 2010

[13] Azmi, I.M.A.G., Zulhuda, S. ,Jarot, S.P.W. "Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on,Haziran 2012 (306 – 311)

[14] PALLOTTI E., MANGIATORDI F, " Smart Grid Cyber Security Requirements", Environment and Electrical Engineering (EEEIC), 2011 10th International Conference on,Mayıs 2011, (1 – 4)

[15] ALTUNDAL Ömer Faruk, "DDoS nedir, ne değildir?", http://www.siberguvenlik.org.tr/makaleler/ddos-nedir-ne-degildir/, Ağustos 2012

[16] Dr.THEİLER Olaf, " New threats: the cyber dimension", http://www.nato.int/docu/ review/2011/11-september/Cyber-Threads, Eylül 2011

[17] "Türkiye'nin Ulusal Siber Güvenlik Politikası Siber Savaş İçin Hazır mı?", http://www.siberguvenlik.org.tr/genel/turkiyenin-ulusal-siber-guvenlik-politikasi-siber-savas-icin-hazir-mi/ ,Nisan 2012

[18] ALKAN Mustafa, SAĞIROĞLU Şeref, TÜREKÇİ Tolga, ATALAY Ahmet Hamdi, BİLİRGEN Cabir, CANBEK Gürol, İNCEEFE Mehmet Ali, ÖZBİLEN Alper, ÜNVER Mustafa, YAZICI Ali, "Ulusal Bilgi Güvenliği Stratejisi", http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Stratejisi.pdf, Ekim 2012

[19] "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", www.resmigazete.gov.tr, Haziran 2013

[20] DURNA İlke Deniz, ÇALIŞKAN Emin, GÜL Ahmed Furkan, ONAY Oktay, GÖZÜKÜÇÜK Merve, TAŞÇI Burak, DÖVER Zeynep Sena, ÇELİK Burak, KINIKOĞLU Batu Yakup, ,ÜNAL Ahmet, Mehmet Bedii KAYA, "Siber Güvenlik Raporu", İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Enstitüsü,http://www.dktr-legal.com/upload/makaleler/Ulusal-Siber-Guvenlik-Raporu-Siber-Guvenlik-Calisma-Grubu-4.pdf, Mayıs 2012

[21] ŞENTÜRK Hakan, ÇİL C.Zaim, SAĞIROĞLU Şeref, " Cyber Security Analysis of Turkey", International Journal of Information Security Science, Vol 1, Mayıs 2012, (112-125)

Seda YILMAZ Gazi Üniversitesi Bilişim Enstitüsü Bilgisayar Bilimleri Bölümünde yüksek lisans eğitimine devam etmektedir. Araştırma konuları arasında kablosuz sensor ağlarda güvenlik, web yazılım güvenliği, siber güvenlik, bilgi ve bilgisayar güvenliği yer almaktadır.

Şeref SAĞIROĞLU Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesidir. Zeki sistem kimliklendirme, tanıma ve modelleme, ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizi ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları; yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar gibi konularda çalışmaktadır. 50'nin üzerinde SCI tarafından taranan uluslar arası dergilerde yayınlanmış makalesi, 50'nin üzerinde ulusal dergilerde yayınlanmış makalesi, 100'ün üzerinde uluslar arası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş100'e yakın bildirisi bulunmaktadır. 3 adet alınmış patenti vardır. 5 adet yayınlanmış kitabı, 2 adet kitapta bölüm yazarlığı bulunmaktadır. 4 kitabın da editörlüğünü yapmıştır.

Ulusal ve uluslar arası pek çok proje yürütmüş ve konferanslar düzenlemiş olup akademik çalışmalarına devam etmektedir.

Security Challengers in Grid Operating Systems

Farhad Soleimanian Gharehchopogh, Neda Jabbari, and Nima Hojjati

***Abstract*—Vast nature of internet causes creation an environment "grid" for a developable system creation with high effectiveness, distributing and reliability. In a distributed system like grid, information safe transfer and duties services security guarantee is an important subject. Different architectures are proposed for creating security in grid that the most important one is a grid operating system (GOS). GOS is trying to create security in transferred information, shared resources by security module and security of each node in grid computational environment. In this paper, we describe a little about GOS and then, we review about security components in grid especially security in GOS.**

***Index Terms*—Grid Operating System, Security, System, Distributed**

I. Introduction

GRID term is proposed as a distributed computational infrastructure for developed science and engineering in 1990 [1]. Grid is a distributed computational infrastructure that causes more usage of computational resources by sharing a lot of heterogeneous resources in outspread geographical distances. Sharing and resource selection are based on their user accessibility, capacity, ability, cost and need to service quality [2]. Grid computational environment is a distributed computational infrastructure that support of virtual organizations creation and exploit with control mechanisms and polar organizational resource sharing [1]. Global registration center is a central storage that grid service creators maintain a database of resources are useful for users admission, recognizing them, dynamic services creation and representation [3]. Because, public operating systems are designed for using in personal level, they can reply to grid need level, so, middle wares came to this area. But, middle wares couldn't solve all problems that it caused creation of GOS. The main and primary idea of GOS came from Faster and et al. [4]. GOS can cause services presentation for sharing function ease in grid environment. In this paper, firstly, we review grid component in section 2 and we continue speaking about security in grid and GOS in section 3.

Manuscript received July14, 2013.

Farhad Soleimanian Gharehchopogh is with the Department of Computer Engineering, Urmia Branch, Islamic Azad University, Iran (corresponding author to provide phone: 00989141764427 and 00905544040942; e-mail: bonab.farhad@gmail.com).

Neda Jabbari is with the Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran (e-mail: nedajabbari.nj@gmail.com).

Nima Hojjati is with the Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran (e-mail: n.hojjati@gmail.com).

II. Grid Operating System

A. Grid Networks

In the last of 1990s, grid computational networks are created as proposed supersede for common super computers to solve problems that need a lot of computations and high content of data and relations. Grid computing by using internet creates use of other system's hardware resources. Use up resource in grid computing, contain huge computers, storage systems which are virtual organizations data resources with different politics that use by scientific, engineering and other computations in a large scale [5]. Virtual organization is a set of distributed resources that searches resources need for users and also share their resources. Although, it is more than a decade that grid is created but because of it doesn't present its acceptable solutions, couldn't find his situation in global area. In recent years, grid middle ware [6, 7] is emerged for more and simpler usage from grid software infrastructure such as, Globus [9], Legion [8], Condor [10] and UNICORE [11] that a lot of distributed computational problems use these tools with good base for writing application and focus on develop grid environment and computational resources but because of that grid developing by grid middle ware need more software layers, so, they aren't safe for information transfer [14]. For representing a safe distributed control, with satiability and high quality of services based on flexibility, nodes heterogeneous in grid cause problem in grid. For aiming to these goals, grid middle ware is classified to these components:

- Middle ware base
- Identity system and justification
- Job management and schedulers
- Data management
- Unblock management
- Information systems

Grid doesn't have any limitation in subject geographical area and also contains heterogeneous resources but it unblock because of transparent in distributed systems from user view. It is used of current computers without additional costs and can include a lot of cluster in geographical areas. Computational resources have big peace of resources that include processors and their relations. In this regard, data resource can be a memory of a processor or secondary memory for saving processed data in grid.

B. Grid Operating System

GOS is proposing for supporting local resource efficient management or grid environment remote resources for a system that is connected with this environment [17]. Grid base operating system play virtual machine role as a layered

interface in grid environment that the most important role of this interface is information safe transferring between connected nodes to grid and it has dynamic resources. In [17], a GOS should contain:

- Creation a simple connection in grid, endurable error in nodes, giving justification for survey applications
- Proposing a platform for user access to grid resources and transparent distributed resources, process access proposition to all resources and resources that are shared between resource and process
- Policies appointment to create local resource in grid
- High efficiency and high accessibility
- High scalability, dynamic system further configuration, omission and adding node and transparent for applications.

Some GOS are same with public operating system in personal computers such as modularity that is one of the important rules in GOS, having politics dispassionate and free mechanisms, having universality in infrastructure for better programs and software's implementation, having low changes in operating system core [5]. GOS project is a GOS that support grid middle ware infrastructure. In [3], GOS made of these components:

GOS Core: In [19], GOS core has very low content and it is so soft that contains all services that are in high layer. Indeed, core is an interface between local operating systems users and grid computational environment. Keeping of core creates a security infrastructure for grid computations that can simply influence by users. Although service developing base on their unblock structure is hard but GOS addressing these problems by preparing a modularity architecture that needs a little changes in core [5].

Resource Management: Operating system uses from resource management modules for proposing related services that contain these components: resource registration, resource search, resource scheduler and devotion, error tolerance and services provider.

Node Description and Using of Resources: Nodes in grid is selected by that node efficiency. The use nodes resources maintains for computing for account of a node separately.

Grid Security: we can arise grid security by two methods: firstly, use of justifications admission before users inter to grid global environment. Secondly, it's done by GOS by using manual control that includes node admission and users identity.

Network Management: Traffic in grid computations makes it better controllable for services better representing by network management. The architecture [5] that is proposed for GOS includes three main parts that each of them has more pieces:

- Grid applications
- Grid middle ware

There are several project for GOS like Vigne [10], XtreemOS [20] and Apple xgrid [21]. XtreemOS is based on Linux and purpose of it is a distributed physical resource underside layer abstract liaison in an open source grid environment [22]. This GOS proposes a set of system services and developing of them in Linux old version for users that we can use all of grid availability. Vigne is a GOS that its purpose is programmers and users escape from shared resources and removing grid computational resources [23]. Apple XGrid is a part of Apple Mac OSX that let an organization to create grid componential or cluster computational.

III. SECURITY IN GRID-BASE OS

For network manager, one of the most important activities is network resources security guarantee. Illegal access to network resource or intentional and unintentional information blemish make network unsafe. This topic in grid network has more importance because of its distributed structure. Grid security infrastructure and its related application software need security module like identity recognizing, access control, unblock independence and lake of denial efficiency. In grid computing for establish security should be a powerful infrastructure in low levels. Security architecture in grid should be useful, developable and unblock. Security in grid is for three groups of grid environment parts:

- A nod of grid that gets present resources and uses it
- Virtual organization
- A user that gives his/her resources to other users

In [23], three main component of security are: privately, integrity and accessibility. In [24], firstly security grafts in grid are:

- **Identity preparation**: identity preparation means we give justification to users for activity that surveys all procedures that includes user computations and resources that use them and justifies their safety [14]. Identity preparation gives this confidence that corporative entity is free. This entity can be a person, tool, service or installed application in network. The user allows ability means user can receive services from network.
- **Single sign on**: for orchestrate different resources that do a single job in grid computational environment, this security module used for identity preparation high suppression in such systems [19]. Indeed, user gets his/her first enter from admission justification module and after that he/she can enter without additional surveys.
- **Credential span and renewal**: different activities in grid componential environment have different longevity and running time and as lots of activities longevity isn't given at the start of the process, so, if they didn't end after a period of time their run time should be extended. Thus, these activity attendance authorities extend in system means risk reduces in identity preparation and single sign-on [1].
- **Justification**: justification is like identity preparation. At first, a user needs justification for access to services in grid. In grid, justification politics should have these forms: both of service

receiver and service sender should export justification.

- **Representation:** Virtual organizations effective function in grid componential environment that are grid services infrastructure is based on trust. For create and manage this trust it needs a representation that has needed justification for survey services from a node to another one and setback their imports to each other's procedures. This deputation is needed for dynamic and static service creation warranty [1, 22].
- **Private sanctum preservation**: in Private sanctum preservation, both of service requester and service replier should require justifications for personal sanctum preservation politics appointment and implementation [17].
- **Privacy**: for maintaining privacy in grid, we need a safe transmission and also message safe encryption and decryption in return way on grid end point [23, 24].
- **Message Integrity**: It guarantees that if a message or a document is changed illegally. It will be recognizing in [18].
- **Exchange Policy**: related policies to service providers and service receivers are for safety from exchange and the change of identity preparation qualification, limitations and ability and security maintain rules support.
- **Secure entry to system**: entry to system should be done safety, as this entry uses in computation so it should be include an entry to secure system by any type of functional information or procedure.
- **Confidence**: It means that require conditions is proposed for security level from a web host environment by each node that include security actions running mechanisms and usage policy of them such as keeping via virus, using of firewall for accessing to internet and use of virtual private network [10, 24].
- **Management**: to have security in grid we need a management that this management contains high level of requirements like antivirus, dominance recognizing and prevention.
- **Firewall**: we can use firewall in grid for security creation without used local control in firewall politics. Access control and identity proportion have a relation between themselves and we can make it that people could access to network services by access level identifying and have some ability such as data repairing and changing, position removing and changing and data storage way. Indeed, access control specifies that who can use some types of services. Lack of denial is preventing and keeping nodes in a service representation relationship compare of other current nodes [24]. To have a safety grid, we should have a safety virtual organization. So, grid security should create a safety virtual organization. Virtual organization has life cycle [23]: recognition, formulization, function, completion and destroy. Now, to have a secure virtual organization, security should be in every point. For users and resource better control in grid network, GOS created a dynamic virtual machine and maintained security of computational resources by virtual machine [17].

  In [24], security in GOS can establish in three levels: grid level, grid application and host grid:

- **Grid level**: contains set of joint nodes that main topics on it are needed resource finding, trust of free node access and prohibition of other nodes accessing to that resource. In this level, for creating require safety, identity proportion should be active in each grid node, thus, free node access is successful and illegal node access is unsuccessful. A grid network is formed of connected nodes to this network that security establishes for a node is so important on it. Users let other nodes to access to their resources by connecting to grid network but, this access can be dangerous and reduce security of service providers and even service providers. Therefore, one of the security problems in GOS is creating security in each node. In grid, a node should be accessible completely or not (all or nothing) [17]. This means that when a node is prepared to survey services for one of the members, another node couldn't use that node services.
- **Application level**: this level includes all nodes that implement a part of grid-base program. If a node GOS procedure has a connection with another node GOS procedure, it should be establishment by service provider and receiver public application. In application level prevents intractable relations creation between nodes and these relations should be accessible by current relation liaison to avoid repugnance among similar nodes. For preventing security in this level we should stop illegal user's intervention in program management. Thus, grid network manager should exports access limitations and justifications for creating safety in this important level.
- **Host level:** for preventing information privacy and unblocking, information security should be in servers.

For creating exchanged information security among service provider and receiver in grid network, GOS stores information in secret and unblock forms and for creating these two needs, it surveys user justifications in grid level.

One of the basic topics in each operating system to create security is having every service justification for users that GOS has it and is one of the most important security creation components. Indeed, users can use of protected resources that have required justification in operating system from resource manager. For example, XtreemOS needs information storage privacy and unblock for having a justification [22]. These represented in XtreemOS GOS [19].

Main security components for XtreemOS are:

- **Privacy**: It represented by ISO (International Standard Organization). Privacy is one of the basic topics in security.
- **Unblocking:** unblocking guarantees that in data transferring, exchanged information are valid and complete. For example, when we want have a copy from a sensitive and important document; information valid and complete transfer is very important, because there is information change probability in transfer.
- **Availability:** availability points to information using ability. Security concept in availability relates to this topic that maybe a person denial access to data or a specific service intentional that is free for users.

GOS implements access control for each node require justification trust attaining for service receive or represent. Single sign-on is another security creator components that it creation, users should have particular and valid identity.

Installed GOS in each system can enter to global grid and use its services after identity acknowledgment that it's arise users safety. Indeed, users should use of GOS permissive copies and updated for arising security coefficient.

IV. RESULTS AND FUTURE WORKS

GOS is in lower level of host operating system, consequently, security component control done near user that it cause represent higher level in security by flexibility creation in grid services. Grid computational environment is a platform for users benefit from other nodes resources in needed time but this array or service receive not only can transfer unsecure information, also can be dangerous for nodes shared resource. So, it is important to have a powerful and safe infrastructure for data transferring. If a user doesn't have trust to grid computational environment, it wouldn't represent its resource and also wouldn't use other resources. We should have a GOS to attain a safe platform in grid that has a light core but with its specific security module. In this paper, we survey researcher's proposed needed security modules, although, we should survey more a lot of security hole that are in GOS.

REFERENCES

[1] I. Foster, C. Kesselman, The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufman Publishers, 2nd edition, 2004.

[2] A. Iamnitchi, D. Talia, P2P Computing and Interaction with Grids, Future Generation Computer Systems, North-Holland, Vol. 21, No.3, pp. 331-332, 2005

[3] S. Ahmed, P. Mahmood, Architecture for Grid Enhanced Operating System, International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, 2007.

[4] I. Foster, C. Kesselman, Steven Tuecke, The Anatomy of the Grid Enabling Scalable Virtual Organizations, International Journal Supercomputer Applications, 2001.

[5] T.M. Pinkston, V.K. Prasanna, GridOS: Operating System Services for Grid Architectures, HiPC 2003, LNCS2913, pp. 353–362, Springer-Verlag, Berlin Heidelberg, 2003.

[6] E. Laure, Middle Ware for the Next Generation Grid Infrastructure, Proceedings of the Computing in High Energy Physics Conference, pp. 826, 2004.

[7] I. Foster, C. Kesselman., Globus: A Meta-Computing Infra-structure Toolkit, Intl J. Supercomputer Applications, Vol. 11, No. 2, pp.115-128, 1997.

[8] V. Huber, UNICORE: A Grid Computing Environment for Distributed and Parallel Computing, Lecture Notes in Computer Science, pp.258–266, 2001.

[9] G. Shaw, A.S. Wulf, The legion Vision of a Worldwide Virtual Computer, Communications of the ACM, Vol. 40, pp. 39-45, 1997.

[10] B. Gleeson, A. Lin, J. Heinanen, T Finland, G. Armitage, A. Malis, IP based Virtual Private Networks, Technical report, Internet Engineering Task Force, 1975.

[11] B. Aziz, A. Arenas, J. Bicarregui, B. Matthews, E. Yang, A Formal Security Requirements Model for a Grid-based Operating System, STFC e-Science Centre, Rutherford Appleton Laboratory, UK Available at: www.e-science.stfc.ac.uk, Last Access: 2013.5.15.

[12] B. Mathews, "Towards a Knowledge Grid: Requirements for a Grid OS to support Next Generation Grids",Core Grid Work- shop on NGN, Belgium, 2005

[13] The Globus Project, Introduction to Grid Computing, Argonne National Laboratory, 2002.

[14] S.Puri,Q.Abbas," Grid Operating System: Making Dynamic Virtual Services in Organizations" International Journal of Computer Theory and engineering, Vol. 2, No. 1 February, 2010.

[15] Burke, S. Campana, S. Lorenzo, P.M. Nater, C. Santinelli, R. Sciaba, A: User Guide, Members of the EGEE-II Collaboration, April 2008.

[16] XtreemOS, Integrated Project, Security Requirements for a Grid-based OS.

[17] Karen Kent Frederick. Ronald W. Ritchey Stephen Northcutt. Lenny Zeltser. Scott winters. INSIDE - Network Perimeter Security. New-Riders, 2003

[18] I. Foster, C, Kesselman. G. Tsudik, S. Tuecke, A Security Architecture for Computational Grids Technical Report, The Globus Alliance, 1998.

[19] J. Belass, Measuring security in a Grid Computing Environment, Master's Thesis, Department of Computer Science and Media Technology, University College, 2005.

[20] S. William, Cryptography and Network Security Principles and Practices, Fourth Edition, 2005.

[21] V. Welch, J. Novotny, S. Tuecke. An Online Credential Repository for the Grid: My Proxy, Technical Report, The Globus Alliance http://www.globus.org, 2001.

[22] M. Adamski. M. Chmielewski, S. Fonrobert, A. Gowdiak, B. Lewandowski. J. Nabrzyski, T. Ostwald, J. Pukacki, Technical report, Available at: http://www.gridlab.org, Last Access: 2013.5.14.

[23] E. Jeanvoine, Using Overlay Networks to Build Operating System Services for Large Scale Grids, The Fifth International Symposium on Parallel and Distributed Computing, pp. 191–198, 2006.

[24] C. Morin, XtreemOS: A Grid Operating System Making Your Computer Ready for Participating in Virtual Organizations", 10th IEEE International Symposium on Object/component/service-Oriented Real-time Distributed Computing (ISORC), 2007.

Uygulamalarda Şifre Güvenliği İçin Yeni Bir Yaklaşım

Y. Sönmez, M. Karabatak ve E. Avcı

Özet **— Günümüz bilgisayar teknolojisinde kullanılan programların çoğunda (masaüstü programlar, e-mail, web sayfaları vs.) kişiye ait bilgiler bulunmakta ve bu ortamlara girişte bu bilgilerin doğru kişiye sunulması için kullanıcı adı ve şifre kombinasyonuna dayalı güvenlik sistemleri kullanılmaktadır. Bu güvenlik sistemlerindeki kullanıcı adı ve şifreler sayısal veya karakter tabanlı olup klavye aracılığı ile girilmektedir. Kişiye ait bilgilere ulaşmaya çalışmak için yapılan saldırılar klavye dinleme donanım veya yazılımları ile yapılmaktadır. Klavye dinleme donanım veya yazılımları tuş vuruşlarını kaydederek saldırıyı yapan kişi/kişilere göndermekte ve kullanıcı adı ve şifreler çalınabilmektedir. Geliştirilmeye çalışılan sistemde şifrenin kişiye özgü olmasını sağlayan bir program yapılmaya çalışılmıştır. Kişiye özgü şifreden kasıt, kullanıcının şifre girişi esnasındaki klavye kullanım tarzını tespit ederek şifre güvenlik düzeyinin arttırılmasına yöneliktir. Bu sayede şifreler saldırı yapan kişi/kişilerin eline geçse dahi, şifrenin gerçek sahibi gibi aynı tarzda yazılamayacağından dolayı girilen şifre yanlış kabul edilecektir. Şifrelerin belirli tarzda yazılmasının tespiti bilgisayarlara duyusal anlama boyutu katmakta ve şifreyi kullanan kişi tarafından yazılıp yazılmadığı kontrolü sağlanmaktadır.**

Anahtar Kelimeler— **Güvenli şifre, Klavye dinleme sistemleri, Klavye kullanım tarzı.**

Abstract— **Many of the programs (Desktop Programs, e-mail, web sites, and etc.), which they have been used thanks to today's computer technology, keep personal information in themselves. In order to present right personal information to right people, a protection system, which is based on user names and password combination, is used. User names and passwords in this protection system, which are entered through a keyboard, are numerical and character based. Attacks, which are aimed to be able to access to exclusive information, are done through a keyboard monitoring system by using related hardware and software. It is likely to steal some of personal information such as user names and passwords by using various kinds of hardware and software tools which works based on keyboard monitoring system. In the program we aim to develop, the main goal is to ensure password security by making passwords private. The main aim of using the term 'Private Password' is to identify keyboard using style of each person, thus aiming at increasing password security level. Thanks to such a this kind of system, even if password are captured by people who attack to our computer systems, these passwords are regarded as wrong passwords or information since passwords cannot be written with the same style of passwords' real owners. The identification of passwords' writing style contributes to sensory analysis of computers, thus establishing control in computers by checking whether passwords are written by real owners of them or not.**

Keywords— **Secure Password, Keyboard Monitoring Systems, Keyboard Using Style.**

I. GİRİŞ

TEKNOLOJİNİN hızla gelişmesi ve sayısal sistemlerin yoğun bir şekilde kullanılmasıyla bu sistemlerdeki veri güvenliği de büyük ölçüde önem kazanmıştır. Bilişim teknolojilerinde güvenliğin sağlanmasındaki temel amaç kullanıcıların bu teknolojileri kullanırken karşılaşabilecekleri tehdit ve tehlikelere karşı gerekli önlemlerin alınmasını sağlamaktır[1]. Kişilere ait bilgilerin veri olarak saklanması ise güvenlik sistemlerinden beklenen iki temel görev, veriyi ait olduğu kişilere sunmak ve yabancı kişilere veriyi kapatmaktır[2]. Bu veriler saklanırken ve kişilerin erişimine sunulurken, ait olduğu kişiye sunulması için kullanıcı adı ve şifre kombinasyonuna dayalı güvenlik sistemleri kullanılmaktadır. Bu tip güvenlik sistemleri bilgi temelli kimliklendirme olarak adlandırılır [3]. Bu çeşit güvenlik sistemlerinde kullanıcı adı ve şifreler bir veri tabanında tutulur. Kullanıcılar bilgilerini sisteme girdiklerinde veritabanında karşılaştırma yapılır. Karşılaştırma sonucu bilgiler aynı ise doğru kullanıcı olduğu anlaşılır ve söz konusu kullanıcının sisteme giriş yapmasına ve sistemde kendisine tanınan yetki dâhilindeki işlemleri gerçekleştirmesine izin verilir. Bu tip sistemlerin en önemli dezavantajlarından biri, kullanıcının şifre bilgisinin bir başkası tarafından elde edilmesinin klavye dinleme sitemleri sayesinde kolay oluşudur [4].

Şifre güvenliğini arttırmaya yönelik olarak; kullanıcı eğitimi, otomatik üretilmiş parolaların kullanımı, ardıl (reactive) parola denetimi ve öncül (proactive) parola denetimi gibi teknikler kullanılmaktadır [5]. Uzun yıllar, "insan-makine ara yüzünde" var olan güvenlik açıkları ise çoğunlukla göz önüne alınmamıştır. Bir "insan makine ara yüzü" olarak bilgisayar kullanırken en çok etkileşimde bulunulan donanımların başında gelen klavyeler, bilgisayar sistemlerinin en az değişen ve üzerinde en az durulan donanımlarından biridir [6]. Kullanıcıların klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırı yapan kişi/kişilere gönderen keylogger olarak adlandırılan kötü amaçlı yazılımlar ile şifreler kolaylıkla çalınabilmektedir. Üstelik kötücül ve casus yazılımlara karşı hazırlanan paket programların (anti virüs) çoğu, klavye dinleme sistemlerini dikkate almadığı öne sürülmektedir [7]. Şifreler kişi/kişiler tarafından ele geçirildikten sonra ilgili sistemlere kötü amaçlı yazılımlar sayesinde rahatlıkla giriş yapılmaktadır. Dolayısıyla günümüz teknolojisinde henüz şifrelerin kişi/kişiler tarafından ele geçirilip kullanılmasına karşı yüzde

yüz güvenli bir yöntem geliştirildiğinden söz edilememektedir.

Şifre kullanımındaki diğer bir sorun da, genellikle birçok ortamda aynı şifrenin kullanılıyor olmasıdır. Kullanıcıların çoğu, farklı şifreler kullanıldığında bunu hatırlamanın çok zor olması nedeni ile aynı şifreyi birçok sistemdeki kullanmaktadır [8]. Bu nedenle şifresi ele geçirilen bir kullanıcının, şifresi ile erişim yaptığı tüm uygulamalara giriş için gerekli olan anahtar olan şifre doğrudan ele geçirilmiş olmaktadır. Bu da şifre güvenliğinin ne kadar önemli olduğunu açık bir şekilde ortaya koymaktadır.

Klavye dinleme yazılımı olarak bilinen ve keylogger olarak adlandırılan kötücül yazılımlara karşı alınan önlemler günümüzde yeterli seviyede değildir. Bu sebepten dolayı, kişilerin klavye kullanım tarzının tespit edilmesi ve güvenlik düzeyinin arttırılması amacı ile şifre girişleri için yeni bir yaklaşım sunulmuştur. Böylece şifreyi yazan kişinin doğru kişi olup olmadığının tespiti yapılmakta ve şifreler başka kişi/kişiler tarafından ele geçirilse dahi şifrenin gerçek sahibi tarafından girilip girilmediği belirlenmektedir. Dolayısıyla, uygulamalara kazandırılan bu boyut sayesinde, yabancı kişi/kişiler tarafından şifre doğru girilse dahi bu giriş sistem tarafından otomatik olarak ret edilecektir.

Geliştirilen bu özellik ile, istenmeyen kişi/kişilerin ellerine geçen şifrelerin kullanılmasında caydırıcılık özelliği de sağlanmaktadır. İstenmeyen kişiler tarafından doğru şifre girilmesine rağmen, sistem tarafından şifrenin yanlış olduğu iletilmektedir. Böylece şifreyi ele geçiren kişi doğru şifreyi girmediğini varsayarak aynı şifreyi tekrar denemeyecek ve sisteme giriş yapma ihtimali kalmayacaktır.

Literatürde, şifre güvenliğinin sağlanmasına yönelik farklı yöntemlere rastlanmaktadır. Bu çalışmada önerilen yöntem, biyometrik kimliklendirme yöntemlerine benzemekte ve sadece kişinin kendine özgü bir davranışının analiz edilerek şifre girişine uygulanmasını içermektedir. Biyometrik sistemler, fiziksel ve davranışsal olmak üzere iki guruba ayrılan özellikleri içermektedir. Davranışsal biyometrik sistemlerden olan el yazısı analizinde, daha önce kişinin yazdığı bir yazı ile yeni yazdığı yazılar çeşitli adli tıp uzmanları veya görüntü işleme teknikleri ile tespit edilmektedir [9]. Bu tespit, kişinin harfleri nasıl yazdığına bakıp karşılaştırmaktadır. Örneğin "j" veya "i" harflerini yazarken nokta bırakma, düz çizgi çizme şekilleri gibi kişiye özgü olan durumlar tespit edilmektedir. Önerilen bu sistemde de kişinin klavye kullanırken bir kelimeyi nasıl kodladığı bu kodlamayı yaparken tuşlara hangi hızda bastığı tespit edilip şifre güvenliğinde kullanılması analiz edilmiştir.

II. YÖNTEM

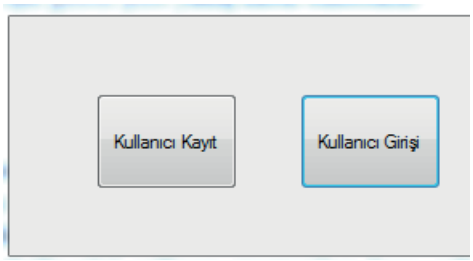
Bilgisayar veya uygulama programlarını kullanan her kişinin, farkında olsun olmasın klavye kullanırken kendine özgü geliştirdiği bir yazım tekniği olduğu yapılan gözlemlerle tespit edilmiştir. Bu gözlemler ile tespit edilen bu teknik kişinin klavye kullanırken yazım hızı ve kodlaması olarak ifade edilmiştir. Şifre bilgisi gibi bilgiler günlük yaşamda çok sık kullanıldığı için bu bilginin bilgisayar sistemlerine girilmesinde kişiye özgü bir tarz ortaya çıkmaktadır. Örneğin kişi "Fırat" kelimesini yazarken, tuşlara "Fı-rat", "F-ırat" veya "Fır-at" yazacak şekilde klavye kullanımı gerçekleştirmektedir. Bu kullanım tarzı şifre gibi aynı bilginin çok sık kullanılması ile daha belirgin hale gelmektedir. Çünkü bilgisayar kullanırken şifre ile giriş yapılan yazılımlarda genellikle aynı şifreler kullanılmakta ve bu şifreler sürekli kullanımdan dolayı sürekli aynı kodlama ve hızda girilmektedir.

Bu aşamada, kişinin klavye kullanım tarzının tespit edilmesi ile kişiye özgü şifre oluşturulması gerçekleştirilecektir. Bu nedenle, şifre ile giriş yapılan yazılımlara (mail, üyelik girişi, kredi kartı şifre girişi vs. gibi) giriş yapmak için kullanılan şifrenin doğru kişi tarafından girilip girilmediğinin kontrol edilmesi gerekmektedir. Bu prensibe dayanarak geliştirilen algoritma ile kişinin şifre girişi esnasındaki tuşlara basma hızı ve kodlama şekli tespit edilmekte ve şifrenin doğru olup olmadığının yanı sıra doğru kodlama ve hız ile girilip girilmediği de kontrol edilmektedir.

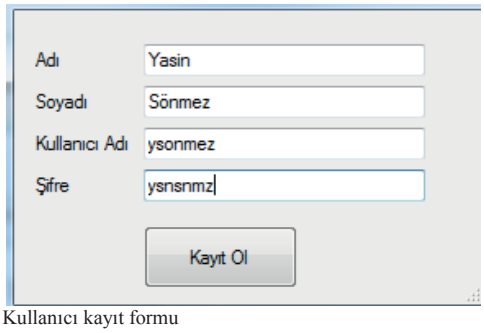
Örneğin kullanıcı, şifre bilgisi olarak “1234” bilgisini yazarken hangi hızla yazdığı veya “12” yazdıktan sonra “2” yi silip tekrar “234” yazarak şifreyi tamamladığında bu giriş tarzı da takip edilerek şifre doğruluğu tespit edilecektir. Bu sayede “1234”olan şifre bilgisi ele geçse dahi istenen şekilde yazılmadıkça uygulama kullanıcı girişine izin vermeyecektir.

III. UYGULAMA

Çalışmada, hedeflenen amaç doğrultusunda, şifre girişi yapan kullanıcının tuşlarını ve tuşlara basma hızını takip edip veri tabanına kaydeden bir yazılım C# ortamında gerçekleştirilmiştir. Bu uygulama, önerilen yöntemin istenen düzeyde başarım gösterip göstermediğini belirlemek amacı ile hazırlanmış olup, oluşturulan bir şifrenin bilgisinin herhangi bir başka kullanıcı tarafından sisteme girmesi istenmiştir. Farklı kullanıcı tarafından aynı şifre girilmesine rağmen sistem şifreyi yazan kullanıcının kayıt yapan kullanıcı olmadığını tespit etmiştir. Hazırlanan program istenen sonuca başarılı bir şekilde ulaşmıştır. Yani bilgisayar sistemi program sayesinde girilen şifrenin aynı kodlama ve hızda olmadığını tespit etmiştir. Geliştirilen yazılımın çalışma şekli görsel olarak aşağıda anlatılmaktadır. Şekil 1’ de görüldüğü üzere programın ana formunda kullanıcı kayıt ve kayıt edilen kullanıcının programa girişini sağlayan iki düğme bulunmaktadır.



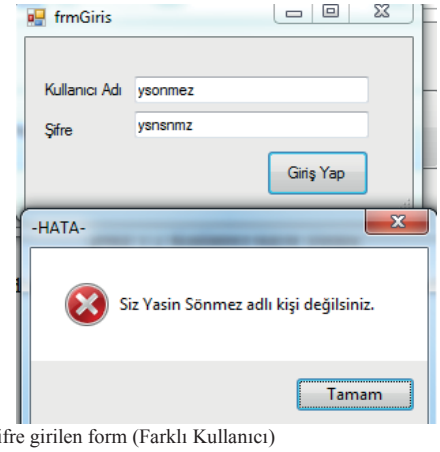
Şekil 1. Programın ana formu



Şekil 2. Kullanıcı kayıt formu

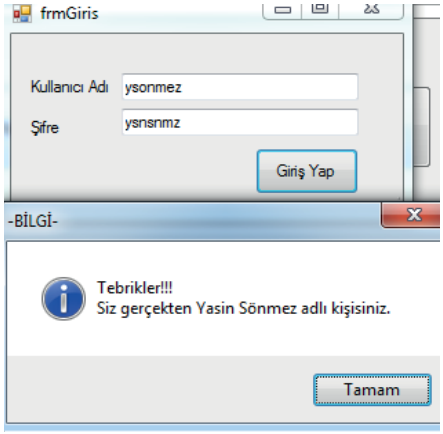
Şekil 2'de görüldüğü üzere kullanıcı kayıt formunda klavyeyi kullanarak kendi yazım tarzı ile şifresini yazmaktadır. Burada şifre "ysnsnmz" olarak belirlenmiş ve "ysn-snmz" şeklinde kodlanmış ve bu kod ile kullanıcının geliştirdiği hız tespit edilerek veri tabanına kayıt edilmiştir. Şifreler ilgili alanlarda normalde yıldızlı veya koyu siyah daireler şeklinde olurken programımızda şifreler açık şekilde belirtilmiştir. Bunun nedeni bir sonraki adımda aynı şifrenin girildiğini belirtmektir.

Bir önceki adımda girilen şifre veritabanına açık şekilde kayıt edilmiştir. Normal durumlarda kullandığımız programlar şifreleri veritabanlarına kayıt ederken belirli algoritmalara göre karıştırarak kaydetmektedir. Ancak veritabanları çalınsa dahi normal sistemlerde uygulanan algoritmaların tersi uygulandığında şifreler ele geçirilmektedir. Hazırlanan yazılımda şifrenin açık şekilde kayıt edilmesinin sebebi, veritabanları çalınır ve şifreler açık şekilde ele geçse dahi önerilen yöntem sayesinde şifrenin güvenli olduğunu ispatlamaya yöneliktir. Şekil 3'te, hazırlanan yazılımın, önerilen yöntemin hedefi doğrultusunda doğru bir şekilde çalıştığı görülmektedir. Şekil 2'de görülen şifrenin aynısı girilmesine rağmen önerilen yöntem sayesinde, yazılım şifreyi yazan kişinin doğru kişi olup olmadığını anlamakta ve uyarı iletisini göstermektedir. Bu şekilde farklı kişilerin doğu şifreyi bilmelerine rağmen sisteme girişleri engellenmektedir. Şifre yanlış kişi tarafından doğru girilmiş ve doğru kişi olup olmadığı kontrolü başarılı şekilde gerçekleştirilmiştir.



Şekil 3. Şifre girilen form (Farklı Kullanıcı)

Şekil 4'te de görüldüğü gibi şifre aynı kodlama ve hız ile girildiğinde, sistem şifreyi kabul etmiş yani sistem şifreyi kullanan kişi tarafından girilip girilmediğini kontrol etmiştir.



Şekil 4. Şifre girilen form (Şifreyi kullanan kişi tarafından girilmesi)

Önerilen yöntemin kullanılabilirliğinin test edilmesi amacıyla farklı ölçütler ile başarım oranı hesaplanmıştır. Bu ölçütler normal şifre kullanımları baz alınarak belirlenmiştir.

A. *Metin tabanlı özgün kullanıcı şifresi.*

Programa daha önce bu programı kullanmış bir kullanıcının karakterlerden oluşan şifresi; on farklı kişiye yazılı olarak verilmiş ve şifreyi girmeleri istenmiştir. Kişilere verilen şifre on farklı kişi tarafından dört denemeden oluşacak şekilde girilmiştir. On farklı kişinin dört farklı denemesinden oluşan kırk farklı giriş isteğinin tümünde de doğru şifre girilmesine rağmen program şifreyi yazan kişinin doğru kişi olmadığını tespit etmiştir.

B. *Sayı tabanlı özgün kullanıcı şifresi.*

Programa daha önce bu programı kullanmış bir kullanıcının rakamlardan oluşan şifresi; on farklı kişiye yazılı olarak verilmiş ve şifreyi girmeleri istenmiştir. Verilen şifre, on farklı kişi tarafından dört denemeden oluşacak şekilde girilmiştir. On farklı kişinin dört farklı denemesinden oluşan kırk farklı giriş isteğinin tümünde de doğru şifre girilmesine rağmen program şifreyi yazan kişinin doğru kişi olmadığını tespit etmiştir.

C. *Metin-Sayı tabanlı denek kullanıcı şifresi.*

Programı ilk kez denek olarak kullanan kişilerden daha önce çeşitli platformlarda (masaüstü programlar, e-mail, web sayfaları vs.) kullandıkları şifrelerinin test için hazırlanan yazılıma kayıt edilmesi istenmiştir. Kaydettikleri kendi şifrelerini programa giren beş denek için yapılan testlerde elde edilen sonuçlar Tablo 1'de verilmektedir.

TABLO 1
METIN-SAYI TABANLI DENEK KULLANICI ŞIFRESI DENEME SONUÇLARI

Kişi	1. Deneme	2. Deneme	3. Deneme	4. Deneme	Şifre Türü
1	Başarılı	Başarılı	Başarılı	Başarılı	Sayı
2	Başarısız	Başarılı	Başarılı	Başarısız	Metin
3	Başarısız	Başarısız	Başarılı	Başarılı	Metin-Sayı
4	Başarılı	Başarılı	Başarılı	Başarılı	Metin
5	Başarılı	Başarılı	Başarılı	Başarılı	Sayı

Tablo 1'de görüldüğü üzere, sadece metin ve sadece sayı tabanlı oluşturulan şifrelerde güvenliğin yüksek düzeyde olduğu metin-sayı kombinasyonuna dayalı şifre kullanımlarında da yöntemin başarılı olduğu ancak başarı oranının biraz daha düştüğü gözlenmektedir.

IV. SONUÇ

Bilgisayar kullanıcıları farkında olsun, olmasın klavye kullanarak yazı yazarken belirli tarzda yazmaktadırlar. Özellikle de çok sık kullanılan bazı bilgilerin klavye ile giriş tarzı kendini büyük ölçüde belirginleştirmektedir. Önerilen yöntem ile bilgisayarın kullanıcıyı tanıma boyutu; kişi - klavye kullanım tarzı kombinasyonunun güvenlik amacıyla kullanılması başarı ile gerçekleştirilmiştir. Böylece şifre yazarken klavye kullanım tarzının güvenlik amacıyla kullanılması fikrinin esasına dayanarak bir yazılım geliştirilmiş ve yapılan denemelerde başarılı sonuçlar üretmiştir.

Deneklerin geliştirilen sistem üzerindeki görüşleri alınırken oluşan fikirlerin ana teması: sistemin eğer sürekli kullandıkları klavye üzerinde denenmesi halinde tüm sonuçların başarılı olabileceği hakkında hemfikir oldukları gözlenmiştir. Bu fikrin ortaya çıkmasındaki temel sebebin kullanıcıların uzun süre kullandıkları klavye üzerinde klavye kullanım tarzı alışkanlıklarının daha da geliştiği fikri öne sürülebilir. Bu fikir çerçevesinde bu çalışmaya konu olan yazılımın şifre kullandığımız platformlarda (masaüstü programlar, e-mail, web sayfaları vs.) kullanılmasının güvenliğini arttıracağı konusunda başarılı olacağı düşünülmektedir. Önerilen yöntemin, güvenliği arttırmaya yönelik özelliğinin yanında caydırma, veritabanı çalınması gibi açıklara da çözüm sunacağı düşünülmektedir.

Önerilen yöntem doğrultusunda geliştirilen yazılım programının günlük kullandığımız programlarda (web sayfası üyelikleri, e-mail programları, Windows sürüm girişleri ve kredi kartı şifre girişlerinde vs. gibi) kullanılması ise ancak bu ara yüzleri yazılım programı olarak yapan kişiler tarafından önerilen sistemimizin kullanılması ile mümkün olacaktır.

Yapılan çalışma sonucunda geliştirilen şifreleme sistemi kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırı yapan kişi/kişilere gönderen, keylogger olarak adlandırılan kötü amaçlı yazılımlara karşı; gelişen teknoloji ile yeni bir şifreleme tekniği olarak kullanılacağı tahmin edilmektedir.

KAYNAKLAR

[1] G., Canbek, Ş. Sağıroğlu, "Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme", Gazi Üniversitesi Politeknik Dergisi, 9.3 (2006).

[2] Ü. A., Aydın, C., Acartürk. "Kullanılabilir Güvenlik ve Grafik Şifreler", Türkiyede İnternet Konferansı. 2012

[3] N. Özkaya, N., Sağıroğlu, Ş., "Açık Anahtar Altyapısı ve Biyometrik Sistemler", I. Ulusal Elektronik İmza Sempozyumu, 7–8 Aralık 2006, s.283-290, Ankara, Türkiye.

[4] R., Şamlı, M.E., Yüksel, "Biyometrik güvenlik sistemleri", Akademik Bilişim'09 (2009): 11-13.

[5] Korkmaz, İlker, and Mehmet Emin Dalkılıç. "Öncül Parola Denetimi Yöntemiyle Parola Seçim Sistemi: Türkçe Parolalar için Bir Araştırma."Akademik Bilişim'10: 206.

[6] G., Canbek. "Klavye dinleme ve önleme sistemleri Analiz, tasarım ve geliştirme", Yüksek Lisans Tezi. YÖK Tez No:184764, 2005

[7] Canbek, Gürol, and Şeref Sağıroğlu. "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Gazi Müh. Mim. Fak. Dergisi 22.1 (2007): 121-136.

[8] Hilmi, G., Karabatak, M., "Online Bilişim Suçları ve Bu Suçlara Karşı Alınacak Önlemler", 1. Uluslar arası Adli Bilişim ve Güvenlik Sempozyumu, 20-21 Mayıs 2013, s. 120-125, Elazığ, Türkiye

[9] Öztürk, E., Duman, E., "Biyometrik Yöntemler ile Kimlik", 1. Uluslar arası Adli Bilişim ve Güvenlik Sempozyumu, 20-21 Mayıs 2013, s. 84-88, Elazığ, Türkiye

Yasin Sönmez - 1986 yılında Diyarbakır'da doğdu. 2010 yılında F.Ü. Bilgisayar Öğretmenliği Bölümünde lisans, 2012 yılında Elektronik ve Bilgisayar Eğitimi ABD'da yüksek lisans programını tamamladı. Halen F.Ü. Yazılım Mühendisliği ABD'da doktora öğrenimine devam etmekte olup Batman Üniversitesinde Öğretim Görevlisi olarak çalışmaktadır. (yasin.sonmez@batman.edu.tr)

Murat Karabatak - 1976 yılında Elazığ'da doğdu. 1999 yılında F.Ü. Bilgisayar Öğretmenliği Bölümünde lisans, 2002 yılında Elektronik ve Bilgisayar Eğitimi ABD'da yüksek lisans ve 2008 yılında Elektrik-Elektronik Mühendisliği ABD'da doktorasını tamamladı. Halen F.Ü. Yazılım Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. (muratkar@hotmail.com)

Engin Avcı - 1978 yılında Elazığ'da doğdu. 2000 yılında F.Ü. Elektronik Öğretmenliği Bölümünde lisans, 2002 yılında Elektronik ve Bilgisayar Eğitimi ABD'da yüksek lisans ve 2005 yılında Elektrik-Elektronik Mühendisliği ABD'da doktorasını tamamladı. Halen F.Ü. Yazılım Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. (enginavci23@hotmail.com)

Bukalemun: Bilişim Güvenliğinde Yeni Bir Sızma Test Platformu

Emrah Ayyüzlü, Emre Özer

***Abstract* – Penetration tests are considered as one of the most important issues in information security. These tests, when applied in a regular basis, establish a process to ensure the reliability and consistency of information systems. These tests are performed by modeling and mimicking the attacks encountered in the real world, helping the security vulnerabilities of IT systems to be observed more clearly. This paper offers an alternative method to other regular approaches used in the penetration tests. With its dynamic and innovative nature, the penetration testing module - subject to the content of this article - called Chameleon, provides the basis of this alternative approach.**

***Index Terms* — Bukalemun, Chameleon, Sızma Testleri , Penetration tests.**

***Özet* – Sızma testleri, bilişim güvenliğinin en önemli konularından birini oluşturur. Sızma testleri, bilişim sistemlerinin güvenilirliğinin ve tutarlılığının düzenli olarak incelenmesini sağlayan bir süreç tesis eder. Bu testler ile mümkün olduğunca gerçek dünyada karşılaşılabilecek saldırıların modellenerek gerçekleştirilmesi sağlanır. BT (Bilişim Teknolojileri) bünyesindeki güvenlik açıkları daha net bir biçimde gözlenir. Bu bildiri, sızma testlerinde kullanılan yaklaşımlara alternatif bir yöntem sunmaktadır. Bukalemun adı verilen sızma testi modülü dinamik yapısı, kolay kullanılabilirliği, esnekliği ile konusunda yenilikçi bir yaklaşım sunmaktadır.**

I. GİRİŞ

GÜNÜMÜZDE bilişim teknolojileri hızla gelişmekte ve hayatımızda her geçen gün daha çok yer almaktadır. Bu gelişme paralelinde, yeni ortaya çıkan güvenlik açıkları ile bilgiye yetkisiz erişim gibi bazı dezavantajları da beraberinde getirir. Bu durumda bilginin yetkisiz değiştirilmesi, görüntülenmesi, silinmesi ve neticesinde kritik hatalar, hizmet kesintileri yaşanması söz konusu olur. Firmaların organizasyon bütünlüğü ve işleyişi dışında kullanıcıların ve\veya müşterilerin kişisel bilgilerine ulaşılabilir ve bu bilgiler kötü niyetli amaçlar doğrultusunda kullanılabilir.

Sızma testi, kurumların bilişim teknolojileri üzerine inşa ettikleri altyapı, yazılım, donanım ve uygulamalara öngörülen yöntemler kullanarak keşif yapılması ve bu müdahaleler sonucunda sistemsel ve organizasyonel açıkların tespit edilip bu açıkları kullanarak sistemlere sızılmaya çalışılması ve bunun sonucunda oluşabilecek zararların tespit edilip raporlanmasıdır [1].

Sızma testi, kurumların bilişim teknolojileri üzerine inşa ettikleri altyapı, yazılım, donanım ve uygulamalara öngörülen yöntemler kullanarak keşif yapılması ve bu müdahaleler sonucunda sistemsel ve organizasyonel açıkların tespit edilip bu açıkları kullanarak sistemlere sızılmaya çalışılması ve bunun sonucunda oluşabilecek zararların tespit edilip raporlanmasıdır [1].

Sızma testi sonucunda oluşturulan raporlar, sistemlerdeki ve organizasyonun iç süreçlerindeki güvenlik zafiyetlerini detaylandırır. Kurum, bu doğrultuda sistemlerini ve organizasyonunu geliştirir.

II. SIZMA TEST MODÜLLERİNDEKİ TEMEL PROBLEM

Bilişim sektöründe, yeni hizmete giren ve mevcuttaki ürünler ile ilgili yeni güvenlik açıkları tespit edilmektedir [2]. Bulunan açıklar ile ilgili çok farklı atak algoritmaları geliştirilmektedir. Sızma testi farklı adımlardan oluşan bir süreçtir [3]. Sızma testi sürecindeki adımlara destek veren, kendini ispatlamış birçok açık kaynak kodlu, lisanslı uygulama bulunmaktadır [4]. Bu uygulamalardan öne çıkanları amaçları doğrultusunda örnek vermek gerekirse;

a. **İstismar Altyapı Uygulaması**: Metasploit[5]
b. **Flood Uygulaması**: Hping[6]
c. **Port ve Açıklık Tarayıcı Uygulamaları**: Nmap[7], Nessus[8]
d. **Ağ trafiği izleyen uygulamalar:** Wireshark [9]
e. **Uygulama Güvenlik Testi Uygulamaları**: Webinspect[10], Acunetix[11]

Bu uygulamalar sadece belirli sistem veya platformlardaki belirli amaçlara hizmet vermektedir[12]. Bu açıdan, sızma testlerinin güncel güvenlik açıklarını tespit edebiliyor olması elzemdir [13].

Sızma testi modülü geliştiren bir firma herhangi bir güvenlik açığı tespit ettiğinde, açıklığı bulan eklenti, sızma test modülüne hızlı bir şekilde entegre edilebilmelidir. Geleneksel yöntemler ile bu işlem zorlu ve maliyetli bir süreçtir [14]. Yeni bir açık bulunduğunda bu açık ile ilgili öncelikle analiz çalışması yapılması ve ardından bulunan açığı tespit eden eklentinin projelendirilip, geliştirilmesi ve hızlı bir şekilde sızma test modülüne entegre edilmesi gerekmektedir.
Günümüzde iletişim teknolojilerinin hızlı bir şekilde gelişmesi sonucunda birçok gönüllü kullanıcı her gün keşfedilen sistem açıkları hakkında haber almakta ve

Emrah Ayyüzlü Kuveyt Türk Katılım Bankası Teknoloji Mimarı
Emre Özer Kuveyt Türk Katılım Bankası Kurumsal Mimari Müdürü

çalışmalar yapmaktadır. Gönüllü kullanıcılar tarafından tespit edilen bu açıkların sistemler üzerinde var olduğunu doğrulayan uygulama kütüphaneleri geliştirilmekte ve bunlar milyonlarca gönüllü kullanıcı tarafından test edilip en performanslı ve güvenli hale getirilmektedir. Fakat gönüllü kullanıcıların geliştirdikleri uygulamalar dağınık halde bulunmaktadır [15]. Bu makalede önerilen ve bilgi güvenliğinde yeni bir sızma test platformu olarak geliştirilen Bukalemun'un asıl hedefi dağınık halde bulunan bu kod parçacıklarını tek bir çatı altında toplayarak kullanılmasını sağlamaktır.

III. SIZMA TESTİ MODÜLÜ BUKALEMUN

Bukalemun C# üzerine kurulan, sızma testi için kullanılan uygulamaları bir arada kullanmamızı sağlayan, kolay kullanımı hedefleyen, kendine özgü bir programlama (scripting) dili olan bir platformdur. Amacı farklı araçları basit bir önyüzde bir arada kullanmayı sağlamaktır. Sızma testi uygulamaları Bukalemun ortamında tanıtıldıktan sonra artık Bukalemun 'un bir fonksiyonu gibi kullanılmaya başlanır. Bukalemun uzak makinalardaki uygulamalarla farklı bağlantı tipleriyle iletişime geçip, uygulamanın varlığını ve sağlık durumunu kontrol eder. Bukalemun bize üç tip bağlantı tipi sunmaktadır. Bunlar aşağıdaki gibidir:

a. SSH
b. Windows Connection (WMI, Powershell, …)
c. Database

Belirtilen bağlantı tipleri doğabilecek gereksinimler içerisinde genişletilebilir yapıdadır. Bukalemun'da tanımlı bağlantı tiplerini destekleyen ve dışarıdan girdi (input) alabilen bütün uygulamalar kolay bir şekilde Bukalemun script dilinde tanımlanabilmektedir.

Tanımlanan bütün uygulamalar artık platformun bir fonksiyonu haline gelir. Oluşan bu fonksiyonlar, Bukalemun proje tanımlama alanında Bukalemun söz dizinine uygun bir şekilde yazılarak kullanılırlar.

Bukalemun, oluşturulan projeleri çalışma zamanında C# dilindeki karşılıklarına dönüştürerek çalıştırır.

Platformda, iki farklı fonksiyon tipi bulunmaktadır. Bunlar; iç fonksiyonlar ve dış fonksiyonlardır. İç fonksiyonlar platforma ait iken dış fonksiyonlar kullanıcıların Bukalemun'a sonradan tanımladıkları, kullanılmak istenen araçların veya sistemlerin komutlarını ve bağlantılarını içeren fonksiyonlardır. Bu fonksiyonlar kullanılmak istenen uygulamaya ait komutları içerdiği için kullanılan uygulamaya direk bağlıdırlar. Bu yapı, bir dezavantaj gibi görünüp Bukalemun 'un entegre olunan uygulamalara bağımlı bir görüntü çizse de, avantaj olarak aynı işi yapan farklı sistemlerin güçlü yönlerini kullanmamızı sağlamaktadır. Örneğin; Sızma testlerinin yapılabilmesi amacıyla kullanılan birçok uygulama bulunmaktadır. Bu uygulamalardan biri port tarama işini iyi yaparken diğer bir uygulama SQL injection işlemini iyi yapmaktadır. Bukalemun, her iki sistemi orkestra ederek, ana güvenlik sızma orkestrasyon görevini devralır ve kurumlara esneklik kazandırır.

Dış fonksiyonları Bukalemun'a entegre etmek için Bukalemun platformunda yer alan altı adım izlenir. Dış fonksiyonlar yerel veya uzak makinalardaki uygulamaları kullanıyor olabilir. Uzak bir makinada veya yerel bir makinada çalışan araç veya sistem için dış fonksiyon tanımlama aşağıdaki adımlarla gerçekleştirilir.

IV. BAĞLANTI İŞLEMLERİ İÇİN ANAHTARLAR TANIMLAMA

Uzak bir makinadaki bir uygulamanın komutunu çalıştırmamız için, ilk önce belirtilen makinaya bağlanmamız gerekmektedir. Bağlantı işleminin güvenli olması için bir anahtar gerekmektedir. Bukalemun'da anahtar tipi olarak kullanıcı adı ve parola kullanılmaktadır. Bukalemun'da uzak bir makinaya bağlanmak için uzak makinada tanımlı ve erişim yetkisi olan bir kullanıcıya ihtiyaç vardır. Bukalemun'a girilen bir kullanıcı hesabı, platform içindeki farklı uygulamaların bağlantıları için de kullanılabilir.

V. BAĞLANTI TİPLERİNİN BELİRLENMESİ

Bukalemun uzak bir makinaya bağlanıp bir komut çalıştırmak için farklı bağlantı tiplerinden birini kullanabilir. Bu bağlantı tipleri gereksinimler çerçevesinde genişletilip Bukalemun'a iç fonksiyon olarak eklenebilir. Bukalemun şu an için birçok bağlantı tipini desteklemektedir:

a. SSH
b. Database (ODBC, OLE DB)
c. TCP/IP üzerinden NetBIOS
d. PowerShell Remoting

Her tip bağlantı tipinin farklı tanımlaması olabilmektedir. Yalnızca her bağlantı tipi için ortak olan tanımlama kullanılacak olan anahtardır. Anahtar seçimi tanımladığımız anahtarlardan seçilerek yapılır.

VI. KULLANILACAK UYGULAMANIN TANIMLANMASI

Yerel veya Uzak makina üzerinde çalışan uygulama tanımlanır. Bu kısma gelene kadar tanımladığımız anahtar ve bağlantı tipini kapsayan bir isim vermektir. Burada vereceğimiz isim dış fonksiyonlar için bir isim uzayı (namespace) görevi görecektir. Bu yüzden benzersiz olmalıdır.

VII. KOMUT TANIMLANMASI

Kullanılacak uygulamanın bağlantı tipi ve kullanılacak anahtar tanımlandıktan sonra entegre edilen uygulama üzerinde çalıştırılacak komutlar tanımlanır. Her bağlantı tipine göre entegre edilen uygulama üzerinde çalışacak komut farklı olacaktır.

Örnek:

ssh: nmap –sS ip
http/https:
www.google.com.tr/search=word

Entegre edilen uygulama üzerinde çalışacak komutlar, entegre edilen aracın kendisine ait komutlarıdır. Komutlar tanımlandığında Bukalemun için artık bir dış fonksiyon halini alır. Fonksiyonun ismi komut tanımlamasında komuta verilen isimle aynıdır.

Örnek:

Tanımlama:
Anahtar=root
Bağlantı Tipi= SSH
Araç= BackTrack
Komut ismi = PortScan
Komut = nmap –sS ip
Komut Parametreleri =
1. parametre: nmap=>static
2. parametre: -sS => static
3. parametre: İp=>string

Chameleon:
PortScan(ip:"127.0.0.1");
Veya
PortScan(3:"127.0.0.1");

Parametresi statik olan fonksiyon (tanımlanan komut) dışardan değer alamaz. Bir parametrenin dışardan değer alması için Bukalemun'un desteklediği değişken tiplerinden biri olması gerekmektedir. Fonksiyonlara dışarıdan değer girilirken, parametre ile girilen değer aynı tipte olmalıdır.

VIII. STATÜ TANIMLANMASI

Tanımlanan komutların durumlarının (komut çalıştırılmaya başlandığında) nereden kontrol edileceğinin belirlendiği kısımdır. Bir programın çalışma durumu farklı yerlerden kontrol edilebilir.
Aynı program üzerinde oluşturulan komut kalıplarının her birinin durumları farklı yerlerden kontrol edilebilir. Kullanıcı, bu farklı tipteki durum kontrollerini sisteme tanıtabilmelidir.
Kullanıcı bazı komut kalıpları için durum kontrolü kısmını boş da geçebilir. Kullanıcı boş geçtiği dış fonksiyonun kontrolünün yapılmadığı kullanıcıya bildirilir. Kullanıcı isterse bu hatırlatmayı iptal edebilir. (Bunu bir daha gösterme).
Durum kontrolünün yapılabileceği alternatif kaynak ve yöntemler aşağıdaki gibidir:

A. Process

Çalıştırılan bütün işlemlerin process id'leri alınarak işlemlerin çalışıp çalışmadığına, sonucunun başarılı olup olmadığına bakılır.

B. Database

İşlemin durumunu ve başarılı sonuçlanıp sonuçlanmadığını anlamak için veri tabanı tablolarına bakılabilir. Örneğin; işlemin çalışıyor olup olmadığını anlamak için bir tablo üzerinde belirli satır ve sütundaki değerin güncel olup olmadığına bakılabilir. Aynı işlem için işlemin sonlanıp sonlanmadığını belirlemek için belirli bir tabloya kayıt atılıp atılmadığına bakılır.

C. Kütük (Registry)

Microsoft ortamında çalışan programların durumunu kütükten okuyabiliriz. Kullanıcı durumunu okuyacağı programın dizinini (RegKey) ve okuyacağı yerin tipini (DWORD, Text, Binary) girerek durumunu kontrol edilir.

D. XML, W3C, CSV

İşlemlerin durumuna belirli bir dizinin altındaki dosyaya yeni bir veri eklenmesiyle veya belirli bir dizindeki, tag'lar arasındaki verinin güncellenmesiyle bakılabilir. İşlemin durumu, farklı durumlar için aynı dosyada veya farklı dosyalarda farklılık gösterebilir. İşlemin çalışması güncellenmeyle, sonlanması dosyaya veri eklenmesiyle kontrol edilir.
Kullanıcılar n tane durum kontrolü oluşturabilir. Kontrollerin hangisinin kullanacağını seçebilirler.

IX. ÇIKTI TANIMLANMASI

Kullanıcılar kalıplarını oluşturdukları komutların çıktılarının ne tipte olabileceğini, nerelerden okunabileceğini sisteme tanıtabilir. Bir komutun birden fazla çıktısı olabilir. Bu çıktılar ihtiyaca göre arttırılabilir.
Bir komutun çıktısı olmayabilir veya çalışma sırasında çıktı kısmı boş olabilir. Bu tip komutlar sisteme esnek bir biçimde tanıtılabilmektedir. Komutların geri dönüş değeri tipleri aşağıdaki veri tiplerinden biri olabilir:

a. Tam Sayı
b. Ondalıklı Sayı
c. String
d. Void (Geri dönüş değeri yok)
e. Array

Kullanıcı varsayılan olarak yukarıda belirtilen geri dönüş değerini sisteme tanıtabilmektedir. Kullanıcı geri dönüş değeri ile ilgili hiçbir işlem yapmadığında geri dönüş değeri olmadığı varsayılacaktır.
Kullanıcı oluşturduğu komut kalıpları için kendi çıktılarını oluşturup çalışma zamanında istediğini kullanabilir. Kullanıcı şu şekilde bir çıktı oluşturabilir: 'Komut sorunsuz olarak tamamlandıktan sonra işlemin sonucunu belirli bir dizindeki dosyadan oku'
Kullanıcı çıktı tanımları farklı tiplerde olabilir:

A. Database

Komut çıktısı belirli bir veri tabanındaki tablodan okunabilir.

B. XML, W3C, CSV, Text

Kullanıcı belirli bir dizinin altındaki dosyadan çıktıyı okumayı isteyebilir. Burada verinin okunacağı yer dosyanın tipine göre değişebilir. Yazı formatı için dosyanın en altındaki veriyi oku derken, XML için belirli tag'lar arasında bulunan veriyi oku denilebilir.

C. Kütük (Microsoft)

Kullanıcı kütükte okuduğu bilgileri çıktı olarak ayarlayabilir.

Kullanıcı çıktı olarak yukarıda belirtilen seçeneklerle (bu seçenekler ihtiyaca göre artabilir) n tane çıktı oluşturabilir.

X. PROJE TANIMLAMA

Dış fonksiyonlar projeler içerisinde çalıştırılır. Proje kısmı Bukalemun dilinde tanımlamaların yapıldığı ve komutların çalıştırıldığı kısımdır. Proje tanımlarken farklı araçlara uygulamalara dış fonksiyonlar bir arada kullanılabilir.

Proje kısmında Bukalemun script dilinde yazılan kod çalıştırılabilir veya ileriki bir zamanda çalıştırılmak üzere kaydedilebilir.

Örnek:

```
Chamelon Projenin_ismi{
        var @ip String;
        @ip = "127.0.0.1";
        #PortScan(ip:@ip);
}
```

Proje tanımlandıktan sonra kullanıcının yazdığı Bukalemun komut dizinini çalıştırması için ilk olarak projeyi derlemesi (compile) etmesi gerekmektedir. Projenin derlenmesi, Bukalemun'nun söz dizeminin uygun bir şekilde yazılıp yazılmadığını kontrol etmek için yapılmaktadır. Kullanıcı isterse projeyi sağlık kontrolü (HealthCheck) işlemine de tabi tutabilir. Sağlık kontrolü işlemi projede yer alan dış komutların ve ona ait olan diğer birimlerin sağlık durumlarını kontrol eder. Tanımlanan aracın doğruluğuna ve çalışıp çalışmadığına bakar. Belirlenen bağlantı tipi kullanılarak araca erişim yapılabiliyor mu? Tanımlanan anahtar belirtilen makinada tanımlı ve yetkili mi? Bu ve buna benzer kontrolleri yaparak projenin sorunsuz çalışmasına katkıda bulunur.

XI. BUKALEMUN PLATFORMUNUN DİĞER SIZMA TESTİ MODÜLLERİNE GÖRE AVANTAJLARI

Sızma testi gerçekleştiren diğer modüller belirli platform ve uygulamalara yöneliktir. Bukalemun farklı platformlarda farklı şekillerde hizmet veren sızma testi modüllerini veya sızma testinin alt işlemlerini yapan uygulamaları tek bir çatı altında toplayıp etkin bir şekilde yönetmemizi sağlar.

Piyasada var olan sızma testi modüllerinin her biri farklı dallarda kendilerini ispatlamış durumdadır. Bir uygulama, sızma testi adımlarından biri olan port tarama işlemini çok iyi yaparken diğer bir uygulama ise SQL injection işlemini çok iyi yapmaktadır. Fakat bütün sızma test adımlarını, işlemlerin hepsini etkin bir şekilde bir arada sunan ve bütün platformları kapsayan bir modül bulunmamaktadır. Bu modüllerin kullanımı sırasında, kullanılan her bir modülün uzman kişilerine ihtiyaç duyulmaktadır. Bu durumda sızma testi işlemini zor bir süreç haline getirmektedir.

Bukalemun sızma testi işlemlerindeki yukarıda belirtilen probleme esnek bir çözüm sunmaktadır. Bukalemun'a kendi dallarında uzman kişilerin bir kere tanıttığı uygulamalar Bukalemun 'un basit ve kontrollü birer fonksiyonu haline gelir. Bu basit fakat etkin fonksiyonlar, platforma tanıtılan diğer fonksiyonlarla bir arada kullanılarak n tane farklı yapıda sızma testi senaryoları oluşturulmasına imkan sağlar. Bunun yanında, sızma testinin alanında uzman olmayan kişilerce kolay ve kontrollü bir şekilde gerçekleştirilmesi sağlanmaktadır.

XII. SONUÇ

Bilişim güvenliğinde yeni bir sızma test platformu olarak geliştirilen Bukalemun yeni bir yaklaşım getirilmektedir.. Sızma testleri, bilişim sistemlerinin güvenilirliğinin ve tutarlılığının düzenli olarak incelenmesini sağlayan bir süreç tesis eder. Güvenilir ve tutarlı sızma testleri yapmak için kullanılan uygulamaların test edilip kendini ispatlaması gerekmektedir. Bukalemun farklı platformlarda çok farklı uygulamalar için geliştirilmiş açık kaynak kodlu veya lisanlı uygulamaları tek bir çatı altında toplayarak kullanılmasına olanak sağlamaktadır. Farklı platformlarda farklı sistemler için geliştirilmiş uygulamaların bir arada kullanılması, bir kod parçacığından veya uygulamadan alınan çıktıyı bir başka kod parçacığı veya uygulamaya girdi olarak verebilme, her platformu kapsayan eşsiz bir üst uygulama oluşturulmasına olanak sağlamaktadır. Bukalemun'un bu avantajı sayesinde birçok farklı sızma test senaryosu oluşturulup kullanılabilir. Bukalemun'a kendini ispatlamış açık kaynak kodlu uygulamalar kolay bir şekilde entegre edilip kullanılabildiği için düşük maliyetli yüksek performanslı sızma testi yapılmasına olanak sağlar.

XIII. KAYNAKLAR

[1] Kenneth R. van Wyk. (2007) "Adapting Penetration Testing for Software Development Purposes" (2012) https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/penetration/655-BSI.html#dsy655-BSI_fyodor2006

[2] Securtyfocus.com (2012). Vulnerabilities [Online]. http://www.securityfocus.com/vulnerabilities

[3] Nitin A. Naik, Mr. Gajanan D. Kurundkar, Dr. Santosh D. Khamitkar, Namdeo V. Kalyankar
"Penetration Testing: A Roadmap to Network Security" (2012) http://arxiv.org/ftp/arxiv/papers/0912/0912.3970.pdf

[4] Bryan Burns, Dave Killion,Nicolas Beauchesne,Eric Moret,Julien Sobrier,Michael Lynn,Eric Markham,Chris Iezzoni,Philippe Biondi,Jennifer Stisa Granick,Steve Manzuik,Paul Guersch, (2007) "Security Power Tools", 4-27

[5] Abhinav Singh, (2012) "Metasploit Penetration Testing Cookbook" , 7-27

[6] Bryan Burns,Dave Killion,Nicolas Beauchesne,Eric Moret,Julien Sobrier,Michael Lynn,Eric Markham,Chris Iezzoni,Philippe Biondi,Jennifer Stisa Granick,Steve Manzuik,Paul Guersch, (2007)" Security Power Tools",132-137

[7] Bryan Burns,Dave Killion,Nicolas Beauchesne,Eric Moret,Julien Sobrier,Michael Lynn,Eric Markham,Chris Iezzoni,Philippe Biondi,Jennifer Stisa Granick,Steve Manzuik,Paul Guersch, (2007)" Security Power Tools",34-35

[8] Jay Beale,Haroon Meer,Charl van der Walt,Renaud Deraison, (2004)" Nessus Network Auditing: Jay Beale Open Source Security Series" 2-19

[9] Angela Orebaugh,Gilbert Ramirez,Jay Beale, (2007)" Wireshark & Ethereal Network Protocol Analyzer Toolkit (Jay Beale's Open Source Security)"52-65

[10] Bryan Burns,Dave Killion,Nicolas Beauchesne,Eric Moret,Julien Sobrier,Michael Lynn,Eric Markham,Chris Iezzoni,Philippe Biondi,Jennifer Stisa Granick,Steve Manzuik,Paul Guersch, (2007)"Security Power Tools" ,76-85

[11] Ec-Council,Course Technology, (2009)" Web Applications and Data Servers [With Access Code]" ,22-23

[12] Thomas Wilhelm, (2009)"Professional Penetration Testing"

[13] Mehdi Khosrow-Pour, (2006)" Emerging Trends And Challenges in Information Technology Management"

[14] Lee Allen, (2012) "Advanced Penetration Testing for Highly-Secured Environments: The Ultimate"

[15]https://buildsecurityin.us-cert.gov/bsi/articles/tools/penetration/657-BSI.html

Emrah Ayyüzlü: 2011 yılında İstanbul Fatih Üniversitesi Bilgisayar Mühendisliği'nden lisansını aldı. Haliç Üniversitesi Bilgisayar Mühendisliği alanında yüksek lisansına devam etmektedir. Kuveyt Türk Ar-Ge merkezinde Teknoloji Mimarı olarak görevine devam etmektedir.

Emre Özer: 2000 yılında İ.T.Ü Kontrol ve Bilgisayar Mühendisliği'nden lisansını aldı. 2010 yılında MIS alanında yüksek lisansını tamamladı.
12 yıldır profesyonel olarak yazılım sektöründe çeşitli kademelerde görev almıştır. IEEE üyeliği ve çeşitli akademik bildirileri mevcuttur. Kuveyt Türk Ar-Ge merkezin Kurumsal Mimari Müdürü olarak görevine devam etmektedir.

Yerel Alan Ağları İçin IP Tabanlı Saldırı Tespit Uygulaması ve Güvenlik Önerileri

[1]M.Zekeriya Gündüz, [2]Resul DAŞ

***Abstract* – The increase of the quantity and the value of the information committed via the internet, establishing a connection with the whole world in a very short period of time has attracted the attention of criminals and directed them to the internet. The criminals adapting to this new world quickly developed themselves in the field of technology rapidly, and began to commit crimes, which are normally too difficult to commit in normal ways, through the internet easily. These crimes called as cyber-crimes are intruding or attacking to a system or any informatic device by the person or persons in virtual platform. In this paper study is presented a sample attack was carried out on the local area network. Then the attacker was detected through IP.**

***Index Terms* - Intrusion Detection Systems, Computer Network Security, Cyber Crime, Information Security.**

***Özet*- İnternet üzerinden işlenen bilginin miktarı ve değerinin artması, bütün dünya ile çok kısa bir sürede bağlantı kurulabilmesi, suçluların da ilgisini çekmiş ve internete yönelmelerini sağlamıştır. Bu yeni dünyaya çok hızlı adapte olan suçlular, kendilerini teknoloji alanında da hızlı bir şekilde geliştirmiş, normal yollar ile oldukça zor gerçekleşecek suçları, internet ortamından kolay bir şekilde yapabilmeye başlamışlardır. Bilişim suçları olarak adlandırılan bu suçlar, sanal ortamda kişi veya kişiler tarafından bir sisteme veya herhangi bir bilişim cihazına izinsiz girme veya saldırıda bulunmadır. Bu makale çalışmasında, yerel alan ağı üzerinde bir saldırı gerçekleştirilmesi sunulmaktadır. Daha sonra saldırgan IP tabanlı tespit edilmiştir.**

***Anahtar Kelimeler* - Saldırı Tespit Sistemleri, Bilgisayar Ağ Güvenliği, Siber Suçlar, Bilgi Güvenliği, Bilgisayar Güvenliği.**

I. GİRİŞ

Teknoloji alanındaki gelişmeler büyük bir ivme kazanarak hızlı bir şekilde değişmekte ve insanların yaşamını kolaylaştıran çok önemli unsurlar haline gelmektedir. Günlük iş süreçlerinin elektronik ortamlara taşınması, manyetik ortamdaki bilgilerin paylaşılması, e-devlet uygulamaları gibi önem arz eden konular yaygınlaşmaktadır. Bu sebeple, kurulan bu sistemlerin bilişim ağ güvenliğinin gerekliliği ve önemi son derece önemlidir. Bu bağlamda olası tehdit ve tehlikelerin araştırılıp, bunlara karşı gerekli önlemlerin alınmasının, bilgi, bilgisayar ve bilgisayar ağ güvenliğinin sağlanması açısından oldukça önem kazandığı görülmektedir. [1]-[3].
Son yıllarda internetin yaygın kullanımının artmasıyla, sanal ortamda oluşabilecek dijital saldırılarda buna paralel olarak artmaktadır. Bu saldırılar, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur.

[1]Bingöl Üniversitesi, Teknik Bilimler Meslek Yüksek Okulu, Bingöl / TÜRKİYE (tel: 0505-9505544; e-mail: zekeriyagunduz@gmail.com)
[2]Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Elazığ / TÜRKİYE (e-mail: resuldas@gmail.com)

Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hâlâ büyük bir tehlike oluşturmaktadır. Bununla beraber kurum ve kuruluşlar, sanal dünyanın uçsuz bucaksız ortamında ağ saldırıları ve ağda yapılan aldatmacalara karşı güvenliklerini sağlamak için güvenlik politikaları da uygulamak zorunda kalmaktadırlar [4].

Bu makale çalışmasında, bir yerel alan ağında ARP Poisoning (ARP zehirlemesi) yöntemi ile bir saldırı gerçekleştirilmiş olup, bu saldırının nasıl tespit edilebileceğine yönelik bir uygulama çalışması yapılmıştır. IP tabanlı tespit edilen saldırgan ve belirtilen çözüm önerilerine göre elde edilen bulgular değerlendirilmiş olup sistem kullanıcıları ve son kullanıcılara yönelik ağ güvenliğinin sağlanması açısından alınabilecek güvenlik önlemleri maddeler halinde sunulmuştur.

II. AĞ GÜVENLİK ARAÇLARI ve SALDIRI YÖNTEMLERİ

Bir ağ sisteminde sistem yöneticilerinin ağı izlemek için kullandıkları ağ izleme yazılımları bazı durumlarda saldırganların elinde tam bir silaha dönüşebilmektedir. Beyaz şapkalı veya etik hacker olarak tanımlanan kişiler genellikle bu araçları, sistemdeki eksiklikleri bulmak için kullanırken, siyah şapkalı veya saldırgan olarak adlandırılan kişiler ise bunları sistemlere zarar vermek ya da veri hırsızlığı için kullanırlar.

Bilgi sistemlerinin güvenliklerini sağlamak amacıyla birçok çalışma yapılmaktadır. Bu çalışmalar genelde sisteme; güvenlik duvarları kurmak, saldırı tespit sistemleri kurmak, güvenli iletişim protokolleri sağlamak, zarar verici kodlara karşı yazılımlar kullanmak gibi çözümler olabilir. Fakat tüm bu yapılan çalışmalardan sonra bile sistemde saldırganların sızabileceği açıklar olabilir. Bu açıklar çeşitli güvenlik araçları kullanılarak tespit edilebilir ve gerekli önlemler alınabilir. Güvenlik araçları ayrıca sistemi izleme olanağı da sunarlar. Var olan güvenlik araçları genelde bilgisayar sistemlerine saldırı amacıyla geliştirilmiştir. Buradaki temel düşünce sistemin açıklarını saldırganlardan önce ortaya çıkarmak ve gerekli önlemleri almaktır [5],[6].

Bu çalışmada, ağı izlemek için kullanılan güvenlik araçları ve saldırı yöntemlerinin genel özellikleri şu şekildedir:

Cain & Abel

Ağ yöneticileri, güvenlik uzmanları ve geliştiriciler için üretilmiş, hedef ağda paket analizi yapma, ağdan şifre gibi bilgileri çekme, şifrelenmiş bilgileri Brute Force (kaba kuvvet) ve Cryptanalysis (şifreleme) metotları ile çözme gibi işlevlerinin yanında kötü niyetli kullanılmak istendiğinde tam bir silaha dönüşebilen yazılım aracıdır. ARP Poisoning saldırılarında en iyi sayılabilecek

yazılımlardan biridir. Güvenli protokollerde bile ARP Poisoning yaparak paket analizi yapabilir, şifrelenmiş veriyi okuyabilir. Ayrıca Cain & Abel Microsoft işletim sistemleri için bir password kırma aracı olarak da kullanılabilmektedir. Cain & Abel programının Linux sistemler için kullanılan formatı DSniff programıdır [7].

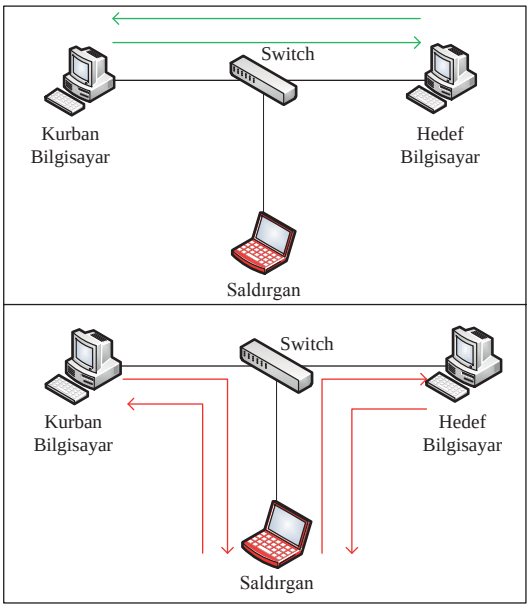
Wireshark

UNIX ve Windows platformları için ücretsiz bir ağ protokolü analizcisidir. Canlı bir ağda veya daha önceden diske kaydedilmiş bir ağ verisi üzerinde çalışarak ağ incelemesi yapar. Kullanıcı, interaktif bir şekilde incelenen veri hakkında ayrıntılı bir bilgi alabilir. Bu bilgi tek bir paket için de söz konusudur. Güçlü özellikleri arasında, zengin bir süzme diline sahip olması ve TCP oturumunu birleştirerek analiz imkanı sağlaması vardır. Wireshark programı Ethereal olarak adlandırılan programın yenilenmiş versiyonudur. Wireshark 750 den fazla protokolü analiz etme özelliğine sahiptir. Belirli kriterlere göre filtreleme yapabilmesi de kullanımını kolaylaştırmaktadır. Diğer paket yakalama yazılımlarının dosyalarını da açabilmektedir [8].

İnternet ortamında veya yerel ağ ortamlarında gerçekleştirilen saldırı ve aldatmaca yöntemlerinden bazıları; DoS saldırıları (Smurf saldırıları, Ping Flood saldırıları, SYN Flood saldırıları gibi), Spoofing saldırıları (ICQ Spoofing, DNS Spoofing, IP Spoofing, E-mail Spoofing gibi) bunların yanında SQL Injection, Sniffing, ARP Poisoning, DNS Poisoning ve DNS Cache Poisoning olarak belirtilebilir. İnternet gibi geniş alan ağlarında güvenlik politikaları tam uygulanmış ise bu saldırı türlerinin uygulanabilirliği çok daha zordur. Ancak yerel alan ağlarında bu saldırı yöntemlerinin gerçekleştirilebilirliğinin daha fazla ve kolay olduğunu söylemek mümkündür. Bu çalışmada bir yerel ağda saldırı için ARP poising yöntemi kullanılmıştır.

ARP Poisoning

ARP, veri göndermek için IP adresinin MAC adresini çözümlemeye yarayan protokoldür. ARP paketleri taklit edilerek saldırgan kendi makinesine verileri yönlendirebilir. Saldırgan ARP poisoning yaparak iki bilgisayar arasındaki trafiğin ortasına geçebilir. Şekil 1'de üst kısım normal ağ trafik akışını gösterirken, alt kısım ise ARP Poisoning saldırısının bulunduğu durumdaki ağ trafik akışını göstermektedir. Saldırgan, IP adresini ve MAC adresini gateway gibi broadcast yayın yaparak duyurur. Kurbanın ağ trafiği, saldırgan üzerinden geçmeye başlar ve saldırgan, kurbanın ağdaki tüm verilerini takip edebilir [6].

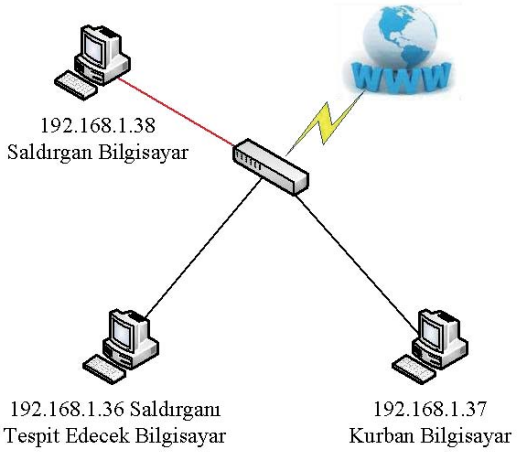


Şekil 1. ARP poisoning saldırı şeması [6]

III. YEREL ALAN AĞINDA VERİ HIRSIZLIĞI UYGULAMASI

Bu bölümde, yerel bir ağ sisteminde gerekli önlemler alınmadığı takdirde bilgisayarlar üzerinde üçüncü kişiler tarafından sniffing işleminin ne kadar kolay gerçekleştirilebileceğini gösteren uygulamalar yapılmıştır. Ağda, istenilen kullanıcının web üzerinde girdiği siteler, kullanıcı adı, şifre bilgileri ve girdiği sitelerdeki hesaplarının ele geçirilebileceği örnek bir uygulama ile gösterilmektedir.

Kapsamlı olan bu uygulamada, saldırı aşamasında kurban bilgisayarın dinlenmesi ve kurbana dair sniffing işlemi gerçekleştirilirken kullandığı kullanıcı hesaplarının nasıl ele geçirilebileceği gösterilmektedir. Kurban bilgisayarın dinlenmesinin sağlanması için Microsoft işletim sistemleri için bir password kırma aracı olarak da kullanılabilen *Cain & Able* aracı kullanılmıştır. Kurban bilgisayarın saldırgan tarafından dinlenmesi işlemi için, ağ üzerinde *ARP Poisoning* saldırı yöntemi kullanılmıştır. Yapılan saldırının tespiti için *Wireshark* ağ dinleme aracı kullanılmıştır. Wireshark programı aracılığı ile ARP Poisoning saldırısını gerçekleştiren saldırganın, ARP filtrelemesi yapılarak IP numarası üzerinden tespit edilmesi sağlanmıştır. Tespit edilen IP numarasının yerel ağdaki hangi kullanıcıya ait olduğu, bilgisayar adının belirlenmesi ile anlaşılmıştır. Uygulama hem kablolu hem de kablosuz ağlar üzerinde gerçekleştirilmiştir. Şekil 2'de uygulamanın gerçekleştirildiği yerel ağ üzerinde bulunan bilgisayarlar ve görevleri gösterilmektedir.



Şekil 2. Yerel ağ saldırısının genel gösterimi

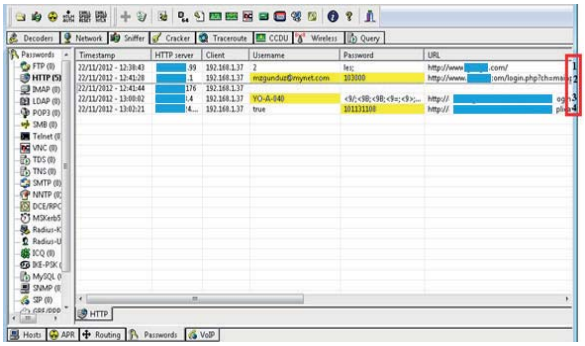
A. Yerel Ağ Üzerinde Saldırının Yapılması

Uygulamada kullanılan ARP Poisoning saldırı yönteminin uygulanmasında kullanılan bilgisayarlar ve çalışmamıza yönelik özellikleri şu şekildedir:
192.168.1.38 IP numarası sahibi olan bilgisayar ARP Poisoning saldırısını gerçekleştirecek, üzerinde Cain & Able programı yüklü olan, saldırgana ait bilgisayardır.
192.168.1.37 IP numarası sahibi olan bilgisayar, ARP Poisoning saldırısına maruz kalan, kurban bilgisayardır.
192.168.1.36 IP numarası sahibi olan bilgisayar, ağdaki saldırganı tespit edecek, üzerinde, protokol temelli ağ dinleme yazılımı olan wireshark bulunan bilgisayardır.

Uygulamada bazı portallar ve siteler üzerinde *kullanıcı adı* ve *şifrenin* elde edilmesine yönelik dört farklı sonuç alınmıştır. Bu sonuçlar şu şekilde belirtilebilir:
1) Kullanıcı adı ve şifrenin tespit edilemediği durumlar.
2) Kullanıcı adı ve şifrenin tespit edildiği durumlar.
3) Kullanıcı adının tespit edilip, şifrenin tespit edilemediği durumlar.
4) Kullanıcı adının tespit edilemeyip, şifrenin tespit edildiği durumlar.

Yapılan uygulamada yukarıda belirtilen sonuçlara göre Şekil 3'de gösterilen durumlar elde edilmiştir. Bunlar;
1. sonuçta hesaba dair bilgiler alınamamıştır.
2. sonuçta portaldan kullanıcı adı ve şifre bilgileri elde edilmiştir.
3. sonuçta kullanıcı adı elde edilmiş olup, password şifreli olarak iletildiğinden ağ üzerinden elde edilememiştir.
4. sonuçta kullanıcı adı elde edilememiş, password elde edilmiştir. Username alanı boolean bir değer döndürmektedir. Bu değerin SQL Injection yöntemleri ile atlatılarak sisteme girilebileceği düşünülmektedir.

Şekil 3 üzerindeki sonuçlar, gerçek uygulama sonuçları olduğu için bazı veriler kurum ve kuruluşların itibarını zedelememek adına gösterilmemiştir.

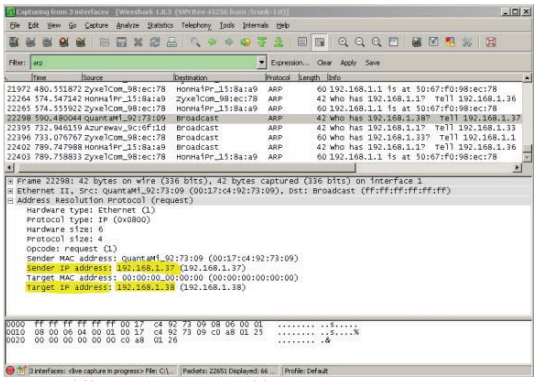


Şekil 3. Saldırı aşamasının sonuçları

B. Saldırganın Ağ Üzerindeki IP Adresinin Tespiti

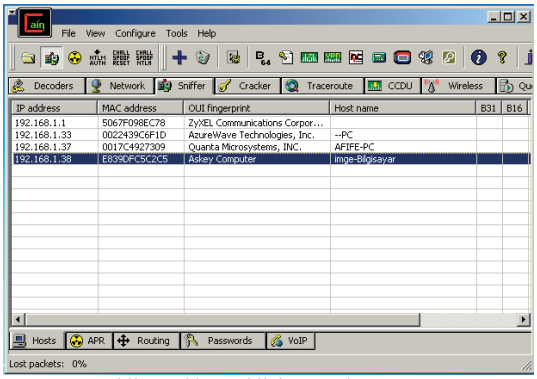
Saldırı hazırlık ve saldırı aşamalarından sonra saldırganın ele geçirdiği bilgiler, saldırgan tarafından kullanılabilecektir. En azından saldırgan istediği tüm bilgilere ulaşamasa bile yerel ağda elde ettiği bilgilerden yola çıkarak istediği kullanıcı üzerinde çeşitli sosyal mühendislik aldatmacaları ile istediği bilgilerin tamamına yakınını elde edebilecektir.

Bu çalışmada, *ortadaki adam* (Man in the Middle) saldırılarından olan ARP Poisoning saldırısının tespiti wireshark programı ile ARP filtresi üzerinden veri paketlerinin incelenmesi ile gerçekleştirilmiştir. Buna göre Şekil 4'de saldırı anında elde edilen wireshark çıktısı incelendiğinde; geçit yolunun (gateway) tüm bağlantı noktaları ile temas halinde olduğu görülmektedir. Ancak, saldırgan IP sinin kurban IP si ile de temas halinde olduğu tespit edilmiştir. Bu ilişkinin detayları incelendiğinde ise Şekil 4'ün alt kısmında görüldüğü gibi kurbanın verilerinin saldırganın IP adresine yönlendirilmiş olduğu gözlemlenmiştir.



Şekil 4. Wireshark ile saldırganın IP adresinin tespiti

Şekil 5'de saldırganın yerel ağda tespit edilen IP numarasının ağdaki başka bir bilgisayardan, Cain & Able programı kullanılarak bilgisayar adı ve MAC adresi tespit edilmiştir. Saldırganın bilgisayarının adı "imge-Bilgisayar" olduğu görülmektedir. Aynı şekilde kurban bilgisayarın IP adresi incelendiğinde bilgisayar adının "AFIFE-PC" olduğu görülmektedir.



Şekil 5. Saldırgan bilgisayar adının tespiti

C. Uygulama Sonuçları

Uygulama basamaklarındaki sonuçlar çizim modellemeleri ile gösterilmek yerine gerçek çıktıları ile gösterilmiştir. Buradaki amaç, hiçbir kurum ya da kuruluşun itibarını zedelemek değil, farkındalık oluşturma amaçlı ağ saldırılarının varlığını göstermektir. Ayrıca bu uygulamalar ile paylaşıldıkça artan bir nesne olarak da tanımlanan bilginin, korunumu ve güvenliği için alınacak tedbirlerin belirlenmesinde katkıda bulunmak amaçlanmıştır. Unutulmamalıdır ki, bir saldırının nereden ve ne şekilde geleceğini bilmek en iyi savunma sanatıdır. Uygulama sonucunda elde edilen bulgulara göre aşağıda belirtilen önemli çıkarımlar elde edilmiştir:

1) Farklı yerel alan ağlarında yapılan uygulamalarda, kablosuz yayın yapan erişim noktalarının (access point) güvenliklerinin genellikle doğru yapılandırılmadığı tespit edilmiştir. Eğer gerekli güvenlik önlemleri alınmadı ise; basit bazı işlemler ile bu erişim noktalarının ağlarına dâhil olunarak istenilen kullanıcılar izlenebilmekte, hatta yönetim paneli ele geçirilebilmektedir.
2) HTTPS protokolünü kullanan sitelerden veri çalınması http ve diğer protokolleri kullanan sitelere göre daha zordur.
3) Wireshark gibi ağ paketleri üzerinde her türlü analizi yapabilen programlar kötü niyetli kullanıcılar elinde bir silaha dönüşebilir. Bu duruma; ağda MSN programı üzerinden görüşme yapan kullanıcıların konuşma metinlerinin ele geçirilmesi örnek olarak gösterilebilir.
4) Kriptolamalı şifrelerin kırılması neredeyse imkânsızdır. Teorik olarak kırılması mümkün olsa bile, uygulamada kriptolu şifrenin elde edilmesi uzun süre ve yüksek maliyet gerektireceğinden dolayı mümkün değildir.
5) Cain & Able aracı ile yapılan uygulamalarda güvenilirliğe önem veren sitelerden ilk denemede bilgiler çalınabildiği halde sonraki denemelerde başarılı olunamamıştır. Kurum ve kişilerin itibarını zedelememek açısından ekran çıktıları verilmemiştir.
6) Saldırının varlığını tespit eden bazı sitelerin Şekil 6'da görüldüğü gibi sunucularına erişimi engelledikleri tespit edilmiştir.



Şekil 6. Güvenlik sertifikası

7) Bazı sitelerin Şekil 7'de görüldüğü gibi kullanıcı adı ve şifre istenecek formlarında hemen *https* protokolüne geçtikleri görülmektedir.



Şekil 7. HTTPS protokolü

IV. SONUÇ VE ÖNERİLER

Bilişim teknolojilerinin yaygınlaşması ile günlük hayatımızdaki iş ve işlemler elektronik ortamlarda artık daha hızlı yapılmaktadır. Bu durum, bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir. Bu nedenle kullanıcılar yaptıkları iş ve işlemlerde bilginin öneminin farkında olup, bu konuda güvenlik unsurlarını, politikalarını ve güvenlik süreçlerini uygulamak zorundadırlar. Böylece belli oranda, karşılaşılabilecek sorunlar ve tehlikeler azaltılabilecek, işgücü, zaman ve parasal kayıplar önlenebilecektir. Aynı zamanda, internet üzerinden gelebilecek zararlı yazılımlara veya program parçacıklarına karşı kişisel ve kurumsal bilgi güvenliğinin arttırılmasına katkılar sağlanacaktır.

Bilgi güvenliği konusunda güvenlik açıklarının önlenebilmesi için kişilerin ve kurumların basitten en karmaşık güvenlik yöntemlerine kadar bir dizi önlemler alması gerekir. Ancak, tüm önlemler alınmış olsa da, sürekli geliştirilen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini %100 güvende hissetmemelidir. Saldırılar; kötü niyetli kişiler, arkadaşlarımız veya tanıdığımız kişilerden gelebilir.

Bu çalışmada kapsamlı literatür taraması sonucunda bilişim suçlarının tespitine yönelik yapılan çalışmalar incelenerek, bilgisayar ağ sistemlerinde yapılan saldırıların, IP tabanlı delil tespitinin yapılması konusunda uygulamalar yapılarak, elde edilen sonuçlara göre; son kullanıcıları ve sistem yöneticilerini yakından ilgilendiren eksiklikler ve alınabilecek önlemler hakkında değerlendirmeler yapılmıştır. Yapılan uygulama aşamalarının ve sonuçlarının değerlendirilmesi neticesinde, ağ sistemlerinde var olan server, switch, hub gibi ağ cihazlarının ve bilgisayarların güvenliğinin artırılmasının yanında, sistem yöneticileri ve son kullanıcılar için aşağıda verilen önemli çıkarımlar belirlenmiştir.

Bilgi güvenliğinin sağlanması adına sistem veya ağ yöneticilerinin alabileceği önlemlerin bir kısmı şu şekilde belirtilebilir:

1) Ağ sistemi üzerinde bulunan güvenlik duvarı üzerindeki yönetim ve güvenlik politikaları analiz edilerek, detaylıca belirlenmelidir.
2) Sunucu hizmetlerinin kullandığı portlar dışındaki diğer kullanılmayan portlar kapatılmalıdır.
3) Ağ trafiğini kontrol etmek ve düzeltmek için VLAN yapıları oluşturulmalıdır.
4) Ağ sisteminde sniffing işlemlerinin tespiti için wireshark gibi birçok ağ dinleme araçları kullanılabilir.
5) Ağ sisteminde yazılımsal veya donanımsal olarak firewall kullanılmalıdır.
6) Saldırı davranışlarının takibi ve analizi için log kayıtları tutulmalıdır. Ayrıca güvenlik duvarlarında log analiz ve yönetim sistemi kullanılmalıdır.
7) Ağda olası tehlikeleri saptamak için IDS/IPS gibi otomatik açık tarama araçları kullanılmalıdır.
8) Ağ ve bilgi güvenliği ile ilgili güncel konular ve bilgiler, özellikle ağ yöneticileri tarafından yakından takip edilmelidir.
9) Dağıtıcı kullanılan sistemlerde güvenliğin sağlanması adına switch veya akıllı switch gibi cihazlar kullanılmalıdır.
10) Sistem için güvenlik politikaları oluşturarak bunların uygulanmasının ve takibinin yapılması sağlanmalıdır.
11) Bazı anahtarlar ve yönlendiriciler üzerindeki yönetim yetkilendirmelerine dikkat edilmelidir.
12) Router ve firewall gibi ağ aktif cihazları üzerinde erişim kısıtlamaları (access-list) oluşturulmalıdır.
13) Sunucu, router, firewall, switch gibi tüm ağ cihazları üzerinde güvenlik önlemleri en başından uzmanlarca yapılıp, herhangi bir güvenlik açığına meydan verilmemelidir.
14) VLAN ağında kullanıcıların yerinin tespit edilmesi için IP temelli erişim kontrol listesi tekniği (IP adresinin erişim yapabileceği portun kenar switch üzerinde sabitlenmesi) kullanılmalı veya her MAC adresinin belli zaman aralığında hangi IP adresini kullandığının kayıt altında tutulmasının en kesin yöntemi olarak yönlendiricinin ARP tablosunun loglanması sağlanmalıdır.
15) Yönlendiricilerin erişim hakları, erişim protokolleri güvenliği, şifrelerin güvenliğinin sağlanması, gereksiz servislerin kapatılması gibi yapılandırma ayarlamaları yapılmalıdır.

Ağ sisteminde ağ yöneticilerinin yanısıra özellikle son kullanıcılar şu hususlara dikkat etmelidir:

1) Web ortamında şahsi bilgiler ve şifre türü veriler dikkatli kullanılmalıdır.
2) Sohbet ortamlarında saldırıların daha fazla olabileceği unutulmamalıdır.
3) Web ortamında güvenliğin hiçbir zaman tam olarak sağlanamayacağı unutulmamalıdır.
4) Güvenilir ve tanınır siteler haricindeki sitelerden dosyalar indirilmemelidir.
5) Bilinmedik ve güvenilirliği şüphe uyandıran sitelere kişisel bilgiler verilmemelidir.
6) Sosyal mühendislik yöntemleri incelendiğinden saldırıların insanın yakınındaki kişilerden de gelebileceği unutulmamalıdır.
7) Kullanıcı internet ortamında kendini %100 güvende hissetmemelidir.
8) İnternet ortamı, gerçek dünyanın, sanal âleme bir yansımasıdır. Bu yüzden sosyal paylaşım sitelerinde paylaşılacak bilgiler dikkatli seçilmelidir.
9) Sazan avlama türündeki saldırılarda çoğunlukla insanların bilgisizliğinden, tecrübesizliğinden ve zaaflarından yararlanıldığı unutulmamalıdır [10].
10) Kişisel, önemli parolalar düzenli bir şekilde değiştirilmelidir.
11) İşletim sistemlerine ait güncellemeler düzenli olarak yapılmalıdır.
12) Lisanslı yazılımlar kullanılmalıdır.
13) Yasal ve güvenli olmayan sitelerden dosya indirme işlemi yapılmamalıdır.
14) İnternet kafe gibi halka açık ve güvenilirliği şüpheli olan ortamlarda internet bankacılık ve e-ticaret işlemleri yapılmamalıdır. Yapılacak ise güvenlik esaslarına dikkat edilmelidir.
15) Online alışverişlerde sanal kredi kartları kullanılmalı ve alışveriş süresince limitleri tanımlanmalıdır.
16) Şüpheli görülen e-posta eklentileri okunmadan ve açılmadan silinmelidir.

Bu çalışmada yapılan uygulamalar sonucunda dünyada ve ülkemizde bilgi güvenliğine yönelik en önemli tehditlerden olan kötücül ve casus yazılımların, yaygın olarak kullanımda olduğu, fakat kullanıcıların bu tür saldırı ve tehditlerden çoğunlukla haberdar olmadığı anlaşılmıştır. Herhangi bir zararla karşılaşılmaması için, konuya gereken önemin verilmesi, bilgi birikiminin arttırılması, bilgi güvenliğine yönelik hassasiyet gösterilmesi ve gereken önlemlerin alınması ile farkındalık oluşturulması gerekmektedir [11].

Bu çalışmanın konu ile alakalı olarak temel kavramsal bilgilerden ziyade uygulamaya yönelik yapılabilecek çalışmalar ve son kullanıcılar ile ağ yöneticilerinin alması gereken önlemler konusunda daha gerçekçi fikirler oluşturabileceği düşünülmektedir. Ayrıca, bu çalışmanın akademik literatüre IP numaralarından yararlanılarak veri hırsızlığının tespit edilmesi konusunda gerçekci bir uygulama ile yeni çalışmalar oluşturulması adına katkıda bulunduğu düşünülmektedir.

KAYNAKLAR

[1] Y.Uzunay, "Dijital Delil Araştırma Süreci", 2.Polis Bilişim Sempozyumu, Ankara, 2005.
[2] Canbek, G., Sağıroğlu, Ş., "Bilgi, Bilgi Güvenliği Ve Süreçleri Üzerine Bir İnceleme", Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570 Maltepe, Ankara.
[3] Daş, R., Kara, Ş., Gündüz, M.Z., "Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri", 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.
[4] Karaarslan E., Teke A., Şengonca H., 2003. Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması, İletişim Günleri, İzmir.
[5] Anuk, E., Güvenlik Araçları, İTÜ Bilişim Enstitüsü, İstanbul.
[6] Gündüz, M.Z., 2013. Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.
[7] *Internet:* http://www.oxid.it/cain.html, 21.05.2013.

[8] *Internet:* http://www.wireshark.org/, 21.05.2013.
[9] Elbahadır, H., 2011. Hacking Interface, Kodlab Yayıncılık, İstanbul.
[10] Şenol, A., Karacan, H., "Sazan Avlama (Phishing): Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri" 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.
[11] Karadoğan, İ., Daş, R., Baykara, M., "Scapy ile Ağ Paket Manipülasyonu", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu), 20-21 Mayıs 2013, Elazığ, Turkey.

M. Zekeriya GÜNDÜZ, 1983 yılında Bakırköy'de doğdu. 2006 yılında Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Sistemleri Öğretmenliği bölümünü bitirdi. 2006-2010 yılları arasında Milli Eğitim Bakanlığına bağlı Endüsri Meslek Liselerinde Bilişim Teknolojileri öğretmeni olarak görev yaptı. Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim dalında Ağ güvenliği konusunda " Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti" adlı yüksek lisans çalışmasını tamamladı. Halen Bingöl Üniversitesi Teknik Bilimler Meslek Yüksek Okulu, Bilgisayar Programcılığı bölümünde öğretim görevlisi olarak çalışmaktadır.

Resul DAŞ, 1975 yılında Elazığ'da doğdu. 1999 yılında Fırat Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Öğr. bölümünü, 2002 yılında Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Sistemleri alanında yüksek lisansını tamamladı. 2008 yılında aynı üniversitenin Elektrik-Elektronik Mühendisliği bölümünde doktora eğitimini tamamlayarak, bu alanda Doktor ünvanını aldı. 2000–2011 yılları arasında Fırat Üniversitesi Enformatik bölümünde öğretim elemanı olarak çalıştı. Kasım 2011 yılından beri Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği bölümünde öğretim üyesi olarak görev yapmaktadır. Bilgisayar Ağları, Ağ Güvenliği, Web ve Veri Madenciliği, Bilgi Keşfi, Adli Bilişim ve Güvenlik araştırma konularında çalışmalar yapmaktadır.

Hava-Hava ve Hava-Yer Taktik Data Link Sistemi için Kriptografi Donanımı

Muhammet Hamdi Yavuz, Osman Buğra Sarıca, Mehmet Haluk Canberi, Alper Kılıç

***Özet*—Geliştirilen "Data Link Tabanlı Dağıtık Gömülü Simülasyon Sistemi" kapsamında muharip hava platformlarının uçuş esnasında havada birbirleriyle ve yer istasyonlarıyla haberleşmeleri gerekmektedir. Haberleşme esnasında askeri açıdan kritik ve gizli bilgilerin paylaşılması gerektiğinden; haberleşmenin güvenilirliğinin sağlanması yani şifrelenmesi gerekliliği ortaya çıkmaktadır. Bu sebeple yüksek başarımlı, esnek ve yüksek güvenilirlikli bir kriptosistem donanımsal olarak FPGA üzerinde gerçeklenmiş ve elde edilen sonuçlar/kazanımlar paylaşılmıştır.**

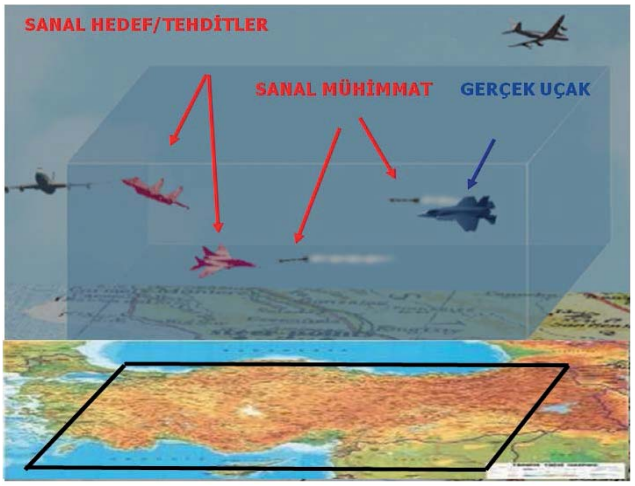
***Anahtar Kelimeler*—aes, data link, fpga, kriptografi, simülasyon**

***Abstract*— Combat aircrafts must communicate with each other and with ground stations during flight within the scope of the project "Data Link Based Distributed-Embedded Simulation System". During communication, because of the transferred data is militarily critical and secret, the necessity of ensuring the reliability of the communication, namely the necessity of encryption of the communication arises. Thus, a cryptosystem with high performance, high reliability and flexibility is implemented on FPGA and the results/benefits of the design are shared.**

***Index Terms*—aes, data link, fpga, cryptography, simulation**

I. GİRİŞ

EĞİTİM ortamı yaratma zorlukları ve fiziksel kısıtlar sebebi ile denenmesi zor olan alt sistemlerin kullanımı, gömülü simülasyon teknolojileri ile sanal olarak gerçekleştirilerek sonuçları görülebilmekte, masraflı olan kullanıcı eğitimlerinin yerini gömülü simülasyon eğitimleri alabilmektedir. Gate Elektronik A.Ş. tarafından geliştirilen Gömülü Eğitim/Simülasyon Sistemi projesi kapsamında; muharip pilotların harbe hazırlık ve harbe hazırlığın devamı niteliğindeki eğitimlerinde yalnızca gerçek uçak kullanılması durumundaki zengin taktik çevre eksikliği ile yer benzetim sistemlerinin kullanımındaki gerçeklik eksiklikleri giderilerek, söz konusu eğitimlerin gerçek uçuş şartlarında, sentetik bir taktik çevre ve sentetik unsurlar oluşturularak yapılması sağlanmaktadır [1]. Şekil 1'de Gömülü Eğitim/Simülasyon Sistemi'nin kavramsal şeması sunulmaktadır. Gömülü Eğitim/Simülasyon Sistemi kapsamında; eğitim senaryosu, pilotun harp zamanında karşılaşabileceği bir taktik durumun, tüm unsurlarını (hız, sürat, tehdit geometrisi yön, irtifa, manevra v.b.), sensör, silah ve meteorolojik şartlar da dahil görüş mesafesi, sistem başarımı v.b.) içerecek şekilde oluşturulabilmektedir. Bununla birlikte hava-hava, hava-yer, yer-hava mühimmatları, elektro-optik mühimmatlar, radar algılayıcıları, IR algılayıcılar, RF karıştırıcılar, karşı tedbir sistemleri (chaff, flare) gibi mühimmat ve algılayıcılar da modellenerek senaryoya dahil edilebilmektedir[1].



Şekil. 1. Gömülü Eğitim/Simülasyon Sistemi Kavramsal Şeması

Gömülü Eğitim/Simülasyon sisteminde, aynı anda yalnızca bir tek pilotun tam olarak eğitimi hedeflenmektedir. Bu projenin devamı niteliğinde olan Data Link Tabanlı Dağıtık Gömülü Simülasyon Sistemi (DLS), Gate Elektronik A.Ş. tarafından, birden fazla hava platformunun aynı senaryo üzerinde eğitimlerini gerçekleştirebilmesi amacıyla geliştirilmektedir. DLS projesi kapsamında, birden fazla muharip uçak, aynı senaryoya dahil olarak birbirleriyle etkileşimli olarak eğitimlerini sürdürebilmektedir. Aynı zamanda; bu uçaklar yer istasyonlarıyla da haberleşerek tüm eğitimin yerde eğitmenler tarafından canlı izlenmesine olanak sağlamaktadırlar. Sözkonusu hava-hava ve hava-yer iletişimi, Gate Elektronik tarafından geliştirilen Data Link Sistemi ile sağlanmaktadır. Data Link ile iletişimde, uçaklar birbirleri ile ve yer istasyonları ile askeri açıdan kritik bilgiler paylaşmaktadır. Bu sebeple; Data Link üzerinden sağlanan veri iletişiminin güvenliğinin sağlanması gerekmektedir. Bu çalışmanın konusu; Data Link sistemi üzerindeki verilerin, sistem mimarisine uygun bir şekilde şifrelenerek güvenli iletişime olanak sağlayacak bir

15.07.2013. Bu çalışma, TÜBİTAK tarafından desteklenen 3110306 numaralı "Data Link Tabanlı Dağıtık Gömülü Simülasyon Sistemi" TEYDEB projesi kapsamında hazırlanmıştır.

Muhammet Hamdi Yavuz, Gate Elektronik A.Ş., Tel: +90 312 257 07 37, e-posta: muhammet.yavuz@gateelektronik.com.tr

Osman Buğra Sarıca, Gate Elektronik A.Ş., Tel: +90 312 257 07 37, e-posta: osman.sarica@gateelektronik.com.tr

Mehmet Haluk Canberi, Gate Elektronik A.Ş., Tel: +90 312 257 07 37, e-posta: haluk.canberi@gateelektronik.com.tr.

Alper Kılıç, Gate Elektronik A.Ş., Tel: +90 312 257 07 37, e-posta: alper.kilic@gateelektronik.com.tr.

kriptografi donanımı tasarımıdır.

II. TEORİ VE SİSTEM MİMARİLERİ

A. *AES Algoritması*

AES (Advanced Encryption Standard) algoritmasından önce var olan DES (Data Encryption Standard) algoritmasının iyi bir algoritma olduğunun kabul edilmesine rağmen; düşük döngü sayısı, düşük şifre parça boyutu sebebiyle ve dönemin meşhur EFF paralel bilgisayarı Deep Crack ile yapılan test saldırılarının sonucunda DES algoritması yerini AES algoritmasına bırakmıştır [2]. Algoritma, NIST (National Institute of Standards and Technology) tarafından düzenlenen yarışma kapsamında Joan Daeman ve Vincent Rijmen tarafından geliştirilmiştir. Doğrulama ve standartlaştırma aşamaları sonrasında NIST, 26 Kasım 2001 yılında FIPS(Federal Information Processing Standard) 197 standardı adı altında AES algoritmasını yayınlamıştır [3]. AES algoritması, 128 bitlik veri bloklarını, 128, 192 veya 256 bitlik genişliklerde şifreleme anahtarları kullanarak şifreleyen bir algoritmadır. Algoritma içerisinde bu veri "state" adı verilen 4x4'lük bayt dizilerinden oluşmaktadır. Algoritmanın dönüşüm işlemleri bu diziler üzerinden uygulanmaktadır [4]. AES Algoritması, "Bayt Değiştirme (SubBytes)", "Satır Kaydırma (Shift Rows)", "Sütun karıştırma (Mix Columns)" ve "Döngü Anahtarı Ekleme (Add Round Key)" adları verilen dört temel dönüşümden oluşmaktadır. Döngü sayısı, anahtar boyutuna bağlı olarak 10, 12 veya 14 olabilmektedir. Şekil 2'de AES şifreleme algoritmasının işleyişi sunulmaktadır [5]. Başlangıçta döngü anahtarı eklendikten sonra, yukarıda ifade edilen dört temel dönüşümü içeren döngü fonksiyonu uygulanır. Son döngüde sütun karıştırma dönüşümü uygulanmaz. Bayt değiştirme dönüşümü, S-kutusu dönüşüm tablosunu kullanarak, 4×4'lük bayt dizilerinin her birini bağımsız olarak, doğrusal olmayan bir şekilde dönüştürme işlemidir. Satır kaydırma dönüşümü, 4×4' lük bayt dizilerinin satırlarını dairesel olarak kaydırma işlemidir. Sütun karıştırma işleminde her bir sütun dört terimli birer polinom olarak düşünülerek sabit bir polinomla çarpılır ve sütunlar dönüştürülmüş olur. Döngü anahtarı ekleme işleminde ise; anahtar genişletme işlemi sonucunda üretilen döngü anahtarlarının, her bir tekrarda diziye özel veya (XOR) işlemi ile katılması söz konusudur.

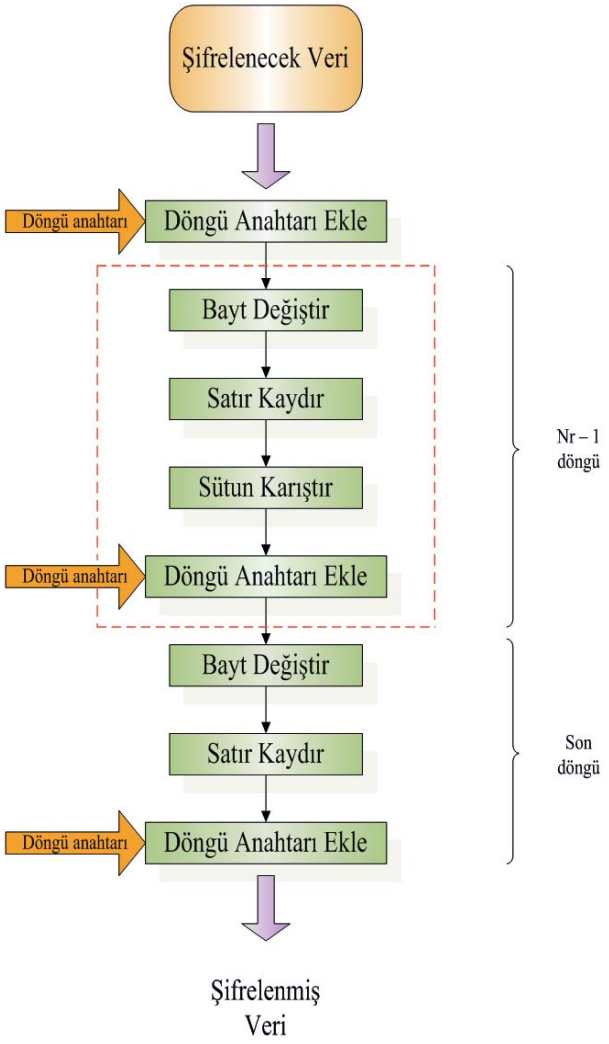
AES şifreleme algoritması ile şifrelenmiş bir veriyi çözmek için AES şifreleme algoritmasında uygulanan dönüşümlerin tersi uygulanmaktadır [6]-[7].

B. *Sahada Programlanabilir Kapı Dizileri (FPGA)*

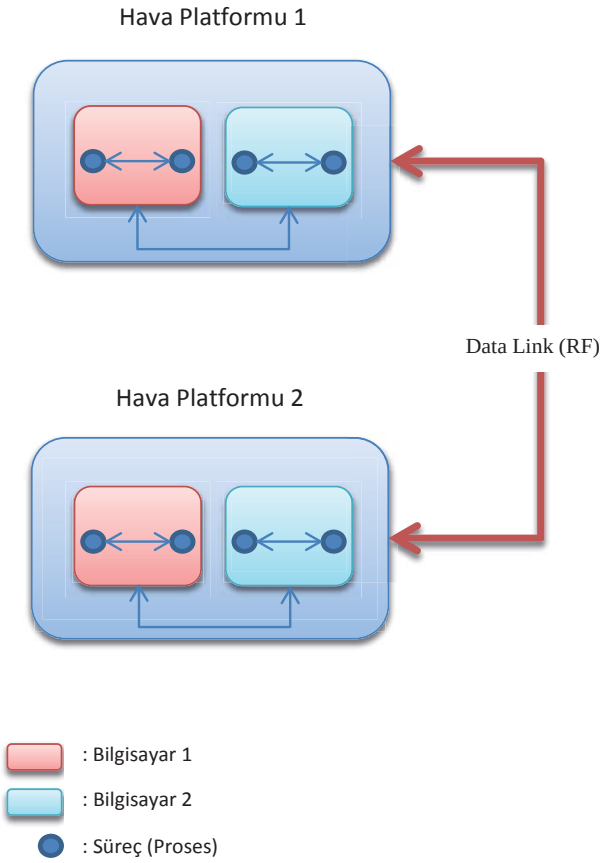
Sahada programlanabilir kapı dizileri (Field programmable gate array), iki boyutlu üreysel mantık hücreleri dizisi ve programlanabilir anahtarları içeren mantıksal aygıtlardır. FPGAlarda mantıksal bir hücre, basit bir işlevi yerine getirmek için programlanabildiği gibi, programlanabilir anahtarlar ise mantıksal hücreler arasındaki ara bağlantıları sağlayacak şekilde düzenlenebilmektedir. Özel bir tasarım, her mantıksal hücrenin işlevinin belirtilmesiyle ve her programlanabilir anahtarın bağlantılarının ayarlanmasıyla gerçeklenebilmektedir. FPGA aygıtları ve geliştirilen donanım tanımlama dilleri sayesinde, üst seviye dillerle, tasarlanan donanımlar tanımlanabilmektedir [8].

C. *Veri Dağıtım Hizmeti (Data Distribution Service)*

Veri Dağıtım Hizmeti (DDS) gerçek zamanlı çalışan dağıtık sistemler için geliştirilmiş bir ara katman hizmetidir. DDS, yüksek başarımlı, güvenilir ve gerçek zamanlı bir yayımcı/abone (publish/subscribe) teknolojisi sunmaktadır. DDS ara katmanı, sağladığı geniş servis kalitesi yönetimi ile gerçek zamanlı ve görev kritik sistemlerin dağıtık ortamdaki ihtiyaçlarını karşılamaktadır. Görev kritik sistemlerde veri aktarımı başarımının öngörülebilir ve deterministik olması beklenmektedir. DDS ara katman mimarisi, DLS projesinde; bu başarımı sağlayarak, süreçler arası haberleşme, bilgisayarlar arası haberleşme ve Data Link vasıtası ile platformlar arası haberleşmede kullanılmaktadır [9].



Şekil. 2. AES Şifreleme Algoritması



Şekil. 3. DLS Haberleşme Mimarisi

D. Data Link Tabanlı Dağıtık Gömülü Simülasyon Sistemi Mimarisi

Birinci bölümde bahsedilen Gömülü Eğitim/Simülasyon sistemlerinin üzerinde çalıştığı hava platformlarının haberleşmesi Data Link ile sağlanmaktadır. Her bir hava platformunun üzerinde iki adet yüksek başarımlı bilgisayar bulunmaktadır. Bu bilgisayarlar hem platform içerisinde birbirleriyle, hem de platformlar arası diğer bilgisayarlar ile haberleşmekte, ayrıca her bir bilgisayar üzerinde çalışan süreçler birbirleri ile haberleşmektedirler. Bahsi geçen haberleşme mimarisi, DDS ara katman mimarisi kullanılarak gerçekleştirildiğinden; bilgisayar içi, platform içi ve platformlar arası haberleşmede yalnızca fiziksel katman tanımlaması değişerek, bellek, Ethernet ya da RF (radio frequency) olabilmektedir[9]. Şekil 3'te DLS haberleşme mimarisi sunulmaktadır.

Muharip hava platformları arasındaki iletişimde, askeri açıdan kritik bilgilerin aktarılması gerektiği için, söz konusu platformlar arasındaki ver iletişiminde bir şifreleme sistemi gereksinimi ortaya çıkmaktadır. Şekil 3'te kırmızı hatla gösterilen iletişim hattı, Data Link kullanılarak radyo dalgaları ile sağlanmaktadır. Bu kırmızı iletişim hattından akan her türlü bilginin gizliliği sağlanmalı, dolayısıyla bir platformdan öteki platforma, bir platformdan yer istasyonuna veya yer istasyonundan bir platforma gönderilecek her türlü veri, kırmızı hatta girmeden önce şifrelenmeli ve alıcı tarafta kırmızı hattan çıktıktan sonra geri çözülmelidir. Güvenli veri ile güvensiz veri soyutlamasının tam anlamıyla yapılabilmesi için; her platformda, görev bilgisayarı ile Data Link anteni arasında şifreleme/çözme (encryption/decryption) işlemlerini yürütecek bir kriptografi donanımına ihtiyaç duyulmaktadır.

III. KRİPTOGRAFİ DONANIMI

Hava-hava, have-yer ve yer-hava Data Link iletişiminde askeri kritik/gizli verilerin güvenli ileitişimini sağlamak üzere bir kriptosistem gerekmektedir. Bu kriptosistemin; uygun bant genişliğinde, güvenli, sürdürülebilir, yüksek başarımlı ve diğer sistem/alt sistemlerden yalıtılmış olarak çalışabilmesi amacıyla yazılımsal çözümden ziyade donanımsal bir çözümün daha uygun olacağı öngörülerek, tasarlanan kriptosistem FPGA üzerinde gerçeklenmiştir.

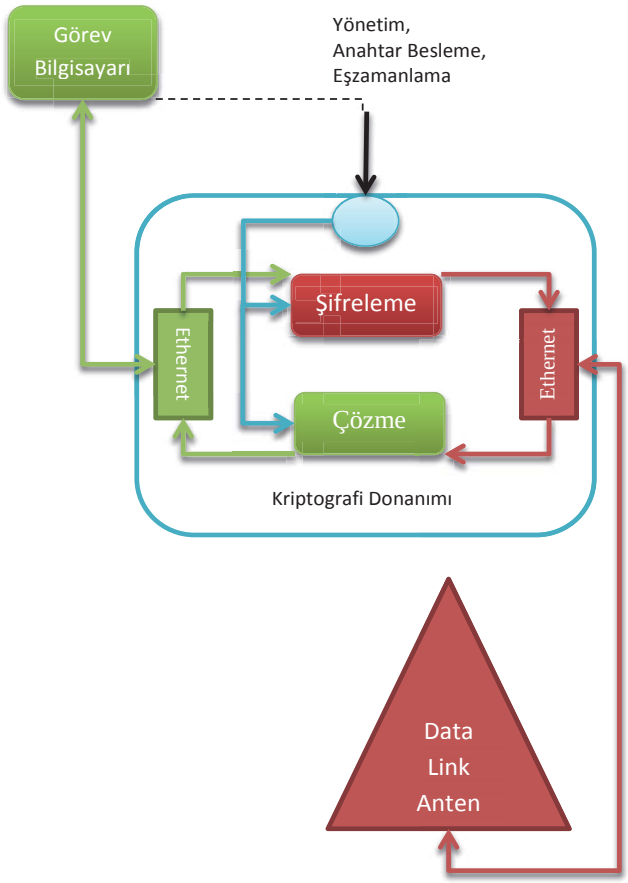
Söz konusu kriptografi donanımı; muharip hava platformunun görev bilgisayarından gelen verileri şifreleyip Data Link antenine, diğer muharip hava platformuna veya yer istasyonuna göndermek üzere iletmekle ve bunun tersi olarak Data Link anteninden gelen verileri çözüp görev bilgisayarına iletmekle yükümlüdür. Bahsi geçen kriptografi donanımının yapısı şekil 4'te sunulmaktadır.

FPGA üzerinde gerçeklenen kriptografi donanımı, veri alış-verişinde Ethernet arayüzünü kullanmaktadır. Donanımın üzerinde iki adet Ethernet arayüzü bulunmaktadır. Bunlardan bir tanesi görev bilgisayarı ile veri alış-verişini sağlarken diğeri Data Link ile veri alış-verişini sağlamaktadır. Şekil 4 üzerinde, yeşil renk ile gösterilen hatlar şifrelenmemiş veri akışını, kırmızı ile gösterilen hatlar ise şifrelenmiş veri akışını ifade etmektedir. Buna göre; görev bilgisayarından, başka bir muharip hava platformunun görev bilgisayarına veya yer istasyonuna gönderilmek istenen veri öncelikle Ethernet arayüzünden kriptografi donanımına iletilir. Uygun zamanlama sağlanacak şekilde bu veriler arabellekte (buffer) tutularak şifreleme birimine iletilir. Burada şifrelenen veri uygun zamanlama için arabellekte biriktirilerek ikinci Ethernet arayüzü yardımıyla Data Link antenine iletilir. Burada radyo dalgalarına çevrilen veri diğer platforma veya yer istasyonuna iletilir. Tersi durumda ise; platforma Data Link vasıtasıyla gelen veri Ethernet arayüzüyle alındıktan sonra arabellekte bekletilerek çözme birimine ulaştırılır. Çözme biriminde şifrelenmiş veriden iletilmek istenen veri elde edilerek arabelleğe ve oradan da Ethernet arayüzü vasıtasıyla görev bilgisayarına aktarılır. Ethernet veri akışının üst seviye görünümü şekil 5'te sunulmaktadır.

A. Şifreleme Algoritmasının Gerçeklenmesi

Sistemde kullanılacak şifreleme algoritması AES-256 olarak seçilmiştir. Data Link için bant genişliği DLS sistem mimarisinin elverdiği ölçüde yaklaşık 6 Mbit/s'dir. DLS'nin esnek yapısı sayesinde, mesafe değiştikçe bant genişliği en uygun seviyeye getirilebilmektedir. Bu sebeple; göreceli olarak çok yüksek bant genişliklerine ihtiyaç duyulmaması hesaba katılarak donanım düşük frekansta çalıştırılarak uçak üzerinde oldukça önemli bir konu olan güç tüketiminin de daha uygun bir seviyeye getirlmesi sağlanabilmektedir.

AES-256 algoritması FPGA üzerinde gerçeklenirken, bayt değiştirme dönüşümünü için 16 adet özdeş S-kutusu (S-box)



Şekil. 4. Kriptografi Donanımı Yapısı

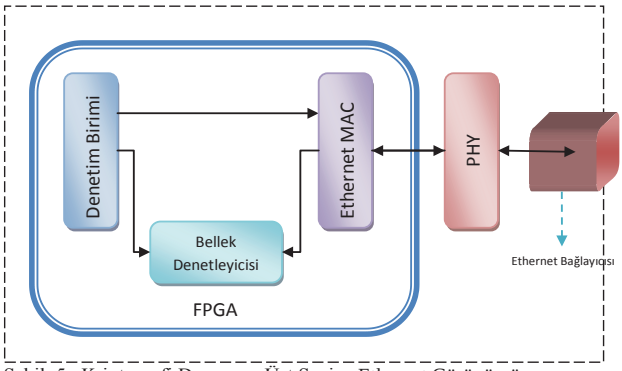
paralel olarak kullanılmıştır. Her bir S-kutusu, FPGA içerisinde birer ROM olarak gerçeklenmiştir. Bu sayede; 128 bitlik bir veri için bayt değiştirme işleminin yalnızca bir saat vuruşu kadar zaman alması sağlanmıştır. Aynı şekilde satır kaydırma işlemi de her bir döngü kütüğü (block) için bir saat vuruşunda yapılabilmektedir. Sütün karıştırma işleminde ise saatten bağımsız bir donanım tasarlanmıştır. Bu dönüşüm, saatten bağımsız olarak gerçekleştirilen en karmaşık bileşen olduğundan, tüm donanımın frekans kısıtının belirlenmesinde önemli rol oynamaktadır. Yalnızca anahtar değişikliği olacağı zaman çalışacak olan anahtar genişletme birimi de aynı paralellikle FPGA üzerindeki mevcut alan gözetilerek tasarlanmıştır [10].

B. Anahtar Yönetimi

Sistemde kullanılacak 256 bitlik anahtarlar iki farklı şekilde elde edilebilmektedir.

Bunlardan ilkinde; kriptografi donanımı üzerinde bulunan seri arayüz kullanılarak, sistemin kullanacağı anahtarlar ve varsa bu anahtarların kullanılacağı zaman bilgileri aktarılır. Bu bilgiler uçuş öncesinde bir USB depolama aygıtına aktarılarak pilota veya diğer yetkili uçuş personeline ilgili sokete takması amacıyla, yetkili kişiler tarafından, yetkili donanımlar kullanılarak güvenli bölgede oluşturularak verilir. Anahtarlar her bir unsurla (diğer hava platformları ve yer istasyonları) haberleşmek için farklı farklı olabileceği gibi, tüm ağda kullanılacak tek bir anahtar da olabilmektedir. Anahtarlar uçuş esnasında pilot isteğine bağlı olarak devingen bir şekilde değişebilmekte veya öntanımlı zaman verileri kullanılarak uygun zamanda sistem tarafından değiştirilebilmektedirler. İstendiği takdirde; bu devingen anahtar değişim kontrolü, görev bilgisayarı üzerindeki yazılım tarafından da, uçuş esnasında elde edilen çeşitli değişkenler yardımıyla, değiştirilebilmektedir.

İkinci yöntemde ise anahtar belirleme amacıyla, Diffie-Hellman protokolü kullanılmaktadır [11]. Bu sayede; muharip hava platformları ve yer istasyonları, güvensiz bir kanal üzerinden devingen olarak güvenli birer anahtar oluşturabilmektedirler. Bu durumda da anahtar zamanlama yönetimi diğer durumla aynı özelliklere sahip olup, ister öntanımlı olarak ister pilot kararı veya yazılım kararıyla yapılabilinmektedir.



Şekil. 5. Kriptografi Donanımı Üst Seviye Ethernet Görünümü

Anahtar girdisinin, sistem yönetiminin ve zamanlama denetiminin yapılabileceği arayüz ve ilgili hatlar şekil 4'te mavi renkle işaretlenmiştir. Kriptografi donanımının her türlü denetimi, uçuş esnasında pilot tarafından da MFD (Multi Function Display) sayfaları yardımıyla yapılabilmektedir.

IV. SONUÇ

AES algoritmasının donanımsal gerçeklemesi yapılırken düşük frekansta yüksek hız kısıtı gözetilmiştir. Boru hattı mimarisiyle paralel olarak tasarlanan donanım, düşük frekansta gereksinimlerinin çok üzerinde bir bant genişliğiyle şifreleme/çözme yapabilme yeteneğine sahip olduğundan, uçak üzerinde en düşük seviyede tutulması gereken güç tüketimi yönünden oldukça olumlu bir başarıma sahip olabilmektedir.

Kriptografi donanımının gerçeklenmesi sonucunda, 16 MHz gibi düşük bir saat sıklığı kullanılarak yaklaşık olarak 120 Mbit/s veri akış hızına ulaşılmıştır. Şifreleme ve çözme donanımı, 10Gbit/s'den daha fazla bir bant genişliğine sahip olması gerekmeyeceği için, FPGA üzerinde oldukça düşük bir alana sahip olmaktadır. Bu sebeple sistem, daha düşük maliyetli FPGAlar üzerinde de rahatlıkla gerçeklenebilmektedir. AES algoritmasının farklı FPGAlar üzerinde veri akış hızları ve kapladığı alanlar Tablo 1'de sunulmaktadır.

Tablo 1'de görüldüğü üzere; göreceli olarak düşük maliyetli bir FPGA (Cyclone III EP3C16F256C8N) oldukça düşük bir frekansta (16MHz) kullanılarak istenilen veri akış hızından daha yüksek bir veri akış hızı sunmaktadır. Saniyede 1 Gb'den daha yüksek veri akış hızları istendiği

TABLO I
AES-256 GERÇEKLEMESININ FARKLI FPGALAR ÜZERINDEKI DEĞERLERI

FPGA	Frekans (MHz)	Kapladığı Alan (%)	Veri Akışı (Mb/s)
Cyclone III EP3C16F256C8N	118.45	14	891.86
Spartan III XC3S2000-5	85.80	< 5	646.02
Virtex 6 XC6VLX550T-2	368.84	< 1	2777.15
Cyclone III EP3C16F256C8N	16	14	120.47

durumda ise; donanım tasarımında ve tanımlamalarında herhangi bir değişiklik yapılmaksızın yalnızca FPGA değiştirilerek (örneğin Virtex 6 XC6VLX550T-2 kullanılarak) istenen veri akış hızları sağlanabilmektedir. Tablo 2'de, yapılan FPGA gerçeklemesinin diğer çalışmalarla karşılaştırılması sunulmaktadır.

TABLO II
AES-256 GERÇEKLEMESININ FARKLI ÇALIŞMALAR İLE KARŞILAŞTIRILMASI

Gerçekleme →	Good [12]	Chodowiec [13]	Rouvroy [14]	Bu Çalışma
FPGA	XC2S15-6	XC2S30-6	XC3S50-4	XC3S2000-5
Frekans (MHz)	67	60	71	85.8
Veri Akışı (Mb/s)	2.2	166	208	646

Sonuç olarak DLS projesi kapsamında kriptografi donanımından beklenen bant genişliği ve frekans değerleri sağlanmakta ve esnek tasarımı sayesinde çok geniş bir aralıkta bu değerlerle oynanabilmektedir

KAYNAKLAR

[1] Kılıç, A., Canberi H., "Muharip Hava Platformları için Gömülü Eğitim/Simülasyon Sistemi", Savunma Teknolojileri Kongresi, SAVTEK, 2012.
[2] Forte, D., The future of the advanced encryption Standard, Network Security, 1999(6), 10-13, 1999.
[3] National Institute of Standards and Technology, Advanced Encryption Standard, FIPS PUB, 197, USA, 2001.
[4] Bruen, A. A., Forcinito, M. A., Cryptography, Information Theory, and Error-Correction : A Handbook fort he 21st Century, Wiley-Interscience, USA, 2005.
[5] Yavuz, M.H., Ergin, O., Verileri Nota Kullanarak Şifreleme ve Ses Dosyası İçerisine Gizleme, 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara", 2008.
[6] Advanced Encryption Standard, Federal Information Processing Standards Publication 197, November, 2001.
[7] S. M. Yoo, D. Kotturi, D. W. Pan, J. Blizzard, "An AES crypto chip usinga high-speed parallel pipelined architecture", Microprocessors and Microsystems, 29(7), pp. 317-326, 2005.
[8] Chu, P.P., FPGA Prototyping by Verilog Examples, Wiley & Sons, New Jersey, 2008.
[9] Türkay, K. D., Canberi, M. H., Kılıç, A., "Görev Kritik Sistemler Açısından DDS Arakatman Mimarisinin Performans Analizi", 5. Ulusal Savunma Uygulamaları Modelleme ve Simülasyon Konferansı, Ankara, 2013.
[10] Yavuz, M. H., "Müzikle Şifreleme-Veri Gizleme Sistemi Tasarımı ve Gerçaklenmesi", Yüksek Lisans Tezi, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara, 2010.
[11] Diffie, W., Hellman, M. E., New directions in cryptography, IEEE Transactions on Information Theory, 22(6), 644-654, 2006.
[12] Good, T., Benaissa, M., AESon FPGA from the Fastest to the Smallest, Cryptographic Hardware and Embedded Systems (CHES 2005), 3659, 427-440, 2005.
[13] Chodowiec, P., Gaj, K., Very Compact FPGA Implementation of the AES Algorithm, Cryptographic Hardware and Embedded Systems, 2779, 319-333- Springer-Verlag, 2003.
[14] Rouvroy, G., Standaert, F. X., Quisquater, J. J., Legat, J. D., Compact efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications, Procedings of the International Conference on Information Technology: Coding and Computing 2004 (ITCC '04), 2, 583-587, 2004

Hücresel Otomata ve Kaos Tabanlı Bir Şifreleme Algoritmasının Güvenlik Analizi

Fatih Özkaynak, Ahmet Bedri Özer, Sırma Yavuz

***Özet*—Kriptolojik sistemlerin tasarımında kaos teorisinin iyi bir uygulama alanı olmasına rağmen birçok uygulama güvenli iletişim için yetersiz kalmaktadır. Çünkü kriptanaliz çalışmaları yetersizdir. Zayıf önerilerin ortaya çıkmasındaki en önemli sebep şifreleme algoritmalarının güvenlik analizinin sadece istatistiki testler ve deneysel sonuçlar ile yapılmasıdır. Machicao ve arkadaşları bir şifreleme algoritması önermişlerdir. Önerilen şifreleme algoritmasının güvenlik analizleri sadece istatistiksel testler kullanılarak yapılmıştır. Bu çalışmada önerilen algoritmanın güvenlik zayıflıkları analiz edilmiştir. Önerilen algoritma için iki farklı saldırı gerçekleştirilmiştir. İlk saldırıda şifreleme algoritmasının gizli anahtarı sadece bir açık/şifreli veri çifti kullanılarak nasıl elde edilebileceği gösterilmiştir. İkinci saldırıda sözde rasgele üretecin çekirdek değerleri kullanılarak lojistik haritanın anahtar uzayının nasıl indirgenebileceği gösterilmiştir. Bu saldırı ile tüm olası çekirdek değerleri açığa çıkarılmıştır.**

***Anahtar Kelimeler*— Kaos; Kriptoloji; Hücresel otomata; Kriptanaliz**

***Abstract*— Although chaos theory is a good application field in the design of cryptographic systems, many proposals become unsatisfactory for secure communication since cryptanalysis studies are not sufficient. One of the important factors resulting in poor proposals is the fact that security analysis of the encryption algorithms is performed with only statistical tests and experimental results. An encryption algorithm was proposed by Machicao et al. Security analyses of the proposed encryption algorithm were done only by using statistical tests. In this study, we analyze the security weaknesses of the proposed algorithm. Two different attacks have been carried out for proposed algorithm. The first attack has shown that how to obtain the secret key of encryption algorithm using only one plaintext/ciphertext pairs. The second attack has shown that how to reduce key space of logistic map, which is used in seed values for pseudo random generator. All possible seed values have been revealed with this attack.**

***Index Terms*— Chaos; Cryptography; Cellular automata; Cryptanalysis**

I. GİRİŞ

AĞ ve iletişim teknolojilerindeki hızlı gelişmeler ile birlikte günlük yaşantımız büyük ölçüde sayısallaşmıştır. Sayısal ortamlarda kritik öneme sahip verilerin işlenmesi, depolanması ve iletilmesi ile bu verilerin güvenliğinin nasıl sağlanacağı sorusunu ön plana çıkarmıştır [1]. Araştırmacılar güvenlik problemini çözebilmek için geleneksel kriptolojik çözümlere alternatif olabilecek etkili, hızlı ve gürbüz algoritmalar geliştirme arayışı içerisine girmiştir. Bu doğrultuda kaos tabanlı kriptoloji çalışmaları da son yirmi yılda önemli bir ilgi odağı olmuştur [2-8].

Kaotik sistemlerin doğrusal olmaması, gürültü benzeri periyodik olmayan bir davranış göstermesi ve başlangıç koşullarına hassas duyarlılığı gibi özellikleri kullanılarak kriptolojik protokollerin tasarlanması birçok araştırmacının ilgisini çekmiştir. Ancak protokollerin analiz çalışmaları ve kriptolojik tasarım süreci yeterince irdelenmediğinden birçok önerinin basit bilinen saldırılara karşı zayıf olduğu gösterilmiştir [9-17].

Machicao ve arkadaşları [18] hücresel otomatanın kaotik davranış göstermesinden yola çıkarak yeni bir kaos tabanlı şifreleme algoritması önermişlerdir. Önerilen yöntemin güvenlik analizleri çeşitli istatistiki testler ile yapılmıştır. İstatistiki analizler sonucunda önceki önerilere göre daha iyi sonuçlar elde edilmiştir. Ancak istatistiki testler bir şifreleme algoritmasının sağlaması gereken unsurlardan biri olmasına rağmen tek başına yeterli değildir.

Bu çalışmada Machicao ve arkadaşları tarafından önerilen algoritmanın detaylı güvenlik analizleri yapılmıştır. İlk saldırıda; sadece bir adet açık/şifreli veri çifti kullanılarak şifreleme algoritmasının gizli anahtarının nasıl elde edilebileceği gösterilmiştir. İkinci saldırıda ise algoritmada rasgele sayı üreteci için çekirdek değerleri üretmede kullanılan lojistik haritanın anahtar uzayının nasıl indirgeneceği gösterilmiştir. Bu saldırı ile üretilebilecek olası bütün çekirdek değerleri açığa çıkarılmıştır. Yapılan analiz çalışmaları sonucunda önerilen yöntemin güvenli iletişim için uygun olmadığı gösterilmiştir.

Çalışmanın geri kalan kısmı aşağıdaki gibi organize edilmiştir. İkinci bölümde analiz edilen algoritmanın yapısı kısaca özetlenmiştir. Üçüncü bölümde analiz edilen algoritmaya yapılan saldırıların mantığı açıklanmıştır. Son bölümde elde edilen sonuçlar tartışılmıştır.

II. ALGORİTMANIN YAPISI

Machicao ve arkadaşları kabaca şekil 1'de gösterildiği gibi bir blok şifreleme algoritması önermişlerdir [18]. Algoritmada her bir blok şifrelenirken anahtar ve kendinden önce şifrelenen blok kullanılmaktadır. Algoritmanın matematiksel gösterimi Denklem 1 ve Denklem 2'de verilmiştir. Önerilen algoritmanın yeniliği ise her bir bloğun şifrelenmesinde kullanılan anahtarların üretim mantığında gizlidir. Machicao ve arkadaşları anahtar üretimi için üç

Fatih Özkaynak, Fırat Üniversitesi Yazılım Mühendisliği Bölümü 23119 Elazığ Türkiye (iletişim yazarı tel: 424-2370000/4241; e-posta: ozkaynak_fatih@hotmail.com).

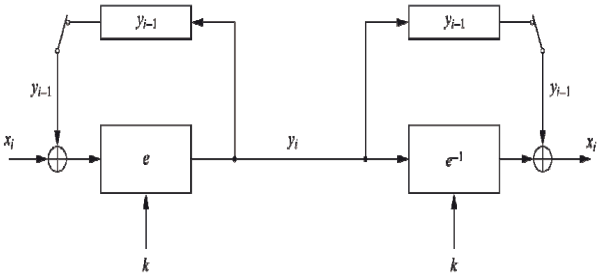
Ahmet Bedri Özer, Fırat Üniversitesi Bilgisayar Mühendisliği Bölümü 23119 Elazığ Türkiye (e-posta: bedriozer@firat.edu.tr).

Sırma Yavuz, Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü 343349 İstanbul Türkiye (e-posta: sirma@ce.yildiz.edu.tr).

aşamalı bir yöntem kullanmışlardır. Her bir aşamada gerçekleştirilen işlemlerin listesi aşağıda adım adım verilmiştir.

$$y_1 = k_1 \oplus x_1 \quad (1)$$

$$y_i = k_i \oplus x_i \oplus y_{i-1}, \quad i > 1 \quad (2)$$



Şekil 1. Şifreleme algoritmasının genel yapısı

Birinci aşama içerinde yapılan işlemler

1. Şifreleme algoritmasının gizli anahtarı olarak 128 bit uzunluğunda bir değer belirlenir.
2. Denklem 3, 4 ve 5 kullanılarak π gizli anahtarından kaotik sistemin başlangıç koşulu x_0 belirlenir.

$$\Omega := \sum_{i=1}^{size(\vec{\pi})} 2^{8*(i-1)} \pi_i \quad (3)$$

$$\Omega = \frac{\Omega}{2^{(8*size(\vec{\pi})+1)}} \quad (4)$$

$$X_0 = \Omega + 0.00001 \quad (5)$$

3. Lojistik harita itere edilir. İlk 1000 iterasyon geçici etkilerin ortadan kalkması için alınmaz.
4. Denklem 6'da verilen niceleme mantığı kullanılarak [0, 1] aralığında üretilen sürekli değerler binary değerlere ayrıklaştırılır.

$$\begin{cases} 1 & if\ X_k < 0.5 \\ 0 & if\ X_k \geq 0.5 \end{cases} \quad (6)$$

5. Lojistik haritanın iterasyonları sonucunda m×n boyutunda binary bir dizi üretilir.

İkinci aşama içerisinde yapılan işlemler

1. m×n boyutundaki binary dizi hücresel otomatın başlangıç değerleri olarak atanır.
2. Doğal hücresel olguları modellemede kullanılan "Gam-of-Life" kuralları kullanılarak yeni jenerasyonlar üretilir. Farklı kuralların kullanılması farklı jenerasyonların elde edilmesine sebep olmaktadır. Detaylar için kaynak [18] incelenebilir.
3. Şifreleme algoritmasında yeni popülasyonların üretilmesi için 64×64 boyutunda bir hücresel otomata ve B1357/S2468 kuralı kullanılmıştır

Üçüncü aşama içerisinde yapılan işlemler

1. 64×64 boyutundaki hücresel otomat bloklara ayrılır.
2. Elde edilen bloklara XOR işlemi uygulanarak her bir bloğun şifrelenmesinde kullanılacak anahtar değeri üretilir.

Anahtar değerinin üretilmesinin ardından Denklem 1 ve Denklem 2'de verilen yapı kullanılarak her bir bloğun şifrelenmesi işlemi gerçekleştirilir.

III. Güvenlik Analizi

A. *Saldırı Senaryosu 1*

Şifreleme sistemlerinin temel gereksinimleri olan karıştırma ve yayılma özelliklerini sağlamak için; doğrusal olmayan dinamikler, kaos, DNA işlemleri ve hücresel otomatlar gibi yapıların teorik olarak zengin dinamikler sunması birçok araştırmacıyı bu konuda çalışmaya yönlendirmiştir. Ancak araştırmacıların genel eğilimi bu yapıları farklı tasarımlarda değişik biçimde kullanarak yeni şifreleme sistemleri geliştirme yönünde olmuştur. Buda kriptolojik tasarım sürecinin gözden kaçırılmasına ve birçok bilinen basit saldırıya karşı zayıf önerilerin ortaya çıkmasına sebep olmuştur [19, 20].

Machicao ve arkadaşları da kaos, hücresel otomata ve Game-of-Life süreçlerini kullanarak şifreleme algoritmasının her bir bloğunda kullanılmak üzere bir anahtar üreteci tasarlamışlardır. Üretilen anahtarlar istatistiki olarak birçok rasgelelik testini geçmesine rağmen şifreleme siteminin cebirsel bağımlılıklar içermesi sonucunda sadece bir adet açık/şifreli veri çiftinin bilinmesi durumunda anahtar değeri elde edilebileceği gösterilmiştir. Denklem 1 ve Denklem 2'de genel yapısı verilen şifreleme algoritması daha açık biçimde Denklem 7'deki gibi yazılabilir. Denklem 7'de XOR işleminin birleşme özelliği kullanılarak yeniden düzenlenirse Denklem 8'deki gibi şifreleme algoritmasının daha basit bir ifadesi ortaya çıkmaktadır.

$$y_i = k_i \oplus x_i \oplus k_{i-1} \oplus x_{i-1} \oplus \ldots \oplus k_2 \oplus x_2 \oplus k_1 \oplus x_1 \quad (7)$$

$$y_i = (k_i \oplus k_{i-1} \oplus \ldots \oplus k_2 \oplus k_1) \oplus (x_i \oplus x_{i-1} \oplus \ldots \oplus x_2 \oplus x_1) \quad (8)$$

En basit saldırı yöntemlerinden biri bilinen açık metin saldırısıdır. Bu saldırıda, saldırgan özel seçtiği bir açık metine karşılık gelen şifreli metni bulur. Açık/şifreli veri çiftlerini kullanarak algoritmanın gizli parametresi olan anahtarı elde etmeye çalışır. Denklem 8'de elde edilen yapı için açık/şifreli veri çiftleri denklemde yerine yazılırsa algoritmanın gizli parametresi olan anahtar değerleri açığa çıkarılmış olur. Anahtar değerine sahip olan bir kişi istediği herhangi bir veriyi şifreleyebilir veya şifresini çözebilir.

Saldırı sonucunda görülmüştür ki; şifreleme algoritması içerisinde kullanılan yapıların kriptolojik olarak güçlü karakteristiklere sahip olması gerekmektedir. Ancak ne kadar güçlü yapılar kullanılırsa kullanılsın asıl önemli olan bu yapıların kriptolojik tasarım sürecinde nasıl kullanıldığıdır.

B. *Saldırı Senaryosu 2*

Kerckhoffs prensibine göre bir şifreleme algoritmasında anahtar dışında her şey açık olmalıdır. n-bitlik gizli anahtara

sahip bir şifreleme algoritmasında anahtar uzayı 2^n'dir. Anahtar uzayındaki olası bütün anahtarların denenmesi ile yapılan saldırı kaba kuvvet saldırısı olarak adlandırılmaktadır. Modern şifreleme algoritmaları için 128-bitlik anahtar uzunluğu kaba kuvvet saldırısını önlemektedir. Analiz edilen algoritmanın anahtar boyu 128-bit olarak belirlendiği için kaba kuvvet saldırısı mantıksızdır [21, 22].

Kriptanalistin amacı kaba kuvvet saldırısından daha az hesaplama maliyetine sahip bir yöntem olup olmadığının araştırılmasıdır. Algoritmada gizli anahtar Denklem 3, 4 ve 5'de gösterildiği gibi lojistik haritanın başlangıç koşullarının belirlenmesinde kullanılmıştır. Gizli anahtar boyutu 128-bit olduğu için lojistik haritanın başlangıç koşulu olarak 2^128 farklı durum söz konusudur. Kaotik sistemler başlangıç koşullarına hassas duyarlı olduğu için teorik olarak 2^128 farklı başlangıç koşulu için 2^128 farklı yörünge elde edilmesi gerekmektedir. Ancak pratik uygulamalar göz önüne alındığında hesaplama duyarlılığına bağlı olarak anahtar uzayının tahmin edilenden daha kısa olduğu bu saldırıda gösterilmiştir.

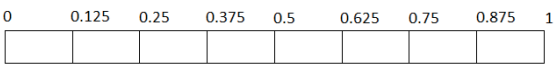
Lojistik harita [0,1] aralığında sürekli değerler almaktadır. Ancak hesaplamaların yapıldığı makinanın hesaplama duyarlılığına bağlı olarak bir sayısal kötüleşme meydana gelmektedir. Hesaplamalarda virgülden sonraki k dijit kullanılıyorsa (k+1). dijit için bir yuvarlama hatası meydana gelecektir. Örneğin hesaplama duyarlılığının virgülden sonraki 3 dijit kullanılarak yapıldığını varsayalım. Olası başlangıç değerlerinin sayısı 2^3=8'dir. Ancak teoride olası başlangıç değerlerinin sayısı n>8 olduğu için güvercin deliği prensibine göre bu başlangıç değerlerinden üretilen yörüngelerde bir çakışma meydana gelecektir. Önerilen saldırı senaryosunun temeli de bu sayısal kötüleşmeden dolayı yörüngelerin birbiriyle çakışmasına ve olası anahtar uzayının teorik hesaplamalardan daha düşük olduğunun gösterilmesine dayanmaktadır.

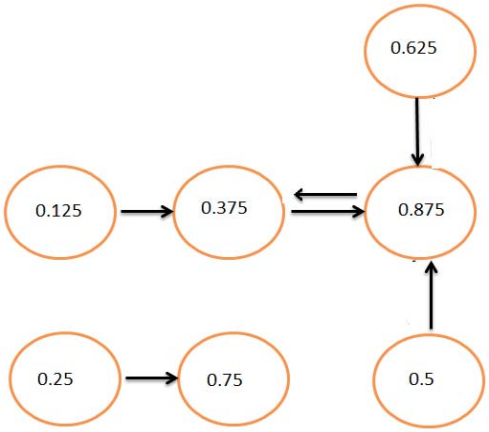
Şekil 2'de 3 bit duyarlılığa sahip bir makine üzerinde lojistik haritanın yörüngelerinin değişimi gösterilmiştir. Şekil 2.(a)'da [0, 1] aralığı 2^3=8 parçaya bölünerek aralıkların alt ve üst limitleri belirlenmiştir. Ardından her bir aralık başlangıç değeri olarak Denklem 9'da verilen lojistik harita için kullanılmış ve çıkış değeri elde edilmiştir. Elde edilen çıkış değeri hangi aralığa denk geliyorsa çıkış değeri o aralığa yuvarlanmıştır. Periyodik bir çevrim bulununcaya kadar iterasyonlara devam edilmiştir.

Örneğin x_0=0.125 başlangıç koşulu için denklem 9 çalıştırılırsa x_1=0.4375 olarak hesaplanmaktadır. Bu değer hesaplama duyarlılığına bağlı olarak 0.375 olarak alınmaktadır. 0.375 değeri için x_2=0.9375 olarak hesaplanır. x_2 değeri de hesaplama duyarlılığına bağlı olarak 0.875 olarak alınmaktadır. 0.875 değeri kullanılarak x_3 değeri hesaplanırsa bir çevrim bulunur.

$$X_{k+1} = 4 * X_k * (1 - X_k) \quad (9)$$

Şekil 2 3-bit hesaplama duyarlılığı için yörüngelerin değişimi gösterilmiştir.





Şekil 2 3-bit hesaplama duyarlılığı için yörüngelerin değişimi

Şekil 2'den görülebileceği gibi teorik olarak 8 farklı başlangıç durumu için 8 farklı yörünge oluşması beklenirken 3 bit hesaplama duyarlılığı için sadece 2 farklı yörünge elde edildiği görülmektedir. Çalışmada gösterim basit olması açısından 3-bit hesaplama duyarlılığı seçilmiştir. Hesaplama hassasiyetinin arttırılmasıyla birlikte farklı yörüngelerin sayısının atması beklenirken bu işlemin her zaman için geçerli olmadığı deneysel sonuçlarla gösterilmiştir. Örneğin hesaplama duyarlılığı 5-bit seçildiğinde maksimum uzunluklu periyot çevrimi 8 iken hesaplama duyarlılığın 6'ya çıkarıldığında maksimum uzunluklu periyot çevriminin 7 olduğu gözlemlenmiştir.

Lojistik haritanın yörüngelerinin çakışması sonucunda hücresel otomatatın başlangıç değerleri aynı olacaktır. Aynı değerler aynı anahtları üreteceğinden anahtar uzayında bir daralma meydana gelecektir. Buda kaba kuvvet saldırılarını mümkün kılacaktır.

IV. SONUÇLAR

Kaos ve kriptoloji bilimleri benzer özellikler göstermesinden dolayı aralarında güçlü bir bağlantı vardır. Ancak iki disiplin arasındaki benzerliklerin yanı sıra farklılıklarda detaylı olarak irdelenmelidir. İki disiplin arasındaki en dikkat çekici ayrımlardan biri kaotik sistemlerin faz uzayının reel sayılar üzerinde tanımlı olmasına rağmen kriptolojik sistemlerin tam sayıların bir kümesini temel alarak tasarlanmasıdır. Dolayısıyla kaotik sistemler kriptolojik uygulamalarda kullanılacaksa bir ayrıklaştırma işlemine gereksinim duyulmaktadır. Ayrıklaştırma işlemi sonucunda bir sayısal kötüleşme meydana geleceği hem teorik hem de pratik olarak bilinmektedir. Sonuç olarak kaotik sistemler yeni kriptolojik sistemlerin tasarımında kullanılacaksa sayısal kötüleşmenin etkileri iyi incelenmelidir. Bu çalışmada hesaplama duyarlılığına bağlı olarak sayısal kötüleşmeden dolayı olası anahtar uzayının teorik hesaplamaların altında olduğu ve bu değerin güvenli iletişim için uygun olmadığı gösterilmiştir.

Çalışmada gösterilen diğer bir saldırı ise şifreleme algoritmasının cebirsel bağımlılıklar içermesidir. Bu sadece kaos tabanlı kriptolojik tasarımlar için değil genel olarak dikkat edilmesi gereken bir konudur. Çünkü kriptanalist bir sistemi analiz ederken tasarımda çok güçlü kriptolojik

elemanların kullanılmasıyla ilgilenmez. Kriptanalistin asıl hedefi elemanların kullanım biçimindeki zayıflıkları ortaya çıkarmak olduğu unutulmamalıdır.

KAYNAKLAR

[1] Katz, J., Lindell, Y., (2008). Introduction to modern cryptography: principles and protocols, Chapman & Hall.

[2] Alvarez, G., Li, S., (2006). Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos, 16/8, 2129–2151.

[3] Amigo, J. M., Kocarev, L., Szczapanski, J., (2007). Theory and practice of chaotic cryptography, Physics Letters A, 366, 211-216.

[4] Fridrich, J., (1998). Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8/6, 1259–1284.

[5] Patidar, V., Pareek, N.K., Sud, K.K., (2009). A new substitution-diffusion based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation, 14/7, 3056–3075.

[6] Liu, L., Zhang, Q., Wei, X., (2012). A RGB image encryption algorithm based on DNA encoding and chaos map, Computers & Electrical Engineering, 38/5, 1240-1248.

[7] Zhu, C., (2012). A novel image encryption scheme based on improved hyperchaotic sequences, Optics Communications, 285/1, 29-37.

[8] Hu, H., Liu, L., Ding, N., (2013). Pseudorandom sequence generator based on Chen chaotic system, Computer Physics Communications 184 (3) 765–768

[9] Özkaynak, F., Özer, A. B., Yavuz, S., (2012). Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences, Optics Communications, 285, 4946–4948.

[10] Rhouma, R., Solak, E., Belghith, S., (2010). Cryptanalysis of a new substitution–diffusion based image cipher, Communications in Nonlinear Science and Numerical Simulation, 15/7, 1887-1892.

[11] Solak, E., Çokal, C., Yildiz, O.T., Biyikoglu, T., (2010). Cryptanalysis of fridrich's chaotic image encryption, International Journal of Bifurcation and Chaos, 20/5, 1405–1413.

[12] Özkaynak, F., Özer, A. B., Yavuz, S., (2012). Cryptanalysis of Bigdeli algorithm using Çokal and Solak attack, International Journal of Information Security Science, 1/3, 79-81.

[13] Özkaynak, F., Özer, A. B., Yavuz S., (2013). Security problems of pseudorandom sequence generator based on Chen chaotic system, Computer Physics Communications 184, 2178–2181.

[14] Özkaynak, F., Özer, A. B., Yavuz S., (2013). Security Analysis of An Image Encryption Algorithm Based on Chaos and DNA Encoding, 21th IEEE Signal Processing and Communications Applications Conference, Cyprus.

[15] Özkaynak, F., Özer, A. B., Yavuz S., (2013). Kriptolojik Uygulamalarda İstatistiki Rasgelelik Testlerinin Problemleri, Kripto Günleri, Bilgem/Tübitak.

[16] Özkaynak, F., Özer, A. B., Yavuz S., (2012). Differential Cryptanalysis of Block Ciphers Based on Randomly Selected Substitution Boxes, 5th International Conference on Information Security and Cryptology, Ankara, Turkey

[17] Özkaynak, F., Özer, A. B., Yavuz S., (2012). Analysis of Chaotic Methods for Compression and Encryption Processes in Data Communication, 20th IEEE Signal Processing and Communications Applications Conference, Muğla, Turkey.

[18] Machicao, J., Marco, A. G., Bruno, O. M., (2012). Chaotic encryption method based on life-like cellular automata, Expert Systems with Applications, 39/16, 12626–12635.

[19] Alvarez, G., Amigo, J. M., Arroyo, D., Li, S., (2011). Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers. In: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications (pp. 257-295). Springer-Verlag.

[20] Solak, E., (2011). Cryptanalysis of Chaotic Ciphers. In: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications (pp. 227-256). Springer-Verlag.

[21] Bard, G. V., (2009). Algebraic Cryptanalysis, Springer

[22] Joux, A., (2009). Algorithmic cryptanalysis, Chapman & Hall.

Son işlemin Gerçek Rasgele Sayı Üreteçleri Üzerindeki Etkisinin İncelenmesi

Erdinç AVAROĞLU, Mustafa TÜRK

***ÖZET*— Rasgele sayı üreteçlerinden elde edilen sayılar bilgi güvenliği anlamında kriptoloji alanında güvenlik açısından bir zorunluluktur. Bu güvenliğin sağlanabilmesi için elde edilen sayıların kestirilememesi, tekrar üretilememesi ve iyi istatistiksel özellikleri sağlaması gerekmektedir. Bu gereksinimlerin sağlaması amacıyla gerçek rasgele sayı üreteçleri kullanılmıştır. Ancak gerçek rasgele sayı üreteçlerinden elde edilen bit dizilerinin bazıları zayıf istatistiki özellikler göstermiştir. Bu nedenle bu eksikliğin giderilmesi amacıyla çeşitli son işlem algoritmaları uygulanmıştır. Bu çalışmada, yeni bir son işlem algoritması önerilmiş ve bunun kısmi istatiksel analizi yapılmıştır.**

Anahtar Kelimeler — Rasgele sayı Üreteçleri, Son işlem, Kaotik çekerler.

***ABSTRACT*— The numbers which are obtained from random number generator is a obligation for the sense of security in the field of information security cryptology. To maintain this security, the numbers which are obtained must be unpredictable, unproducible second time and provide good statistical properties. To provide these needs, true random number generators are used. But some of the sequences from true random number generators have shown poor statistical futures. In order the eliminate this deficiency, various post processing algorithms have been applied. In this study, a new post processing algorithm was proposed and its partial statistical analysis was carried out.**

Keywords: Random number generator, Post Processing, Chaotic attractor

I. GİRİŞ

Rasgele sayı üreteçlerinden elde edilen sayılara istatistikte örnekleme, simülasyon, nümerik analiz, eğlence gibi alanlarda ve kriptografide ihtiyaç duyulmuştur. Özellikle rasgele sayılar çeşitli kriptografik uygulamalar için zorunluluktur. Çünkü kriptografi anahtarların üretimi ve dağıtımında, başlangıç vektörü oluşturulmasında, kimlik doğrulama protokollerinde, asal sayı ve şifre üretiminde rasgele sayılara ihtiyaç duyar. Bir kriptografik sistemin güvenliği elde edilen sayıların gerçek rasgeleliliğine dayanmaktadır. Bu sebepten dolayı kriptografik sistemlerde kullanılan rasgele sayıların bazı sıkı gereksinimleri sağlamaları gerekmektedir. Bu gereksinimler kestirilememe (tahmin edilememe), tekrar üretilememe ve iyi istatistiksel özelliklerdir [1].

E.Avaroğlu, İnönü Üniversitesi Bilgi İşlem Daire Başkanlığı, Malatya, TÜRKİYE. (Telefon: 04223773266, e-posta: erdinc.avaroglu@inonu.edu.tr)
M.Türk, Fırat Üniversitesi Elektrik Elektronik Mühendisliği, Elazığ, TÜRKİYE (Telefon: 424-2370000-5208, e-posta: mturk@firat.edu.tr)

Bu rasgele sayıların elde edilebilmesi amacıyla çeşitli rasgele sayı üreteçleri (RSÜ) geliştirilmiştir. Bu rasgele sayı üreteçleri gerçek rasgele sayı üreteçleri (GRSÜ), sözde rasgele sayı üreteçleri (SRSÜ) ve hibrit rasgele sayı üreteçleri olmak üzere sınıflandırılmıştır.

Sözde rasgele sayı üreteçleri herhangi bir başlangıç (tohum) değeri olmadan başlayamaz. Tohum rasgele seçilmiş olmalıdır. Belirlenen tohum değeri belirli bir algoritmaya tabi tutularak uzun rasgele sayı dizileri üretilmiştir. SRSÜ'nün avantajlı yanı diğer uygulamalara oranla ucuz olması, kolay gerçeklenebilir olması, hızlı olması ve donanım ihtiyacına gerek duymamasıdır. Ancak SRSÜ'ler ile üretilen sayılar tohum değeri tespit edildiğinde veya sistemde kullanılan fonksiyonlar yeterince karmaşık olmadığı taktirde tahmin edilebilmiştir. Ayrıca belli bir süre sonra üretilen dizi kendini tekrar etmeye (periyodiklik) başlamıştır. Belirtilen bu eksiklikler nedeniyle SRSÜ'ler kriptografik uygulamalar için uygun değildir [2-4].

Gerçek rasgele sayı üreteçleri gürültü kaynağı olarak kontrol edilemeyen ve kestirilemeyen gerçek fiziksel süreçleri kullanarak rasgele sayı üretmiştir. GRSÜ tarafından üretilen rasgele sayıların özellikleri ve rasgeleliliği fiziksel süreçlerin rasgeleliliğine bağlıdır. Kontrol edilemeyen fiziksel süreçler olduğu taktirde üretilen sayılarda kestirilemez ve kontrol edilemez. Ancak bazı üretilen bit dizisi istatistiki zayıflıklar göstermişlerdir. Bu zayıflıkların giderilmesi amacıyla üretilen bit dizisi son işleme tabi tutulmuştur. Son işlem uygulamaları zayıflıkları giderirken bit oranında azalmaya sebep olmuştur. GRSU yavaş, maliyetli ve donanıma bağımlı olması dezavantajlı tarafıdır. Ancak GRSÜ'ler kriptografik uygulamalar için zorunlu olan kestirilememe, tekrar üretilememe ve iyi istatistiki özellikleri sağlaması sebebiyle kriptolojide birçok uygulamada kullanılmıştır [1].

Hibrit rasgele sayı üreteci GRSÜ'den elde edilen rasgele sayının SRSÜ'de tohum değeri kullanılmasıyla her iki sistemin birlikte çalıştığı rasgele sayı üretecedir.

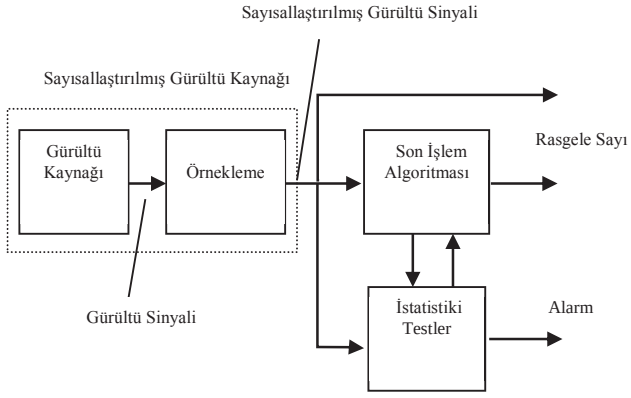
Kaotik sistemlerin en önemli özelliği başlangıç şartına bağlı olmalarıdır. Bu sistemler uzun dönemlerde tahmin edilemez davranışlar ve periyodik olmayan özellikler göstermişlerdir [5]. Kaotik sistemlerde elde edilen işaretlerin rasgele özellikler göstermesi (gürültü benzeri işaretler olması) nedeniyle gerçek rasgele sayı üreteçlerinde gürültü kaynağı olarak kullanılmışlardır. Ayrıca kriptolojide de kaos bir çok uygulamada kullanılmıştır [6,7].

Bölüm 2 de gerçek rasgele sayı üreteçlerinden ve son işlemden bahsedilmiştir. Bölüm 3'te rasgele sayı üretiminde kullanmış olduğumuz kaotik çekerlerden ve örnekleme işleminin nasıl yapıldığı açıklanmıştır. Bölüm 4'te elde edilen

bit dizisinin saf halinin ve son işlemden geçirilmiş halinin istatistiksel test sonuçları incelenmiştir. Bölüm 5'te sonuç verilmiştir.

II. GERÇEK RASGELE SAYI ÜRETECİ

Şekil1.'de GRSÜ genel tasarımı gösterilmiştir. GRSÜ'lerde entropi (gürültü) kaynağı deterministik olmayan doğal fiziksel olaylar olarak tanımlanmış ve rasgele sayı üretmede kullanılmıştır. Genellikle analog gürültünün dijital sinyale dönüşümünü içerir. İyi tasarlanmış bir GRSÜ'de bu entropi kaynağı, son işlemden geçirilen istatistiksel bağımsız bit dizilerini elde etmek için örneklenmiş ve gerçek rasgele sayı dizileri ile sonuçlanmıştır. Üretilen rasgele bitten bir sonraki bit tahmin edilememelidir ve aynı rasgele bitin üretilmesi engellenmiş olmalıdır. GRSÜ'lerde örnekleme işleminden sonra elde edilen rasgele bit dizisinde bulunan potansiyel zayıflıkları (bitler arası korelasyon olması) gidermek amacıyla elde edilen bit dizisi son işleme tabi tutulmuştur. Ancak bu işlem bit dizisinde ki zayıflıkları giderirken çıkıştaki bit oranını azaltmakta ve çalışma hızını düşürmekte olduğuna dikkat edilmelidir. Bu yüzden güçlü gürültü kaynakları kullanmak gerekmektedir [2,3,8].



Şekil 1. GRSÜ Genel Tasarımı

Gerçek rasgele sayı üretecinin temel blokları aşağıda açıklanmıştır.

A. *Gürültü (Entropi) Kaynağı*

GRSÜ'lerde kullanılan çeşitli tiplerde gürültü kaynakları bulunmaktadır. GRSÜ için entropi kaynağı fiziksel rasgelilik kaynağıdır. GRSÜ'lerde kullanılan gürültü kaynakları:

- Elektriksel Gürültü: Isıl gürültü, termal gürültü, saçma gürültüsü ve titreme gürültüsü kullanılmaktadır.
- Fotonların kuantum mekanik özellikleri
- Mekanik sistemler
- İnsan kaynaklı etkileşimler: fare ve klavye hareketleri

B. *Örnekleme(Sayısallaştırıcı)*

Örnekleyici gürültü sinyalinin gerekli örneklemesini yapmış ve fiziksel gürültü kaynakları için üretim mekanizması (Harvesting Mechanism) olarak adlandırılmıştır. Analog sinyalden sayısallaştırılmış sinyal üretir. Genellikle D-tip flip flop örnekleyici olarak kullanılmıştır. Gerilim kontrollü osilatörde bazı gürültü kaynakları için kullanılmıştır.

C. *Son İşlem (Post Processing)*

Son işlem genellikle sinyaldeki rasgeleliliği artırmak için kullanılmıştır. Son işlem uygulanmış sinyal değerleri saf sinyal ile karşılaştırıldığında düzenli (uniform) dağılımlıdır. Örneklenmiş rasgele sayı başına entropi artacaktır. Son işlemin aktif hata ve yan kanal analizi saldırılarından dolayı daha da önem kazanan ikinci amacı, saldırgan kurcalamaları ve çevresel değişikliklere karşı dirençli hale getirmesidir. Son işlem algoritmasına bağlı olarak üretecin güvenliği artmıştır. Xor doğrulama [9], von neumann doğrulama [10], H fonksiyonu [11] ve resilient fonksiyonlar [12] gibi çeşitli son işlem algoritmaları uygulanmıştır. Bu uygulamalardan en çok kullanılan 2 son işlem aşağıda açıklanmıştır ve yeni bir son işlem uygulaması önerilmiştir.

- **Xor Son İşlem :** Xor doğrulama bir çıkış biti üretmek amacıyla n bit (n=2) blok üzerinde xor işleminin uygulandığı basit doğrusal bir fonksiyondur. Çıkış bitindeki korelasyonu giderirken bir yandan da çıkış bit verimini 1/n kez azalmasına neden olmuştur. Ancak, çıkış bit dizisindeki korelasyon giriş bitlerinin bağımsız olması şartıyla düşmüştür. Bu doğrulamanın avantajı, basitliği ve sabit çıkış bit hızını sağlama olasılığıdır.
- **Van Neumann Son İşlem :** En eski ve en basit son işleme yöntemidir. Bit dizisindeki düzensizlikleri gidermiştir. Tablo 1'de gösterildiği gibi Van neumann düzgün dağılımlı 0 ve 1 bitleri üretmiştir. GRSÜ'den gelen eşzamanlı çiftleri dikkate almıştır. Eğer bit dizisi (1,0) ise 1 biti üretmiş, eğer bit dizisi (0,1) ise 0 biti üretmiştir. (0,0) ve (1,1) bit dizileri atılmıştır. Bu doğrulama entropiyi ideal değer 1'e yaklaştırarak ürettiği bitler ile entropinin iyileştirilmesine katkıda bulunmuştur. Ancak, GRSÜ'den gelen bazı bit dizilerinin atılmasından dolayı Van neumann çıkış bit hızı GRSÜ'nün çıkışına bağlıdır ve bundan dolayı sabit değildir. Bit hızı giriş bit hızının 1/4'ü kadar azalmıştır.

Tablo 1. Van Neumann Son İşlem

Girilen Bit Çiftleri	Van neumann çıkışı
00	Çıkış yok
01	0
10	1
11	Çıkış yok

- **Önerilen Son İşlem :** Önermiş olduğumuz sistemde van neumann tarafından önerilen sistemde atılan 00 ve 11 bitleri yerine 00 bitleri 0, 11 bitleri 1 olarak alınmıştır. Bu şekilde alınması ile van neumann son işleminde bit dizisi 1/4 oranında azalırken önerdiğimiz son işlemde azalma 1/2 oranında meydana gelmiştir.

Tablo 2. Önerilen Son İşlem

Girilen Bit Çiftleri	Önerilen son işlem çıkışı
00	0
01	0
10	1
11	1

Gerçek rasgele sayı üreteçleri iyi istatistiksel özellikler göstermesi ve elde edilen rasgele sayıların kestirilememesi sebebiyle kriptografik uygulamalarda kullanılmıştır. Ancak bu iyi özellikler yanında donanımsal tasarımlarının zor olması ve sistemin SRSÜ'lere göre çok daha yavaş çalışması dezavantajlı yanıdır. Bu yüzden kaotik sistemler kullanılmaya başlanmıştır. Çünkü kaotik devrelerin donanımsal olarak uygulanması daha kolay olmuştur. Ayrıca üretilen kaotik işaretler daha iyi rasgele özellikler ve performans göstermişlerdir.

III.KOATİK ÇEKERLER

Kaotik sistemlerin en önemli özelliği başlangıç şartına bağlı olarak uzun dönemlerde kestirilemeyen davranışlar ve periyodik olmayan özellik göstermesidir. Kaotik sistemlerde elde edilen işaretlerin gürültü benzeri işaretler olmasından dolayı rasgele sayı üretiminde gürültü kaynağı olarak kullanılmaktadır. Kaotik işaretler geniş aralıklarla örneklenerek kullanılması testlerde başarılı sonuçlar vermiştir. Kaotik işaretler kullanılarak yapılan çeşitli çalışmalar mevcuttur [13]. İlki sürekli zamanda çift sarmallı kaotik yapı [14] diğeri de osilatör örnekleme yöntemidir [15].

Bu çalışmamızda 2+2 çeker kullanılarak gerçekleştirilmiştir.

A. 2+2 çeker elde edilmesi

Bu çalışmamızda kullanmış olduğumuz genelleştirilmiş Chua devre denklemleri (1) 'de gösterilmiştir.

$$\begin{aligned} \dot{x} &= y + f_1(y) \\ \dot{y} &= z \\ \dot{z} &= -a \cdot x - a \cdot y - a \cdot z + f_2(x) \end{aligned} \qquad (1)$$

Burada

$$f_1(y) = \sum_{i=1}^{M_1} g_{\frac{(-2i+1)}{2}}(y) + \sum_{i=1}^{N_1} g_{\frac{(2i+1)}{2}}(y)$$

$$f_2(x) = \sum_{i=1}^{M_2} g_{\frac{(-2i+1)}{2}}(x) + \sum_{i=1}^{N_1} g_{\frac{(2i+1)}{2}}(x)$$

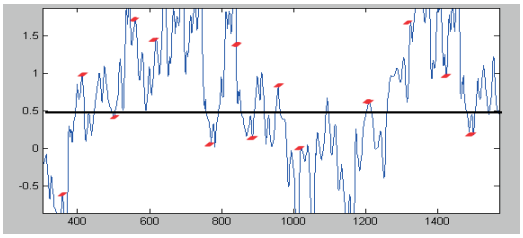
$$g_\theta(\alpha) = \begin{cases} 1 & \alpha \geq \theta, \theta > 0 \\ 0 & \alpha < \theta, \theta > 0 \\ 0 & \alpha \geq \theta, \theta < 0 \\ -1 & \alpha < \theta, \theta < 0 \end{cases}$$

Şeklinde olup, $M_1, N_1, M_2, N_2, i, j \in \Re^+$'dır. $f_1(y)$ sisteme etkisi ihmal edilmiştir ve a değeri 0.4 alındığında sistem çift çeker davranış göstermiştir. $f_1(y)$ ve $f_2(x)$ çok kırılma noktalı parçalı doğrusal elemanları temsil etmekte olup aynı özelliklere sahiptir. Y durum değişkeni $f_1(y)$ etkiler, x durum değişkeni de $f_2(x)$'i etkiler. M ve N parametrelerine bağlı olarak bu elemanlar dinamik yapı gösterirler. M ve N değerleri ile kırılma noktaları sayısı ve yerleri belirlenir.

Sistemde, x ve y=-ax+b doğruları boyunca kaotik çekiciler oluşacaktır. $f_2(x)$ etkisi altında olan kaotik sarmallar x ekseni boyunca oluşur, $f_1(y)$'nin etkisi altındaki kaotik sarmallar y=-ax+b doğrusu boyunca oluşur. Her iki yönde de kaotik çekiciler oluştuğu için bu davranış tipi n+n çekici olarak adlandırılır. İlk n değeri x ekseni diğer n değeri de y=-ax+b doğrusu boyunca oluşan toplam sarmalları gösterir.

Denklem (1) 'de verilen diferansiyel denklem çözülerek sistemin davranışı elde edilmiştir. Matlab programı kullanılarak, 4 adımlı Runge-Kutta metodu kullanılmıştır. Durum değişkenlerinin başlangıç değerleri (x_0,y_0,z_0)=(0.1,0.1,-0.1) ve a değeri 0.4 alınmıştır. 2+2 çeker elde etmek için M_1=1, N_1=2, M_2=0 ve N_2=1 alınmıştır[16]. 2+2 çekerden elde edilen X durum değişkeninden ilk 500 sayıdan itibaren 300 adımda bir değer alınmıştır. Elde edilen bu değerlerde aşağıdaki Şekil 2'de gösterildiği gibi ve (2)'de gösterilen kural (0.5 değeri simülasyon sonucu ortaya çıkan minimum ve maksimum değerlerin ortalaması olarak belirlenmiştir) uygulanarak herhangi bir son işleme tabi tutulmadan 108418 bit dizisi elde edilmiştir. Elde edilen bit dizisi [17]'deki çalışmamızda herhangi bir son işlem uygulamadan sadece istatistiksel testlere tabi tutulmuştur. Buradaki çalışmamızda elde edilen bit dizisi yukarıda açıklanan son işlemlerden geçirilerek saf bit dizisi üzerindeki etkileri incelenmiştir.

$$S(x) = \begin{cases} 0 & x < 0.5 \\ 1 & x >= 0.5 \end{cases} \qquad (2)$$



Şekil 2. 2+2 çekerin belli bir alanının simülasyonu

IV. SON İŞLEM SONRASI İSTATİSTİKSEL TEST SONUÇLARI

Gerçek rasgele sayı üreteçlerinden elde edilen bit dizileri sıcaklık,basınç gibi çevresel etkenler nedeniyle zayıflıklar gösterebilir. Bu zayıflıkların giderilmesi amacıyla son işlem uygulanmıştır. Elde edilen bit dizilerinin rasgele olup olmadığına geçerli istatistiksel testler uygulanarak karar verilebilmiştir. Bilinen en geçerli test Ulusal Standartlar ve Teknoloji Enstitüsünün yayınladığı NIST 800-22'dir. Bu testlerin yazılımı yazılmış olup elde edilen sonuçlar aşağıdaki tabloda gösterilmiştir.

Tablo 3. Elde edilen bit dizileri

Saf Bit Dizisi	108418 Bit
Xor Son İşlem	54209 Bit
Önerilen Son İşlem	54209 Bit
Van Neumann	27009 Bit

Tablo 4. 2+2 çeker için NIST testi sonuçları

Test Adı	**Saf bit Dizisi P değeri**	**XOR p değeri**	**Van neumann p değeri**	**Önerilen Son İşlem P değeri**	**Sonuç**
Frekans	0.151	0,412	0,421	0,112	Başarılı
Blok Frekans	0.484	0,086	0,835	0,789	Başarılı
Akış	**0.028**	**0,548**	**0,199**	**0,641**	**Başarılı**
Blok İçindeki En Uzun Birler Akışı	0.069	0,521	0,850	0,236	Başarılı
İkili Matris Rankı	0.675	0,021	0,177	0,725	Başarılı
Ayrık Fourier Dönüşümü	0.442	0,774	0,215	0,880	Başarılı
Örtüşmeyen Şablon Eşleştirme	0.086	0,557	0,832	0,705	Başarılı
Örtüşen Şablon Eşleştirme	0.778	0,698	0,744	0,928	Başarılı
Maurer'in Evrensel İstatistik	0.050	0,231	0,324	0,493	Başarılı
Doğrusal Karmaşıklık	0.580	0,950	0,997	0,320	Başarılı
Seri	0.246	0,400	0,926	0,850	Başarılı
	0.594	0,530	0,940	0,928	
Yaklaşık Entropi	0.106	0,241	0,383	0,414	Başarılı
Kümülatif Toplam	0.085	0,288	0,659	0,093	Başarılı

Elde edilen sonuçlar incelendiğinde her ne kadar saf bit dizisi istatistiksel test sonuçlarını geçmiş olsa bile son işlem uygulandığı taktirde bit dizisi kalitesinin arttığı gözlenmiştir. Son işlem bitleri daha düzgün dağılımlı hale getirmiştir. Bu düzelme üçüncü test olan akış testi ile anlaşılmıştır. Akış testi 0 ve 1'ler arasındaki değişime bakmaktadır. Sonuç değeri ne kadar büyük ise 0 ve 1' ler arası geçişin çok olduğunu ve aralarındaki korelasyonun az olduğunu göstermiştir. Tablo 4'de üçüncü teste bakıldığında son işlemin ne kadar etkili olduğu görülmüştür ve önerdiğimiz son işlemde sonuç çok daha iyi çıkmıştır.

V. SONUÇ

Bu çalışmamız da gerçek rasgele sayı üretecinden elde edilen bit dizilerine son işlem uygulanması ve bu uygulamanın sonuçları üzerinde durulmuştur. Saf bit dizileri her ne kadar testleri geçmekte olsa bile kriptografik güvenlik için gerekli olan kaliteli bit dizilerin son işlem sonrası elde edileceği ve gerçek rasgele sayı üretiminde son işlemin önemli bir aşama olduğu görülmüştür. Önermiş olduğumuz son işlemde sonuçlar başarılı olmuştur. Van neumann son işlemini iyi sonuç vermesine rağmen çıkış bit oranını 1/4 oranında azaltmaktadır. Ancak önerdiğimiz sistemde bu oran 1/2 olmuş ve daha iyi sonuçlar vermiştir. Daha ileriki çalışmalarda bit oranını düşürmeyen daha iyi sonuçlar alınabilecek son işlem algoritmaları önerilmesi düşünülmektedir.

KAYNAKLAR

[1] Koç, C.K.,"Cryptographic Engineering", *Springer*, 2009

[2] Akram, R.N., "Pseudorandom Number Generation in Smart Cards: An Implementation, Performance and Randomness Analysis", *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*, 1-7, 7-10 May 2012

[3] Yıldırım S., Bazlamaccı C., "A True Random Number Generator and Test Platform Built in FGPA.", *International Information Security and Cryptology Conference - ISCTURKEY 2012, Ankara*, Turkey, pp.262-267, May 17-18, 2012

[4] Sobotka, J. and Zeman, V., "Design of the true random numbers generator", *Elektrorevue*, 2(3):1-6, September 2011

[5] Strogatz, S., "Nonlinear Dyanamics and Chaos", *Westview Press*, Cambridge, 2001

[6] Özkaynak,F., Özer, A. B., Yavuz, S.,"Cryptanalysis of A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences", *Optics Communications*, 285(24): 4946-4948, 2012

[7] Özkaynak,F. and Özer, A. B.," A method for designing strong S-Boxes based on chaotic Lorenz system", *Physics Letters A*, 374(36): 3733-3738, 2010/8/9

[8] Murphy, J.P., "Field-programmable true random number generator", *Electronics Letters*, 48(10):565 - 566,10th May 2012

[9] Davies, R.B., "Exclusive OR (XOR) and Hardware Random Number Generators", February 28, 2002, 1{11, http://webnz.com/robert

[10] Suresh,V.B., Burleson, W.P., "Entropy Extraction in Metastability-based TRNG", *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on* ,135-140, 13-14 June 2010

[11] Dichtl, M., "Bad and Good Ways of Post-Processing Biased Physical Random Numbers", *Fast Software Encryption Lecture Notes in Computer Science Volume 4593*, 137-152,2007

[12] Sunar, B., Martin, W.J., and Stinson, D.R.,"A Provably Secure True Random Generator with Built-In Tolerance to Active Attacks", *in IEEE Transaction On Computers*, vol. 56, No.1, January 2007

[13] Yalçın, M.E. , "Şifreleme için çok sarmallı kaotik çekici temelli rastgele sayı üreteci tasarımı ve elektronik gerçeklenmesi", *Tübitak Proje(108E219)*, Eylül 2011

[14] Ergün, S. and Özoğuz, S., "A chaos-modulated dual oscillator-based truly random number generator.", *In Proceedings, International Symposium on Circuits and Systems*, 2482–2485, 2007

[15] Yalcın, M. E., Suykens, J. A. K. and Vandewalle, J., "True random bit generation from a double scroll attractor.", *IEEE Trans. Circuits and Systems-I*, 51(7):1395–1404, 2004

[16] Türk, M. and Ata, F., "The multi-mode chaotic behaviours: N+N and 2D N-scroll chaotic attractors", *COMPEL: The nternational Journal for Computation and Mathematics in Electrical and Electronic Engineering* , 25(4):929-939, 2006

[17] Avaroglu, E., Türk,M.," Random number generation using multi-mode chaotic attractor", *Signal Processing and Communications Applications Conference (SIU)*, 2013 21st ,1-4, 2013

Siber Caydırıcılık ve Türkiye'nin İmkân ve Kabiliyeti

Y. İduğ, F. Çalışkan, T. Güler

***Özet*— Bilgi teknolojilerinin günlük yaşamın vazgeçilmez bir parçası olması, kamu ve özel kurumların -özellikle finans, enerji ve güvenlik- faaliyetlerini bilgi sistemleri üzerinden yürütmesi, siber güvenlik kavramını hayati kılmaktadır. Tehdidin büyüklüğü ve gerçekleşme ihtimalinin yüksek oluşu devletleri kritik savunma, finans ve ulaşım altyapılarına yapılabilecek olası siber saldırılara karşı caydırıcı stratejiler geliştirmeye yöneltmektedir. Türkiye de diğer devletler gibi bilgi sistemlerinin güvenliğini sağlamak maksadıyla çalışmalar yapmaktadır. Bu çalışmada, siber caydırıcılık kavramı ile Türkiye'nin mevcut siber caydırıcılık kabiliyeti incelenmiş ve Türkiye'nin siber savunma ve taarruz alanında atması gereken adımlar ele alınmıştır.**

***Terimler* — Caydırıcılık, Nükleer Caydırıcılık, Siber Caydırıcılık.**

Abstract— Establishing cyber security is more important than ever because information technologies have become essential part of daily life, and public and private activities –particularly on finance, energy, and security- have been carried out via information systems. Since the threat is tremendous and most likely to occur, states are forced to develop deterrence strategies against any possible cyber attack to their crucial defense, finance, and transportation infrastructures. Considering the criticality of ensuring cyber security, Turkey has initiated a process of strengthening the security of its information systems. This work examines the concept of cyber deterrence, cyber deterrence capability of Turkey, and finally the necessary measures should be taken by Turkey to deter cyber threats.

***Keywords* — Deterrence, Nuclear Deterrence, Cyber Deterrence.**

I. GİRİŞ

BİLGİ teknolojilerinin günlük yaşantımızda yaygın olarak yer alması beraberinde bilgi sistemlerinin güvenliğini önemli hâle getirmiştir. Dünya genelinde bilgisayar kullanımı hızla artmaktadır. 2011 yılında 1,6 milyar bilgisayar kullanılırken bunun 2016'da 2,45 milyara ulaşması beklenmektedir [1]. Yedi milyar insanın yaşadığı dünyamızda altı milyar insan da cep telefonu kullanmaktadır [2].

Yavuz İduğ, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yeni Levent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: yavuzidug@gmail.com.

Ferhat Çalışkan, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yeni Levent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: fcaliskan10@gmail.com.

Talip Güler, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yeni Levent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: talipguler99@gmail.com.

Devletlerin ve içinde yaşayan bireylerin bilgi sistemlerine olan bağımlılıkları onları siber saldırılara karşı hassas duruma getirmektedir. Bir devlete karşı yapılmış örgütlü ilk siber saldırının örneğini gördüğümüz 2007 yılında Estonya'ya karşı gerçekleştirilen botnet istilası, gerekli siber savunma tedbirlerinin alınmadığı ülkelerde kamu hizmetleri ile finans ve medya faaliyetlerinin bu tip saldırılara karşı ne kadar hassas olduğunu göstermekte ve devletleri siber savunma ve caydırıcılık stratejileri geliştirmeye teşvik etmektedir.

II. CAYDIRICILIK

Caydırıcılık; bir devlet veya topluluğun, başka bir devlet veya topluluğun aleyhine olabilecek hareketlerden sakınması için gerekli tedbirleri alması olarak tanımlanabilir. Caydırıcılığın; belirli bir menfaati koruma niyetinin belirtilmesi ve bu menfaati savunmak için gerekli imkân ve kabiliyetin gösterilmesi olmak üzere iki temel unsuru bulunmaktadır [3]. Bu kapsamda caydırıcılık, bir bakıma anlaşmazlığın tırmanarak askeri kuvvet kullanımını gerektirmesine engel olur.

Uluslararası güvenlik literatüründe caydırıcılığın esirgeme (deterrence by denial) ve misilleme (deterrence by retaliation) olmak üzere iki yönü bulunmaktadır. Sağlam kalelerin inşa edildiği ve topun muharebe sahasında henüz yerini almadığı ortaçağda hasmın saldırılarını boşa çıkarmasından dolayı caydırıcılığın esirgeme yönü ağır basmaktayken, nükleer silahların hüküm sürdüğü ve bunlara karşı savunmanın imkânsızlaştığı Soğuk Savaş boyunca caydırıcılığın misilleme yönü ön planda olmuştur [3]. Ancak, hem Soğuk Savaş'ın hatıralarımızda yer alması hem de bu dönemde caydırıcılık ile ilgili üretilen politikaların fazlalığı nedeniyle caydırıcılık kavramı daha çok literatürde nükleer caydırıcılık olarak yer almaktadır.

III. SİBER CAYDIRICILIK

Siber caydırıcılığın önemi konusunda uzmanlar arasında bir fikir birliği bulunmamaktadır. Clarke'ın da başını çektiği kimi ulusal güvenlik uzmanları siber caydırıcılığın siber savaşları önleyemeyeceğini belirtmektedir. Bu uzmanlara göre; nükleer savaşta her iki tarafın da taarruz kabiliyeti bilindiğinden ve savaşın sonucunda büyük olasılıkla dünyadaki yaşamın yok olacağı düşünüldüğünden uluslararası ilişkilerde nükleer caydırıcılık etkilidir. Ancak, siber savaşta saldırının gücü bir sır olarak kalmaya devam edeceğinden ve etkin bir savunma kurma olasılığı bulunmasından dolayı nükleer savaşı engelleyen güç olan caydırıcılık bu uzmanlara göre siber savaşta bulunmamaktadır [4].

Siber silahların nükleer silahlar gibi kullanılamayacağı bir gerçektir. Nükleer silahların teşhiri bir caydırıcılık etkisine sahipken siber silahların teşhiri potansiyel hasımların bu teknolojiyi çalmalarına ve/veya siber savunmalarını bu silahlara karşı sağlamlaştırmalarına neden olacağından siber taarruz yeteneğini işe yaramaz kılmaktadır [5]. Ancak, siber

caydırıcılığı nükleer caydırıcılık ile mukayese eden uzmanlar konuyu Soğuk Savaş teorileri ile ele alarak caydırıcılığın misilleme dışında esirgeme yönünün de olduğunu göz ardı etmektedirler. Nükleer caydırıcılık misilleme odaklıyken siber caydırıcılık daha çok esirgeme odaklıdır. Siber caydırıcılıkta, potansiyel saldırganların hedeflerine ulaşmada başarısız olacaklarına ikna edilerek harekete geçmekten vazgeçmeleri esas alınır [6].

Siber kabiliyet yalnız başına bir caydırıcılık etkisi oluşturabileceği gibi ekonomik ve diplomatik güç, konvansiyonel ve nükleer kabiliyetler ile de beraber bir etki oluşturabilir. Şekil 1'de belirtildiği üzere siber etki yalnız kullanıldığında şiddet olarak ekonomik ve diplomatik yaptırımlardan daha yüksek seviyede olacakken, konvansiyonel ve nükleer etkiden daha düşük olacaktır [3]. Bir devlet beliren bir tehdidi yok etmek maksadıyla diplomatik yaptırımlardan nükleer güç kullanımına kadar şiddeti değişen geniş bir yelpazede karşılık verecektir.



Şekil 1. Güç ve Kabiliyetlerin Şiddet Hiyerarşisi.

Nükleer bir saldırının çok büyük yıkımlara sebep olacağı muhakkaktır. Nükleer tesisleri kontrol eden sistemlere yönelik bir siber saldırı da benzer bir etki gösterecek ve hedeflenen devlete büyük bir darbe vuracaktır. Bu açıdan siber yeteneği nükleer bir saldırıyı tamamlayıcı bir unsur olarak görmekteyiz.

Bunun yanında siber kabiliyet diğer kabiliyetleri de destekleyici bir unsur olarak kullanılabilir. Nükleer bir saldırı ile eş zamanlı olarak yapılacak etkili bir siber saldırı hazırlıksız yakalanan hedefin bilgi sistemlerini sekteye uğratacak ve misilleme yapmasına engel olabilecektir.

Kritik altyapı sistemlerinin imhasına yönelik yeterli büyüklükteki siber saldırıya uğrayacak bir devletin siber misilleme yapabilmesi için on yıla varabilecek uzun bir zaman gerekecektir [7]. İran nükleer tesislerinde fiziksel hasar meydana getiren Stuxnet virüsü belki de bu tür saldırıların başlangıcını oluşturmaktadır. Bundan dolayı, siber savunma yeteneği olmaksızın siber taarruz kabiliyetleri işe yaramayacaktır.

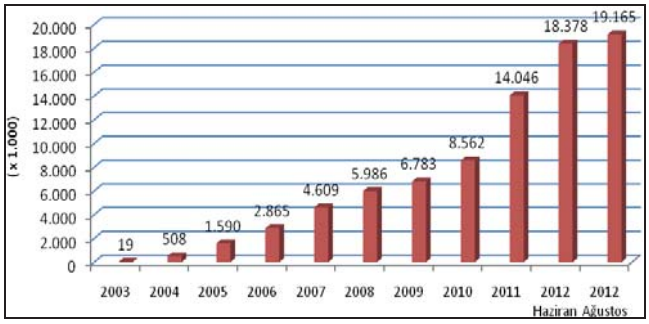
Siber caydırıcılığa yapılan en büyük eleştiri, bir siber saldırının nereden gerçekleştiğini bulmanın güç oluşudur. Siber savunma kabiliyeti yüksek olduğu müddetçe siber saldırılar boş çaba olarak görülecek ve bu yola başvurulmayacaktır. Böylece siber savunma kendi başına bir caydırıcılık sağlayacaktır. Yine Stuxnet örneği göstermiştir ki, hedefte büyük tahribata yol açmayan siber saldırılar hedefin güvenlik açıklarını görmesini sağlayarak bu açıklıkları gidermesine olanak verecek ve bir sonraki benzer saldırıyı boşa çıkaracaktır.

IV. TÜRKİYE'NİN SİBER CAYDIRICILIK KABİLİYETİ

"Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılardır, bunların üzerinde çalıştıkları bilgi sistemleri de kritik bilgi sistem altyapılarıdır" [8]. Örgütlü olarak yönlendirilen siber saldırıların öncelikli hedefi kritik altyapılar olacağından Türkiye'nin de kritik altyapıları siber tehdit altındadır.

Artan şekilde teknolojiye olan bağımlılık, kamu ve özel sektörün yaygın olarak internet üzerinden hizmet vermeleri Türkiye'nin siber saldırılara olan hassasiyetini artırmaktadır.

Türkiye'de 2002 yılında geniş bant erişim abone sayısı 100 binin altındayken, 2012'de bu rakam 19 milyon kişiyi geçmiştir (Bakınız Şekil 2). Bunun yaklaşık 11 milyonu mobil internet kullanan abonelerdir. Bu da toplamda Türkiye'de 50 milyon internet kullanıcısı olduğuna göstermektedir. Mobil internet abone sayısı da son bir yılda yüzde 80'in üzerinde artmıştır. Türkiye'de cep telefonu abone sayısı da 67 milyona ulaşmıştır. Yaklaşık 39 milyon 3G abonesi bulunmaktadır. Cep telefonu kullananların içinde yüzde 58 olan bu oran, yüzde 30 olan Avrupa ortalamasının çok üzerindedir [9].



Şekil 2. Genişbant İnternet Abone Sayısındaki Gelişim [10].

Türkiye'nin bilgi teknolojilerine olan bağımlılığı onu siber saldırılara karşı hassas duruma getirmektedir. Bu hassasiyeti gidermek maksadıyla 20 Ekim 2012 tarihinde yürürlüğe giren Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararıyla Genelkurmay MEBS Başkanı ve MSB müsteşarının da üyesi olduğu, Ulaştırma Denizcilik ve Haberleşme Bakanının başkanlık ettiği Ulusal Siber Güvenlik Kurulu oluşturulmuştur [11].

Kara, deniz, hava ve uzay harekât alanlarının yanında, yeni bir harekât alanı olarak ortaya çıkan siber ortama ilişkin yetenekleri geliştirmek maksadıyla 2012 yılında TSK Siber Savunma Merkezi Başkanlığı kurulmuştur [12].

Bu kapsamda siber tehditleri önleyerek, gelişmiş siber savunma ikaz ve tepki sistemlerine sahip güçlü bir merkezi siber savunma yeteneği kazanmak hedeflenmektedir. TSK Siber Savunma Merkezi Başkanlığı; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, TÜBİTAK ve diğer kamu kurumları ile koordineli olarak faaliyetlerini icra etmektedir. Ayrıca, NATO ile eşgüdüm içerisinde görevlerini ulusal ve uluslararası alanda yürütmektedir [13].

Mevcut duruma bakıldığında siber taarruz ile ilgili olarak herhangi bir yetenek geliştirme çalışmasının olmadığını görmekteyiz. Siber savunma konusunda ise devlet bünyesinde çalışmalar ancak 2012 yılında başladığından tecrübe eksikliği bulunmaktadır. Siber savunma alanında uzman personelin yetişmesi için en az beş yıl gerektiği [13] değerlendirildiğinde Türkiye'nin siber savunma konusunda daha yolun başında olduğu söylenebilir.

Siber güç siber savunma ve siber taarruzun birleşiminden oluşmakta ve siber caydırıcılık da siber güç ile doğru orantılı olarak ele alınmaktadır. Siber konusunda tecrübeli devletlere baktığımızda siber savunma ve taarruzun ayrı ayrı ele alındığını görmekteyiz. Savunma yapan personel ile taarruz yapacak personelin profillerinde de farklılık bulunmaktadır. Siber savunma yapan personel belli kurallar çerçevesinde çalışan bir özellik gösterirken, siber taarruz yapan personelin kuralların sınırı zorlayan kişilik özellikleri gösterdikleri kabul edilmektedir [13]. Bundan dolayı siber savunma ve taarruz için gerekli insan gücünün temininde siber savunma ve taarruz ayrı ele alınmalıdır.

Türkiye'nin siber hassasiyetleri yüksektir, fakat siber savunma konusunda ise daha yolun başındadır. Siber caydırıcılık kabiliyetini artırması için Türkiye'nin siber savunma kabiliyetini geliştirmesi, hassasiyetlerini gidermesi ve siber taarruz kabiliyeti elde etmesi gerekmektedir.

V. SONUÇ

Bilgi teknolojilerinin günlük hayatın vazgeçilmez bir parçası olduğu ve siber uzayın muharebe sahasının yeni bir boyutunu oluşturduğu bu çağda devletlerin ulusal güvenliklerini sağlayabilmeleri için siber caydırıcılık kabiliyetine sahip olmaları elzemdir.

Siber caydırıcılığın esirgeme ve misilleme olmak üzere ilki savunmaya, diğeri taarruza yönelik olmak üzere iki yönü bulunmaktadır.

Türkiye siber kabiliyetlerinin bir devlet çatısı altında koordineli olarak yönetilmesi için 2012 yılından itibaren çalışmalara başlamış ve siber hassasiyetlerin belirlenerek giderilmesi konusuna odaklanmıştır. Türkiye'nin siber gücü bir bütün olarak ele alması ve siber savunmanın yanında siber taarruz kabiliyetini de geliştirmesi siber caydırıcılık kabiliyeti elde edebilmesi bakımından önemlidir.

KAYNAKLAR

[1] Computer Industry Almanac Inc. http://www.c-i-a.com/pr02012012.htm. Erişim Tarihi: 08 Temmuz 2013.

[2] UN News Centre. http://www.un.org/apps/news/story.asp?NewsID=44452. Erişim Tarihi: 08 Temmuz 2013.

[3] M.L.Libicki, Cyberdeterrence and cyberwar. RAND Corporation, 2009.

[4] R. Clarke, R. Knake, Siber savaş: Ulusal güvenliğe yönelik yeni tehdit. İKÜ Yayınevi, 2011, s. x, 99.

[5] S. Weiner, Searching for cyber-deterrence. Center for Strategic and International Studies, 26 Kasım 2012.

[6] A. Lupovici, Cyber warfare and deterrence. Military and Strategic Affairs, 3Aralık 2011, s. 51.

[7] C. Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress. 2008, s.18.

[8] H. Bahşi, B. Karabacak, Ü. Tatar, Sayısal Ortamda Savunma ve Bilgi Güvenliği Yol Haritası, Bilişim Kurultayı, Ankara, 2009.

[9] Türkiye Avrupa birincisi oldu. http://www.sabah.com.tr/Teknoloji/Haber/2012/08/21/turkiye-avrupa-birincisi-oldu. Erişim tarihi:11Temmuz 2013.

[10] Genişbant Hizmetlerinde Şeffaflık Düzenlemeleri ve Hizmet Kalitesi Uygulamaları. http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/arastirma_raporlari/dosyalar/genisbant_hizmetlerde_seffaflik_ve_hizmet%20kalitesi-05_10_2012.pdf. Erişim Tarihi: 10 Temmuz 2013.

[11] Bilgi ve Teknoloji Yüksek Kurulu 25. Toplantısı Hazırlık Dosyası. http://www.tubitak.gov.tr/sites/default/files/btyk25_gelismeler.pdf Erişim Tarihi: 09 Temmuz 2013.

[12] C.Çatal, TSK'dan siber savunma merkezi. http://www.hurriyet.com.tr/teknoloji/22405874.asp Erişim tarihi:11Temmuz 2013.

[13] Ü. Tatar, Geleceğin muharebelerinde siber savaş boyutu. HAK Geleceğin Harekât Ortamı ve Harp Teknolojileri Paneli. 2013, s.65.



Yavuz İduğ lisans eğitimini 2003 yılında Uluslararası İlişkiler ve Liderlik & Yönetim dallarında ABD Kara Harp Okulu, West Point'te tamamlamıştır. Yüksek lisans eğitimini 2011 yılında ABD Deniz Kuvvetleri Yüksek Lisans Okulu (Naval Postgraduate School)'nda Mali Yönetim dalında yapmıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, liderlik & yönetim ve siber savaş konularına ilgi duymaktadır.



Ferhat Çalışkan lisans eğitimini 2003 yılında Sistem Mühendisliği dalında Kara Harp Okulu'nda tamamlamıştır. Yüksek Lisans Eğitimini 2011 yılında ABD Deniz Kuvvetleri Yüksek Lisans Okulu (Naval Postgraduate School)'nda Güvenlik İncelemeleri-Orta Doğu dalında yapmıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, oyun teorisi, Orta Doğu çalışmaları ve siber savaş konularına ilgi duymaktadır.

Güvenli Yazılım Geliştirme Yaşam Süreci ve Statik Kod Analizi

Güncel SARIMAN, Ecir Uğur KÜÇÜKSİLLE

***Özet*— Geliştirilen yazılımların, teknolojik cihazlardaki kullanımı son zamanlarda giderek artmaktadır. Yazılımlar günümüz kritik altyapılarında, finansal sistemlerde, tıbbi bilgi sistemlerinde kullanılmaktadır. Sistemlerin çoğalmasıyla güvenli yazılımların geliştirilmesi, giderek artan güvenlik açıkları nedeniyle aynı oranda ilerleyememektedir. Yazılım güvenlik açıklarının artması ulusal alanda da ciddi bir tehdit oluşturmakta ve bu tehdit güvenli yazılım gelişimi için yeni yaklaşımları ortaya çıkarmaktadır. Yazılım ürünlerinde güvenilirliği arttırmayı düşünen kurumlar, yazılım güvenliğini keşfetmeye ihtiyaç duyarlar. Bununla birlikte güvenli yazılım kolay kolay gerçekleştirilememekte ve gerçek hayatta yatırımcılar yazılım geliştirme sürecinde yazılım ataklarına veya mevcut güvenlik açıklarına karşı direnememektedirler. Bu bildiride güvenli yazılım geliştirme modeli (G-YGYD) ve güvenliğin yazılıma olan etkisi anlatılmaktadır. Bildiride statik kod analizinin detaylarından ve güvenli yazılım geliştirme kodlama tekniklerine de değinilmektedir.**

***Anahtar Kelimeler*—Yazılım Güvenliği, Yazılım Yaşam Döngüsü, Statik Kod Analizi**

***Abstract*— The use of technological devices in developed software has been increasing in recent times. Software used in today's critical infrastructures, financial systems and medical systems. The development of secure software with the proliferation of systems cannot propagate at the same rate due to security vulnerabilities. Increase of Software vulnerabilities are a serious threat in the national area and this threat reveals new approaches for the development of secure software. Organizations, who minded to increase the reliability of the software products, need to explore software security. However, secure software cannot be accomplished easily and in real life, investors unable to resist existing vulnerabilities or software attacks in software development process. In this paper, secure software development model (S-SDM) and the impact of security to the software are described. Also details of static code analysis techniques and secure coding of software development are discussed.**

Keywords— Software Security, Software Life Cycle, Static Code Analysis

I. GİRİŞ

GÜNÜMÜZ teknolojisinde yazılım ürünlerine artan talep, yazılım geliştirme süreçlerinin derinlemesine araştırılmasını sağladı. Uygulama geliştirici firmalar kurumsal kimlik ve bilgileri korumak amacıyla bilgi güvenliği ve güvenlik mühendisliğinin önemini arttırmıştır [1]. CERT güvenlik raporuna göre yazılım güvenlik açıkları güvenlik uzmanlarıyla yakından ilgilidir [2]. Bilgi Güvenliği SSE-CMM[3], ISO/IEC 15408 [3] gibi standartlarla bağlantılıdır.

Güvenlik açıklarını engellemek için, güvenli yazılım geliştirme yaşam döngüsü ve mühendislik süreçlerindeki güvenlik gereksinimleri kapsamında birçok yazılım güvenlik aracı bulunmaktadır. Geleneksel olarak, yazılım güvenliği yazılım geliştirme yaşam döngüsünün(YGYD) başlarında dikkate alınmaz ve sadece geliştirmenin sonraki aşamalarında yazılıma entegre edilmeye çalışılır. Sonuç olarak, yazılım geliştirmenin çeşitli aşamalarında güvenlik açıklarının riskleri artmaktadır [8]. Güvenli yazılım mühendisliği YGYD 'nin başında ve ilerleyen aşamalarında güvenlik problemlerini dikkate alarak güvenlik açıklarını önlemeyi amaçlamaktadır. Güvenli yazılım mühendisliği tasarım, yapı ve test süreciyle güvenilirliği sağlamaktadır. Yazılım güvenliği, güvenli yazılım yaşam döngüsü süreçlerini ve güvenli yazılım geliştirme yöntemlerini içermektedir. Bir Güvenli Yazılım Geliştirme Yaşam Döngüsü (G-YGYD) süreci yazılım geliştirme yaşam döngüsü boyunca güvenli yazılım geliştirme yöntemlerini (GYG) kullanan güvenlik yöntemlerini dikkate alır. GYG yöntemleri, güvenlik özelliklerini, mühendislik süreçlerindeki güvenlik gereksinimlerini ve yazılım güvenliği güvence yöntemlerini içermektedir. Şunu belirtmek gerekir ki; yazılım güvenliği kaygıları uygulama güvenliği sorunlarından farklıdır. Uygulama güvenliği, yazılımın geliştirildikten ve yayınlandıktan sonra korunması ile ilgilidir. Genellikle giriş filtreleri, saldırı tespit sistemleri ve diğer koruma mekanizmalarını içermektedir[8]. Geliştirme yaşam döngüsü boyunca güvenlik konularına yol göstermesi açısından uygun G-YGYD süreci seçmek önemlidir. Ayrıca, eğer geliştirilen uygulamanın piyasaya sürümünden hemen sonra hata siliniyorsa, bir hatayı silmek için geliştirilen ve yayınlanan bir yama 200 kat daha fazla pahalı olabilmektedir. Hatalar göz önüne alındığında, uygun güvenli gereksinim mühendisliği yöntemlerinin kullanılması gereklidir.

Geliştirmenin en başından beri yazılımda güvenliği fikir olarak gören, çeşitli GYG yöntemleri önerilmiştir. Bununla birlikte, uygulamalar halen geleneksel YGYD modeliyle geliştirilmekte ve geliştiricilerin uygun gördüğü çeşitli GYG yöntemleri geliştirmenin farklı aşamalarda kullanılmaktadır. Geliştirme süresince farklı GYG yöntemlerini kullanan birçok G-YGYD süreci önerilmektedir. Bu G-YGYD süreçlerin her birinin kendi güçlü ve zayıf yönleri vardır [7].

Yazılım geliştirme sürecinde güvenlik açıklarının en sık rastlandığı bölüm olan statik analiz, yazılımı ve sistemlerinin

Manuscript received July 15, 2013. (Write the date on which you submitted your paper for review.)

G. SARIMAN Süleyman Demirel University, Electronics and Communicating Engineering, Isparta 32100 Turkey (corresponding author to provide phone: 505-804-8988; e-mail: guncelsariman@mu.edu.tr).

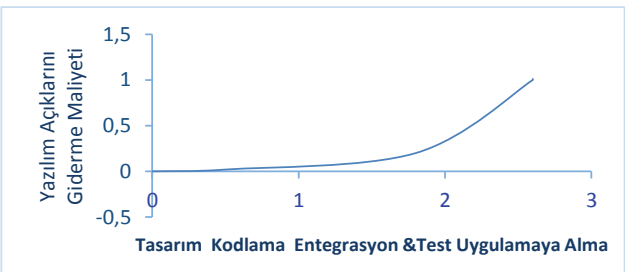
E. U. KÜÇÜKSİLLE, was with Süleyman Demirel University,Computer Engineering, Isparta, Turkey. (e-mail: ecirkucuksille@sdu.edu.tr).

güvenliğini geliştirmek için umut verici bir teknoloji olarak ortaya çıkmıştır. Statik analiz araçları, derleyiciler, manuel kod inceleme ve test etmek gibi geleneksel tekniklerle tespit edilemeyen hataları bulmak için yazılımları analiz eder. Bununla birlikte bir dizi kısıtlamalar yazılımın gelişimini engellemiştir [4].

Giderek artan yazılım projelerinin mimarisi ilk günkü gibi olmamakla birlikte işlevsellik gün geçtikçe artmakta ve beraberinde karmaşık ve detaylı bir projeyi oluşturmaktadır. Yazılımdaki kalite ve güvenliğin kaybıyla ilgili birçok problem, etkili bir şekilde yönetilemeyen karmaşıklığın büyümesi ile ilişkilendirilebilir [5]. Örneğin masaüstü işletim sistemlerinin kod tabanı şaşırtıcı bir şekilde artmaktadır. Microsoft işletim sistemi 1993 yılında 6 milyon, 2000 yılında 29 milyon kod satırından oluşurken, 2005 yılında 50 milyon kod satırına ulaşmıştır. Bir debian linux işletim sistemine ait kod satırı 2000 yılında 55 milyon kod satırından 2005 yılında 215 milyon kod satırına daha hızlı bir şekilde ulaşmıştır [6]. Güvenlik açıklarının sıklığı, yazılım karmaşıklığının etkisini izlemek için bir lider gibi davranır. CERT istatistiklerine göre, belgelendirilen güvenlik açıklarının sayısı katlanarak artıyor. Bu güvenlik açıkların sayısı 1999 yılında yaklaşık 400, 2002 yılında 4000'den fazla ve 2006 yılında 8000'den fazla olmuştur [2].

II. GÜVENLİ YAZILIM GELİŞTİRME

Yazılım, bir problemi çözmek amacıyla farklı cihazların birbirleriyle iletişim kurabilmesini sağlayan ve görevlerini ya da kullanılabilirliklerini geliştirmeye yarayan, bilgisayar dili kullanılarak oluşturulmuş bir ifadedir [10]. Geliştirilen yazılımların gün geçtikçe artması yazılımlara ilişkin çalışmaları hızlandırarak yeni yazılım geliştirme yöntemlerini, yeni programlama kurallarını ve derleyici çeşitlerini ortaya çıkarmaktadır. Geliştiricilerin piyasaya hızlı ürün sürme isteği ve hatalı kod geliştirilmesi güvenilirliği sağlayamama ve düşük kalite gibi sorunlara yol açmaktadır. Araştırmalara göre bilişim güvenliği ihlallerinin %80 gibi büyük bir bölümü yazılım güvenliğinin eksikliğinden oluşmaktadır [11]. Genel olarak problemlerin çoğu, yazılım geliştirme sürecinde gereksinim ve sistem analizlerinin doğru ve yeterli yapılmamasından kaynaklanmaktadır. Yazılımlardaki analiz eksikliği güvenlik riski oluşturmakta, bu durum bilgiye yönelik tehditlerin ortaya çıkmasında önemli bir açıklık oluşturmaktadır. Yazılım geliştirmenin başlarında farkına varılan yazılım açıklıklarının düzeltilmesinin daha ileri süreçlerde farkına varılan açıklıklara göre daha az maliyetli olacağı kabul edilmiştir [7]. Şekil-1 de yazılım geliştirme sürecinde, yazılım açıklarının maliyet analizi gösterilmektedir.



Şekil. 1. Güvenli Yazılım Sürecinde Hata Düzeltme Maliyeti

III. YAZILIM GELİŞTİRME SÜRECİNDE GÜVENLİK UYGULAMALARI

G-YGYD güvenli yazılım geliştirme yaşam döngüsünün kısaltılmış halidir. Kısaca YGYD süreç, yöntem ve bir dizi metodolojiyi yazılım projeleri oluşturmak veya geliştirmek için uygular. Bu metodolojiler yeni bir yazılım modülü geliştirmek için tek bir yol tanımlar. Yazılım geliştirme yaşam döngüsünün temel ayağı olan 4 genel yaklaşım bulunmaktadır. YGYD metodolojisi şelale modeli, artırımlı model, spiral model, prototip modeli olarak sınıflandırılmaktadır.

Dizayn ve tasarım hataları, üzerinde çok düşünülmemiş güvenlik açıkları, yeni geliştirilen malware uygulamaları ve bunlar gibi birçok neden, geliştirilen uygulamaların debug ve patching süresini maksimuma çıkartır. Bu debug seansları uzun zaman almasının yanında yazılımcıyı moral olarak da kötü etkiler. Dolayısıyla programın yapımına harcanılan bütçeyi bile geçebilecek yatırımlar yapılması zorunlu hale gelir. Daha güvenli bir yazılım geliştirebilmek için güvenliğin yazılım yaşam döngüsüne dâhil edilmesi gerekmektedir. Genel olarak güvenlik YGYD sürecine 6 aşamada eklenebilmektedir [9]. Bu süreçler içerisinde sırasıyla eğitim, gereksinim analizi, tasarım, geliştirme, test ve dağıtım sıralanmaktadır. Şekil-2 de YGYD aşamaları Şekil-3 de ise G-YGYD aşamaları gösterilmektedir.

Güvenliği sağlamak için, güvenli geliştirme kavramlarını var olan geliştirme sürecine entegre etmek gerekmektedir. Güvenli yazılım geliştirme süreci yaşam döngüsündeki aşamalar aşağıda açıklanmıştır.

A. Uygulamalar İçin Temel Güvenlik Eğitimi

Bir yazılım geliştirme takımındaki geliştiriciler, test elemanları ve program yöneticileri gibi çalışanlar, güvenlik temelleri ve güvenlikteki son yaklaşımlar hakkında bilgili kalmak için uygun bir eğitim almalıdır. Güvenlik eğitimi aşağıdaki temel kavramları içermelidir;

a) -Güvenlik tasarımı

Saldırı yüzeyi azaltma, Derinlemesine savunma, En az ayrıcalık ilkesi

b) -Tehdit Modelleme

Tehdit modellemeye genel bakış, Bir tehdit modelin tasarım ilkeleri, Tehdit modelindeki kısıtları kodlama

c) -Güvenli kodlama

Arabellek taşmaları, Tamsayı aritmetik hatalar, Cross Site Scripting, Sql Injection, Zayıf Şifreleme

d) -Güvenlik Testi

Güvenlik testi ve fonksiyonel test arasındaki farklar, Risk değerlendirmesi, Güvenlik test yöntemleri

e) -Gizlilik

Gizlilik duyarlı veri türleri, gizlilik tasarımının en iyi uygulamaları, Risk değerlendirmesi, En iyi gizlilik geliştirme uygulamaları



Şekil. 2. Yazılım Geliştirme Yaşam Döngüsü (YGYD)



Şekil. 3. Güvenli Yazılım Geliştirme Yaşam Döngüsü (G-YGYD)

IV. GÜVENLİ YAZILIM GELİŞTİRME YAŞAM DÖNGÜSÜ

A. Gereksinim ve Risk Analizi

Gereksinim aşaması, geliştirme takımlarının güvenlik, plan ve programın herhangi bir kesintiye uğramasını engellemeyi amaçlar. Güvenlik ve gizlilik ihtiyaç analizi proje başlangıcında yapılır ve uygulama için minimum güvenlik gereksinimlerinin özelliklerini içerir. Yazılım geliştirme yaşam döngüsü gereksinim aşaması ile başlar. Gereksinim aşamasının amacı müşterinin taleplerini yerine getiren yazılım gereksinimleri belirlemek ve aynı zamanda açık ve anlaşılır bir şekilde temsil etmektir. Yazılım ihtiyaçlarının belirlenmesi ile birlikte, çalışmalar güvenlik gereksinimlerini belirlemek için yapılır. Güvenlik gereksinimleri farklı kaynaklardan farklı zamanlarda gelmektedir. Bazı güvenlik gereksinimleri, tasarım aşamasında tehdit modellemeden sonra tanımlanır. Tanımlama yapıldıktan sonra, güvenlik gereksinimleri diğer yazılım gereksinimleriyle birlikte analize tabi tutulur. Analizden sonra, gereksinimler belgelendirilir. Gereksinim belgeleri işlevsel, işlevsel olmayan ve güvenlik gereksinimlerini içermektedir. Bu belgeyi kullanarak, proje takımı Use Case diyagramları oluşturur. Use Case ler yüksek düzeydeki sistemler için önemli bir tekniktir. Yeni gereksinimler tanımlandığında var olan gereksinimlerin değiştirilmesi muhtemeldir ve bazı gereksinimler use case diyagramları yanlış kullanım durumlarında silinmektedir. Bu gereksinimler, gereksinim dokümanlarını güncellemek için çağrıda bulunur.

B. Tasarım ve Tehdit Modelleme

Tasarım özellikleri, kullanıcının doğrudan maruz kalacağı güvenlik ve gizlilik esaslarını açıklamalıdır. Ayrıca, fonksiyonların güvenli bir şekilde nasıl uygulanacağını da açıklar. Tasarım aşaması boyunca güvenlik ve gizlilik kaygılarını dikkate almak çok önemlidir. Tasarım aşaması yazılım mimarisinin oluşturulması ile başlar. Güvenlik mimarisi de yazılım mimarisinden geliştirilmiştir. Tasarım aşamasında ilk olarak etkileşim noktaları tanımlanır. Bu noktalar yazılımın iş akışını anlamada yardımcı olur ve ortaya çıkabilecek güvenlik sorunları hakkında derinlemesine bir bilgi verir. Güvenlik tasarımının bir sonraki aşaması ise varlık ve erişim noktalarını belirlemektir. Bu varlıkların erişim noktaları da daha önceden tespit edilen erişim noktalarından olabilir. Güvenlik tasarımındaki diğer bir nokta ise saldırı yüzeyini en aza indirgemektir. Bu aşama çok çaba gerektirmemekle beraber, saldırganın çalışma alanını azaltmanın en etkili yoludur. Yazılım tasarımı ayrıntılı olarak analiz edilir ve maximum kullanıcı sayısının ihtiyaçlarını etkilemeden etki altında kalan yüzey alanının azaltılması konusunda çaba gösterilir. Tasarımdaki diğer bir nokta ise yazılım için geçerli olan tehditleri tespit etmektir. Tehdit modelleme güvenli yazılım aşamasında önemli bir kilometre taşı olarak kabul edilebilir. Tehdit modelleme güvenlik sorunlarının bileşen veya uygulama seviyesinde dikkate alınmasını sağlar [12]. Güvenlik tasarım uygulamaları bir yazılımın nasıl saldırıya maruz kalabileceğine, neyin saldırabileceğine, hangi alanlarda saldırı eğilimi olabileceğine, ne tür atakların uygulanabileceğine dair tam bir bilgi sağlar. Bu bilgiler ışığında, güvenlik tasarımı şirketler için devamlı olarak güncellenir [13].

C. Uygulama

Güvenlik perspektifinden bakıldığında uygulama aşaması iki aşamalı rol oynamaktadır. İlk rol yazılıma giren güvenlik açıklarını ve ikinci rol ise yazlımda mevcut olan açıkları engellemektir. İlk rol güvenli kod yazarak gerçekleştirilir. Güvenli kod yazmak oldukça önemlidir, çünkü yapılmadığı takdirde bütün çabalar boşa gidecektir. Güvenli kod, tasarım aşamasında(tasarım aşamasında kurulan güvenlik tasarımı) tanımlanan tehdit modelindeki tehditler ve genel güvenlik kuralları dikkate alınarak yazılır. Tüm bu faktörler, güvenli kod yazmak için çok önemlidir ve herhangi birinin eksikliği güvenlik açıklarına sebep olabilir. İkinci rol ise güvenlik açıklarını tespit etmek için statik analizin kullanılmasıdır. Geliştirme ekibi tarafından yazılmış kod otomatik araçlar yardımı ile analiz edilir. Bu otomatik araçlar ortak güvenlik açıklarını arar [13].

Geliştirme ekipleri yeni güvenlik analizi ve korumalarından yararlanmak için onaylanmış araçların en son sürümünü kullanmalıdır. Bu araçların listesi proje ekibi için güvenlik danışmanı tarafından onaylanmalıdır[12]. Ayrıca proje ekibi kullanılan yazılımın api ve fonksiyonlarını kontrol etmelidir çünkü kullanılan birçok api ve fonksiyon güncel saldırı ve tehditler karşısında güvenli değildir. Bu fonksiyonlar güvenli olanlarıyla değiştirilmelidir. Otomatik statik analizden sonra gözden geçirmeler yapılmaktadır. Gözden geçirme yazılım kodundaki güvenlik açıklarını bulmanın etkili yoludur.

D. Üretim ve Test Aşaması

Geliştirilen uygulama yayınlanmadan önce doğrulama ve

test aşamalarından geçirilmelidir. Bu aşamalar ise dinamik kod analizi, fuzz testi, tehdit modeli ve saldırı yüzey incelemesidir. Bir uygulamadaki zayıflıkları tespit edebilmek için uygulamaya rastgele veriler göndererek, uygulamanın farklı isteklere verdiği cevaplar analiz edilir. Bu rastgele veri gönderme işlemine fuzzing (fuzz testing), bu işlemi yapmaya yarayan araçlara ise fuzzer denilmektedir. Fuzz testing; test yapılacak uygulamaya ait işlevsel ve yazılımsal özellikler bilinmediğinden ve gönderilen verilerin uygulamada oluşturduğu etki ve sonuçların analizine dayandığından, uygulama test tekniklerinden black-box kategorisine girmektedir. Fuzz testing; yazılım geliştirme, test süreçlerinde ve ters mühendislik işlemlerinde kullanıldığı gibi, web uygulamalarında zayıflık tespiti veya bilgi toplama amaçlı da kullanılmaktadır [14].

Test aşaması test planlamasıyla başlar. Güvenlik test durumları, yazılımları güvenlik seviyesinde başarılı bir şekilde savunmaları için tasarlanmıştır. Test planlaması boyunca, yazılım tasarımındaki herhangi bir değişiklik test ekibine iletilmelidir aksi takdirde test takımı değişiklikleri farketmeden analize devam edecektir. Yazılımın doğasına dayanarak uygulanabilir tehditler, hata şiddeti gözden geçirilir çünkü yazılım kodundaki küçük bir hatayı düzeltmek birkaç dakikayı alabilir fakat güvenliğe olan etkisi büyük olabilir. Test planlamasından sonra bir test sistemi tasarlanır. Test sistemi, muhtemelen test doğasına bağlı olarak çeşitli yazılım ve donanım ortamları içerir. Test süresince geliştirme takımı ve test takımı iş birliği halindedir. Test takımı güvenlik açıklarını tanımlayarak geliştirme ekibine raporlar ve geliştirme ekibi açıkları giderir.

E. Yayın ve Dağıtım

Yazılımın geliştirilmesi bittiğinde, son kullanıcıya dağıtıma başlanmadan hemen önce geliştirilen yazılımın güvenli olup olmadığının kontrol edilmesi ve her şeyinin güvenli olduğundan emin olunması gerekmektedir [15]. Gözden geçirme yapılarak kalan güvenlik açıklarının gözden geçirilmesi gerekmektedir. İnceleme sonunda gözden geçirme raporu üretilir. Geliştirme ekibi raporda tanımlanan güvenlik açıklarına karşı kodu düzeltir. İncelemeden sonra, bir güvenlik denetimi yapılır. Tüm proje ekibi denetimde yer almaktadır. Eğer sorunlar denetim sırasında tespit edilirse, yazılımda değişikliğe gidebilir. Denetim sonunda denetim raporu oluşturulur. Denetim raporuna göre, proje yönetimi yazılımın yayınlanma durumuna karar verir. Yayınlandıktan sonra yazılım dağıtım için hazır hale gelir.

V.GÜVENLİ YAZILIM GELİŞTİRME SÜRECİNDE STATİK KOD ANALİZİ

Güvenli yazılım geliştirme süreci, geliştirilen projeye güvenliğin yanı sıra mali açıdan önemli katkılar sağlamaktadır. Yazılımda ortaya çıkan açıklara yama geliştirmek, bu açıkları daha yazılım geliştirme sürecinde fark edip önlemeye nazaran çok daha fazla mali yük getirmektedir. Üstelik sonradan ortaya çıkacak olan bu güvenlik açıkları şirket imajının zedelenmesi, hukuki açıdan sorunlar, maddi kayıplar, şirketin borsa hisse değerinin düşmesi ve hatta şirketin iş hayatının son bulması gibi sonuçlar dahi doğurabilirler [16]. G-YGYD süreciyle beraber tehdit modelleme, risk analizi, yazılımcılar için güvenlik eğitimleri ve dokümanları, mimari analiz, kaynak kod analizi, sızma testleri gibi güvenlik için vazgeçilmez gereksinimler bir bütün olarak yazılım sürecine entegre edilirler. Statik kod analizi de bu süreçte önemli bir rol oynamakta ve yazılımın çalıştırılmadan kodlama zamanında analiz edilmesini ve olası hataların tespit edilmesini sağlamaktadır.

Yazılımın koşturulması sırasında fark edilemeyecek veya geç fark edilecek bazı hatalar statik kod analizleri ile bulunabilir. Statik kod analizleri yazılımın kalitesi, çalışma performansı, işlevselliği, güvenirliliği açılarından önemli olmakla beraber statik kod analizlerinin temel mantığı kod üzerinde sorgulamalar gerçekleştirmektir. Gözden geçirme yoluyla da yapılabilen statik kod analizi, günümüzde otomatik kod analiz araçlarıyla zamansal ve ekonomik maliyet açısından daha uygun olmasından dolayı hızlandırılmıştır. Geliştirilen uygulamaların üzerinde gerçekleştirilen hata tespiti vb. durumların yazılım yaşam döngüsünün ilerleyen aşamalarında giderek artmasından dolayı yazılımın erken aşamalarında kullanılan otomatik statik kod analiz araçları, daha kaliteli ve maliyetli uygun yazılımların geliştirilmesine olanak sağlamaktadır. Farklı boyutlardaki yazılımlara ait hatalar benzer maliyetlerle tespit edilebilmektedir. Statik analiz araçları daha çok atama ve denetim gibi programlama hatalarını tespit ederken, gözden geçirme ile yapılan kod analizi fonksiyonel hataları da ortaya çıkarabilmektedir[17]. Gözden geçirmeyle yapılan aşamada dikkat edilmesi gereken nokta ise hataların gözden kaçırılabilir olmasıdır.

A. Statik Kod Analizinde Kullanılan Yöntemler

Geliştirilen yazılımlardaki kodlar çeşitli kategorilerde incelenebilmektedir. Statik analiz; duyarlı fonksiyon analizi, veri akış analizi, fonksiyon değer analizi, kodlama standartı analizi, bilgi akış analizi ve yanlış yol budama analizi olarak kategorize edilebilmektedirler.

Duyarlı fonksiyon analizi ile fonksiyon/prosedürler-arası ilişkiler ve veri akışları sorgulamaları gerçekleştirilir. Fonksiyon değer analizi, yazılımdaki fonksiyonların dönüş değerlerinin analizinin yapıldığı yöntemdir.

Veri Akış analizinin amacı ise değer atanmadan bir değişkene erişebilen verilerin yazılımda uygulama yollarının olmadığını göstermektir.

Bilgi akış analizi, bir birim kodun yürütülmesi sırasında koddaki giriş ve çıkışlar arasında nasıl bir bağımlılık kurulacağını tanımlar. Bu analiz, yazılım/donanım ara yüzündeki girişlere doğru tüm yolları izleyebilen kritik çıkışlar için önemlidir.

Yol fonksiyon analizi, resmi bir belirtim gerektirmeden, matematiksel işlemler vasıtasıyla bir programın özelliklerini doğrulamak için kullanılır. Çok sayıda yolun bulunduğu durumlarda, bazı yollar hiç çalıştırılmadan kalabilir. Yazılım içinde çalışması mümkün olmayan yollar belirlenir.

Kodlama Standartı analizinde, çalışan kod yazmanın yanında iyi kod yazmanın gerekliliği vurgulanmaktadır. Kodlama yaparken isimlendirme standartlarına dikkat edilmelidir. Sık kullanılan isimlendirme standartları şu şekildedir;

Kod geliştirilirken ara yüz isimlendirmelerinde "I" ön eki, değişkenler için anlamlı ve açıklayıcı kelimeler

kullanılmalıdır. Kısaltmalar kullanılmamalıdır. Tek karakterlik değişken isimleri kullanılmalıdır, fakat döngülerdeki parametreler tek karakterlik olabilmektedir. UI elemanlarını kullanırken programlama dilinin belirlediği kısaltmalar kullanılmalıdır. Sınıfların bulunduğu fiziksel dosya isimleri sınıf ismi ile aynı olmalıdır. Editörde kod geliştirirken daha anlaşılır kod satırları için girintiler ve yorum satırları kullanılmalıdır. Kullanılan süslü parantezler if, for gibi kodlarla aynı satırda olmalıdır. Kod parçalarını gruplamak için varsa editöre ait gerekli kod kullanılmalıdır. Yazılımdaki hata ayıklama türleri detaylandırılmalı ve ne tür hata alınabileceğine göre detaylandırılmalıdır. Aynı zamanda fonksiyonlara isim verirken kısaltmalardan kaçınılmalıdır ve yorum satırına gerek olmadan anlamlı isimler verilmelidir.

B. Statik Kod Analiz Araçları

Birçok kaynak kod analiz programı aynı kaynak dosyada olmayan kodlar arasında karmaşık etkileşimlerin sebep olduğu hataları bulan tam bir program analizi gerçekleştirir. Araçların bir kısmı yazılımın kaynak kodunu metinsel olarak incelemektedir. Daha kapsamlı analiz yapan araçlar kullanılan programlama diline ve editöre ihtiyaç duymaktadır. Microsoft .Net ortamında FxCop, Gendarme, StyleCop, Java platformunda CheckStyle, Findbugs, Hammurapi, PMD araçları geliştiriciler tarafından sıkça kullanılan analiz araçlarıdır.

VI. SONUÇ

Yazılım güvenliği günümüzün yazılım bağımlı toplumunda önemli bir sorun haline gelmiştir. Güvenli uygulamalar çeşitli güvenli yazılım geliştirme yöntemleri kullanılarak elde edilir. Güvenli yazılım geliştirmek için güvenlik konusu yazılım geliştirme yaşam döngüsünün her aşamasında göz önünde bulundurulmalıdır. Yazılım geliştirme aşamaları güvenlik açıklarını minimize eden tek bir ortak amacı içermelidir. Güvenli yazılım geliştirme süreci kullanılmadan geliştirilen yazılımların oluşturduğu açıkların sonradan farkedilerek düzeltilmesi ve buna ait yamaların yayınlanmasının, şirketleri hem mali hem de prestij bakımından kayba uğrattığı gerçeği her zaman göz önünde bulundurulması gereken bir gerçektir.

KAYNAKLAR

[1] F. J. B. Nunes, D. A. Belchior, A. B. Albuquerque, A Knowledge Management Approach to Support a Secure Software Development, International Conference on Availability, Reliability and Security, March. 16-19, 2009, s. 829-834

[2] CERT, Coordination Center Statistics. www.cert.org/stats/cert_stats.html.

[3] ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security, 2005.

[4] N. D. Kleidermacher, "Integrating Static Analysis into a Secure Software Development Process Technologies for Homeland Security", 2008 IEEE Conference, May. 12-13, 2008, s. 367 – 371.

[5] Robert Parker, Are Vendors Doing Enough To Improve Software?. Optimize Magazine; http://www.optimizemag.com/issue/009/squareoff.htm.

[6] Wikipedia Source lines of code http://en.wikipedia.org/wiki/Source_lines_of_code.

[7] M. U. A. Khan, M. Zulkernine, "On Selecting Appropriate Development Processes and Requirements Engineering Methods for Secure Software" Computer Software and Applications Conference. July. 20-24, 2009, s. 353–358.

[8] G. McGraw, Software Security: Building Security In, Addison Wesley, 2006.

[9] G. İ. Özbilgin, Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi. http://www.bilgiguvenligi.gov.tr/yazilim-guvenligi/yazilim-gelistirme-surecleri-ve-iso-27001-bilgi-guvenligi-yonetim-sistemi.html

[10] Yazılım, Türk Dil Kurumu Büyük Sözlük, http://tdkterim.gov.tr/bts/

[11] B. Dayıoğlu, Yazılım Geliştirme Yaşam Döngüsü ve Güvenlik, http://www.pro g.com.tr/ pciveriguvenligi 2008/pdf/pro-g-presentation-v1.1.pdf

[12] New SDLC: Security Development Life Cycle. http://codespread.com/new-sdlc-security-development-life-cycle.html.

[13] S. R. Ahmed, Secure Software Development-Identification of Security Activities and Their Integration in Software Development Lifecycle. School of Engineering Blekinge Institute of Technology.Yüksek Lisans Tezi. 2007.

[14] O. Yilmaz, Fuzz Testing. http://webguvenligi.org/dergi/FuzzTesting-Agustos2009-OnurYilmaz.pdf.

[15] E. Burak, Microsoft'un Güvenli Geliştirme Süreci (SDL). http://www.bilgiguvenligi.gov.tr/yazilim-guvenligi/microsoftun-guvenli-gelistirme-sureci-sdl.html.

[16] İ. E. Tatli, Java'da Güvenli Yazılım Geliştirme. www.webguvenligi.org/.../Javada_Guvenli_Yazilim_Gelistirme_OWASP

[17] Secure Coding Guidelines for the Java Programming Language, http://java.sun.com/security/seccodeguide.html

Güncel SARIMAN 1986 yılında Muğla'da doğdu. Süleyman Demirel Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği lisans eğitimini tamamladı. Yüksek lisans eğitimini Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Ana Bilim Dalında yaptı. Doktora eğitimi Süleyman Demirel Üniversitesi Mühendislik Fakültesi Elektronik ve Haberleşme Mühendisliği Ana Bilim Dalında tez aşamasında devam etmektedir. 2010 ve 2012 yılları arasında Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı yazılım biriminde yazılım mühendisi olarak çalışmıştır. Halen Muğla Sıtkı Koçman Üniversitesi Bilgi İşlem Daire Başkanlığı yazılım biriminde yazılım mühendisi olarak çalışmaktadır. Bilgisayar, güvenlik ve yapay zeka alanlarında çalışmaları bulunmaktadır.

Ecir Uğur KÜÇÜKSİLLE 1976 yılında Isparta'da doğdu. Gazi Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği lisans eğitimini tamamladı. Yüksek lisans eğitimini Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Makine Eğitimi Ana Bilim Dalında yaptı. Doktora eğitimini Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü İşletme/Sayısal Yöntemler Ana Bilim Dalında tamamladı. Halen Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır.. Bilgisayar, güvenlik ve yapay zeka alanlarında çalışmaları bulunmaktadır.

MARTİN C. LIBICKI'NİN "SİBER CAYDIRICILIK" KAVRAMININ NÜKLEER CAYDIRICILIK OLGUSU İLE KARŞILAŞTIRILMALI ANALİZİ

Uğur Ermiş*, Barış Özdal**

***Özet*—Günümüz uluslararası ilişkilerinde nükleer caydırıcılığa benzer bir şekilde siber caydırıcılığın olup olamayacağı tartışma konusudur. Devletlerin kritik altyapılarını SCADA (Supervisory Control and Data Acquisition) sistemleri ile kontrol ettikleri ve ağ merkezli muharebeye geçtikleri günümüz dünyasında, yapılacak bir siber saldırı ile ciddi zararlar verebilmek mümkündür. İkinci Dünya Savaşı'nın sonunda başlayan nükleer silahların kullanımı ise hatırlanacağı üzere beraberinde nükleer caydırıcılığı getirmiştir. Çalışmada Soğuk Savaş boyunca iki blok arasında dengenin sağlanması noktasında çok önemli bir yer tutan nükleer caydırıcılığın doğurduğu etkiyi, siber uzayda siber caydırıcılığın doğurup doğurmayacağı sorusuna cevap aranmıştır. Bu bağlamda siber caydırıcılık üzerine en yetkin eserleri kaleme alanlardan biri olan Martin C. Libicki'nin görüşlerine yer verilerek siber caydırıcılığın mümkün olup olmadığı tartışılmıştır. Tüm bu etki kapasitesine rağmen siber uzayın kendisine özgü özellikleri nedeniyle nükleer caydırıcılık etkisinde bir siber caydırıcılığın oluşmasının mümkün olmadığı savunulmuştur.**

***Anahtar Kelimeler*— Siber Caydırıcılık, Siber Savaş, Nükleer Caydırıcılık**

***Abstract*—Can we make comparisons of nuclear deterrence and cyberdeterrence in modern era. States conduct their critical infrastructures with SCADA systems. Also states make network centric warfare in our age. Because of all these reasons, cyber-attacks costs high damages. During Cold war, nuclear deterrence provided a diplomatic balance between Soviets and USA. In this article, we are questioning that does cyberdeterrence affect the world as much as nuclear deterrence? Despite all of this capacity, cyberdeterrence isn't effective as much as nuclear deterrence because characteristic of cyber space is very different from our conventional war types and rules.**

***Key Words*—Cyberdeterrence, Cyber War, Nuclear Deterrence**

I. Giriş

BU çalışmada Martin C. Libicki'nin "Cyberdeterrence and Cyberwar" eseri incelenmiş olup siber caydırıcılık ve nükleer caydırıcılık kavramları karşılaştırılmıştır.

Çalışmanın ilk bölümünde nükleer caydırıcılık ele alınmış olup bu çerçevede nükleer silahlanma ve buna bağlı olarak farklı nükleer caydırıcılık stratejileri genel ve soyut olarak incelenmiştir.

Çalışmanın ikinci bölümünde ise siber caydırıcılığın ne olduğu üzerinde durularak siber caydırıcılığın, nükleer caydırıcılıkla benzerlikleri ve farklılıkları Libicki'nin eserinde ortaya koyduğu üç temel ve altı destekleyici soru üzerinden incelenmiştir.

Sonuç bölümünde ise Libicki'nin eserinde verdiği cevaplar doğrultusunda güncel gelişmeler göz önünde bulundurularak, siber uzayda siber caydırıcılığın sağlanıp sağlanamayacağı sorusu analiz edilmiştir.

II. Nükleer Caydırıcılık

Varlığı siyasi oluşumların varlığıyla eş tutulabilecek olan caydırma stratejisi, ilk nükleer silahın 2. Dünya Savaşı'nda Japonya'da kullanılmasıyla farklı bir boyut kazanmıştır. Kısa süre sonra Sovyet Sosyalist Cumhuriyetler Birliği'nin de nükleer stoklara sahip olması caydırıcılık stratejisinin anlamı değişime uğramıştır. Özellikle Soğuk Savaş boyunca nükleer güce sahip devletler bu güçlerini diplomatik müzakerelerde pazarlık güçlerini arttırmak için kullanmışlardır. Diğer bir değişle her iki kutup liderinin de yaşanan tüm gerilime rağmen doğrudan çatışma noktasında karşı karşıya gelmemeleri nükleer silahların sağladığı caydırma işlevine bağlanabilir. Bu bağlamda nükleer güç ve bu gücün sonucu olarak nükleer caydırıcılık bir önleyici diplomasi aracı olarak kullanılmıştır. Kullanılması durumunda eğer bir taraf sahipse karşıdaki ülkeyi, iki taraf birden sahipse çatışan iki devleti ve hatta tüm dünyadaki insan varlığını ortadan kaldırma potansiyeli olan nükleer silahlar, caydırma stratejisinde zirve noktayı temsil etmektedir.

Stratejistler tarafından nükleer caydırıcılık stratejisi minimum caydırma stratejisi ve nihai caydırma stratejisi olarak ikiye ayrılmaktadır. Minimum caydırma stratejisi, rakibin kaldıramayacağı ölçüde bir misilleme saldırısına yetecek kadar nükleer silaha sahip olmayı öngörmektedir. Nihai caydırma stratejisinde ise rakibin misilleme kapasitesini de yok etme amaçladığından, ilk vuruşta rakibin tüm nükleer cephaneliğini ortadan kaldırmaya yetecek kadar silahlanmayı gerektirmektedir. Bu bağlamda nihai caydırma stratejisi nitelik ve nicelik olarak çok daha fazla silaha sahip olmayı gerektirmektedir. Minimum caydırmada ise stratejik dengeyi sağlayacak kadar silaha sahip olmak yeterlidir. [6]

NATO konseptleri içinde "Esnek Karşılık" ve "Topyekûn Karşılık" doktrinlerini genel ve soyut olarak ele almak gerekirse örgüt 1949 yılında kurulduğunda temel stratejilerin oluşturulması büyük ölçüde ABD'nin kontrolünü altında olmuştur. 1953 yılında ABD Genelkurmay Başkanı Oramiral Redford'un hazırlanmasına katkı verdiği yeni bakış olarak bilinen NSC(National Security Council) 162[1] isimli rapor, kitlesel topyekûn karşılık doktrininin temellerini oluşturmaktadır. Topyekûn karşılık doktrini temelde Batı Bloğu olarak lanse edilen bölgeye olası Komünist saldırı karşısında Amerikan Stratejik Hava Kuvvetlerine bağlı

* Araştırma Görevlisi, Uludağ Üniversitesi, Uluslararası İlişkiler Bölümü, Siyasi Tarih A.B.D.
** Doçent Doktor, Uludağ Üniversitesi, Uluslararası İlişkiler Bölümü, Siyasi Tarih A.B.D.

uçakların Sovyetler ve Çin Halk Cumhuriyeti'nin stratejik endüstri merkezleri ve şehirlerine nükleer silahlarla saldırılmasını öngörmektedir. Bu örnekten de anlaşıldığı üzere Topyekûn Karşılık doktrini iki noktaya dayanmaktadır:

1. Nükleer silahlarla karşılık yeteneği düşmanı hem sınırlı hem de topyekûn bir savaştan caydıracaktır
2. Nükleer silahlar durum gerektiğinde kullanılacaktır. Bu nedenlerle, Avrupa Müttefik Kuvvetleri Başkomutanlığı'na askeri savunmasını taktik nükleer silahları kullanabilecek biçimde yeniden düzenlemesi yetkisi verilmiştir.

Genel olarak bakıldığında ise nükleer silahlar üzerinden oluşturulan bu yapı hem Sovyetleri girişeceği olası bir savaştan caydırmış hem de Batı Bloğu üyesi Avrupa devletlerini ve ABD'yi büyük kara orduları oluşturma masrafından kurtarmıştır.

1949 yılında Sovyetlerin ilk denemesini yaptığı nükleer silah her ne kadar ABD'nin nükleer tekelini kırmışsa da ABD'yi stratejisini değiştirmeye asıl iten olay 1957 yılında Sovyetlerin Sputnik isimli yapay uyduyu başarılı bir şekilde uzayda yörüngeye yerleştirmesi olmuştur. Diğer bir deyişle Sputnik'in uzaya yerleştirilmesi iki okyanus tarafından coğrafi olarak korunun ABD'nin tarihte ilk defa kendi topraklarında vurulma ihtimalini ortaya çıkarmıştır.

Bu gelişmenin arından sınırlı savaş kavramı ABD tarafından kabul edilmeye başlamıştır. ABD artık havadan filolar üzerinden yapılarak nükleer saldırılar yerine, yerlerinin saptanması çok güç olan ve Polaris tipi güdümlü füzelerle yüklü nükleer denizaltıları ve ICBM (Inter-Continental Ballistic Missile)'leri geliştirmeye başlamıştır. ABD tarafından bu strateji uyarınca, tam anlamıyla yaşamsal çıkarlarının olduğu durumlarda güvenliğini nükleer silahlarla koruyacağı, diğer durumlarda ise savunmanın geleneksel silahlarla yapılacağı anlayışına dayanan bir doktrin geliştirilmiştir. Esnek karşılık stratejisinin sonucu olarak NATO'nun kara kuvvetlerinde bir artışı gerçekleşmiştir. [5]

III. Siber Caydırıcılık

Caydırıcılık teorisinde amaç saldırının maliyetini ve sonuçlarını beklenen yarardan daha fazla hale getirerek saldırının önünü kesmektir. Bu stratejinin yerine getirilebilmesi noktasında da iki önemli unsur vardır. Bu unsurlardan ilki sağlam bir savunma kapasitesine sahip olmaktır. Eğer bir devletin savunması, olası bir saldırıyı son derece zor hale getiriyorsa, saldırma potansiyelini barındıran devlet durmayı seçebilir. Siber uzayda, bu durumu sağlayabilmek saldırıların büyük birçoğu için çözüm sunmaktadır. Caydırıcılıkta ikinci önemli unsur ise misillemenin önem kazanmasıdır. Eğer başarılı saldırganlar, eylemleri neticesinde misilleme ile yüzleşirse, bu durum diğer saldırganları saldırıdan vazgeçirebilmektedir.

Siber caydırıcılığın klasik caydırıcılıktan ayıran en önemli unsuru, saldırının kaynağının tespit edilmesidir. Siber uzayda, dijital dünyanın doğası gereği sağladığı anonimlik, misillemenin doğru kaynağa yapılması noktasında engeldir. Bu durum bizi siber caydırıcılığın üçüncü unsuru olan Tespit/İsnata götürmektedir. [2]

Nükleer caydırıcılık ise tekil ve simetriktir. Bu noktada nükleer caydırıcılığın tekil olması nükleer silaha sahip olan devletin yapabileceği saldırının sonuçları neticesinde kimsenin bu devleti tahrik etmek istememesidir. Eğer nükleer misilleme meydana gelirse ki bu durum misilleme ve karşı misillemeyi de içerebilir, caydırıcılığın altında yatan koşulları fazlasıyla değiştirebilir. Zira misillemeyi yapan taraf ya da her iki taraf birden ortadan kalkabilir, hareket kabiliyetlerini yok olabilir yada güçsüz kalabilirler. Aynı durum ağır konvansiyonel caydırıcılık içinde geçerlidir. Eğer misilleme başlarsa bu daha büyük bir savaşa yola açacaktır ki bu durumda taraflardan birinin varlığı ortadan kalkabilecektir. [4]

Siber caydırıcılık ise tekrarlanabilir olmalıdır. Çünkü yapılacak olası siber misilleme ne saldırgan devleti devre dışı bırakabilir, ne hükümetlerin değişmesine yol açabilir ne de silahsızlandırabilir. Böylelikle devlet saldırabilir, misillemeden zarar görür ve başka bir zaman saldırmak için varlığını devam ettirebilir. Fakat siber caydırıcılıkta simetriktir çünkü eşitler arasında gerçekleşir. Hedef devlet (potansiyel misillemeci) saldıran devletten daha üstün bir ahlaki zemine sahip değildir. Aynı zamanda hedefin çatışmanın ilerlemesi durumunda kazanacağına inanmak için herhangi bir neden yoktur. Bu yüzden misillemeci daimi karşı misillemeden endişelenmelidir. [4]

Siber caydırıcılık tekrarlanabilmesi ve simetrik olması noktasında eşsiz değildir. Bu tür caydırıcılık genelde çekişme içinde bulunan ve birbirleri karşısında sürekli savunmada olan iki devlet ya da bazı durumlarda grup arasında gerçekleşmektedir. Anarşik sistem içinde, şiddetin salgın gibi yayıldığı böyle durumlarda ise caydırıcılık barışı koruma noktasında yeterli değildir. [4]

Daha somut bir biçimde vurgularsak sahip olduğu konvansiyonel güç, ABD'nin karşısındakinin tepkisini önemsemeden küresel bir polis gibi davranmasına müsaade etmektedir. Lakin bu durum siber uzayda geçerli değildir. ABD üstün saldırı kabiliyetine sahip olmak için bu alana büyük miktarlarda yatırım yapmaktadır. Devletin sistemleri en iyiler tarafından yazılmakta ve yazılım noktasında ABD dünyanın tek ithalatçısı konumundadır. Tüm bu durumuna karşın ABD hala saldırıya açıktır. Zira Amerikan toplumunun özellikle de ağ merkezli muharebe yapan ordusunun büyük ölçüde bilgi sistemlerine bağlı olduğu bilinmektedir. Oluşan bu bağlılık daha az gelişen ve daha az demokratik olan ülkelere karşın ABD'yi özel ve kamusal alanda saldırıya daha açık hale getirmektedir. Ayrıca Amerikan kurumları arasında güvenlik politikaları noktasında çok az benzerlik bulunmaktadır. Bu durum toplumu daha güçlü hale getirse de kurumların bağlantılarına zarar vermeyi kolaylaştırmaktadır. Ayrıca çatışmadan konvansiyonel olarak zarar gören taraf eşitliği sağlamak adına siber karşılık verebilir. Diğer bir deyişle ABD tüm avantajına rağmen misilleme eğer karşı misillemeyi getirirse düşmanlarından daha fazla zarar görülecektir. [4]

Uluslararası ilişkilerde oyun teorileri bağlamında bakıldığında siber caydırıcılık işe yarar bir enstrüman olarak görülmektedir. Soğuk Savaş boyunca ABD ile SSCB arasında yaşanan nükleer restleşmenin sağladığı tarihsel veriler siber caydırıcılığında kullanılabilir olduğunu düşündürmektedir. Aşağıda bulunan üç temel ve altı

destekleyici soru ise siber caydırıcılığı nükleer ya da kinetik caydırıcılıktan ayırmaktadır. Sorulan sorulara verilen cevaplarda oluşan bu farklar kinetik ve nükleer silahların aksine siber caydırıcılığın problemlerini ortaya koymaktadır. Nükleer caydırıcılığın temelini oluşturan ve siber caydırıcılıktan ayıran cevapları sağlayan üç temel soru incelendiğinde: [4]

A- Kimin yaptığını biliyor muyuz?

Misilleme yapılmadan önce saldırıyı yapanın kim olduğunun açıkça bilinmesi gerekmektedir. Eğer ilk misilleme gerçekleşmeden önce caydırıcılık işe yarayacaksa, diğerleri caydırıcı devletin kendisine saldıran devletin kimliğinden emin olacağını bilmelidir. Yanlış kişinin saldırıya uğraması sadece caydırıcılığın mantığını güçsüzleştirmeyecek aynı zamanda yeni düşmanların edinilmesini sağlayacaktır. "Eğer masum olmak umursanmıyorsa neden masum olmalı?" sorusu bağlamında ise muhtemel bir siber savaş yerine, kazayla saldırılan devletinde müdahil olmasıyla kendisini savunan devlet iki siber saldırıyla karşı karşıya gelecektir. [4]

B- Düşmanın varlığı risk altında tutulabilir mi?

Savaş zararı çok yönlü bir konudur. Saldırı ya da misilleme gerçekleşmeden önce, saldıranda hedef olanda saldırının doğurabileceği sonuçlar konusunda tam anlamıyla fikir sahibi değildir. Sonrasında dahi saldıranda, saldırılanda verilen hasarın boyutu noktasında emin olamayabilirler. Bu bağlamda bir petrol rafinerisini havaya uçurmak ve bu sayede bir yakıt kaynağının kullanılmasını engellemekle, rafineri kontrol sisteminde değişikliklere yol açan ve bu sayede yakıttaki kimyasal oranlarını değiştirerek araçlara zarar veren kurnazca saldırılar yapmak aynı şey değildir. [4]

C- Yapılan saldırı tekrarlanabilir mi?

Eğer bugün yapılan saldırı yarın ya da ondan sonraki gün yapılacak saldırıyı engelleyecekse caydırıcılık kırılganlaşabilir. Çoğu caydırıcılık şeklinde bu durum herhangi bir problem teşkil etmezken siber caydırıcılıkta bu durum problem oluşturmaktadır. Bazı caydırıcılık türleri (nükleer) o kadar kötü etkiye sahiptir ki hiç kimse bu yönde bir girişimde bulunmazken bazılarında ise yapılan misilleme bir sonraki saldırıyı engellememektedir. Siber uzayda misillemenin tekrar ve tekrar kullanımı gerekli olabilir fakat her kullanım bir sonraki kullanımın beklenen sonuçlarını olumsuz yönde etkileyebilir. [4]

a. Misilleme caydırıcılığı sağlamasa da silahsızlandırmayı sağlayabilir mi?

Misilleme saldırıları sadece caydırıcılık noktasında etkilidir. Konvansiyonel ve nükleer silahların aksine siber silahlar ise genel olarak saldırganın silahsızlandırılması noktasında etkisizdir. Bu durumda misilleme caydırıcılık etkisi doğuramıyorsa herhangi bir anlam taşımamaktadır. [4]

b. Üçüncü gruplar mücadeleye katılır mı?

Caydırıcı kapasite, saldıran devlete yaptığı saldırının istenmeyen sonuçları olabileceğini göstermek için bir sinyaldir. Tarafların belli olmaması ve muhtemel hasarın tespiti noktasındaki sorunlar ise yanlış algılamalara yol açabilir. Bunun dışında herkesin kafasını karıştıracak şekilde saldırı ya da karşı saldırı beklenenin dışında bir üçüncü gruptan da gelebilir. Bunun en önemli nedeni ise hackerların saldırmak için herhangi bir izne ihtiyaç duymamaları ve saldırılarını üçüncü bir devlet üzerinden gerçekleştirebilme kapasiteleridir. [4]

c. Misilleme tarafımıza doğru mesajı verir mi?

Siber hedeflerin bir kısmı hükümet sistemleriyken bir kısmı da özel sektöre aittir. Özel sektöre ait olan bu hedefleri örneğin ABD'de enerji, iletişim ve finans kritik altyapıları oluşturmaktadır. Bu hedeflere yapılan saldırılar halkın dikkatini çekme potansiyelini sahipken birkaç istisna hariç devlet devlete ait sistemler gündelik hayatta çokta önemli değildir. Özel sektöre ait sistemlerin savunulması ise genelde özel ellerdedir. Bu yapılar üzerinde devletin dolaylı olarak uygulamaya koyacağı düzenlemeler ve kanuni zorlamalar dışında, doğrudan etkisi bulunmamaktadır. Özel sistemlerdeki açıkları hükümetler tespit etme şansına sahip değillerken, şirket sahipleri de bunları söyleme konusunda istekli değillerdir. [4]

d. Saldırıya cevap vermek için bir eşik var mıdır?

Ne kadar sert bir saldırı misilleme yapmayı haklı kılar? Savunucu siber uzayda yeteneklerine zarar verdiğini düşündüğü herhangi bir girişim için misillemede bulunabilir. Yani sonrasında saldırıyı yapacağını duyurduğu bir anı eşik olarak belirleyebilir. [4]

e. Tırmanmadan kaçınılabilir mi?

Nükleer caydırıcılık noktasında stratejistler nükleer gerginliğin ötesinde ne olacağı noktasında endişelenmezler. Zira eğer saldırgan devlet nükleer silah kullanırsa misilleme durumunda bundan daha fazla ne yapacağını tartışmak mantıklı değildir. Siber caydırıcılık noktasında ise stratejistler sonrasında ne olacağını düşünmelidir. Siber misilleme sonrasında saldırgan buna kinetik hatta nükleer güç kullanarak karşılık verebilir. Bu çerçevede Rusya Federasyonu stratejik bir siber saldırıya cephaneliğin de bulunan herhangi bir stratejik silahla karşılık vereceğini deklare etmiştir. Saldırgan devlet gerilimi tırmandırma noktasında eğer:

1- siber misillemenin hak edildiğine inanmıyorsa,

2- iç kamuoyundan sert bir biçimde cevap verilmesi şeklinde baskı görüyorsa,

3- yada siber misillemeye siber saldırıyla karşılık vermesi durumunda kaybedeceğine inanmıyorsa,

Farklı enstrümanlarla cevap verebilir. [4]

f. Saldırgan devlette vurmaya değer bir şey yoksa ne olur?

Özelliklede ABD'nin karıştığı durumlarda tamamen simetrik bir savaş durumu mümkün değildir. Fakat siber savaş bu durumdan daha da asimetrik olabilir. Birleşik Devletler ekonomisi ve toplumundaki fazlasıyla ağ tabanlılık* ordusuna da yansımaktadır. Aksine saldırgan devlette ise karşılık olarak saldırılabilecek dijitallikte bir hedef bulunmayabilir, devlet bu ağları yeterince önemsemeyebilir ya da bu hedefler dış dünyaya bağlı olmayabilir. Örneğin Estonya'ya 2007'de yapılan DDOS saldırıları büyük bir şoka neden olmuşken, 2008'de Gürcistan'a yapılan saldırılar o kadar etkili olmamış, 2009'da Kırgızistan'a yapılan saldırılar ise neredeyse fark edilmemiştir. [4]

* "networked" kelimesi için kabul gören bir Türkçe karşılığa rastlanmamaktadır.

IV. SONUÇ

Yukarıdaki makalenin sınırları dâhilinde genel ve soyut olarak belirttiğimiz veriler göz önüne alındığında ABD her ne kadar resmi hiç bir belgede deklare etmese de Pentagon raporlarından sızan[3] şekliyle kendisine yapılan bir siber saldırıya konvansiyonel silahlarla karşılık verebileceğini belirtmiştir. ABD'nin ayni ile mukabele yerine geliştirdiği bu stratejinin temelinde Libicki'nin de belirttiği gibi ABD'nin nükleer ve konvansiyonel anlamda sağladığı caydırıcılığı, bu alanda tüm çabasına rağmen sağlayamaması/sağlayamayacağı gerçeği yatmaktadır.

Silahlanmanın tüm alanlarında olduğu gibi siber uzayda silahlanma noktasında da savunma yapısını geliştirmek, saldırıdan çok ekonomik güç, teknoloji ve emek gerektirmektedir. Siber saldırı noktasında ise diğer alanların aksine çift yönlü bir farklılık bulunmaktadır. Birinci olarak asgari düzeyde teknik imkânlar konvansiyonel silahlanmanın aksine belli bir tekel ya da grubun elinde bulunmamaktadır ve edinilen imkânlar diğer devletler tarafından takip edilememektedir. İkinci ve daha önemli olan farklılık ise siber uzayda teknolojik olarak en gelişmiş devletin siber saldırıya en müsait devlet olduğu gerçeğidir. Bu noktada kritik altyapıların yönetimi ve kontrolü ön plana çıkmaktadır.

Devletten devlete tanımı ve içinde bulunan unsurlar belli oranlarda değişmekle birlikte devletin devamlılığı noktasında fiziki gereklilik olan tüm yapılar kritik altyapı olarak adlandırılabilmektedir. En genel kabul olarak: su, su tutma ve iletim sistemleri, enerji üretim ve iletim sistemleri, iletişim, finans ve ulaşım altyapısı kritik altyapılar olarak kabul edilmektedir. Devletlerin siber uzayla ilişkileri arttıkça bu yapılar üzerindeki kontrol mekanizmaları mekanik ve insan odaklı yapıdan, ağ merkezli yönlendirilen dijitalleşmenin hâkim olduğu SCADA sistemlerine geçmektedir. Örneğin 2010 yılında STUXNET isimli kötücül yazılımla İran nükleer tesislerine, resmen kabul edilmese de ABD ve İsrail tarafından yapıldığı düşünülen saldırı SCADA sistemlerine gerçekleşmiş, bu sistemlere yapılabilen bir saldırının ne kadar zarar verebileceği ilk defa pratik olarak gözlemlenmiştir. Yapılan saldırı her ne kadar üstü örtülü olarak ABD'nin gücünü göstermiş olsa da buna paralel olarak zafiyetini de ortadan koymuştur. Zira dünyadaki çoğu devletin aksine birçok kritik altyapısı özel sektörün elinde olan ABD'nin, dünyada teknolojiyi üreten ülke olarak sistemleri de çok daha fazla ağ merkezli ve SCADA sistemlerinin kontrolündedir. Kritik altyapı sistemlerinin büyük oranda özel sektörün elinde olduğu göz önünde bulundurulduğunda bu sistemleri savunmak ekonomik maliyetin yanında kanuni düzenlemelerde gerektirmektedir. Ancak, serbest piyasa işleyişini bozacak bu düzenlemeler ABD'nin liberal ilkeleriyle ters düşmektedir. Tam tersi durumdan bakıldığında ise siber saldırı için gerekli teknik imkânı sağlayan herhangi bir üçüncü dünya ülkesinin, doğru insan gücünü yetiştirdiğinde kritik altyapıları siber uzaya bu kadar bağımlı olmadığı için saldırı yapması durumunda, yapılacak siber misillemeden çok daha az düzeyde etkilenecek ya da hiç etkilenmeyecektir. Çalışmada siber caydırıcılığın etkisiz olabileceğine verilen örneği tekrarlamak gerekirse 2009 yılında Kırgızistan'a yapılan saldırılar bu anlamda Estonya'nın aksine gündelik yaşamı ve devlet işleyişini çok daha az etkilemiştir. ABD bu durumun bilincinde olduğu için siber saldırılara karşı konvansiyonel karşılığı öne sürmektedir. Bu bağlamda bizce Libicki'nin de eserinde belirttiği gibi siber caydırıcılığın nükleer caydırıcılığa benzer şekilde etkili olması mümkün değildir.

KAYNAKLAR

[1] http://investigatinghistory.ashp.cuny.edu/images/m12/nsc162.htm

[2] http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/

[3] http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html

[4] Martin C. Libicki, Cyberdeterrence and Cyberwar, Rand Corparation, 2009.

[5] Oral Sander, Siyasi Tarih 1918-1994, 18. Baskı, Ankara: İmge Kitabevi, 2009.

[6] Tayyar Arı, Uluslararası İlişkiler ve Dış Politika, 7. Baskı, Bursa:MKM Yayınları, 2008.

Irregular Warfare with Cyber Means

H. Kendircioğlu, T. Kaymazlı, A.A. Eker

***Abstract*—Conventional Warfare tries to defeat the enemy's military and coerces the opponent government to come to terms with. On the other hand Irregular Warfare concentrates on the population and tries to gain popular support and erode the opponent's legitimacy over people. Irregular adversaries are embedded in society and their easy access to communication and information technologies let them reach and organize people regionally and globally. Cyberspace presents lots of perfect tools to irregular warriors in the irregular battlefield.**

***Index Terms*— Irregular Warfare, Cyber Warfare, Cyberspace, Social Media, Social Networks.**

I. Introduction

THE collapse of the Soviet Union ended the Cold War era. CIA Director James Woolsey described the post-Cold War environment during his confirmation hearing in 1993 by saying "We have slain a large dragon (the USSR). But we now live in a jungle filled with a bewildering variety of poisonous snakes. In many ways, the dragon was easier to keep track of [1]." The end of the cold war was the beginning of new economic, social, and military challenges including ethnic conflicts, terrorism, and irregular warfare crises. While trying to get used to new irregular security environment, we faced another dimension of warfare; cyberspace. Cyberspace offers lots of tools for irregular actors to fight against states. Cyber warriors can target critical infrastructures to erode popular support and will of population to continue the war. Information and communication networks can be used to win the "battle of narratives", "war of ideas" and helps winning "hearts and minds" in the long run. Cyber capabilities, particularly the use of internet and social media enable "self organized civilians" to resist against states. It becomes harder for states to differentiate between combatants and non combatants causing collateral damage and arousing international interest over the conflict.

II. Irregular Warfare

Irregular Warfare is defined as; "a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will [2]." Irregular Warfare (IW) is not a new type of warfare. It is both a reality of our past and will be an indispensible part of our future. Although it is used to define the post cold war security environment, 9/11 terrorist attacks let the world realize the real scope and effects of the threat facing the world. As long as there are weaker and stronger parts of a conflict we will witness IW. Militarily weaker opponents will resort to irregular tactics to gain popular support and compensate the power gap between their enemies [3]. IW is thought to consist of guerrilla warfare, terrorism, sabotage, subversion, criminal activities, and insurgency [4].

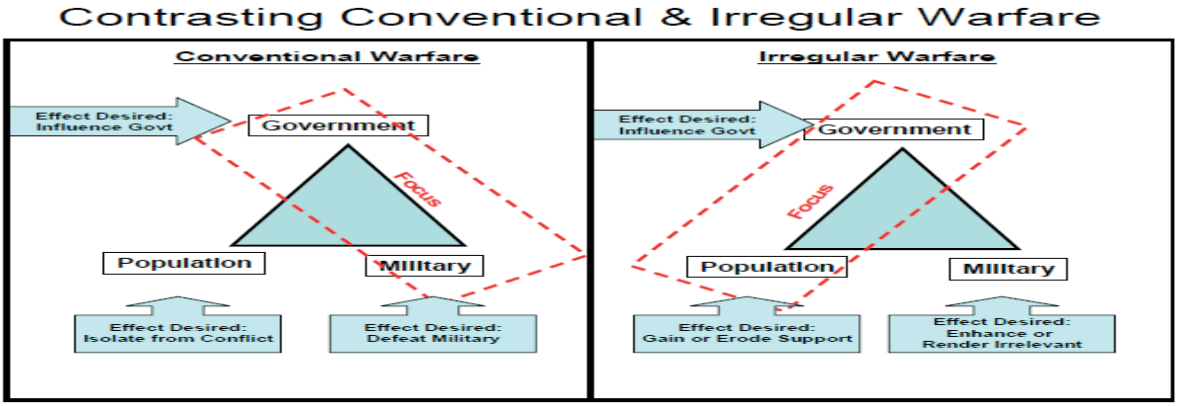


Fig. 1. Contrasting Conventional and Irregular Warfare [5].

H. K. War Colleges Command, Army War College, Student Officer, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: hkendircioğlu@yahoo.com)
T. K. War Colleges Command, Army War College, Instructor, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: tuncaykaymazlı@gmail.com)
A. A. E. War Colleges Command, Army War College, Instructor, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: alpereker99@gmail.com)

IW is a struggle directly related with the influence and legitimacy over population. As explained in the figure below, conventional warfare aims the destruction of the enemy militarily and then coerces the adversary government come to terms with. On the contrary, IW focuses on the population and tries to weaken the government's legitimacy over population by gaining or eroding support. In IW threats

posed by adaptive opponents such as terrorists, criminal networks and insurgents as well as states cannot merely countered by military means alone [6]. Threats are intermingled with population and "increasingly networked, adaptable and empowered by cyberspace to find new ways to recruit, collect intelligence, train, distribute propaganda, finance and operate [7]."

To deal with IW threats there are several mutually inclusive spheres which are "all facets of the same form of warfare" [8] as;

- Counterterrorism (CT),
- Unconventional Warfare (UW),
- Foreign Internal Defense (FID),
- Counterinsurgency (COIN),
- Stability Operations,
- Peace Keeping,
- Security Force Assistance (SFA),

Dealing with IW threats requires a "whole-of-government" approach. The two trends of 21st century; growing insurgencies, terrorism and growing use of web make it more complicated for military to cope with. As it is clarified in the table below, irregular actors are directed locally, logistically independent, ad hoc forces. They are self-organized civilians who come together for raids and skirmishes and then merge into community and continue their routine daily life.

TABLE I
CONTRASTING DIMENSIONS OF WAR**[9].**

Contrasting Dimensions of War	
Modern	**Irregular**
Organized	Informal
Advanced technology	At-hand technology
Logistics-dependent	Logistics-independent
National direction	Local direction
Coherent doctrine	Ad hoc doctrine
Decisive battle	Raids and skirmishes
Soldier	Warrior
Allies	Accomplices
Segregation	Integration

III. CYBERSPACE AND CYBER WARFARE IN THE NEW SECURITY ENVIRONMENT

Human kind have been living in four physical domains; land, sea, air, and space, and now we how the fifth one cyberspace. How cyberspace and cyber warfare effect IW? In order to answer this question first we have to define cyberspace and cyber warfare. Policy makers recognized the importance of cyberspace and cyber warfare with the cyber attacks on some countries' network systems in 2007 and 2008 [10]. But it is still impossible to draw the borders of cyberspace and cyber warfare. Cyber is a new phenomenon that no one knows where it begins and where it ends. It is a multidimensional dynamic stuff connected with lots of domains, and has many diverse characteristics that suggest that its future may differ significantly from its present [11]. The term "cyberspace" is used by William Gibson in his science fiction novel "*Neuromancer*" and took its place in our lexicon for two decades. Even so there is no consensus over the meaning of it. To give a comprehensive definition, Cyberspace is "*a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies* [12]."

It is possible to say that cyberspace and cyber warfare mainly take place through interconnected and interdependent information and communication technologies. Both of information and communication technologies are extremely used by IW actors such as, insurgents, terrorist organizations, multinational criminals and states.

In cyber warfare, preemptive strikes are favored. Well-trained cyber soldiers make it hard for any government to track down the origin of the attack and retaliate. As we mentioned before irregular warfare is about the legitimacy and popular support. The most critical impact of the cyber-attacks will be on the will of the population. Cyber weapons can be used to cause a cascading series of technology failures, beginning with the telecommunication systems, DDoS attacks against government sites, banking systems, and civil corporation networks. Cyber warriors target military technologies and critical civilian infrastructures, or anything else the adversary values, to create a chronic loss of services, such as, transportation system, causing mess in the airports, harbors, railways, damaging water pipeline, oil and nuclear power plants, electricity, overloading emergency calls, hospitals, releasing water from dams and causing flood, cutting media and communication channels, television, telephone services to name few. If attacks continue for weeks either in a continuous or sporadic mode, may cause chaos and loss of confidence in the government's capability to secure daily life and erodes popular support.

Besides aforementioned capabilities, cyberspace presents perfect tools for irregular fighters. According to the "Social Movement Theory" organizational skills are one of the most essential elements for success of any social movement [13]. In order to organize people without a targetable leadership is a significant asset for irregular warriors. With the invent of at-hand technology devices such as, smart phones and tablet PC's, cyberspace and social media offered opportunity for irregular warriors to influence people with activities including internet, television, radio, cell phones and special applications to generate self organized civilians. After the appearance of the internet, as can be seen in the Arab Spring, the ability of IW actors to organize simple minded civilians around a mutual goal to participate in their plans has risen significantly [14]. An Egyptian blogger explains it as; "*Before this social revolution, everyone was very individual, very single, very isolated and oppressed in islands. But social media has created bridges, has created channels between individuals, between activists, between even ordinary men, to speak out, to know that there are other men who think like me. We can work together, we can*

make something together [15].*"*

Legitimacy is directly linked with the strategy of "winning hearts and minds", "battle of narratives" or "war of ideas" and winning this battle is more important than actual achievements on the military battlefield. Cyberspace, particularly internet and social media have become the main arena for these battle of narratives. Social networks "open new opportunities to recruit the essential public support, international as well as domestic, to military operations [16]." Wars of ideas "…help boost morale and generate material contribution and other support for the physical fighting [17]".

Irregular warfare is generally not a technology intensive activity. It is a human centric form of warfare. But most of the modern armies are equipped with cutting edge weapon systems and experiencing difficulties in adapting to new irregular security environment. While dealing with irregular threats these $ billion investments get useless or in some cases harmful for the grand strategy by inflicting unintended casualties on civilians. It is difficult to differentiate between combatants and non combatants in an irregular conflict because combatants are inherent parts of the society and manage to get innocent civilians involve in the conflict by information and communication technologies. These collateral damages arouse international interest in the conflict and help insurgents or terrorists convey their purposes, goals and ideology by using cyberspace assets, social media, and internet to gain popular support and question the legitimacy of the states.

On the other hand, contrary to the states' $ billion investments, irregular warriors can cultivate simple tactics and weapons like improvised explosive devices and overcome technological superiority in irregular warfare. They can easily access every bit of information about weapons and their vulnerabilities and spread it worldwide through internet.

IV. Conclusion

New security environment resembles "a jungle filled with a bewildering variety of poisonous snakes." Militarily weaker parts of any conflict will most probably resort to tactics such as guerrilla warfare, terrorism, sabotage, subversion, criminal activities, and insurgency.

Cyberspace is also a new phenomenon which took place in our lexicon almost for two decades. Although there is no consensus over the definition of cyberspace, there is no doubt that it will be one of the indispensible parts of our life in the future. Interdependent and interconnected networks and devices using information and communication technology, offers perfect tools for irregular actors to gain or erode popular support and question the legitimacy of the opponent. It helps winning hearts and minds in the long run.

To win an irregular conflict which is a prolonged and low-technology intensive conflict, states have to have highly trained, culturally educated, joint capacity and interagency efforts.

Acknowledgment

We thank to War Colleges Command, Army War College, Dept. of Combat Tactic staff officers for their valuable contributions.

References

[1] I. Berman, Reviewed by Samara Greenberg, "Retaking the Offensive Against Radical Islam", *inFocus*, Winter 2010, vol 4, number 4, (2010), July 22, 2011, pp.140. http://www.jewishpolicycenter.org/2147/winning-the-long-war accessed by July 05, 2013.

[2] US Department of Defense,*: Dictionary of Military and Associated Terms*, Joint Publication 1-02 (JP 1-02), 2007 http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf accessed July 08, 2013.

[3] R. B. Scaife, "The Regularity of Irregular Warfare", *Small Wars Journal Article*, October 16, 2012. http://smallwarsjournal.com/jrnl/art/the-regularity-of-irregular-warfare accessed, July 08, 2013.

[4] S. G. Jones, *The Future of Irregular Warfare*, RAND Corporation March 27, 2012. http://www.rand.org/content/dam/rand/pubs/testimonies/2012/RAND_CT374.pdf accessed July 08, 2013

[5] US Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (JP 1-02), 2007 http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf accessed July 08, 2013.

[6] R. B. Scaife, "The Regularity of Irregular Warfare", *Small Wars Journal Article*, October 16, 2012. http://smallwarsjournal.com/jrnl/art/the-regularity-of-irregular-warfare accessed, July 08, 2013.

[7] S. G. Jones, *The Future of Irregular Warfare*, RAND Corporation March 27, 2012. http://www.rand.org/content/dam/rand/pubs/testimonies/2012/RAND_CT374.pdf accessed July 08, 2013

[8] R. B. Scaife, "The Regularity of Irregular Warfare", *Small Wars Journal Article*, October 16 2012. http://smallwarsjournal.com/jrnl/art/the-regularity-of-irregular-warfare accessed, July 08, 2013.

[9] J. B. White, *Some Thoughts on Irregular Warfare; A Different Kind of Threat*, Defense Intelligence Agency, April 14, 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a07p.pdf accessed July 09, 2013.

[10] S. Mansfield-Devine, Estonia: "What doesn't Kill You Makes You Stronger", *Network Security*, July 2012, pp.12-20 http://www.sciencedirect.com/science/article/pii/S135348581270065X accessed June 10, 2013

[11] F. D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework", *Cyberpower and National Security*, Center for Technology and National Security Policy, Potomac Books, 2009. pp.3-23

[12] D. T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", *Cyberpower and National Security*, Center for Technology and National Security Policy, Potomac Books, 2009. pp.24-42

[13] C. Jenkins, "Resource Mobilization Theory and the Study of Social Movements", *Annual Review of Sociology*, vol 9, 1983. pp.527-553

[14] O. Fridman, *The Power of Social Media: Analyzing Challenges and Opportunities for the future Military Operations*, University of London, March 20, 2013. http://academia.edu/3622572/The_Power_of_Social_Media_Analyzing_Challenges_and_Opportunities_for_the_Future_Military_Operations accessed July 09, 2013

[15] Egptian blogger Hassan Mostafa, cited in "Streetbook….." http://www.technologyreview.com/featuredstory/425137/streetbook/ accessed, July 10, 2013.

[16] O. Fridman, *The Power of Social Media: Analyzing Challenges and Opportunities for the future Military Operations*, University of London, March 20, 2013. http://academia.edu/3622572/The_Power_of_Social_Media_Analyzing_Challenges_and_Opportunities_for_the_Future_Military_Operations , accessed July 09, 2013

[17] A. J. Echevarria, *Wars of Ideas and the War of Ideas*, Strategic Studies Institute US Army War College, 2008. p.3 http://www.strategicstudiesinstitute.army.mil/pdffiles/pub866.pdf accessed, July 08, 2013.

AUTHORS' PROFILE



Hilmi Kendircioğlu received the B.S. degree in System Engineering from Turkish Military Academy in 2003. He was accepted in the Naval Postgraduate School (NPS) in California, and received M.S. degree in Special Operations Defense Analysis in 2011. He currently continues his study at the Turkish Army War College. He is interested in international terrorism, terrorism financing, cultural awareness, special operations, irregular warfare, cyberspace and cyber warfare.

Tuncay Kaymazlı War Colleges Command, Army War College, Instructor, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: tuncaykaymazlı@gmail.com)

Alper Alpaslan Eker War Colleges Command, Army War College, Instructor, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: alpereker99@gmail.com)

Bulut Ortamında Adli Bilişim

Onur SEVLİ, Ecir Uğur KÜÇÜKSİLLE

***Özet*—Bulut bilişim, sunduğu olanaklarla bilgi teknolojileri alanında önemli bir noktaya gelmiş ve son yıllarda bulut bilişime olan yönelim hızlı bir artış göstermiştir. Sunduğu imkânların yanında bir takım riskleri de beraberinde getiriyor olması bulut ortamına aktarılan verilerin güvenliği konusundaki kaygıları arttırmaktadır. Ayrıca bulut bilişim, yapısal özelliklerini çıkar amaçlı kullanmaya yönelen suçluların da hedefi haline gelmiştir. Bunun sonucu olarak bulut üzerinde işlenen bilişim suçları yaygınlaşmakta ve bulut üzerinde yapılan adli soruşturmaların önemi artmaktadır. Bulut üzerinden delil elde etme önemli hale gelmekte ve dijital adli bilişim bulut bilişimi de kapsayacak şekilde yeniden biçimlenmektedir.**

***Anahtar Kelimeler*—Adli bilişim, Bulut bilişim, Dijital delil, Veri güvenliği**

***Abstract* —Cloud computing has come to an important point in the field of information technologies thanks to the opportunities it provides. Recently, tendency to the cloud computing has remarkably grown. Besides it's opportunities cloud computing brings up a number of risks, thus security concerns for the data transferred to cloud environment have been increasing. In addition, cloud computing has become a target for criminals who tends to use cloud's structural features for their own benefits. As a result of these, cyber crimes on the cloud have been widespread and the importance of forensic investigations on the cloud has been increasing. Obtaining digital evidence from cloud environment has been becoming more important and digital forensics have been reshaping to cover the cloud computing.**

***Index Terms* —Computer forensic, Cloud computing, Digital evidence, Data security**

I. GİRİŞ

BİLGİ teknolojilerinin tarihi gelişim sürecinde, bir sistem ya da uygulama üzerinde depolanan verilerin, yasadışı erişimlere karşı hiçbir zaman, tam anlamıyla korunaklı olmadığı görülmektedir [1]. Bulut bilişim ortamlarında ise bu risk daha da artmaktadır.

Bulut bilişim, bir veri merkezindeki çok sayıda bilgisayarı birbirine bağlayıp bunlar üzerinde sanallaştırılmış bir platform oluşturarak, yazılım ve donanım servislerinin kullanımına yeni bir yaklaşım getiren dağıtım modelidir [2]–[3]. Kaynakların birden çok kullanıcı arasında paylaşımı temeline dayanan bulut bilişimde, kullanıcıların alt yapı yatırım maliyetleri sıfıra iner ve hizmet sağlayıcının sunduğu ortak altyapı kiralanarak kullanılır. Ancak bu ortak kullanım belirli güvenlik risklerini de beraberinde getirmektedir.

Bulut bilişim sistemleri, dijital verilerin dağıtık olarak işlenmesine yönelik yeni bir kavram ortaya koyar [4]. Veriler birden çok sunucu üzerinde, kullanıcıdan soyut bir şekilde, dağıtılarak işlenir. İşlem anında verilerin hangi konum ve cihazlar üzerinde yer aldığı konusunda hizmet kullanıcıları bilgi sahibi değildir. Bulut bilişim, bu dağıtık ve sanallaştırılmış yapısından dolayı kullanıcıların güvenlik kaygılarını arttırmaktadır [5]–[6].

Bulut servis sağlayıcıları, servis erişilebilirliği ve maliyet uygunluğunu sağlayabilmek için veri merkezlerini dünyanın farklı coğrafyalarına inşa ederler. Bir veri merkezinde depolanan veriler, güvenlik risklerini azaltmak için başka konumlara da yedeklenir [20]. Farklı ülkelerin veri güvenliği konusundaki farklı yaptırımları, adli bilişim soruşturmalarda sorun teşkil edebilmektedir [4].

Bulut bilişim, internet tabanlı bir model olmasından dolayı güvenlik tehditleri ve gizlilik ihlallerine açıktır [7]. Suçlular bulut bilişimi, suç delillerini saklamak, saldırılar yapmak, şifreleme anahtarlarını kırmak gibi çeşitli amaçlar için kullanmaktadırlar [8]. Bulut bilişim servisleri içerisinde en çok kullanılanlardan biri depolama servisidir [9]. Zaman içinde kuruluşlar, bulut depolama hizmetini kredi kartı bilgileri ve diğer hassas verilerini de depolamak amacıyla kullanmaya yönelmişlerdir. Suçlular bulut ortamındaki bu verileri hedef aldıkları zaman, karmaşık bir adli soruşturma süreci başlamakta ve dijital soruşturmacıların olayla ilgili delil elde edebilmeleri için zorlu bir yol izlemeleri gerekmektedir[8].

Adli bilişim, bilişim sistemleri üzerinden veri olarak elde edilen delillerin toplanması, saklanması, derlenmesi ve analizi konusunda ilke ve standartlar oluşturan disiplinler arası bir bilim dalıdır [10]. Bulut ortamlarında potansiyel dijital riskleri tanımlama, dijital delilleri elde etme ve analiz kritik bir öneme sahiptir. Geleneksel adli bilişim yaklaşımı bulut bilişime tam olarak hitap etmediğinden dolayı, adli bilişim süreci bulut bilişim üzerinde yeniden yapılanma yoluna gitmiştir.

II. BULUT BİLİŞİM

Bulut bilişim; bir kuruluşun kendi bünyesinde ya da kamusal bir ağda, çok sayıda bilgisayar ve ağ cihazının birbirine bağlanması ile oluşturulan bir veri merkezi üzerine kurulu sanallaştırılmış bir ortamda, altyapı ve uygulamaların hizmet olarak sunulduğu dağıtım ve destek modelidir. Bulut bilişim bilgisayarların yeteneklerini genişleterek, kullanıcıların bir veri merkezinde yer alan bir dizi yazılım ve

Onur SEVLİ, Mehmet Akif Ersoy Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, 1530, Burdur, Türkiye. (Telefon:+90 248 213 4130 e-mail: onursevli@mehmetakif.edu.tr).

Ecir Uğur KÜÇÜKSİLLE, Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 32260, Isparta, Türkiye. (e-mail: ecirkucuksille@sdu.edu.tr).

servise web servisi ya da web tarayıcı benzeri yazılımlarla, internet üzerinden erişebilmelerini sağlar [11] – [12].

Dijital cihazların ve internet kullanımının yaygınlaşması ile birlikte bulut bilişime rağbet artmıştır. Servis mimarisine dayalı bulut bilişim; veri ve uygulamalara, cihazdan bağımsız olarak erişebilmeyi, uygulamaların yaygınlaştırılıp kolaylıkla ölçeklenebilmesini sağlamaktadır. Bulut ortamına taşınan uygulamalar sayesinde yazılımlar pahalı birer ürün olmaktan çıkıp, "kullandığın kadar öde" mantığı ile hizmete sunulmuştur. Bu anlamda bulut bilişim uygulama geliştiriciler için de yeni bir pazar haline gelmiştir [13].

Zaman içinde bulut bilişim, teknolojik yaşamın vazgeçilmezi haline gelmiştir [14]. Bulut servislerinin kullanımı, büyük şirketlerin tekelinden çıkmış, küçük işletmeler ve bireysel kullanıcılar da bulutun işlem gücüne erişebilir hale gelmişlerdir.

A. *Bulut Bilişimin Karakteristik Özellikleri*

Bulut bilişimin temelinde aşağıdaki karakteristik özellikler yer almaktadır:

Sanallaştırma

Sanallaştırma; fiziksel bir kaynağı, ihtiyaçlar doğrultusunda, istenilen sayıda mantıksal parçaya bölerek, toplam sunucu verimliliğini optimize hale getirmeye yönelik bir teknolojidir. [15]. Bulut mimarisinde, bir veri merkezimin yekpare fiziksel altyapısı, sanallaştırma teknolojisi ile çok sayıda sanal sistem haline getirilip, her bir sistem farklı müşterilere hizmet olarak sunulabilmektedir.

İhtiyaca Bağlı Ölçekleme

Bulut bilişim platformları, kullanıcıların isteğine bağlı olarak, mevcut altyapıya yeni servis ve kaynakların eklenebilmesine imkân sunar. Yeni kaynak sisteme son derece hızlı bir şekilde eklenip, kullanıma hazır hale getirilir. Bu durum maliyet ve zaman açısından son derece kazançlıdır.

Farklı Coğrafyalarda Konuşlanmış Veri Merkezleri

Dünya çapında hizmet sunarken, farklı coğrafyalarda veri merkezlerine sahip olmak büyük öneme sahiptir. Bu yapının oluşturulması; ulusal ya da uluslararası yasalar, jeopolitik fikirler, yük dengeleme, ağ gecikmelerini minimuma indirme gibi durumlar açısından gereklidir [16].

B. *Bulut Bilişim Servisleri*

Kabul edilen üç genel bulut servis dağıtım modeli vardır:

Servis Olarak Altyapı (IaaS)

Bulut bilişim altyapısında, yığının en alt tabakasındaki fiziksel servisleri ifade eder. Bu tabaka; sanal makineler, yük dengeleme servisleri, ağa bağlı depolama servisleri gibi temel donanım servislerini içerir.



Şekil 1. Bulut bilişim servisleri

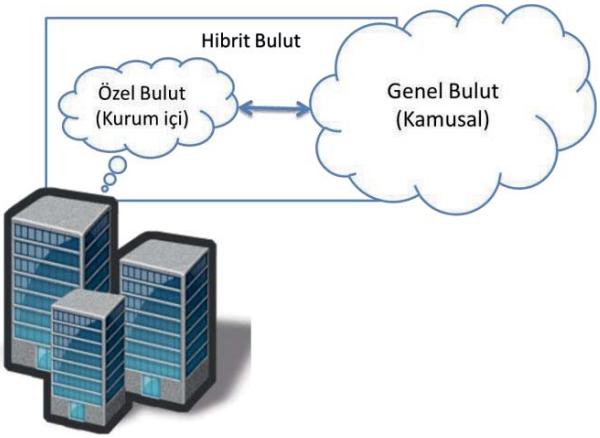
Servis Olarak Platform (PaaS)

Uygulama geliştirmek için kullanılan altyapıyı oluşturur. Bulut hizmeti alan kullanıcılar, geliştirdikleri uygulamaları, servis sağlayıcı tarafından sunulan platform üzerinde, özelleştirilmiş bir ortamda çalıştırırlar. Bu ortam çoğu zaman kısıtlanmış, düşük imtiyazlı bir yapıdadır.

Servis Olarak Yazılım (SaaS)

Hazırlanan bulut uygulamalarının sergilendiği katmanı ifade eder. Bir bulut altyapısı üzerinde çalışan uygulamalar, servis kullanıcılarına, bu katmanda hizmet olarak sunulmaktadır. Sunulan uygulamalara, internet üzerinden zaman ve konum kısıtlaması olmaksızın erişilebilmektedir.

C. *Bulut Bilişim Mimari Modelleri*



Şekil 2. Bulut bilişim mimari modelleri

Özel Bulut

Bir kurumun kendi bünyesinde yer alan veri merkezleri üzerinde kurmuş olduğu bulut yapısıdır. Bilişim dünyasında uzun süredir uygulanan geleneksel modeldir. Veri güvenlik ve gizliliğinin üst düzeyde tutulmasını gerektiren durumlarda tercih edilmektedir. Özel bulut, bir güvenlik duvarının ardında, şirketin sınırlı sayıdaki kullanıcılarına hizmet vermektedir.

Genel Bulut

Standart olarak kabul edilen bulut bilişim modelidir. Bir

bulut servis sağlayıcı tarafından oluşturulan altyapı üzerindeki kaynaklar, uygulamalar, hizmetler, internet üzerinden kamusal ölçekte kullanıma sunulur. Veriler kamusal bir ağda yer alacağı için yapının kendine has güvenlik riskleri mevcuttur.

Hibrit Bulut

Bir kuruluşun kendi bünyesinde barındırıp yönettiği kaynaklarla, harici altyapı kaynaklarının birleştirilmesi sonucu oluşan bulut modelidir. Bu modelde kurum içi servislere harici bulut servisleri entegre edilip, bir bütün oluşturacak şekilde çalıştırılır.

D. Bulut Bilişimde Güvenlik ve Kriptografi

Güvenlik ve veri gizliliği, bulut bilişimin yaygınlaşması açısından önemli bir konudur [17]. Ancak bulut bilişimde aynı fiziksel altyapıyı birden fazla kullanıcının paylaşarak kullanması, altyapı üzerinde barındırılan verilerin güvenliği konusunda süregelen riskler oluşturmaktadır [18].

Bilhassa genel bulut mimarisinde kullanıcılar, hassas bilgilerin de içerisinde yer aldığı verilerini servis sağlayıcı altyapısında barındırma ihtiyacı duymaktadır. Bulut servis sağlayıcılar her ne kadar üst düzey güvenlik önlemleri alsalar da veri güvenliği konusundaki riskler bitmemektedir. Bulut mimarisinde farklı kullanıcıların ortak altyapıda depolama yapmalarından dolayı, bellek alanlarını birbirinden ayıran iç mekanizmalarda ortaya çıkabilecek sızıntılar yahut saldırılar sonucu kullanıcıların özel verilerinin üçüncü şahıslar tarafından ele geçirilme tehlikesi vardır [19].

Gizlilik ihlali riskinden korunmak için farklı yöntemler uygulanabilir. Bu yöntemlerden biri hibrit bulut modelini kullanıp gizliliği yüksek verileri kurum içi altyapılarda işlerken, güvenlik açısından risk teşkil etmeyen işlemleri genel bulut servisleri üzerinde gerçekleştirmektir.

Veri güvenliği ve gizliliği konusunda ortaya çıkan riskleri azaltmak için kullanılan bir başka temel yöntem ise kriptografidir. Homomorphic kriptografi gibi çeşitli algoritmalar ile şifrelenen veri, gizliliği ihlal eden üçüncü şahıslara karşı anlaşılmaz hale getirilmektedir. Kriptografik işlemler bulut servis sağlayıcılar tarafından gerçekleştirilebildiği gibi, veri sahibi kullanıcılar tarafından da yapılabilmektedir.

Kriptografi veri güvenliği için vazgeçilmez yöntemlerden biri olmakla birlikte, adli bilişim sürecinde belirli sorunlara yol açmaktadır. Bulut üzerinde elde edilen delillerin şifrelenmiş olması adli bilişim sürecine ek bir yük getirmektedir.

III. ADLİ BİLİŞİM

Teknolojinin gelişip yaygınlaşması ile birlikte bilişim suçları da artış göstermiştir. Bu durum suçla mücadelede, adli bilişimin önemini arttırmaktadır.

Adli bilişim; bilimsel prensipler ve teknolojik olanakların suçların çözümlenmesi ve yargılanmasında kullanılmasıdır. Diğer bir ifadeyle adli bilişim, bilgisayarlı soruşturma ve analiz tekniklerinin potansiyel delilleri tespit etmek amacıyla kullanılması olarak tanımlanabilir [21].

Geleneksel adli bilişim; bir soruşturmada ele geçirilen bilgisayar, yazılım, veri, işletim sistemlerinin analizi ile ilgilenmektedir. Fakat bu geleneksel bakış; kullanıcıdan uygulamalara, sunuculardan verilere kadar her yönüyle dağıtık olan bulut bilişim modelini tam anlamıyla kapsayamamaktadır.

A. Adli Bilişim Soruşturma Süreci

Adli bilişim soruşturmaları doğrusal bir işlem süreci izler. Bu sürecin temel adımları; tanımlama, çıkarım, analiz ve delilin sunumudur.

İlk aşamada, analist potansiyel delil kaynağını tanımlar: Şüphelenilen suç ne, şüpheli tarafından hangi donanım ya da yazılımlar kullanılmış, deliller nerede saklanıyor?

İkinci aşamada deliller, potansiyel kaynaklar üzerinden, bütünlüğü sağlanacak şekilde çıkarılır. Bilgisayar ortamı somut bir ortam değildir ve sanal ortamdaki veriler uçucudur. Analist bu uçuculuğun farkında olmalı ve çıkarım sürecinde bu problemi azaltacak araç ve teknikleri kullanmalıdır.

Üçüncü aşamada, çıkarım sonucu elde edilen veriler analiz edilir. Analiz, olay anında canlı olarak yapılabilir veya veriler bir adli bilişim laboratuvarına nakledilerek orada incelenebilir.

Son aşamada ise elde edilen sonuçlar, geçerli bir delil teşkil edecek şekilde hazır hale getirilir ve mahkemeye sunulur.

Bulut bilişim ortamında gerçekleştirilen adli bilişim süreci daha karmaşık yapıdadır. Bulutun dinamik ve dağıtık yapısından dolayı, altyapı üzerinden potansiyel delil verileri elde etmek ve verilerin doğruluğunu garanti edecek şekilde korumak daha zor bir hâl almaktadır.

IV. BULUT ORTAMINDA ADLİ BİLİŞİM

Bulut bilişimin sanallaştırılmış bir ortamda dağıtık veri işleme modeli, dinamik ölçeklenebilen altyapısı, farklı coğrafyalara yayılan veri merkezleri, kaynaklarının çok sayıda kullanıcı arasında paylaşılarak kullanılması gibi özelliklerinden dolayı bulut ortamında yapılan adli soruşturmalar daha karmaşık bir hâl almaktadır. Geleneksel adli bilişim yaklaşımı bulut bilişim ortamında karşılaşılan sorunları tam olarak çözümleyemediği için; adli bilişime, buluta doğru genişleyen yeni bir bakış kazandırmaya yönelik çalışmalar yapılmaktadır.

Bulut adli bilişim, bulut bilişim ile dijital adli bilişimin kesişim noktasında, ağ adli bilişimin bir alt parçasıdır. Ağ adli bilişim, bilgisayar ağları üzerinde yapılan adli soruşturmalar ile ilgilidir. Bulut bilişimin de geniş bir ağ üzerine kurulu olmasından dolayı bulut adli bilişim, ağ adli bilişimin işleyiş sürecini temel alır [20].

Bulutun son derece esnek bir yapısı vardır. Bu nedenle bulut ortamında yapılan adli soruşturmalarda, delil toplamaya yönelik araç ve süreçlerin de aynı esneklikte olması gereklidir. Bulutun önemli bir karakteristiği de kaynakların, çok sayıda kullanıcı arasında paylaşılarak kullanılmasıdır. Bu nedenle soruşturmalar sırasında aynı fiziksel kaynak üzerindeki farklı kullanıcılardan yalnız soruşturmaya hedef olanın ayırt edilmesi gereklidir.

Soruşturma esnasında bulut bilişim hizmetlerinde herhangi bir aksamaya da meydan verilmemelidir.

A. Bulut Üzerinde Adli Bilişim Süreci

Dijital adli bilişim uygulamalarına temel oluşturmak üzere geliştirilen ISO 27037 standardına göre, adli bilişim sürecinde tanımlama, toplama ve koruma adımları yer alır. Buna ek olarak analiz, yorumlama ve raporlama adımları da sürece dâhil olmuştur.

Delili Tanımlama

Potansiyel dijital delilin fark edilip belgelendirilmesi için yapılan aramayı kapsayan süreçtir [22]. Bulut bilişim ortamında tanımlama süreci son derece karmaşık bir hâl alabilmektedir.

Bulut bilişim altyapıları, büyük ölçekli bir veri merkezi üzerinde çok sayıda depolama ve işlem kaynağının birbirine bağlanması ile meydana gelir. Hatta bulut bilişim platformları birden çok veri merkezini de birbirine bağlayarak çok sayıda kaynağı yekpare bir bütün olarak çalıştırmaktadır. Bulut ortamına aktarılan veriler, sistem içerisindeki dağıtım mekanizmaları tarafından çok sayıda depolama ve işlem kaynağı üzerine aktarılır. Bulut ortamında saklanan verilerin gerçek anlamda hangi konumda depolandıkları ve işlem gördükleri kullanıcılardan soyutlanmıştır. Bundan dolayı delil toplama sürecinde verinin bulunduğu konumun tespiti ve delilin elde edilmesi zorlaşmaktadır. Delillerin potansiyel konumlarına, servis sağlayıcıların sunduğu kayıtlar ya da çeşitli uygulama logları üzerinden elde edilen izlerle ulaşılabilmektedir.

Delil Toplama

Kanunlar çerçevesinde, potansiyel delil içeren unsurları derleme sürecidir.

Bulut mimarisinde veriler dağıtık bir altyapı ve sanallaştırılmış bir ortamda tutulduğundan dolayı delil toplama süreci zorlaşmaktadır. Çok sayıda kaynak üzerine dağılmış verilerin toplanıp, bütünlüğünün sağlanarak kabul edilebilir bir delil haline dönüştürülmesi kolay değildir. Bulut bilişimin sanallaştırılmış yapısından dolayı bir takım veriler belirli bir süre sonra yok olabilmektedir. Delil toplama aşamasında bu durumun da dikkate alınarak, işlemlerin son derece seri bir şekilde gerçekleştirilmesi gerekmektedir.

Koruma

Potansiyel dijital delilin bütünlük ve orijinal durumunun muhafaza edilmesi sürecini ifade eder [22]. Koruma, hukuk mahkemesinde delilin kabul edilebilirliğine etki eder. Dijital delillerin değiştirilmesi ya da yok edilmesi kolaydır. Bu nedenle koruma sürecinde, verilerin kazara ya da kasti bir şekilde değiştirilmesine karşı gerekli önlemler alınmalıdır.

Analiz

Potansiyel bir delil kaynağından elde edilen delil öğelerinin işlenmesi sürecidir [22]. Analiz, durağan ya da canlı olarak yapılabilir. Yinelemeli bir süreç olup, süreç içinde ortaya çıkan sorular yeni analiz süreçleri doğurabilir.

Yorumlama

Soruşturmayı gerçekleştirmek için, analiz ve incelemeler sonucu elde edilen verilerin sentezlenerek gerçeğe dayalı delilin ortaya çıkarılması sürecidir [22].

Raporlama

Analiz ve yorumlama sonucunda elde edilen sonuçların yazılı veya sözlü olarak sunumunu içine alan süreçtir.

B. Bulut Ortamından Delil Elde Etme ve Karşılaşılan Zorluklar

Bulut bilişim ortamlarında yürütülen adli soruşturmalarda, kullanılan bulut bilişim mimari modeline bağlı olarak çeşitli zorluklar ortaya çıkabilmektedir. Başka bir kuruluş tarafından yönetilen genel bulut mimarisi üzerinden delil elde etmek, bir kuruluşun kendi bünyesindeki özel buluta nazaran daha zordur [23].

Özel bulut mimarisinde bilgi teknolojileri altyapısı kuruluşun kendi bünyesinde yer almaktadır. Bu nedenle potansiyel delillerin araştırılacağı alan kapalı ve sınırlıdır. Genel bulut mimarisinde ise kamusal bir ağ üzerinde son derece geniş ve çok sayıda kullanıcının paylaştığı, dinamik olarak ölçeklenen bir altyapı vardır. Genel bulut mimarisinde veriler farklı ülkelerde yer alan veri merkezlerinde tutulabilir. Veriler, kullanım esnasında bir noktadan başka bir noktaya sürekli göç halindedir. Ayrıca verinin birden çok noktada kopyaları da bulunabilir. Bulut servisi üzerinde yer alan verilerin herhangi bir zaman diliminde hangi konumda tutulduğunu kestirmek zordur.

Sanallaştırılmış bulut ortamında yer alan bazı veriler uçucu nitelikte olabilmektedir. Bu da bir takım verilerin geri getirilemez olmasına neden olmaktadır.

Kamuya açık bir ağa, hassas verilerini göndermek bulut bilişim kullanıcılarını endişelendirmektedir. Altyapının internete açık olması, paylaşılarak kullanılan kaynaklar veri güvenliği üzerinde risk oluşturmaktadır. Bu nedenle kullanıcılar, verilerini bulut ortamına göndermeden önce şifreleme yoluna gitmektedir. Bu durum veri güvenliğini arttırmakta ancak, adli bilişim soruşturmalarında potansiyel delillerin çözümlenmesini zorlaştırmaktadır.

Genel bulut mimarisinde veriler ülke sınırları dışında yer alan veri merkezlerinde de tutulabilmektedir. Bulut hizmetinin kullanıldığı ülkede suç teşkil eden bir durum, iş sürecinin üzerinde gerçekleştiği veri merkezlerinin sınırları içinde bulunduğu ülke yasalarınca suç sayılmayabilir. Bu gibi durumlarda adli bilişim soruşturmaları ve uygulanacak yaptırımlar için uluslararası işbirliklerine gerek duyulmaktadır.

Bulut ortamından delil elde etme konusunda kullanıcıların yetenekleri, kullanılan bulut bilişim servis modeline bağlı olarak kısıtlılıklar göstermektedir. Kullanıcıların kısıtlandığı durumlarda bulut servis sağlayıcılardan talepte bulunulmaktadır. Kullanılan servis modeline bağlı olarak delil elde etme konusunda kullanıcılar ve servis sağlayıcıların olanakları şu şekildedir:

SaaS Modeli

SaaS modeli kullanıcıların delil elde etme yeteneği açıcından en kısıtlı olduğu modeldir. Hizmet kullanıcıları altyapının işleyen mekanizmaları (sunucular, işletim

sistemleri kaynak kodlar vs.) üzerinde kontrole sahip değildir. Bu durum kullanıcıların adli bilişim yeteneklerini de kısıtlar. SaaS ortamlarında adli bilişim araştırmacıları uygulama loglarına ve servis sağlayıcının sunduğu adli bilişim fonksiyonelliklerine güvenirler. Gerekli olan adli bilişim fonksiyonellikleri, kullanıcılar ile servis sağlayıcılar arasında yapılan servis düzeyi anlaşmaları (SLA) içerisinde belirtilmektedir.

PaaS Modeli

PaaS modelinin en büyük avantajlarından biri; hizmet kullanıcılarının, geliştirilen uygulamayı ve kaynak kodları kontrol etme yeteneğine sahip olmalarıdır. Bu durumda kullanıcılar, uygulamaların içerisine adli bilişim yeteneklerini (otomatik log mekanizmaları vs.) yerleştirebilirler. Kullanıcılar uygulamanın fonksiyonelliğini kontrol etme gücüne sahip olmakla birlikte, uygulamanın çalışması yine servis sağlayıcı altyapısında gerçekleşmektedir. Bu nedenle, PaaS modelinde, kullanıcı ve servis sağlayıcılar arasında bir koordinasyona gerek duyulur.

IaaS Modeli

SaaS ve PaaS ile kıyaslandığında IaaS, büyük bir delil elde etme potansiyelini kullanıcıların kontrolüne sunar. Kullanıcılar, altyapı kaynaklarına daha çok müdahile edip ve bu kaynaklardan veri elde edebilmektedir. Bunun yanında bazı, belki de çok kritik veriler servis sağlayıcı altyapısında ve onun kontrolündedir. Bu nedenle, yine kullanıcılar ve servis sağlayıcılar arası bir koordinasyon gereklidir.

C. Servis Düzeyi Anlaşması (Service Level Agreement – SLA)

Bulut bilişim servis sağlayıcıları ile hizmet kullanıcıları arasında, hizmetin sürekliliği ve güvenliğini garanti eden "Servis Düzeyi Anlaşması" (SLA) yapılır [16]. Bu sayede tarafların sorumlulukları belirlenmiş, hizmette süreklilik ve erişilebilirlik garanti edilmiş olur.

Bulut ortamında yapılacak soruşturmalar servis sağlayıcılar ile kullanıcılar arasındaki bu karşılıklı anlaşmalar ve yasal düzenlemelere bağlıdır. Bulut servis sağlayıcılar ile kullanıcılar arasında yapılan SLA, herhangi bir soruşturma anında kullanıcı ve servis sağlayıcının yükümlülüklerini belirler.

D. Bulut Bilişim Ortamında Adli Soruşturma Prosedürleri

Bulut bilişim ortamındaki adli soruşturmalarda ilk göz önünde bulundurulması gereken, hangi bulut bilişim mimari modelinin kullanıldığıdır [7]. Modele bağlı olarak sürecin işleyişi farklılık gösterir. Özel bulut yapısında veriler bir kuruluşun kendi bünyesindeki ya da bir dış destekçinin bilgi işlem altyapısındaki sunucularda yer alır. Ayrıca soruşturma sırasında, kilit isimler olan sistem yöneticisi ya da çalışanlarına da ulaşmak kolaydır.

Kamusal ölçekte bir bulut ortamında işler daha karmaşık hale gelir. Bu ortam dinamiktir ve ihtiyaca göre şekillenebilmektedir [2]. Kullanıcı, tek bir mantıksal konuma erişiyor gibi görünürken arka planda çok sayıda uygulama ile görünmez bir şekilde etkileşim halindedir. Arka plandaki bu görünmez etkileşim ve dağıtım potansiyel delil kaynaklarının tanımlanmasını karmaşıklaştırır.

Soruşturma sırasında altyapıdaki tüm cihazların yerinde ve çalışır vaziyette olması gerekir. Bulut altyapısında veriler farklı konumlarda depolandıkları için her hangi bir sunucunun aktif olmaması delil bütünlüğünü bozabilir.

Bulut ortamında soruşturmaya ilişkin verinin aranacağı geniş bir altyapı olmasına karşı kaynakların erişilebilir olduğu zaman dilimi kısıtlıdır. Bu nedenle araştırmaların son derece planlı ve seri bir şekilde yürütülmesi gerekmektedir.

Kamusal bulut üzerinde adli soruşturma yaparken bulut hizmetinin işleyişi aksatılmamalıdır. Soruşturma esnasında hedefte olmayan diğer kullanıcılar herhangi bir zarara uğratılmamalıdır.

Adli bilişim sürecinde kişisel verilere erişim, kanunlar çerçevesinde gerçekleşir. Soruşturma sırasında bu verilere nasıl ulaşılacağı ve nasıl işleneceğini yasalarca belirlenir ve kişisel veriler koruma altına alınır. Veriler yalnız soruşturma ekibi tarafından incelenebilir, üçüncü şahıslar tarafından görülemez.

V. TÜRKİYE'DE BULUT BİLİŞİM VE ADLİ BİLİŞİM

Son yıllarda hızlı bir gelişim gösteren bulut bilişime yönelim ülkemizde de hızla artmaktadır. Telekomünikasyon, bankacılık, elektronik belge yönetimi gibi pek çok alanda bilgi teknolojileri altyapıları buluta doğru genişlemektedir. Ülkemizde bulut hizmeti veren servis sağlayıcıların sayısı da her geçen gün artmaktadır. 2013 yılı bitimine kadar küresel pazarda bulut hizmetlerindeki büyümenin yüzde 26 seviyesine ulaşacağı, Türkiye'deki büyümenin ise yüzde 54 civarında artacağı tahmin edilmektedir [24].

Bilişim sektöründeki hızlı gelişmeye paralel olarak bilişim alanında işlenen suçların sayısı da giderek artmaktadır. Türkiye dışındaki pek çok ülke daha erken dönemlerde adli bilişim faaliyetlerini başlatmışken, ülkemizde 2006 yılından itibaren aktif anlamda adli bilişim çalışmaları başlamıştır [25].

Ülkemizdeki adli bilişim faaliyetleri gün geçtikçe hızlanmakta, resmi kurumlar ve dernekler adli bilişim konusundaki çalışmalarına ivme kazandırmaktadır. Ancak adli bilişim konusunda ülkemizde yürütülen çalışmalar henüz yeterli seviyede olmayıp bilhassa yeni şekillenen teknolojik gelişmelere paralel ilerlemelerde eksiklikler mevcuttur. Küresel ölçekte bulut bilişim alanında yürütülen adli bilişim çalışmaları da yeni yeni şekillenirken, ülkemizde bulut adli bilişim konusunda henüz önemli bir adım atılmamıştır. Bu anlamda Türkiye'deki adli bilişim çalışmalarına ve çağın teknolojisi olan bulut adli bilişim konusundaki çalışmalara daha çok önem verilmeli ve hız kazandırılmalıdır.

VI. SONUÇ

Bulut bilişim sunduğu olanaklarla günümüzün yaygın kullanılan teknolojilerinden biri haline gelmiştir. Ancak, sunduğu olanakların yanında bir takım güvenlik risklerini de beraberinde getirmektedir. Bulutun sanallaştırılmış, dağıtık

ve paylaşılan altyapısı kullanıcıların veri güvenlik ve gizliliği konusundaki kaygılarını arttırmakta ve bu konuda işlenecek bilişim suçlarına açık kapı bırakmaktadır. Bulut bilişim servis sağlayıcılarının veri merkezlerini farklı ülkelere konuşlandırmaları, veriler üzerinde sınırları içerisinde bulundukları ülkenin yasalarını geçerli kılmaktadır. Ülkelerin veri güvenliği konusundaki yasal boşlukları ve bulut bilişimin sunduğu diğer açık kapılar, bilişimin suçlularını bulut platformlarına doğru çekmektedir. Bulut üzerinde işlenen adli suçların artması ve geleneksel adli bilişim yaklaşımının bulut bilişimi tam anlamıyla kapsamıyor oluşu, adli bilişimin bulut bilişime özgü olarak yeniden yapılanmasını gerektirmiştir. Bulut bilişim sistemlerinden dijital delil elde etmek geleneksel sistemlere nazaran daha karmaşıktır. Adli soruşturmalarda delil elde etme konusunda bulut servis sağlayıcıları ve hizmet kullanıcıları arasındaki karşılıklı sorumluluklar ve koordinasyon önemlidir. Servis sağlayıcılar ve kullanıcılar arasında yapılan servis düzeyi anlaşmaları, tarafların sorumluluklarını belirler. Herhangi bir adli soruşturmada delil elde etme konusunda bulut müşterileri çok sıkıntı yaşadıkları için doğru servis sağlayıcının seçimi büyük önem taşımaktadır. Soruşturma esnasında verilen hizmetinin aksamadan devam etmesi, soruşturmanın hedefinde olmayan kullanıcıların etkilenmemesi, verilerin gizliliğinin korunması gerekmektedir.

KAYNAKLAR

[1] Cloud Security Alliance," Mapping the Forensic Standart ISO/IEC 27037 to Cloud Computing", June 2013.
[2] B. Treacy, "Cloud computing: data protection concerns unwrapped", Privacy and Data Protection, vol. 9(3), 2009, pp. 1-3.
[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Brobery, I. Brandic "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", Future Generation Computer Systems, vol. 25(6), 2009, pp. 599-616.
[4] M. Taylor, J. Haggerty, D. Gresty, R. Hegarty, "Digital evidence in cloud computing systems", Computer Law & Security Review, vol. 26, 2010, pp. 304-308.
[5] Y. Zhang, A. Juels, M. Reiter, T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys", In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, 2012, pp. 305-316.
[6] T. Risenpart, E. Tromer, H. Shacham, S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds" In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). ACM, New York, 2009.
[7] M. Taylor, J. Haggerty, D. Gresty, D. Lamb, "Forensic investigation of cloud computing systems", Network Security, vol. 2011, 2011, pp. 4-10.
[8] E. Casey, "Cloud computing and digital forensics", Digital Investigation, vol. 9, 2012, pp. 69-70.
[9] H. Chung, J. Park, S. Lee, C. Kang, "Digital forensic investigation of cloud storage services", Digital Investigation, vol. 9, 2012, pp. 81-95.
[10] M.G. AHI. (2009, Mart) ."Adli Bilişim Nedir?". *Güncel Hukuk* [Online]. Erişilebilir: http://www.guncelhukuk.com.tr/dergi/
[11] J.F. Rayport, A. Heyward. (2009)." Envisioning the Cloud: The Next Computing Paradigm". *MarketspaceNext* [Online]. Available: http://marketspacenext.com/inthemedia/envisioning-the-cloud/
[12] E. Knorr, G. Gruman. (2008)." What cloud computing really means". *InfoWorld* [Online]. Available: http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031
[13] F. Chong, G. Carraro. (2006, April) ."Architecture Strategies for Catching the Long Tail". *MSDN* [Online]. Available: http://msdn.microsoft.com/en-us/library/aa479069.aspx
[14] T.V. Lillard, C.P. Garrison, C.A. Schiller, J. Steele, *The Future of Cloud Computing*. Boston: Elseiver Inc., 2010, ch.12.
[15] M. Çelik.(2009, Ekim). "Neden Sanallaştırma?".*Bilisim News* [Online]. Erişilebilir: http://www.bilisimnews.com/?p=475
[16] S. Krishnan, *Programming Windows Azure*. USA: O'Reilly Media, 2010.
[17] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol.34 (1), 2011, pp. 1-11.
[18] D. Svantesson, R. Clarke, "Privacy and consumer risks in cloud computing", Computer Law & Security Review, vol. 26 (4), 2010, pp. 391-397.
[19] Y. Korkmaz.(2010, Haziran). "Bulut Bilişim Risk Değerlendirmesi – I". *Tübitak Bilgem* [Online]. Erişilebilir: http://www.bilgiguvenligi.gov.tr/ guvenlik-teknolojileri/bulut-bilisim-risk-degerlendirmesi-i.html
[20] K. Ruan, J. Carty, T. Kechadi, M. Crosbie, "Cloud Forensic", IFIP Advances in Information and Communication Technology, vol. 361, 2011, pp. 35-46.
[21] X. Li, J. Seberry, "Forensic Computing", in *Proc. 4th International Conference on Cryptology in India, New Delhi, India, 2003*, pp.18–35.
[22] *ISO 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence*, ISO/IEC 27037, 2012.
[23] R. Grossman,"The case for cloud computing", IT Professional, vol. 11(2), 2009, pp. 23-27.
[24] Capital Online. (2012, Eylül) ." Türkiye'de Bulut 2013'te yüzde 54 büyüyecek". Capital İş & Ekonomi [Online]. Erişilebilir: http://www.capital.com.tr /turkiyede-bulut-2013te-yuzde-54-buyuyecek-haberler/24990.aspx
[25] S. Kurt.(2011, Aralık). "Adli Bilişim ve Türkiye'de Adli Bilişim". *Çözüm Park* [Online]. Erişilebilir: http://www.cozumpark.com/forums/thread/290988.aspx

Onur SEVLİ, 1987 yılında Isparta'da doğdu. Lisans eğitimini Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Elektronik-Bilgisayar Eğitimi Bölümün'nde 2009 yılında tamamladı. Yüksek lisans eğitimini, Süleyman Demirel Ünivesitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı'nda 2011 yılında tamamladı. Aynı yıl Süleyman Demirel Ünivesitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Ana Bilim Dalı'nda doktora eğitimine başladı. Doktora süreci, tez aşamasında devam etmektedir. Halen Mehmet Akif Ersoy Ünivesitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Bölümü'nde öğretim görevlisi olarak çalışmaktadır. Yazılım, bilişim ve güvenlik konularında çalışmalar yapmaktadır.

Ecir Uğur KÜÇÜKSİLLE, 1976 yılında Isparta'da doğdu. Gazi Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği lisans eğitimini tamamladı. Yüksek lisans eğitimini Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Makine Eğitimi Ana Bilim Dalında yaptı. Doktora eğitimini Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü İşletme/Sayısal Yöntemler Ana Bilim Dalında tamamladı. Halen Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. Bilgisayar, güvenlik ve yapay zeka alanlarında çalışmaları bulunmaktadır.

Bulut Bilişimde Bilgi Güvenliği ve Standardizasyon Çalışmaları

Gökhan Şengül, Atila Bostan

***Abstract*— Widespread usage and increasing speed of digital communication bring about proliferation and rising number of cloud applications which greatly depend on online information and service sharing. Although the technical qualifications have got quite close to user expectations, the principle problem of cloud services is still the security mechanisms between user and service provider, which have not reasonably matured yet. In forming the security mechanisms, dissemination of common standards is of great importance to provide grounds for common understanding and monitoring capability. Furthermore, these standards need to be published and necessary legal actions should be activated. This study aims to call attention to the importance of common security standards in cloud computing and provide a concise summary of ongoing standardization studies in Turkey. The study also points out the significance of cloud computing standards in e-government services.**

***Index Terms*— Security in cloud computing, Cloud computing standards.**

***Özet*— Sayısal iletişimin süratinin artması ve yaygınlaşması, ağ üzerinden hizmet ve veri paylaşım esasına dayanan bulut bilişim uygulamalarının da sayıca atması ve yaygınlaşması için ortam oluşturmaktadır. Teknik yeterliliği kullanıcıları tatmin noktasına oldukça yaklaşan bulut bilişim hizmetlerinin temel problemi hizmet sağlayıcı ve kullanıcı arasında güven mekanizmasının henüz yeterli olgunluk seviyesinde oluşturulamamış olmasıdır. Bu güven mekanizmasının oluşturulmasında ortak anlayış ve denetlenebilirlik sağlaması açısından standardların yayımlanması ve bu standartların rehberliğinde gereken hukuki düzenlemelerin hayata geçilmesine ihtiyaç vardır. Bu çalışmada, bulut bilişimin yayınlaşmasının önündeki en önemli engel olan güvenlik boyutuna dikkat çekilmekte ve Türkiye'de bulut bilişim konusunda devam etmekte olan standart çalışmaları hakkında bilgi verilmektedir. Bulut bilişim ve e-devlet hizmetlerinin bu standard çalışmalarına paralel geliştirilmesinin önemi vurgulanmaktadır.**

***Anahtar Kelimeler*— Bulut bilişimde güvenlik, bulut bilişim güvenlik standardları**

I. GİRİŞ

SAYISAL çağ olarak isimlendirilen 21nci yüzyılın ilk on yıllık döneminde, sayısal ortamların büyük bir hızla sosyalleşmesi gözlenirken, veri saklama ve hesaplama hizmetlerine donanım ve fiziksel mekândan bağımsız erişim sağlayan bulut bilişim uygulamaları da yaygınlaşmaktadır. Bilgisayar ağ altyapısında erişilen sürat ve yaygınlaşmaya paralel olarak, veri ve hizmetlerin ağ üzerinden kullanılması daha cazip hale gelmektedir. E-ticaret, e-bankacılık, e-devlet ve uzaktan eğitim gibi geniş kullanıcı kitlesine hitap eden hizmetler internet ağı üzerinde başarılı bir şekilde kullanılmaktadır. Bütün bu gelişmelerin yanında bulut bilişim yaklaşımı özellikle hizmet maliyetlerini düşürmesi ve yüksek erişilebilirlik özellikleri ile yeni fırsatlar yaratmaktadır. Yapılan stratejik değerlendirmeler, bulut bilişim uygulamalarının yaygınlaşacağını ve bu alanda ekonomik gelişmeler yaşanacağına işaret etmektedir. Dünya genelinde bu alandaki pazarın 2010 yılında 21,5 milyar dolar olduğu belirtilirken, 2015 yılı için bu rakamın 73 milyar dolara ulaşacağı öngörülmektedir [1]. AB ekonomisinde de bulut bilişimin önemli bir stratejik etken olması beklenmektedir [2].

Bulut bilişim konusunda yapılan inceleme ve araştırmalar güvenlik ve kişisel bilginin korunması boyutlarının bu teknolojinin yaygınlaşmasının önünde en önemli engelleri oluşturduğu konusunda hem fikirdir [3], [4], [5]. Bu engellerin aşılması için ise öngörülen çözüm yolu, alanda ortak standartların belirlenmesi ve hukuki düzenlemelerin yapılması olarak ortaya çıkmaktadır.

Varadi ve diğerlerinin [6] de belirttiği gibi, bilgi güvenliğinin sağlanması ve kişisel bilginin koruması konuları teknik çözümlerin yanında hukuksal düzenlemelerle de yakından ilgilidir. Mevcut hukuki düzenlemelerin ise devletlerin hâkim oldukları coğrafya ile sınırlanmış olması, bulut bilişimin doğasında var olan coğrafyadan bağımsız olma ve hizmet yerinin bilinmemesi prensipleri ile yan yana konduğunda problemi daha da karmaşık hale getirmektedir. Güvenin sağlanması ve kişiselliğin korunması problemleri bankacılık sisteminin kurulduğu yıllarda da ortaya çıkmış, ancak bu problemler devletlerin hukuki düzenlemeleri ile günümüzde aşılmıştır. Ne var ki, bankacılık konusundaki hukuki düzenlemeler devletlerarasında farklılık gösterebilmektedir. Geçerli olan düzenleme, bankacılık hizmetinin verildiği devlet sınırları ile belirlenmektedir. Bulut bilişim ise hizmetin coğrafyadan bağımsız olarak ve farklı devlet hâkimiyetlerinde bulunan sistemlerden alınmasını öngörmektedir. Bu tür bir hizmet sunumu teknik olarak mümkün olsa da hangi hukuki düzenlemeye tabi olacağı konusu halen tartışılmaktadır [7], [8].

Diğer taraftan birçok ülkede e-devlet uygulamaları ile kamu hizmetlerinin bir bulut içerisinde vatandaşa ulaştırılması ve böylece, bu hizmetlerin maliyetlerinin düşürülmesinin yanında, hizmet süratinin ve erişilebilirliğin artırılarak vatandaş memnuniyetinin yükseltilmesi amaçlanmaktadır. Bu amaçla Türkiye'de 2003 yılından itibaren Bilgi Toplumu Stratejisi yayınlanmış ve buna uygun bir eylem planı hazırlanarak uygulamaya geçilmiştir. Ancak özellikle kamu kurumlarının kendi sorumluluklarına verilen bilgi ve süreçleri, kurum dışına açmasında ortak standart ve hukuki düzenleme yetersizliği önemli bir engel oluşturmaktadır. Zira her kurum kendi sorumluluğundaki bilginin korunması ve hizmetlerin uygun şekilde

Manuscript received July 15, 2013.

Gökhan Şengül is with Computer Engineering Department, Atilim University, Gölbaşı, Ankara TURKEY (tel:+90 312 586 8826 e-posta:gsengul@atilim.edu.tr). Atilla Bostan is also with Computer Engineering Department, Atilim University, Gölbaşı, Ankara TURKEY (e-mail: abostan@atilim.edu.tr)

çalışmasından sorumlu ve yetkili iken, kurumsal sorumluluk alanında uygun düzenlemeler yapılmadan yetkinin başka otoritelere devrine karşı çıkmaktadır. Bu konuda yaşanmış olan ve bulut servis sağlayıcısından kaynaklanan hizmet aksaması ve veri kaybı olayları da kaygıları kuvvetlendirmektedir. Bulut hizmeti vermekte olan Intuit sitesi 15-16 Haziran 2010 tarihinde 24 saati açan bir süre zarfında hizmet verememiş, bu da birçok kullanıcı için mağduriyet oluşturmuştur [9]. En yeni olaylardan birisi de, bulut hizmet sunucusu Evernote'un Mart 2013 tarihinde 50 milyon kullanıcı parolasının saldırgan kişilerce değiştirildiğini açıklamasıdır [10]. Bütün bunlara rağmen bulut bilişimin vaat ettiği hizmet edinme ve işletmesindeki düşük maliyet ve hizmet sunumundaki esneklik, devlet bulutunun bir ön adımı olabilecek kamuda veri merkezlerinin birleştirilmesi [11] gibi bazı çalışmaların başlatılmasının önüne geçememektedir.

Bu çalışmada öncelikle bulut bilişim kavramı, hizmet modelleri, faydaları hakkında özet bilgi verilecek ve bulut bilişimim yaygınlaşmasının önündeki sorunlar listelenecektir. Daha sonra bulut bilişimin önde gelen sorunlarından olan güvenliğin sağlanmasında standartların önemi ve Türkiye'de sayısal güvenlik standardı çalışmaları anlatılacaktır. Sonuç bölümünde ise ülkemizdeki güvenlik standartları konusunda beklenen gelişmeler ışığında bulut bilişim ve e-devlet uygulamalarında gerçekleşebilecek açılımlar vurgulanacaktır.

II. BULUT BİLİŞİM

Bulut bilişim konusunda üzerinde uzlaşı sağlanan bir tanımlama henüz bulunmasa da; bu kavramı, erişim noktaları arasında ortak bilgi ve hizmet paylaşımını sağlayan platform olarak tanımlamak mümkündür. Tanından da anlaşılacağı üzere erişim noktaları arasında iletişimi, bilgi akışını sağlayabilmek için bir iletişim ağına ihtiyaç vardır ve bu ağ bulut bilişimi mümkün kılan en temel bileşendir. Bir başka bakış açısından bulut bilişim için veri ve hizmetlerin bir ağ üzerinden ve kullanıcılar arasında ortaklaşa kullanılmasıdır tanımı da yapılabilir. Aslında ağ üzerinden hesaplama, dağıtık hesaplama veya ağ üzerinde dağıtık veri saklama bilişim dünyasında uzun zamandan beri yapıla gelen uygulamalardır. Son zamanlarda, veri ağlarının yaygınlaşması, süratlerinin artması, erişim ve kullanım maliyetlerindeki düşüş ile sanal işlem ve sanal saklama alanlarındaki ilerlemeler, tüm bu özellikleri içeren hizmetlerin daha etkin ve düşük maliyetle üretilmesini mümkün kılmıştır. Artık kullanıcının fiziksel olarak kaynağını bilmediği hizmetleri kullanması veya yine fiziksel olarak makine ve ortamını bilmediği alanlarda verilerini saklaması mümkündür. Kullanıcı bakış açısından hesaplama hizmetleri ve veri saklama alanları fiziksel bir cihaza karşılık gelmeyen bir ortam (bulut) tarafından sağlanmaktadır.

Yukarıda bahsedilen karakteristikteki hizmetlerin İnternet gibi evrensel bir ağ üzerinde çalıştırılması ile mekândan ve donanımdan bağımsız erişim altyapısı sayesinde, hem hizmetlerin erişilebilirliği artmakta hem de daha geniş bir kullanıcı kitlesine hizmet vermek suretiyle kullanıcı başına düşen maliyetler azalmaktadır.

Günümüzde kullanılmakta olan bulut bilişim hizmetleri farklı bakış açılarından değişik sınıflandırmalar altında toplanabilmektedir. Aşağıda sırası ile bulut bilişimin farklı bakış açılarından sınıflandırmaları, bulut bilişimin faydaları ve sorunları sunulmuştur.

A. Bulut bilişim Sınıflandırmaları

1. *Verilen Hizmet Açısından Bulut Modelleri*

Bulut bilişim hizmetleri genellikle üç hizmet modeli ile sınıflandırılmaktadır. Hizmet sağlayıcılar bu modellerden herhangi birisini veya birkaç tanesini eş zamanlı sunabilmektedir. Bu hizmet modelleri ve özellikleri aşağıda özetlenmiştir.

i. Hizmet Olarak Yazılım (Software as a Service--SaaS).

Bu hizmet modelinde kullanıcı terminallerine yazılım yüklemesi yapılmadan, yazılımlar hizmet bulutu içerisindeki sunucular üzerinde çalıştırılır.

ii. Hizmet olarak platform (Platform as a Service-PaaS).

Kullanıcıya geliştirme ortamı gerekli tüm yazılım, donanım ve konfigürasyonları ile sağlanır. Kullanıcı bu ortamı, kullandığı terminalden ve mekândan bağımsız olarak kullanır.

iii. Hizmet olarak Altyapı (Infrastructure as a Service-IaaS)

Kaynak bulutu olarak da adlandırılır. Bilişim altyapı elemanı hizmetlerini bir bulut içerinde sunma esasına dayanır. Veri saklamak için disk alanı, ağ güvenliği için ateş-duvarı hizmetleri bu model için örneklerdir.

2. *Kullanım Biçimine Göre Bulut Modelleri*

Kullanım Biçimine göre bulutlar dört sınıfa ayrılmaktadır.

i. Genel Bulut.

Genele açık bir ağ üzerinden verilen bulut bilişim hizmetleridir.

ii. Özel Bulut.

Bir kurum, firma gibi belirli bir grup kullanıcı için verilen bulut hizmetleridir. Hizmetler kurumun, firmanın kendisi tarafından veya farklı bir kuruluş tarafından çalıştırılabilir.

iii. Melez Bulut.

Genel ve özel bulutun karışık ve eş zamanlı kullanımıdır. Belirli bir kurum, firma bazı hizmetleri genel buluttan alırken diğerlerini özel buluttan alabilir..

B. Bulut Bilişimin Faydaları

Bulut bilişim donanım, yazılım ve altyapının ortaklaşa kullanılmasını sağlaması nedeni ile bu maliyetlerin paylaşılmasını sağlamaktadır. Ayrıca sistem işletmesi, güvenliğin sağlanması ve yedekleme gibi bazı özel hizmetlerin de daha kaliteli yerine getirilmesine yardımcı olmaktadır. Servis model ve kullanım şeklinden bağımsız olarak bulut bilişimin faydaları;

i. Donanım ve yazılım maliyetlerinin azalması
ii. Uzaktan erişim kolaylığı
iii. Veri saklama maliyetlerinin veri miktarı ile orantılı olması.

olarak sıralanabilir. Bütün bunlara ek olarak, Avrupa Komisyonu 2012 yılı raporuna göre bulut bilişim sayesinde mobil çalışma %46, üretim %41 ve standartlaşma %35 artmıştır [12]..

C. Bulut Bilişimin Sorunları

Bulut bilişimin faydalarının yanında nispeten yeni bir

yaklaşım olması ve ülke sınırlarını aşan bir hizmet olması nedenleri ile halen bazı teknik ve hukuksal sorunları bulunmaktadır. Özellikle hukuksal sorunların bulut bilişimin yaygınlaşmasının önünde önemli engel oluşturduğu değerlendirilmektedir. Bulut bilişimin mevcut sorunları başlıklar halinde aşağıda listelenmiştir.

i. Uygulamaların yavaş çalışması
ii. Geniş bant ağ erişimine ihtiyaç duyması
iii. Uzaktan erişim güvenlik sorunları
iv. Hizmet ve/veya verinin nerede olduğunu bilmeme
v. Bulut hizmeti veren firmanın yeterliliğinin ve güvenirliliğinin bilinmemesi ve denetlenememesi
vi. Bulut hizmeti veren firmaların güvenlik, veri bütünlüğü ve erişim denetimi konularında sorumluluk üstelenmemeleri
vii. Bulut hizmeti veren firmaların hizmet sürekliliği konusunda taahhütte bulunamaması
viii. Buluttaki içeriğin mülkiyet hakkı ve kullanımı konusunda belirsizlik
ix. Sayısal deliller ve adli inceleme işlemleri, süreçleri konularındaki belirsizlikler.
x. Siber saldırılar için bulut alanlarının hedef haline gelmesi.

Yukarıdaki listede belirtilen ilk iki madde dışında kalan diğer maddelerin hepsi bulut hizmeti kullanıcısının hizmeti veren makamla olan güven ilişkisini doğrudan etkileyen hususlardır. İlk iki maddede belirtilen bulut sorunları halen alanda sorun olarak yer almakla beraber, günümüzde erişilen durum itibarı ile kullanıcı rahatsızlığı açısından çok ön planda olan konular değildir. Bir başka ifade ile bulut bilişimde en temel sorun, hizmet sağlayıcısı ve kullanıcısı arasındaki güven mekanizmasındaki eksiklikler ve bu alanda geçerli olacak hukuksal düzenlemelerin eksikliği olarak göze çarpmaktadır.

III. GÜVENLİĞİN SAĞLANMASINDA STANDARTLARIN ÖNEMİ

Herhangi bir ürünün, sürecin, sistemin ya da kişinin, önceden belirlenmiş kriterlere göre değerlendirilmesi ve söz konusu kriterlere uygunluğunun üçüncü taraflarca doğrulanması süreci belgelendirme olarak adlandırılmaktadır. Genellikle değerlendirme kriterleri, üzerinde tüm paydaşların katılımı ile belirlenir ve ulusal ve uluslararası standardizasyon kuruluşları tarafından standart olarak yayınlanır. Herhangi bir standardda ürünün belirli özelliklere göre sağlaması gereken kriterler yer alır. Örneğin bilgi teknolojileri cihazları ile ilgili bir standart, cihazın sağlaması gereken işlevselliğe odaklanırken bir başka standart aynı ürünün uyması gereken bilgi güvenliği prensiplerine odaklanabilir.

Türkiye'de standartların hazırlanması ve standartlara uygunluk sağlayan firma ve ürünlerin belgelendirilmesi görevi 132 sayılı kanunla Türk Standardları Enstitüsü'ne (TSE) verilmiştir. 1960 yılında kurulan TSE, o günden bu yana farklı alanlarda standart hazırlama faaliyetlerini sürdürmektedir. Bugün itibariyle TSE tarafından yayınlanmış olan yürürlükte 30000'den fazla standart bulunmaktadır. Uluslararası alanda ise standart hazırlama çalışmalarını yürüten farklı kuruluşlar bulunmaktadır. Uluslararası düzeyde standart hazırlama çalışmalarını yürüten en büyük kuruluş hiç kuşkusuz ki Uluslararası Standardizasyon Teşkilatı (ISO) 'dur. Uluslararası alanda standart hazırlama faaliyetinde bulunan bir diğer büyük kuruluş ise Uluslararası Elektroteknik Komisyonu (IEC)'dir. Türk Standardları Enstitüsü hem ISO'nun hem de IEC'nin üyesidir ve söz konusu kuruluşların standartlarını da Türk Standardı olarak kabul etmekte ve yayınlamaktadır. Türk Standardları Enstitüsü (TSE) ayrıca, 2011 yılında Avrupa Birliği (AB) standardizasyon kuruluşları olan Avrupa Standardizasyon Komitesi (CEN) ve Avrupa Elektroteknik Standardizasyon Komitesi (CENELEC)'ne de tam üye olmuştur. Türk Standardları Enstitüsü, hem ülkemiz ihtiyaçlarına yönelik standart hazırlama faaliyetlerine devam etmekte, hem de mevzuatlar gereği üyesi bulunduğu uluslararası standardizasyon kuruluşlarının standart hazırlama çalışmalarına katılmakta ve bu kuruluşlarca yayınlanan standartları Türk Standardı olarak kabul etmektedir.

Bilgi güvenliği konusundaki standartlara değinmeden önce söz konusu standartlara göre belgelendirme yapmanın öneminden bahsetmek gerekir. Bilgi güvenliği standartlarına uygunluğun sağlanması ve dolayısı ile belgelendirme yapılması, BT ürünleri ya da sistemlerinde en az bilgi güvenliği açığı ya da zafiyeti bulunduranların tespit edilmesi ve temini ile bilgi güvenliği konusundaki risklerin en aza indirgenmesini sağlayacaktır. Bu sayede gerek maddi gerekse de manevi kayıpların en aza indirilmesi mümkün olabilir.

Bilişim sektöründeki ürünler ve sistemler baz alındığında gerek uluslararası düzeyde gerekse de ulusal düzeyde birçok standardın bulunduğu görülebilir. Ancak söz konusu olan bilgi güvenliği olduğunda, ulusal ve uluslararası standartları iki temel grupta ve standart başlığı altında toplamak mümkündür: Sistem tabanlı standartlar (ISO/IEC 27001 grubu) ve ürün tabanlı standartlar (ISO/IEC 15408 grubu).

TS ISO/IEC 27001 [13], ilk olarak ISO tarafından 2005 yılında yayınlanmış, müteakibinde Türkçeye tercümesi yapılarak Türk standardı olarak TSE tarafından da yayınlanmış bir sistem tabanlı bilgi güvenliği standardıdır. Standard herhangi bir ürünün taşıması gereken güvenlik kriterlerini belirlemez. Bunun yerine BT ürünlerini kullanan bir sistemi ele alarak Bilgi Güvenliği politikası, risk analizi, iç denetimler, yönetim desteği ve yönetimin gözden geçirmesi gibi konuları ele alarak bir kuruluştaki bilgi varlıklarının korunmasına yönelik olarak sistemin gereksinimlerini belirler. ISO tarafından söz konusu standardı destekleyici diğer bir dizi standart da (ISO 27000, ISO 27002, ISO 27004, ISO 27005, ISO 27006, vb) yayınlanmıştır. Söz konusu standartlar yine TSE tarafından Türk standardı olarak kabul edilmiş ve yürürlüktedir.

Bunun yanında BT ürünlerinin taşıması gereken asgari güvenlik kriterlerini belirleyen ve belgelendirilmesini sağlayan ürün temelli bir standart olan ISO/IEC 15408 standardı bulunmaktadır [14]. Ortak kriterler olarak da bilinen ISO/IEC 15408 standardı ilk kez 2005 yılında yayınlanmış, 2009 yılında da revize edilmiştir. Ortak kriterler ISO 15408 -1,2,3 şeklinde üç bölümden oluşmaktadır ve belirli bir BT ürününe özgü olmayıp tüm ürünlere uygulanabilirdir. Standart EAL olarak adlandırılan ve 1'den başlayıp 7'ye kadar uzanan yedi güvenlik seviyesi belirlemektedir. Bu seviyelerden EAL-1 en düşük seviyeyi, EAL 7 ise en yüksek seviyeyi ifade eder. Genellikle yazılım ürünleri için EAL 4 ya da EAL 4+ en yaygın karşılaşılan

güvenlik seviyeleridir.

Bulut bilişim açısından güvenlik ele alındığında yukarıda bahsedilen standartlara göre belgelendirme yapmak mümkün olmakla birlikte bulut bilişimin doğası gereği bu belgelendirmelere hazırlanmak ve gerekli denetimleri gerçekleştirmek zordur. Bunun yanında güncel bir teknoloji olması itibariyle bulut bilişim alanında bilgi güvenliği kriterlerini belirlemek amacıyla henüz yayınlanmış özel bir standart da bulunmamaktadır. Ancak gerek sektördeki gerekse de bulut bilişimin hızla yaygınlaşması ve bu nedenle de bilgi güvenliği hususlarının irdelenmesi ihtiyaçları nedeniyle hem ISO bünyesinde hem de TSE bünyesinde standardizasyon çalışmalarına başlanmıştır.

ISO bünyesindeki çalışmalar incelendiğinde ISO/IEC 27017 [15], ISO/IEC 27018 [16] ve ISO/IEC 27036-4 [17] standartları konusunda çalışmalara başlandığı görülmektedir. Bu standart çalışmalarından ilki olan ISO/IEC 27017 çalışması, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardını temel alarak bulut bilişim hizmetleri için bilgi güvenliği kontrolleri için en iyi uygulama örneklerini, ISO/IEC 27018 çalışması halka açık bulut bilişim hizmetlerinde veri koruma kontrollerinin en iyi uygulama örneklerini ve ISO/IEC 27036-4 ise tedarikçi hizmetleri açısından bulut bilişim güvenliği kılavuzu sağlamayı hedeflemektedir. Her üç standart çalışması da incelendiğinde ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi tabanlı oldukları ve henüz standart hazırlama çalışmalarına yeni başlandığı ve standardların yayınlanmasının zaman alacağı görülmektedir. Ancak yine de bulut bilişim konusunda hizmet sağlayan firmaların bu standardizasyon çalışmalarının farkında olmaları ve ürün tasarımlarını bu standardlara göre planlamaları faydalı olacaktır.

IV. TÜRKİYE'DE BULUT BİLİŞİM KONUSUNDAKİ STANDARDİZASYON ÇALIŞMALARI

TSE bünyesinde 2013 yılı ilk çeyreğinde oluşturulmuş olan "Siber Güvenlik Özel Komitesi" tarafından, bulut bilişim altyapılarının güvenliğine ilişkin standartların belirlenmesi yönünde çalışmalara başlanmıştır. Çalışma kapsamında bulut bilişim alanındaki uluslararası kuruluşlar ile başta Amerika olmak üzere öncü ülkelerin özellikle bulut bilişim güvenliğine yönelik çalışmaları incelenecek ve Türkiye için standartlar belirlenecektir. Bulut bilişim hizmet sağlayıcıları ülkemizde sayıca az olmakla birlikte, çok sayıda firmanın kişisel verilerini barındırıyor olmaları sebebiyle kritik öneme sahiptir. Bu nedenle bulut bilişime yönelik güvenlik standartları önemli görülmekte ve bu alandaki çalışmaların bir an önce bitirilmesi yönünde çaba harcanmaktadır.

Bulut bilişim kullanımının dünyada ve Türkiye'de yaygınlaşmasının önünde en önemli engel hizmet sağlayıcı ve kullanıcı arasında yeterli seviyede bir güven mekanizmasının sağlanamamış olmasıdır. Gerek hizmet sağlayıcıların belirli sorumlulukları üstelenmemesi ve gerekse alandaki hukuksal düzenleme belirsizliği bu karşılıklı güvenin oluşturulmasını engellemektedir. Kullanıcılar hizmetleri bulut üzerinden alırken ilave güvenlik risklerini üstelenmek istememektedir. Bu riskler, bilginin ve verinin güvenliği boyutunda olabileceği gibi, hizmetin sağlanması ve erişilmesi konularında da olabilmektedir. Kullanıcı açısından kişisel veya kurumsal verinin kaybı, bozulması, erişilememesi veya kendi kontrolü dışında üçüncü şahıslarca kullanılmasının yanında aldığı hizmetin sürekliliği ve erişilebilirliği önemli güven parametreleridir. Hizmet sunucusu ve kullanıcısı arasından bu alanda yapılacak sağlıklı anlaşmalar için hizmet güvenlik standardlarının belirlenmiş olması ve bir garantör otoritenin varlığına ihtiyaç duyulmaktadır. Standartların hizmet güvenlik seviyesi ve içeriği konusunda ortak anlayışı ve denetlenebilirliği sağlaması, garantör otoritenin ise bu standart ve düzenlemelerin ihlali durumunda zarar gören tarafın korunmasını garanti altına alması beklenmektedir. Aslında bu iki boyut birbiri ile çok yakından ilgilidir. Zira alanda ortak anlayış ve tanımlama sağlanmadan denetlenebilirlik ve hukuki düzenleme yapmak imkânsızdır.

V. SONUÇ VE ÖNERİLER

Günümüzde oldukça yüksek hızlara ulaşmış olan sayısal iletişim ve bilgi işleme teknolojisi kaynakların, hizmetlerin ve verinin ortaklaşa kullanılmasını sağlayan ve bulut bilişim olarak adlandırılan hizmet platformlarının yaygın olarak kullanılmasına imkân tanımaktadır. Ancak teknolojik olarak uygulanabilir olan bu hizmetler, alandaki güven problemlerinden dolayı yeterince hızlı yaygınlaşamamakta ve geniş kullanıcı çevrelerince tercih edilmemektedir.

Bulut bilişim hizmetleri için geliştirilecek ulusal ve evrensel standartların hukuksal düzenlemeleri de mümkün kılması ve hizmet sağlayıcı ile kullanıcı arasında oluşturulacak güven mekanizması için temel oluşturması beklenmektedir. Türkiye'de ISO/IEC kapsamında geliştirilmekte olan 27017, 2718 ve 27036-4 standartları ile bulut bilişim hizmetleri ve bulutta bilgi güvenliği konularında düzenleme çalışmaları başlatılmıştır. Ancak yeni yayınlanacak bu standartların temel olarak ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'ne dayanacak olması hizmet ve ürünlerde temel niteliklerin neler olacağı konusunda belirleyici faktördür. Bulut bilişim hizmet sağlayıcılarının hizmetlerini bu öngörü dâhilinde yapılandırmaları onlara gelecekte avantaj sağlayacaktır. Ayrıca e-devlet çalışmalarında ulaşılması hedeflenen devlet-bulutu hizmetlerinin de bu standart öngörüsüne paralel geliştirilmesi uygun olacaktır.

Standart çalışmalarına benzer şekilde bulut bilişime özgü hukuksal alanın düzenlenmesi konusunda da ulusal ve uluslararası çalışmaların bir an önce başlatılması zaman kazandıracaktır.

Bulut bilişimin yaygınlaşması ve daha geniş kullanıcı kitlerine ulaşması ancak hizmet sağlayıcı ve kullanıcı arasında karşılıklı güven mekanizmasının oluşturulması ile sağlanabilecektir. Standartların tanımlanmasını ve hukuki düzenlemeleri takiben bulut hizmetlerine talebin daha da artması ve bu hizmetlerin yaygın olarak kullanılması beklenmektedir.

KAYNAKLAR

[1] Fox B. (2012), Cloud computing a "game-changer" for EU economy, Kroes says, 30 Haziran 2013 tarihinde "http://euobserver.com/news/117695" adresinden erişildi.

[2] Kroes, N. (2012), Cloud computing and data protection reform. 30 Haziran 2013 tarihinde http://blogs.ec.europa.eu/neelie-kroes/cloud-data-protection adresinden erişildi.

[3] Khatibi V, Khatibi E. (2012), Issues on Cloud Computing: A Systematic Review, International Conference on Computational Techniques and Mobile Computing (ICCTMC'2012) December 14-15, 2012 Singapore, pages 212-216Henkoğlu T., Külcü Ö. (2012), Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme, Bilgi Dünyası, 2013, 14 (1) 62-86

[4] Brodkin J, 2008, 'Gartner: Seven cloud-computing security risks', Infoworld, 30 Haziran 2013 tarinde http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 adresinden erişildi.

[5] Varadi, S., Kertesz, A. ve Parkin, M. (2012). The necessity of legally compliant data management in European cloud architectures. Computer Law & security Review, 577-586.

[6] Kroes, N. (2012), Why we need a sound Do-Not–Track standard for privacy online, 30 Haziran 2013 tarihinde http://blogs.ec.europa.eu/neelie-kroes/donottrack/ adresinden erişildi.

[7] Catteddu D., (2010), Cloud Computing: Benefits, Risks and Recommendations for Information Security, Web Application Security Communications in Computer and Information Science Volume 72, 2010, p 17

[8] Hachman M. (2013), Update: Intuit Sites Outage Strands Thousands of SMBs, PCMag.com, 30 Haziran 2013 tarihinde http://www.pcmag.com/article2/0,2817,2365179,00.asp adresinden erişilmiştir.

[9] Hernandez D. (2013), Evernote Hack Exposes User Data, Forces Extensive Password Resets, wired, 30 Haziran 2013 tarihinde http://www.wired.com/threatlevel/2013/03/evernote-hack-password-resets/ adresinden erişilmiştir.

[10] Veri Merkezleri ve Güvenliği Konferansı 2013, 30 Haziran 2013 tarihinde http://www.webhostingturkey.com/post/2013/03/19/Veri-Merkezleri-ve-Guvenligi-Konferans%C4%B1-2013.aspx adresinden erişilmiştir.

[11] European Comission (2012), Unleashing the Potential of Cloud Computing in Europe, 03 Temmuz 2013 tarihinde http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf adresinden erişilmiştir.

[12] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements

[13] ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

[14] ISO/IEC WD 27017 Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

[15] ISO/IEC CD 27018 Code of practice for data protection controls for public cloud computing services

[16] ISO/IEC WD 27036-4 Information technology -- Information security for supplier relationships -- Part 4: Guidelines for security of Cloud servic

Metin İçin Yapay Sinir Ağı Tabanlı Hash Fonksiyonu

Yakup KUTLU ve Apdullah YAYIK

***Özet*—Bu çalışmada 5 katmanlı Yapay Sinir Ağı (YSA) ile tek yönlü hash (özet) fonksiyonu tasarlanmıştır. Bu fonksiyon herhangi bir uzunluktaki açık metni şifreleyerek sabit uzunlukta (256-bit veya 512-bit) veri elde edilmesini sağlamaktadır. Hash değerlerinin metindeki karakterlere bağlı duyarlılıkları incelenmiş ve grafiklerle gösterilmiştir. Analizler sonucunda, gerçekleştirilen YSA tabanlı hash fonksiyonunun yüksek duyarlılığa sahip olduğu görülmüştür.**

***Anahtar Kelimeler*—Yapay Sinir Ağı, Hash Fonksiyonu, Duyarlılık, Tek Yönlülük**

***Abstract* — In this paper 5 layered neural network based one way hash function is designed. This function is used to obtain 256-bit or 512-bit length data by encrypting any length text. The hash values are tested for sensitivity and shown by graphics. It is learned that ANN based hash function is on a one-way and seems to be sufficiently high sensitivity.**

***Index Terms*— Neural Network, Hash Function, One-Way**

I. GİRİS

BUGÜNE kadar haberleşmede kullanmak maksadıyla güçlü kripto sistemi geliştirmek için birçok çalışma yapılmıştır. Yakın geçmişe dikkatle bakıldığında yapay sinir ağları ile şifreleme teknikleri sıklıkla kullanılmakta olduğunu görmekteyiz. SHA-2 güvenli hash fonksiyonunu ve yapay sinir ağı tabanlı hash fonksiyonu istatistiksel testlerden geçirilmiş ve neredeyse aynı sonuçlar elde edilmiştir [1]. Bu çalışmada metnin hash değeri YSA tabanlı hesaplanmıştır. Hash değeri birçok çalışmada hexadecimal olarak hesaplanmıştır. Bu çalışmada ise hash değeri iki farlı şekilde; "yalnızca büyük harf, büyük ve küçük harflerden oluşan kombinasyon şeklinde "256-bit ve 512-bit " uzunluklarında oluşturulmuştur.

II. MATERYAL VE YÖNTEMLER

Hash fonksiyonları ile büyük tanım bölgeleri küçük değer bölgelerine dönüştürülür.

Birinci Yazar Yakup KUTLU, Mustafa Kemal Üniversitesi Bilgisayar Mühendisliği Bölümü, Hatay Türkiye,Tel: +90 (326) 613-5600/ 4323; e-mail=ykutlu@mkü.edu.tr

İkinci Yazar. Apdullah YAYIK, Türk Silahlı Kuvvetleri, Mustafa Kemal Üniversitesi Fen Bilimleri Enstitüsü Enformatik Ana Bilim Dalı, Hatay Türkiye, e-mail=apdullahyayik@gmail.com.

Elde Hash değerleri duyarlılık testi sınanmıştır. Sonuç olarak YSA' nın tek yönlü hash fonksiyonu olarak kullanılabilirliği gösterilmiştir.

Hash fonksiyonu girdi olarak bir mesajı alır ve hash kodu, hash sonucu, hash değeri, mesaj özeti veya kısaca hash ile belirtilen bir çıktı üretir. Daha kesin bir ifadeyle bir hash fonksiyonu keyfi sonlu boyutlu bit şeritlerini n-bit diyebileceğimiz sabit uzunluklu şeritlere dönüştürür. En iyi bilinen hash fonksiyonları MD-2, MD-4, MD-5, SHA-1, SHA-2 ve SHA-3' dür. Hash fonksiyonları veri bütünlüğü ile dijital imza tasarıları için kullanılırlar. Açık anahtarlı bir algoritmayla hazırlanan dijital imza, gönderilen bilginin sayısal içeriğinin değiştirilmediğinin ve gönderen tarafın kimliğinin ispatı için atılır. Teknik olarak dijital imza, imzalanmış belgenin özünü, özetini (hash) içeren, elektronik mesaja eklenmiş bilgidir. İçerikte yapılacak bir değişiklik hash' ı geçersiz kılacaktır.

Başka bir ifadeyle hash fonksiyonu gönderilecek mesajdan matematiksel yollarla sabit uzunlukta sayısal bilgi üretme işlemidir. Üretilen sayısal bilgi "mesaj özeti" olarak bilinir. Mesaj özeti anlamsız bir bilgidir. Hash fonksiyonu geri dönüşümü olmayan bir fonksiyondur; yani mesaj özetine bakarak mesajın kendisini elde etmek mümkün değildir. Aynı özeti veren iki farklı mesaj bulmak da imkânsız olmalıdır. Her mesajın farklı özetinin olması, mesajda yapılacak en ufak bir değişiklikte imzanın geçersiz kalmasını sağlayacaktır. Kriptografinin böyle fonksiyonlara ihtiyacı vardır. Çünkü bu fonksiyonların ana özellikleri tersinin hesaplanmasının güç olmasıdır [2].

Ayrıca, kullanıcı yetkileri sunucu üzerinde kayıt edilirken kullanılmaktadır. Kullanıcı, programa önceden kayıt edilmemişse uygulamayı kullanamamaktadır. Bu kayıt girişinde kullanıcı, bir şifre girer. Bu şifre doğrudan veri tabanına kaydedilmez. Bu şifre, hash fonksiyonları ile geri dönüşümü olmayan başka bir veri haline dönüştürülerek veri tabanına kaydedilir. Bu yöntemle veri tabanına erişen kötü niyetli kişilerin bu şifreleri ele geçirmeleri zorlaştırılmış olur [3].

Bir mesaj ilk olarak özetlenir ve sonra hash değeri mesajın bir temsilcisi gibi orijinal mesaj yerine imzalanır. Örneğin bir mesajının orijinal mesaj ile aynı olup olmadığına bakılırken hash değeri hesaplanır ve korunan orijinal hash değeri ile kıyaslanır. Değerler eşitse girdilerinde eşit olduğu kabul edilir. Bu durumda mesaj değiştirilmemiş demektir.

5070 sayılı Elektronik İmza Kanunu'nda yer alan şekliyle elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar.

Elektronik İmza Kanunu'nda; güvenli elektronik imza, elle atılan imzaya eşdeğer kabul edilmiş ve elektronik imza ile oluşturulmuş verilerin senet hükmünde olacağı belirtilmiştir [4].

A. *Yapay Sinir Ağları*

İnsan vücudu, sinir sistemi sayesinde yaşadığı olaylardan meydana gelen her türlü fiziksel, biyolojik ve kimyasal değişimlere alışabilmek maksadıyla kendisini yenilemekte ve çeşitli reaksiyonlar üretmektedir. Bütün sistemleri uyumlu çalışan bu sistem birçok araştırmacıya çalışmalarında esin kaynağı olmuştur. Etrafımızda meydana gelen değişimler, vücuttaki sinirler tarafından algılanmakta, beyne iletilmekte ve karar mekanizması olarak çalışan beyin, algıya karşılık en uygun tepkiyi üretmek için vücuttaki gerekli alt sistemleri uyarmaktadır. Yani, insan vücudundaki sinir sistemi, Algılama-Karar Verme-İcra Etme fonksiyonlarını yürüten harika bir yapıdır [5].

Doğada olduğu gibi yapay sinir ağlarında da elementler arasındaki bağlantı ağ fonksiyonunu belirtmektedir. Elementler arasındaki bağlantılar (ağırlıkları) değiştirilerek yeni bir yapay sinir ağı geliştirilebilmektedir. Yapay sinir ağlarının ağırlıkları belirli giriş değerleri ile belirli çıkış değerleri elde edene kadar değiştirilir, yani eğitilir. Yapay sinir ağlarının eğitimi hedeflenen çıkış değeri ile mevcut çıkış değeri aynı olana kadar (veya çok yakın) olana kadar devam eder [6]. Net bir ifadeyle, yapay sinir ağları yapay nöronların ağırlıklandırılmış grafiğidir [7]. Yapay sinir ağlarının avantajlarından bazıları; bilinen durumlardaki sonuçları kullanarak bilinmeyen durumlar hakkında karar verilebilmesi, işletiminde hızlı tepki verilebilmesi ve güvenilirlik ile verimlilik derecesinin yüksek olmasıdır [5].

Çok katmanlı ağlar (MLP) giriş, bir veya daha fazla sayıda ara ve çıkış katlarına sahip olup mimari açıdan ileri beslemeli, öğrenme algoritması bakımından danışmanlı öğrenen ağları sınıfındandır. Çok sayıda öğrenme algoritması kullanılarak eğitilebilen bu ağ yapısında; giriş, çıkış ve ara katlarda bulunan nöron sayısı problemin karmaşıklığı ile ilgili olup bu sayı tecrübeye dayalı olarak belirlenir. MLP ağlarında, uygulanan girişe karşılık üretilen çıkış ile hedef çıkış arasındaki hata, kullanılan öğrenme algoritmasına göre tekrar değerlendirilerek; hata değeri en aza düşürülünceye veya belirlenen iterasyon sayısına ulaşılıncaya kadar ağın ağırlıkları değiştirilir. Ayrıca ağ içerisinde ara bağlantılar girişten çıkışa doğru olduğu için herhangi bir andaki çıkış sadece o andaki girişin bir fonksiyonu olarak ifade edilir. Bundan dolayı bu tür ağlar statik ağlar olarak da bilinmektedir [8].

B. *Yapay Sinir Ağlarının Tek Yönlülüğü*

Yapay sinir ağlarının kriptoloji uygulamalarının birçok avantajı vardır [8]. Eğer ulaşılması hedeflenen değer (y_k) giriş değerine (x_k) göre çok farklılık gösteriyor ise, giriş değeri kullanılarak ulaşılması hedeflenen değere ulaşmak çok zor olurken hedeflenen değerden giriş değerini hesaplamak kolay olmaktadır. Yapay sinir ağları bu özelliğinden dolayı hash fonksiyonlarında kullanılmaktadır.

$$y_k = \emptyset(\sum_{j=1}^{m} w_{k.}\, x_j\, b_k) \qquad (1)$$

Yapay sinir ağlarında paralel uygulama önemli bir özelliktir. Her katman paraleldir. Böylece her katmanda bağımsız fonksiyon uygulanabilir. Bu yüzden veri işleme uygulamaları için uygundur. Yapay sinir ağlarının doğrusal olmayan ve karmaşık değerler arasında ilişki kurma yeteneği vardır. Karmaşıklık yapay sinir ağlarının doğrusal olmayan yapısından kaynaklanan özel bir özelliğidir. Bu özellik hedeflenen değer ile giriş değerleri arasında doğrusal olmayan ve karmaşık bir bağ kurulmasını sağlar. Yani, çıkış değerlerinin her biri giriş değerlerinin her birine karmaşık bir bağ ile bağlıdır. Bundan dolayı, giriş değerlerinin tam olarak belirlenmesi çok zordur.

D. *Açık Metin Duyarlılığı (AMD)*

Hash fonksiyonunda amaç farklı mesajlar için farklı mesaj özetlerinin (hash değeri) elde edilmesidir. Buna hash fonksiyonunun açık metin duyarlılığı denilmektedir. Açık metindeki küçük değişimlerin hash değerinde büyük değişimlere neden olmalıdır.

$$\boldsymbol{Duyarlılık} = \frac{Fark(H_o, H_i)}{S_b} \times 100 \qquad (2)$$

$\boldsymbol{H_0}$ = Orijinal verinin Hash Değeri

$\boldsymbol{H_i}$ = % i kadar değişiklik yapılmış olan verinin Hash Değeri

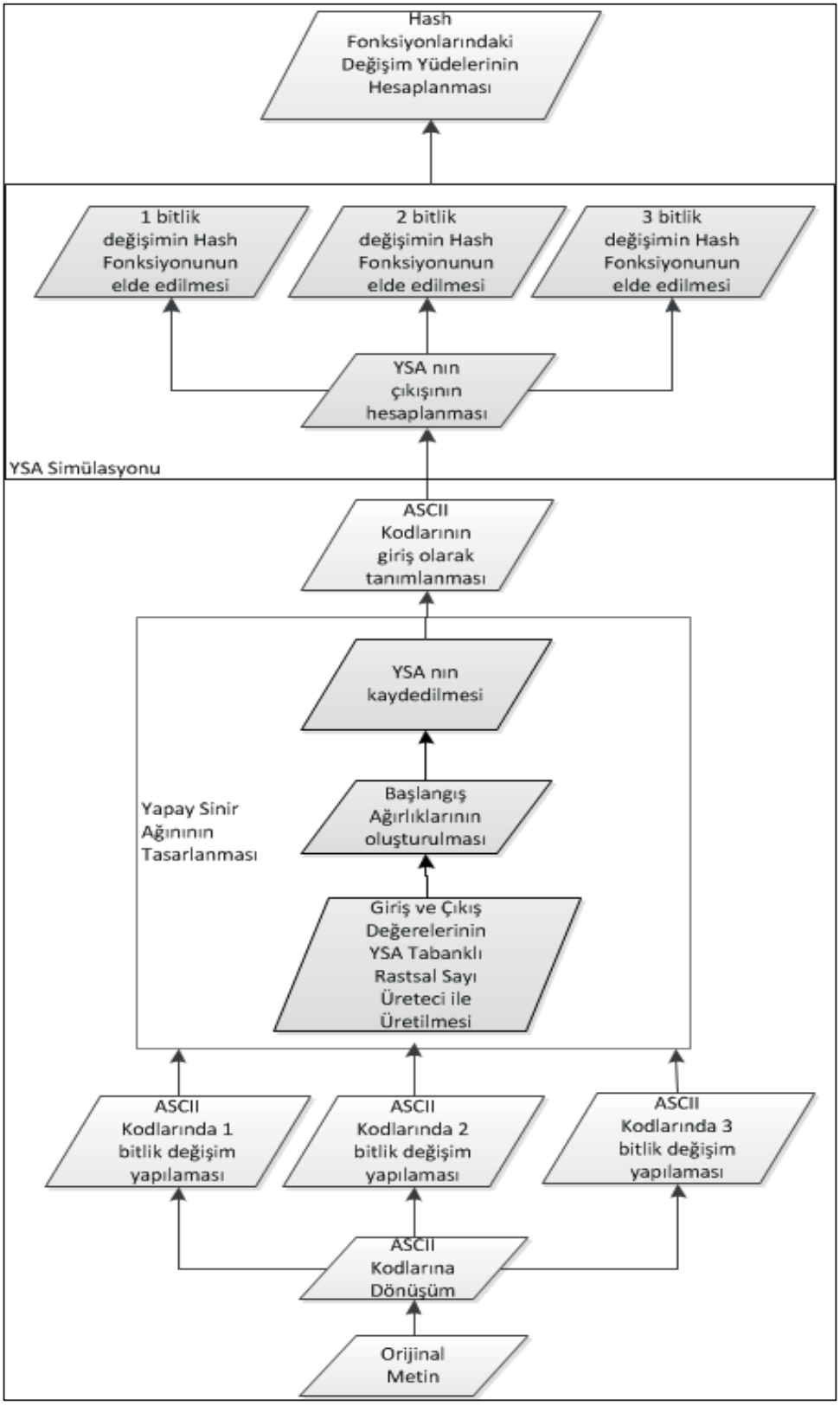
$\boldsymbol{S_b}$ =Hash Değerinin karakter sayısı

Fark işlemi parantez içerisindeki değerlerin birbirlerine göre farklılık seviyesini belirlemektedir.

Böylelikle algoritma istatistiksel saldırılara karşı güvenlidir denilebilir [1]. YSA tabanlı hash fonksiyonunun açık metin duyarlılığını test etmek maksadıyla açık metinin (orijinal metin) ASCII karakterlerinde küçük değişiklikler yapılarak hash değerindeki değişimler gözlemlenmiştir.

E. *Hash Değeri Üretim Aşamaları*

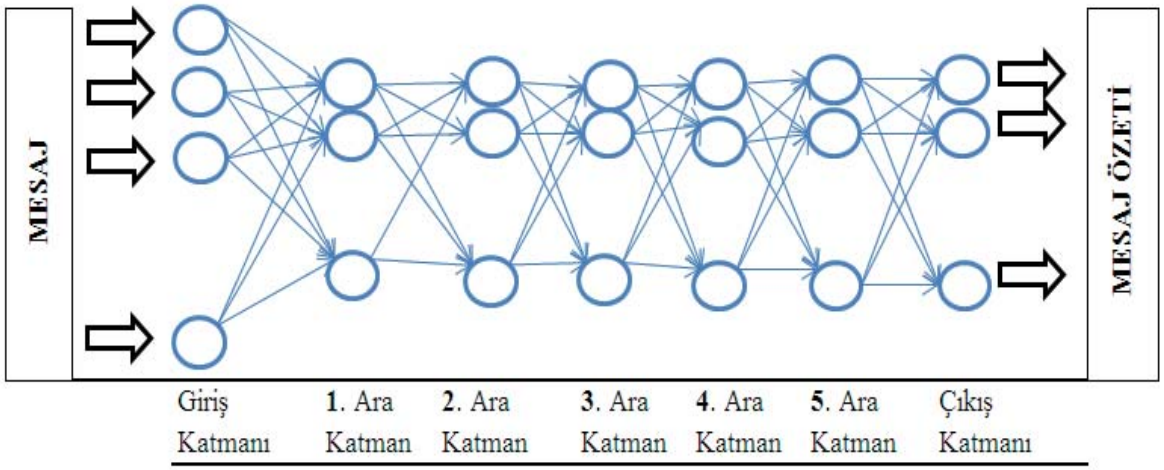
Bu uygulamada kullanılan YSA tabanlı hash fonksiyonu üretim aşamaları Şekil 1'de belirtilmiştir.



Şekil 1 Yapay Sinir Ağı Tabanlı Hash Fonksiyonu.

Girilen orijinal metin ASCII kodlarına dönüştürülür. Giriş ve çıkış değeri sözde rastsal sayı üreteci [10] ile üretilen 5 ara katmanlı (33-45-6-17-11) Yapay Sinir Ağının geri yayılım algoritması ile eğitilerek kaydedilir. Kaydedilen YSA nın giriş değeri olarak orijinal metinin ASCII kodları kullanılır. Ağın 5. ara katmanının transfer fonksiyonu tansig olduğundan çıkış değeri 0 ve +1 aralığında isteğe göre 1x32, 1x128, 1x256 veya 1x512

uzunluğunda vektör olarak elde edilir. Normalizasyon ve dönüşüm işlemleri sonunda büyük ve küçük harflerden veya yalnızca büyük harflerden oluşan hash değeri elde edilmektedir. Kullanılan Yapay Sinir Ağının yapısı Şekil 2' de gösterilmiştir.



Şekil 2 Hash Fonksiyonu YSA Yapısı

Hash Fonksiyonu alınacak olan metin; "*Günümüz bilgi teknolojileri dünyasında bilginin her geçen gün öneminin ve yaygınlığının artması, bilgiye her noktada erişilebilme isteklerinin artışa geçmesi ile beraber bu hususlara izin verecek olan teknolojik imkânlar her geçen gün hızla gelişmektedir*." dir. 256 karakterden oluşan bu metnin 32-bit hash fonksiyonu;

"uJOYbbBfsDbcRQGTGKXCKFTChCVTKBij" dir.

Metinin ASCII kodlarında değişiklikler yaparak hash fonksiyonunun değişimi gözlemlenmiştir. Metnin ASCII kodlarında;

- *1 bitlik değişiklik yapıldığında hash fonksiyonu*

"kNQYbnBklZnjGVIEIWVTKDRDsTPEGNxf " olmaktadır ve orijinal metnin hash fonksiyonuna göre %96,7 değişiklik göstermektedir.

- *2 bitlik değişiklik yapıldığında hash fonksiyonu*

"rAVSdwAthLwuRBASEGEHIGXVtBMARVdy" olmaktadır ve orijinal metnin hash fonksiyonuna göre %90,9 değişiklik göstermektedir.

- *3 bitlik değişiklik yapıldığında hash fonksiyonu*

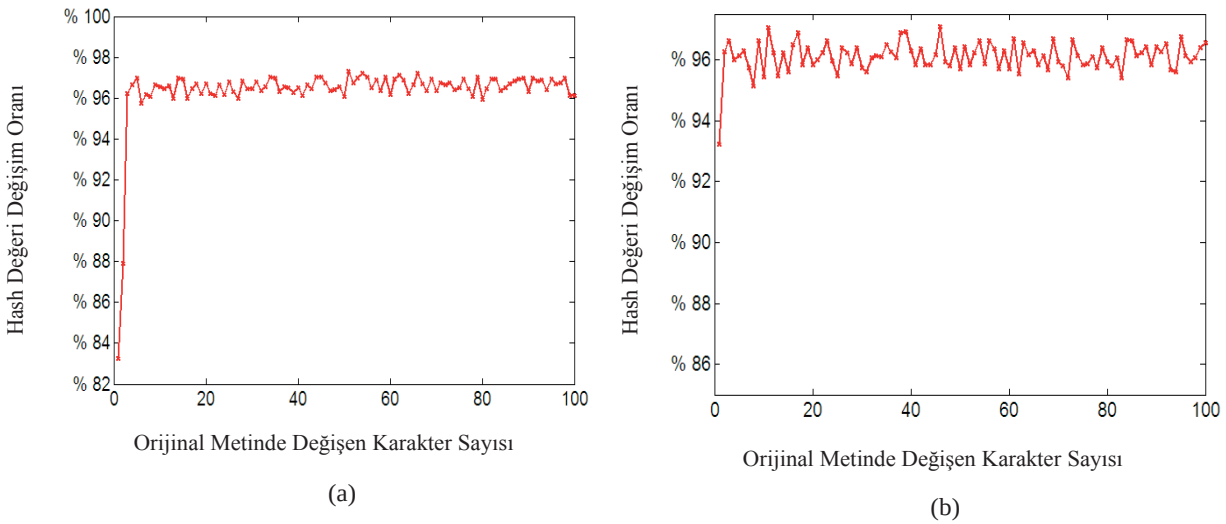
"rMWLuiIxtUgbJETHDBCAGMUJjMTEWWyl" olmaktadır ve orijinal metnin hash fonksiyonuna göre %96 değişiklik göstermektedir.

III. SONUÇ

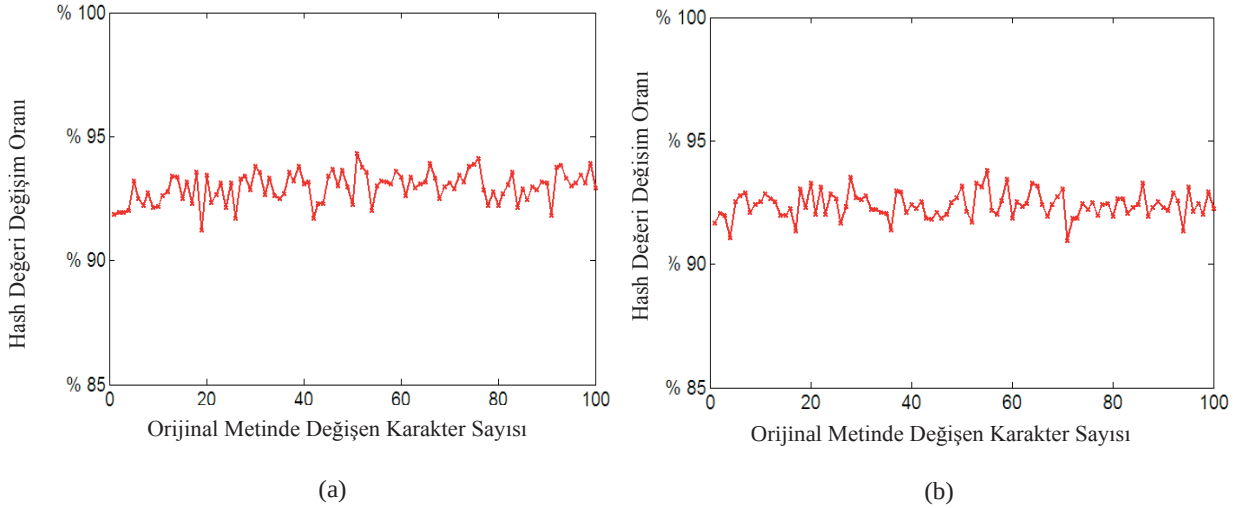
Bu çalışmada; hash değeri YSA tabanlı hesaplanmıştır. Hash değeri birçok çalışmada hexadecimal olarak hesaplanmıştır. Bu çalışmada ise hash değeri iki farlı şekilde; "yalnızca büyük harf, büyük ve küçük harflerden oluşan kombinasyon" şeklinde "32, 128, 256 ve 512bit " uzunluklarında oluşturulabilmektedir.

Hash Değerinin Duyarlılığı

Metnin 256 ve 512 bitlik yalnızca büyük harflerden oluşan ve büyük ve küçük harf kombinasyonundan oluşan hash fonksiyonlarının açık metin duyarlılıkları, Şekil 3 ve Şekil 4' de gösterilmiştir.



Şekil 3 YSA Tabanlı (a) Yalnızca büyük harflerden oluşan, (b) Yalnızca büyük ve küçük harflerden oluşan 256- bit Hash Değerinin Duyarlılığı.



Şekil 4 YSA Tabanlı (a) Yalnızca büyük harflerden oluşan, (b) Yalnızca büyük ve küçük harflerden oluşan 512- bit Hash Değerinin Duyarlılığı.

2011 yılında, giriş katmanında 768, ara katmanda 64, çıkış katmanında 256 adet nöron bulunan ileri beslemeli YSA tabanlı hash fonksiyonunun açık metine karşı duyarlılığı %50 civarında [1] olarak rapor edilmiştir. Bu çalışmada ise; giriş katmanında 100, ara katmanlarında sırasıyla 33, 45, 6, 17, 11, çıkış katmanında ise hash değerinin bit sayısına karar veren 256 veya 512 adet nöron bulunan 2 adet geri beslemeli YSA tasarlanmıştır. Tasarlanan YSA ile metin ve resmin hash değerleri hesaplanmıştır. Farklı bit sayılarının kullanılması hash değerinin bit sayısına göre ne gibi farklılıklar gösterdiğini tespit etmektir.

Metin ve resmin hash değerinin duyarlılığını anlayabilmek için metnin üzerinde belirli oranlarla artan değişiklikler yapılmış, resme ise belirli oranlar ile gürültüler eklenerek hash değerindeki değişim gözlemlenmiştir. Hash fonksiyon eğer doğru işlem yapıyor ise hash değerinin duyarlılık değeri kesinlikle düz çizgi olmamalıdır sürekli salınım yapmalıdır ve %100 'e yakın olmalıdır.

Metinin üzerindeki değişikliklerin hash fonksiyonunda değişim oranı %90 ile %100 arasında (Şekil 3 ve Şekil 4) olan yüksek miktarda değişikliğe sebep olduğu sonucuna ulaşılmıştır. Dolayısıyla YSA' nın hash fonksiyonu uygulamalarında doğru bir etkili tercih olduğunu söylenebilir. Farklı YSA yapıları ile daha yüksek sonuçlar elde edilebileceği düşünülmektedir.

Ayrıca, YSA tabanlı Hash fonksiyonunun hash değerini üretme süresi de incelenmiştir. Metnin hash değeri 1sn in altında oluşturulabilmektedir. Dolayısıyla kullanım etkinliğinin gayet uygun olduğu değerlendirilmektedir.

TEŞEKKÜRLER

Bu çalışma Mustafa Kemal Üniversitesinin 8702 numaralı Bilimsel Araştırma Projesi (BAP) desteği ile yapılmıştır.

KAYNAKLAR

[1] Gadgi Sumangala, V.R. Kulkarni, Shridevi Sali, and Sulabha Apte, "Perfoance Analayses of SHA-2 Algorithm with and without Using Artificial Neural Networks," *World of Science and Technology* , pp. 12-20, 2011.

[2] Seniye Soyalıç, "Kriptografik Hash Fonksiyonları ve Uygulamaları," *Erciğes Üniverstesi Matematik Anabilim Dalı Yüksek Lisans Tezi*, 2005.

[3] Mustafa Dülgerler and N.S. Sarısakal, "Elgamal Şifreleme Algoritmasını Kullanan Güvenli Bir E-Posta Uygulaması: Md Message Controller," *İstanbul Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü*, 2003.

[4] Resmi Gazete, Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliği, 30.01.2013.

[5] İlker Dalkıran and Kenan Danışman, "Artificial Neural Network Based Choatic Generator For Crytography," *TUBİTAK Eng&Comp.Sci.*, vol. 12, no. 18, 2010.

[6] The Matworks. [Online]. www.mathworks.com/help/techdoc/rendstream.html, (2013)

[7] Bruce Scheinder, "Applied Cryptography Protocols Algorithms and Source in C," *2nd New York John Wiley & Sons Inc.*, 1996.

[8] Çetin Elmas, *Yapay Zeka Uygulamaları*. Ankara: Seçkin Yayımcılık, 2011.

[9] N. Mohammed and S. Babak, *Desigh of S-box on Neural Network*.: International Conferance on Electronics and Information Engineering (ICEIE), 2010.

[10] Yayik and Kutlu , "Improving Randomness of Pseudo-Random Number Generators," *Signal Processing and Communicaion Conferance April, 2013*

Yakup KUTLU (1977) Lisans eğitimini 2001 yılında Dokuz Eylül Üniversitesi Elektrik ve Elektronik Mühendisliği bölümünde, Yüksek Lisans eğitimini 2004 yılında Mustafa Kemal Üniversitesi Elektrik ve Elektronik Mühendisliği Ana Bilim Dalında, Doktora eğitimini ise 2010 yılında Dokuz Eylül Üniversitesi Elektrik ve Elektronik Mühendisliği Ana Bilim Dalında tamamlamıştır.
2002-2005 yılları arasında Mustafa Kemal Üniversitesi Elektrik ve Elektronik Bölümünde araştırma görevlisi olarak görev yapmıştır. 2011 yılından itibaren Mustafa Kemal Üniversitesi Bilgisayar Mühendisliği Bölümünde öğretim üyesi olarak çalışmaktadır.
Yardımcı Doçent Doktor KUTLU, Biyomedikal Sinyal İşleme, Kriptoloji, Örüntü Tanıma, Yapay Sinir Ağları ve Genetik Algoritma konularında çeşitli çalışmalar yapmıştır.

Apdullah YAYIK (1986) Lisans Eğitimini 2008 yılında Akdeniz Üniversitesi Fizik Bölümünde, Yüksek Lisans Eğitimini 2013 yılında Mustafa Kemal Üniversitesi Enformatik Ana Bilim Dalında tamamlamıştır.
2010 yılından itibaren Türk Silahlı Kuvvetlerinde çalışmaktadır.
Biyomedikal Sinyal İşleme, Örüntü Tanıma ve Kriptoloji konularında çeşitli çalışmalar yapmıştır.

Cyber Attack Timing

Ferhat Çalışkan, and Yavuz İduğ

***Abstract*—Cyber attacks range in magnitude from large scale attacks to more targeted small attacks. Ill-timed and ill-planned sequence of large scale cyber attacks may weaken the power of the ones next to it. Small scale targeted cyber attacks will mostly have one shot opportunity because of the countermeasures taken by the defender soon after the attack. In this case acceleration trend of the progress of targeted development project will be the determinant factor to decide when to launch cyber attack. This work examines the timing factors in large scale cyber attacks and targeted small scale cyber attacks**

***Index Terms*—Cyber Attack Planning, Timing, Cyber Defense.**

I. INTRODUCTION

CYBER attacks range in magnitude from large scale attacks to more targeted small attacks. The first type of attacks targets whole infrastructure of a country such as the case of an Eastern Europe country in 2007. This cyber attacks resulted in paralyzing the ability of the state to govern [1]. Not only the government agencies but also the national media was affected severely [2]. The second types of attacks are more targeted and have a goal of disrupting progress of a project. This may be a high-tech military technology development project or other balance tipping capabilities such as uranium enrichment. Stuxnet is the most known example of these targeted cyber attacks. Although no government has taken credit for this attack, officials acknowledged the effect of Stuxnet on nuclear site in Natanz [3]. In terms of timing of the attacks, large scale attacks and targeted small attacks provides the cyber attack planners with different and crucial considerations.

II. DETERMINANT TIME FACTORS IN CYBER ATTACKS

A. Purpose of the Study

Cyber warfare studies mostly deals with the defense side of the cyber space. But a better understanding of the cyber attack planning factors will also contribute to cyber defense with the help of increased deterrence by means of enhanced offensive capability. This deterrence can only be reached by detecting security gaps in the networks or systems of the opponent. Gathered intelligence about the gaps will constitute the cyber build-up against a given opponent. This build-up should be kept until the appropriate time comes to launch attack. In this paper time factor in cyber attacks will be examined by differentiating between large scale cyber attacks and small scale targeted cyber attacks.

B. Large Scale Cyber Attacks

Compared with the attack, defense in cyber warfare is more difficult, expensive and needs more effort. The more network operations becomes complex the more they become vulnerable to cyber attacks. This trend always works to the advantage of the cyber attacker rather than the defender [4]. Therefore attacker should gather information about the security gaps in its opponents' networks and critical infrastructures. Then this gathered information should be kept in a vulnerability log of that opponent. This vulnerability log is the cyber version of conventional military build-up. The real advantage lies in the vulnerabilities that are not known by the attacker but not detected by the defender. In Art of War, Sun Tzu puts emphasis on this issue and states that: "We should hide the point where we want to attack the opponent. In this case the opponent will have to consider lots of probabilities at the same time. This will prevent it from massing its power to a point [5]."

Importance of determining time of attack comes to fore at this point. Because ill-timed and ill-planned sequence of cyber attacks will deprive the attacker of the benefits the cyber build-up offers. But only by means of properly determining time and sequence of attacks, this benefit can be transformed to a successful cyber attack.

Between 27 April and 18 May 2007, a series of cyber attacks hit the Eastern Europe country's ministries, banks and other institutions. First wave of attacks started on 27 April and hit the web sites related with the government, on 4 May more organized second wave included botnets and roughly one million computers were used. Third wave of attacks was the most powerful one with a size roughly 2,5 times the bandwidth capacity of country. But because of the countermeasures taken by the officials, when the third wave started on 9 May it did not bear the desired end. It caused a huge damage but this was short of shutting down the entire internet in country [6]. First and second wave of attacks became a warning for the officials in defending country and they raced with time to take countermeasures. Time interval between waves of attacks was enough wide for the defending country to detect security gaps and find solutions.

The response time and countermeasure capability of the defender is the key planning factors for the cyber attack planners. Figure 1 explains the side effects of sequential

Ferhat Çalışkan, War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Turkey, e-mail: fcaliskan10@gmail.com

Yavuz İduğ, War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Turkey, e-mail: yavuzidug@gmail.com.

cyber attacks. The key point here is the time interval between waves and the response time of the defender. Response time is a factor of speed of bureaucracy in a given country. If the cyber attack planners do not integrate the time planning vis-à-vis countermeasure response time, each waves of attacks will weaken the power of the subsequent cyber attacks. This will also harm the cyber buildup of the attacker, which will end up with weakened cyber deterrence.

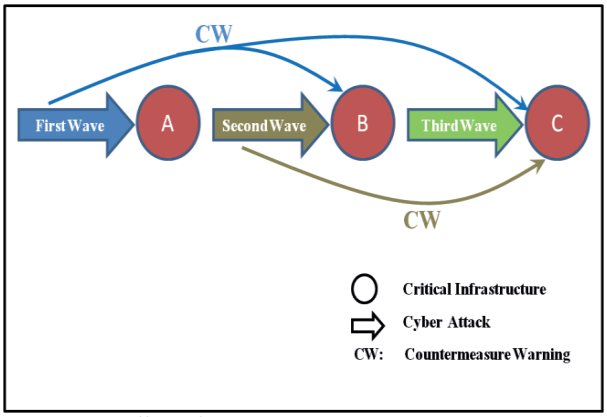
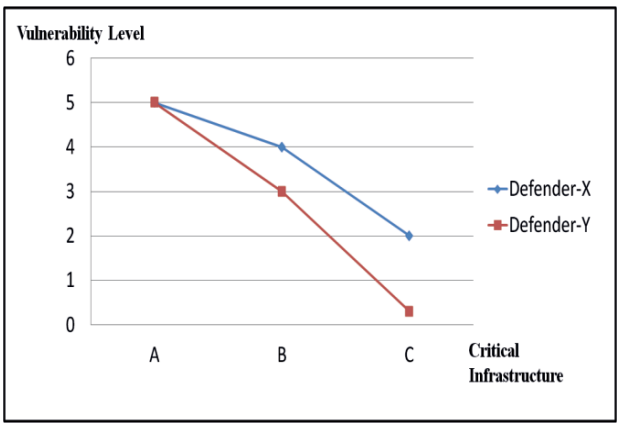


Figure 1. Side Effects of Sequential Cyber Attacks

Vulnerability level of the defender to cyber attacks will depend on the capabilities of the cyber experts working for the defending country. As illustrated in Graph 1, vulnerability level of the critical infrastructures A, B and C, will decrease to the extent of the capabilities of the cyber experts working for X or Y. Cyber expert working for Y are more adaptive than cyber expert working for X to improvising countermeasures. Therefore each wave of attacks to the critical infrastructures A, B and C results in different size of damage in Y and X.



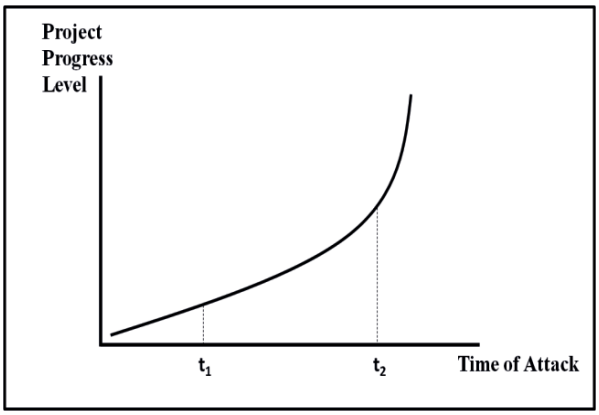
Graph 1. Countermeasure Capability

C. Small Scale Cyber Attacks

Stuxnet attack targeted the frequency-converters that control the speed of centrifuge motors. After Stuxnet reached the centrifuges in Natanz, it stayed inert and one month later it started to change spin frequency from 1410 Hz to 2 Hz. This sudden change caused the physical damage to the centrifuges. This cyber attack certainly caused a drop in the numbers of the machines in the facility. But the timing of the attack was not quite good to get the most of the security gap detected by the attackers. Defending country took necessary measures and closed the security gap, which made the subsequent attacks much more difficult to infiltrate. If the attack was made when the engineers reached the weapons grade level the time provided by the delay in the uranium enrichment would be more valuable [7].

Targeted small scale cyber attacks differ from large scale attack in the conditions that are advantageous for the defender. Since a given infrastructure or a development project will probably have less security gap than whole country network, the attackers will have one shot opportunity to reach the desired end. In short we cannot mention about subsequent waves of cyber attacks which we see in large scale attacks. Therefore vulnerability log of the targeted project is more important than that of large scale attacks and there is no place for wasting. The detected security gap must be kept until suitable time comes to launch cyber attack.

If the aim of the cyber attacks to retard the progress of the project, cyber attack planners must consider the acceleration trends in the progress of the project and then determine the time of attack. In short, acceleration trend of the targeted project and the time of the attack are two crucial factors that lead to success or failure. As seen in Graph 2, acceleration of the Project Progress Level on t_2 more than that of on t_1. Time gained in an attack staged on t_2 will be more valuable than the one staged on t_1. Therefore best time for cyber attack is t_2. If not kept for the suitable time, the security gap will be closed after an attack on t_1.



Graph 2. Timing in Small Scale Cyber Attacks

III. Conclusion

Cyber attacks are different from the conventional ones in their side effects on the subsequent attacks. Ill-timed and ill-planned sequence of large scale cyber attacks may weaken the power of the ones next to it. The determinant timing factors in large scale cyber attacks are the response time of the defender and the interval between the waves of attacks. In small scale targeted cyber attacks there will be one shot opportunity because of the countermeasures taken by the defender soon after the attack. In this case acceleration trend of the progress of targeted development project will be the determinant factor to decide when to attack. The period when the project's progress gains acceleration will be the best time to launch cyber attack.

ACKNOWLEDGMENT

We thank to War Colleges Command, Army War College, Dept. of Combat Tactic staff officers for their valuable contribution.

REFERENCES

[1] E. T. Jensen, "Cyber Warfare and Precautions Against the Effects of Attacks," *Texas Law Review*, Vol. 88, pp.1533-1569.
[2] S. Mansfield-Devine, "Estonia: What Doesn't Kill You Makes You Stronger," *Network Security*, July 2012, p.13.
[3] I. Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on The Iranian Enrichment Praogramme," *The Rusi Journal*, April/May 2013, 158:2, p.48.
[4] R.A. Miller, D.T. Kuehl, and I. Lachow, "Cyber War: Issues in Attack and Defense," *JFQ*, Issue 61, 2d quarter 2011, pp.18-23.
[5] Sun Tzu, *Savaş Sanatı*, Trans.. Adil Demir, Kastaş Yayınevi, 2012, p. 58
[6] S. Mansfield-Devine, "Estonia: What Doesn't Kill You Makes You Stronger," *Network Security*, July 2012, p.14.
[7] I. Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on The Iranian Enrichment Programme," *The Rusi Journal*, April/May 2013, 158:2, p.54.



Ferhat Çalışkan received his B.S.degree in System Engineering from Turkish Military Academy in 2003. He was accepted in the Naval Postgraduate School (NPS) in California, and received M.A. degree in Security Studies-Middle East in 2011. He currently continues his study at the Turkish Army War College. He is interested in international relations, Middle East, game theory, cyber attack planning.



Yavuz İduğ received his B.S.degree in International Relations and Leadership&Management from the United States Military Academy at West Point in 2003. He received his MBA in Financial Management from the Naval Postgraduate School in California. He currently continues his study at the Turkish Army War College. He is interested in international relations, leadership & management studies and cyber attack planning.

Siber Tehdit Ortamında Muharebe Sahasının Sayısallaştırılması

Selçuk DAL, Eşref FIRAT, Serbülent EKEN

***Özet*—Muharebe sahasının sayısallaştırılması bugün bütün modern ordular tarafından uygulanmaya çalışılan bir faaliyettir. Siber tehdit ortamında muharebe sahasının sayısallaştırılmasının faydalarının yanında çeşitli mahzurları da bulunmaktadır. Muharebe sahası sayısallaştırılırken mahzurları da dikkate alınmalı ve siber tehdidi asgari seviyeye indirecek şekilde planlama yapılmalıdır.**

***Anahtar Kelimeler*—Muharebe Sahasının Sayısallaştırılması, Siber Tehdit**

***Abstract*—Today, battlefield digitization is a concept which has been tried to be applied by all modern armed forces. In a cyber threatened environment, battlefield digitization brings not only advantages but also disadvantages. While digitizing the battlefield, the disadvantages should also be taken into account and planned to minimize the cyber threat.**

***Index Terms*—Battlefield Digitization, Cyber Threat**

I. GİRİŞ

Muharebe sahasının sayısallaştırılması ve bilgi teknolojilerinin silahlı kuvvetler tarafından yoğun olarak kullanılmaya başlaması çağımızda olmazsa olmaz bir gereklilik olarak ortaya çıkmaktadır. Öte yandan bilgi teknolojilerindeki ilerlemeler yepyeni bir tehdit kavram meydana getirmiştir: siber tehdit. Bu makale muharebe sahasının sayısallaştırılması ve bilgi teknolojilerindeki ilerlemelerin siber tehdit ortamında kullanımı ve etkinliğini irdelemektedir.

II. SİBER TEHDİT ORTAMINDA MUHAREBE SAHASININ SAYISALLAŞTIRILMASI

A. Çalışmanın Amacı

Muharebe sahasının sayısallaştırılması kavramı ortaya çıktığında bugünkü gibi bir siber tehdit ortamı bulunmamaktaydı. Bugün bilgi teknolojilerindeki gelişmeler ve siber dünyada oluşan tehditler kapsamında muharebe sahasının sayısallaştırılmasının yeniden sorgulanması gerekmektedir. Bu çalışma muharebe sahasını sayısallaştırılmasının siber tehdit ortamında fayda ve mahzurlarını ortaya koyarak güvenli bir sayısallaştırma için neler yapılabileceğini belirlemeyi amaçlamaktadır.

B. Muharebe Sahasının Sayısallaştırılması

Muharebe sahasındaki gelişmeler teknolojideki gelişmelere paralel olarak ilerlemektedir. Çift yönlü olan bu ilişkide muharebe sahasının gereksinimleri kimi zaman teknolojiye önderlik etmiş, kimi zamanda muharebe sahası teknolojinin geldiği noktadan süratle istifade etmeye çalışmıştır. Bu yarışta öncülük eden ülkelerin silahlı kuvvetleri, bu sayede çok büyük bir kuvvet çarpanı oluşturmuşlardır. Son çeyrek yüzyılda internetle gelen bilgi aktarımındaki hız ve bilginin bu sayede eş zamanlı ve çok yönlü paylaşımı muharebe sahasının sayısallaştırılması kavramını ortaya çıkarmıştır.

Sayısallaştırma; sinyali bölerek ve ikili sayı sisteminde kod değerleri tahsis ederek herhangi bir bilginin ayrışık veya fasılalı sinyaller şeklinde kodlanmasıdır. Hepimizin sıklıkla duyduğu "0" ve "1" lerden oluşan bu dünyada sinyaller artık daha az karışıklığa maruz, daha uzağa gönderilebilirdir. Ancak bu özelliklerinin yanında sayısal sinyallerin belki de en önemli özelliği matematiksel algoritma kullanılarak bilgisayarlar tarafından işlenebilir olmasıdır. Bir veri sayısallaştıktan sonra bilgisayar ortamında işlenebilir bir veri haline gelir ve bilgisayarların gücü ve programcının hayal gücüne göre istenilen her şey bu verilerle yapılabilir. Bu nedenle yaşadığımız çağa sayısal bilgi çağı demek mümkündür. Sayısal bilgi; aldığımız tıbbi tedaviyi, banka hesaplarımızın güvenliğini, içtiğimiz suyun, yediğimiz yemeğin kalitesini, birbirimizle iletişim kurma kabiliyetimizi ve evlerimizi kışın sıcak, yazın soğuk tutmak için ihtiyaç duyduğumuz enerjiye erişimimizi kapsayacak kadar hayatın ayrılmaz bir parçası haline gelmiştir [1].

Sayısallaştırmanın getirdiği yeni dünyadan doğal olarak muharebe sahası da etkilenmiştir. Günümüzde gelişmiş bütün ülkelerin savunma sistemleri, ateş gücünü barındıran tank, uçak, gemi gibi sistemlerle; bu sistemlerin üzerindeki veya bu sistemleri destekleyen komuta kontrol, atış kontrol, muhabere, dost düşman tanıma vs. gibi tamamlayıcı savunma sistemleri olarak ikiye ayrılmaktadır. Tamamlayıcı savunma sistemleri sayısal kodlar sayesinde sayısal teknoloji ile geliştirilen ve yazılım kontrolünde çalışan yeni sistemlerle değiştirilmeye başlanmış ve buna "muharebe sahasının sayısallaştırılması" denilmiştir [2].

Muharebe sahasının sayısallaştırılması sayesinde bütün komuta kademelerinde taktik resmin elde edilmesi sağlanmış ve muharebe sahasının bilinmeyenleri azaltılmaya çalışılmıştır. ABD silahlı kuvvetlerinde özellikle otomasyon alanında muharebe sahasının sayısallaştırılmasına yönelik bu faaliyetler "Askeri Sistemlerde Çağdaş Devrim (ASÇD) (The contemporary Revolution in Military Affairs) olarak adlandırılmaktadır [3]. ABD Kara Kuvvetleri ASÇD faaliyetlerine ilk olarak 1978'te komuta kontrol sistemlerine yönelik olarak Sigma Star programıyla başlamış ve o günden beri de savaş kabiliyetlerini geliştirmeye devam etmektedir. Bu kapsamda ABD Kara Kuvvetlerinin ilk sayısallaştırılmış birlikleri mekanize birlikler olmuştur. Meskûn mahallere yönelik olarak bazı piyade birliklerinde kısmi sayısallaştırma

Selçuk DAL, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: selcuk2001@gmail.com.
Eşref FIRAT, , Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: esreffirat2001@gmail.com.
Serbülent EKEN, , Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: serbulenteken@gmail.com.

faaliyetleri olsa da ABD Kara Kuvvetleri sayısallaştırma konsepti ağır mekanizbirlikler üzerine kurulmuştur.

(I) Sayısallaştırmanın Faydaları (Şekil 1)

Bu tür birliklerde sayısallaştırmanın en önemli faydalarından birisi bazı birliklerin lağvedilmesi, genel olarak da ihtiyaç duyulan personel ve malzeme oranında da ciddi biçimde azalmadır. Buna karşın bir tümenin etki alanı, sayısallaştırmanın kazandırdığı imkân ve kabiliyetlerle 10.000 km^2 den 24.000 km^2 ye çıkmıştır [4]. Sayısallaşma sayesinde askeri literatüre "hassas angaje" kavramı girmiştir. Artık birlikler çok uzak mesafelerden düşmanı hassas olarak ateş altına alabilmekte, hem personel hem de malzeme zayiatı azalmaktadır. Sayısallaştırmanın bir diğer avantajı da kazandırdığı üstün hız sayesinde kendi içinde çok organize, hızlı hareket eden birliklerle caydırıcı savaşlar yaratmasıdır [3]. Ancak sayısallaştırmanın getirdiği en önemli fayda şüphesiz ki bilgi üstünlüğüdür. Askeri teorisyenlere göre bilgi üstünlüğünün getirdiği üç avantaj [3] bulunmaktadır. Birincisi, düşman, arazi ve kendi kuvvetlerimiz hakkında doğru, tam ve gerçek zamanlı bilgi vererek durumsal farkındalığı artırmaktadır. İkincisi, durumsal farkındalık sayesinde Calusewitz'in bahsettiği "savaşın sis perdesi" [5] büyük ölçüde dağılmakta ve her seviyedeki her asker, savaşın her aşamasında taktik resmi elde edebilmektedir. Üçüncüsü, bu bilgi üstünlüğüne sahip olan kuvvetler düşman kuvvetlerinin ne şekilde hareket edeceğini tahmin edebilmektedirler.



Şekil 1. Muharebe Sahasının Sayısallaştırılmasının Faydaları

(II) Siber Tehdit

Bilgi teknolojilerindeki gelişmeler bugün neredeyse her bireyi en az bir, hatta birden fazla bilgisayar sahibi yapmıştır. Yapılan araştırmalara göre dünya üzerinde iki milyarın üstünde pek çoğu internete bağlı kişisel bilgisayar bulunmaktadır [6]. Küçük birer kişisel bilgisayar olan ve hemen hemen onların yaptığı her şeyi yapan cep telefonlarının sayısı ise yaklaşık 6 milyardır [7]. Bütün devlet kurumları da bir şekilde çevrim içi yapılarla sistemlerini internete bağlamaktadırlar. Bu sayede birbirine bağlı bu yapıda, sınırlar kaybolmakta ya da belirsizleşmekte, bu okyanusun içinde ada olarak kalan bilgisayarların sayısı ise çok azalmaktadır [8].

2007 yılında Baltık ülkelerinden birinde yaşanan siber taarruz [9], 2008 yılında Karadeniz ülkelerinden ikisi arasında yaşanan savaş öncesi yapılan siber taarruz [9] ve bir ülkenin nükleer araştırma merkezlerinde ortaya çıkan "stuxnet" virüsü [10] bize bilgi teknolojilerindeki gelişmelerin aynı zamanda nasıl bir siber tehdit dünyası oluşturduğu hakkında da fikir vermektedir. Çağımızda bilgisayarların vazgeçilmez unsurlar olarak –çamaşır makinelerinden nükleer başlıklara kadar- her türlü sistemin içinde bir şekilde yer alıyor olması hayatımızı kolaylaştırdığı kadar aynı zamanda yanlış emellerle kullanıldığında bunların birer tehdit olarak kullanılması olasılığını da gündeme getirmiştir.

2007 yılında bir Baltık ülkesinin yaşadığı da tam olarak siber bir kâbustur. Yurt çapında bedava sınırsız internetin olduğu, dünya çapında e-devlet sistemine ilk geçen ve ekonomisini internet ve bilgi sistemleri üzerine oturtmuş olan bu ülke, bir alışveriş merkezi önüne konan işgalci bir ülke döneminden kalma bir anıtın kaldırılması üzerine haftalar süren bir siber taarruza maruz kalmıştır. Bu taarruzda ilk önce devlet kurumlarının haber sistemleri, sonra bütün medya sonra da bankalar hedef alınmıştır. Büyük bir panik havası yaşayan servis sağlayıcılar sistemlerini yeniden başlatmak zorunda kalmış ve ülkenin bilgi teknolojilerindeki ünü bir anda yerle bir olmuştur [11]. Çevrimiçi sistemlerin ne kadar güvensiz olduğu böylece anlaşılmıştır.

Çevrimdışı sistemlerin çevrim içi olmaması yönüyle güvenli oldukları söylenebilir mi? Bu konuda verilebilecek en iyi cevap meşhur "stuxnet" virüsüdür. Nükleer geliştirme merkezlerindeki trafoların aşırı derecede ısınmasını sağlayarak patlamalarını sağlayan bu virüs hiçbir ağa bağlı olmayan bu sisteme bir şekilde sızmış ve siber taarruz bakımından harika bir iş çıkararak yeni bir çığır açmıştır [12]. Peki çevrimdışı bir sisteme nasıl oldu da bir virüs bulaşabildi? Cevabı tam olarak bilinmese de virüsün bir taşınabilir bellek vasıtasıyla bulaştığı tahmin ediliyor. Şayet durum böyleyse çevrimdışı olduğu için güvende olduğu düşünülen pek çok sistemin aslında o kadar da güvenilir olmadığı, istenildiği takdirde bir şekilde saldırıya maruz kalabileceği söylenebilir.

(III) Siber Tehdit Ortamında Bilgi Teknolojilerindeki Gelişmelerin ve Muharebe Sahasının Sayısallaştırılmasının Mahzurları

Muharebe sahasının sayısallaştırılmasının daha önce bahsedilen pek çok avantajının yanında çeşitli mahzurları da olduğu görülmektedir. Bu mahzurları; sayısallaştırmanın tahakkuku ve idamesi için çok sayıda yüklenici veya taşeron sivil firmadan faydalanma zorunluluğu, bazı komuta kademelerinin kaybolması ve karar verme zaafiyeti, ağ yönetiminde ortak bir doktrin oluşturma gerekliliği, asimetrik tehdide sebebiyet vermesi, iletişimin sekteye uğraması ya da istismar edilmesi ve sayısal sistemlerin ele geçirilmesi olarak sıralamak mümkündür [3] (Şekil 2).

Muharebe sahasının sayısallaştırılması adına yapılan bütün faaliyetler ancak ve ancak çok daha fazla sayıda sivil firmanın eliyle yapılabilmektedir. Örneğin, bugün TSK'nin iletişim alt yapısını oluşturan TAFICS sistemi ASELSAN firmasının ana yükleniciliği altında 3 firmanın katılımıyla gerçekleşmiştir. Sivil firmalara olan bu derece bir bağımlılık harp zamanında değişik komplikasyonların oluşmasına sebebiyet verebilecektir. Her ne kadar sivil de olsalar askeri sistemlere verecekleri destek bu kişileri savaş zamanında savaş hukuku bakımından hedef haline getirebilecektir. Bu nedenle gerçek bir savaş zamanında bu kişilerin nasıl

davranacağını, kesintisiz bir biçimde hizmet vermeye devam edip edemeyeceği tam olarak belli değildir. Bu da mevcut yapıda bütün sayısallaştırma faaliyetlerinin üzerine bina edildiği TAFICS iletişim alt yapısı adına ciddi bir zafiyet olarak önümüze çıkmaktadır.



Şekil 2. Muharebe Sahasının Sayısallaştırılmasının Mahzurları

Sayısallaştırmanın bir başka mahzuru da taktik resmin her kademe tarafından rahatlıkla görülebilmesi sayesinde ara kademe komuta ihtiyaçlarını ortadan kaldırmasıdır. İlk bakışta olumlu gibi görünen bu merkezileşmenin, dikkatli bakıldığında karar verme yetisine sahip komutanların yetişmesi adına büyük bir zafiyet olduğu görülecektir. Çünkü komutanlar ancak her kademede görev yaptıktan sonra bulunduğu konumun gereğini yerine getirecek bilgi ve tecrübeye sahip olurlar. Hâlbuki muharebe sahasının sayısallaştırılması ile küçük birlik komutanları daha fazla önlerindeki ekranlara bağımlı, dış çevredeki ipuçlarını daha az değerlendirebilir hale gelmektedirler [3]. Ara komuta kademelerinin de kaybolmasıyla bu imkâna bile yeterince sahip olamayan komutanlar ileride daha büyük sorunları çözmek ve daha zor kararlar vermek gerektiren komuta kademelerine gelerek bir karar zafiyeti oluşturabileceklerdir.

Silahlı kuvvetlerin çok daha fazla müşterek ve birleşik harekâtı icra etmeye yönelik ortaya çıkan ihtiyaçlar kapsamında, sayısallaştırmanın karşılaşacağı bazı problemler olacağı aşikârdır. Çünkü bütün kuvvetlerin gerek personel gerek malzeme gerekse kurumsal kültür bakımından çeşitli farklılıkları bulunmaktadır. Bu nedenle daha fazla sayısallaştırma daha fazla aynı dili konuşmaya ve ortak doktrine ihtiyaç manasına gelmektedir. Gerek mevcut yapının gerekse gelecekte inşa edilecek yapıların mutlaka bu kapsamda ele alınması gerekecektir.

Öte yandan muharebe sahasının sayısallaştırılmasını başarıyla ifa eden birlikler karşısında, hiç bir düşman kuvveti bulunmak istemeyecektir. Kilometrelerce öteden hassas angaje ile ateş altına alma kabiliyeti olan bir güce karşı kim konvansiyel bir şekilde açık arazide karşı koymak ister? İşte bu nedenle muharebe sahasını sayısallaştırabilmiş güçler karşısında ya en az onların kadar sayısallaştırmayı başarabilmiş ya da asimetrik bir güç karşı koyabilecektir. Bu bakış açısıyla sivil kıyafetler içinde bir zırhlı taşıyıcıya 5 m. uzaklıkta bulunan bir düşman askeri 1000 m. deki bir tanktan daha zararlı olabilir. Özellikle meskun mahallerdeki muharebeler sayısallaştırma konseptinin çok uzağında cereyan etmektedir. Böylece sayısallaştırılmış birlikler bu tür muharebelerde etkinliklerini yeterince gösterememektedirler. Bu tür bir asimetrik muharebe anlayışı ise sayısallaştırmadan beklenen hemen hemen her şeyi boşa çıkarabilecek kadar tehlikelidir [3].

Muharebe sahasının sayısallaştırılması çerçevesinde en önemli unsur iletişim olarak karşımıza çıkmaktadır. Sayısallaştırılmış birliklerde taktik resmin elde edilmesi, emirlerin iletilmesi, ihtiyaçların tespit edilmesi, ikmal faaliyetlerinin icra edilmesi gibi pek çok hayati önemi haiz faaliyet hep iletişim kanalları üzerinden gerçekleştirilmektedir. Dolayısıyla bu iletişim kanallarının çalışması sekteye uğradığında ya da uğratıldığında sonuç bu tür birlikler için bir faciaya dönüşmektedir [13]. İletişim kanallarının sekteye uğraması doğal koşullar nedeniyle (kötü hava koşulları, arazideki engebeler vs.) olabileceği gibi suni nedenlerle (elektromanyetik yayım, karıştırma vs.) de olabilmektedir. Her iki halde de sayısallaştırılmış bilgiye tabi olan dost unsurlar böyle bir durumda çok yakınına kadar gelen bir düşman unsurunu göremeyecek veya bu nedenle dost ateşine maruz kalma ihtimali artabilecektir. Ancak tek endişe edilen şey iletişim kanallarının sekteye uğraması değildir. İletişimin ele geçirilerek yanlış bilgi üretilmesi ise şüphesiz daha büyük bir tehlikedir.

Bütün bir harekâtı icra ederken dost birliklerin güvendiği en önemli şey eldeki bilgilerin doğruluğudur. Muharebe sahasının sayısallaştırılması da daha önce ifade edildiği gibi zaten düşman, arazi ve mevcut kuvvetler hakkındaki bilgilerin doğruluğunu artırmak için ortaya konulmuş bir sistemdir. Peki ya elimizdeki bilgiler doğru değilse? O zaman en iyi senaryo ile hiç kuvvet ayırmamanız gereken yere kuvvet ayırırsınız en kötü senaryo ile de hiç düşman ateşine maruz kalmaksızın ekranınızda dost unsurların düşman olarak görünmesiyle dost ateşleriyle birlikleriniz imha olur. Peki bu nasıl mümkün olabilir? Sayısallaştırma işleminin her aşamasında mutlaka bir takım algoritmalar, bilgisayarlar veya işlemcisi, belleği olan bilgisayar benzeri yapılar kullanılmaktadır. Bu nedenle bu tür yapıların gerek çevrimiçi gerekse çevrimdışı yollarla (virüs, truva atı, sniffer, kötücül yazılımlar vs.) ele geçirilmesi ihtimali bulunmaktadır.

III. SONUÇ

Bilgi teknolojilerindeki gelişmeler kapsamında muharebe sahası daha fazla sayısallaşmaya başlamıştır. Muharebe sahasının sayısallaştırılması karar vericilere tüm komuta kademelerinde taktik resmin sağlanması, yüksek bir hız ve hassas angaje imkanını kazandırmıştır. Bu tür sayısallaştırılmış bir birlik için etki alanı artmış ve muharebe sahasının bilinmeyenleri azalmıştır. Ancak bu faydaların yanında muharebe sahasının sayısallaştırılmasının siber tehdit ortamını da dikkate alarak getirdiği bir takım mahzurlar da bulunmaktadır. Bu mahzurları, sayısallaştırmanın tahakkuku ve idamesi için çok sayıda sivil firmadan faydalanma zorunluluğu, bazı komuta kademelerinin kaybolması ve karar verme zaafiyeti, ağ yönetiminde ortak bir doktrin oluşturma gerekliliği, asimetrik tehdide sebebiyet vermesi, iletişimin istismar edilmesi ve sayısal sistemlerin ele geçirilmesi olarak sıralamak mümkündür.

Gelişmiş ülkelerin silahlı kuvvetleri artan bir hızla muharebe sahasını sayısallaştırma faaliyetlerine devam etmektedirler. Günümüzde teknolojinin imkânlarını

kullanmayan bir ordunun muharebelerde başarılı olmasını düşünmek imkânsızdır. Adeta bütün doktrinler, elde edilen sayısallaştırma faaliyetleri ölçüsünde bir değişim göstermektedir. Ancak siber tehdit göz önünde bulundurulmadan sarf edilen muharebe sahasını sayısallaştırma çabaları getirdiği faydadan daha fazla mahzur doğuracaktır.

KAYNAKLAR

[1] http://www.northropgrumman.com/MediaResources/Presentations/2013/Pages/052113MikePapayCyberThreatsandSecuritySolutions.aspx erişim tarihi 11.07.2013.

[2] TÜBİTAK Savunma Havacılık ve Uzay Sanayi Panel Raporu 2003, s.6.

[3] Mitchell, Elizabeth a. Stanley, Technology's Double-Edged Sword:The Case of US Army Battlefield Digitization, Defense Analysis Vol.17, No.3, 2001, s.267-280.

[4] Battlefield Automation, United States General Accounting Office, 2000 s.15.

[5] Clausewitz, Carl von, Savaş Üzerine, Çev. Şiar Yalçın, İstanbul, Spartaküs Yayınları, 1997, Kitap II, Bölüm 2, Altbölüm 24.

[6] State of the Future 2012 Report, (Executive Summary) http://www.millennium-project.org/millennium/SOF2012-English.pdf erişim tarihi 11.07.2013.

[7] https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html erişim tarihi 10.01.2013.

[8] Libicki, Martin C., Cyberdeterrence and cyberwar, RAND, 2009, s.4.

[9] Moore, Ryan J., Prospects For Cyber Deterrence, NPS, Monterey, 2008, s.27, 54.

[10] Shanker Tom, Sanger David, U.S. Suspects Iran Was Behind a Wave of Cyberattacks,New York Times, Washington, 13 Ekim 2011.

[11] Mansfield, Steve, Estonia:What doesn't kill you make you stronger., Network security,2012, s.12.

[12] Farwell, James P.-Rohozinski Rafael, Stuxnet and the Future of Cyber War, Survival vol.53. no.1,2011, s.24.

[13] Finley, Dorothy, Handling degraded communications, Military Review,2001, s. 33.

Selçuk Dal Kara Harp Okulundan 2001 yılında Sistem Mühendisi diploması aldı. 2004-2006 yılları arasında Naval Postgraduate School Monterey, California ABD'de Manpower Systems Analysis bölümünde yüksek lisans eğitimini tamamladı. Halen Kara Harp Akademisinde eğitim görmektedir.

Eşref Fırat Kara Harp Okulundan 2001 yılında Sistem Mühendisi diploması aldı. 2005-2007 yılları arasında Konya Selçuk Üniversitesinde Halkla İlişkiler Bölümünde yüksek lisan eğitimini tamamladı. Halen Kara Harp Akademisinde eğitim görmektedir.

Serbülent Eken Kara Harp Okulundan 1997 yılında Sistem Mühendisi diploması aldı. Kara Harp Akademisinde yüksek lisans eğitimine müteakip halen Kara Harp Akademisinde öğretim elemenı olarak görevine devam etmektedir.

Askerî Alandaki Bulut Sistemi Kullanımına Güvenlik Yaklaşımları

İsmail Aydın, Recep Kılıç, A. Zeki Gerehan

***Özet*—Bulut sistemi, günümüzün en gelişmiş sistemlerinden biridir. Hayatın her alanına giren bu teknoloji askerî alanda da kullanılmaktadır. Tüm ordular muharebe sahasını yönetmek için güvenlik ve teknoloji kullanımı dengesini koruyarak taktik resmi oluşturulmaya çalışmaktadır. Muharebe sahasındaki karmaşıklığın giderek artması önümüzdeki yıllarda taktik resmin oluşturulmasında daha fazla teknoloji ve daha fazla güvenlik tedbirleri gerektirecektir. Askerî alanda bulut sistemi kullanımı, sistemin karşılaştığı riskler ve bunlara karşı çözüm önerilerini içeren bir yazı takdim edilmiştir.**

***Anahtar Sözcükler* —Askerî uygulamalar, Bulut sistemi**

***Absract*— Cloud Computing is one of the most improvement system in the present-day. *This* technologies have become into all areas of life so that it's not without military. All armies in the world is try to make tactic picture, it's made for managing combat area, with using technology and security balance. While complexity in the field of battle is increasing, the next few years making tactic picture will be necessary more technology and more security protection. In this paper is presented using cloud computing in the military area, risks faced by the system and solving suggestions.**

***Index Terms* —Military applications, cloud computing**

I. GİRİŞ

BULUT sistemi her ne kadar net olarak tanımlanamasa da hayatın her alanında kullanılmaktadır. İnternetin askeri gereklilikleri karşılamak için oluşturulduğu düşünüldüğünde interneti aktif olarak kullanan bulut sistemi askeri uygulamalardan ayrı olması düşünülemez. Bulut sistemi, askerî uygulamalardan özellikle taktik resmin oluşturulması, ani durumların açıklığa kavuşturulması ve günlük rutin faaliyetlerin yürütülmesinde kullanılmaktadır. 1'inci Dünya Savaşı ile başlayan telsiz kullanımı, 2'nci Dünya Savaşı sonrası ihtiyaçları giderme maksadıyla ArpaNet'i ve daha sonra global olarak kullanılan İnternet ortaya çıkmıştır [1]. Ancak internetin askerî olmayan unsurlarca fazlaca kullanılması güvenlik açısından askeri kanadın başka yöntemlere başvurması gerekliliğini ortaya çıkarmıştır. Bu kapsamda maliyetlerin artması ve güvenlik hususları askerî kanadın bulut sistemini kullanmaya zorlamıştır. Askeri harekât açıdan çok önemli verilerin hem kullanabilir hem de güvenli olması dengesi bulut sistemini kaçınılmaz yapıp, yeni güvenlik risklerine karşı, yeni önlemler alma gerekliliğini yanında getirmiştir.

Askerî bulut sistemlerinin maruz kalabileceği riskleri 3 ana başlık altında toplamamız mümkündür. Bunlar;

A. Donanımsal Riskler

Alt yapı donanımlarının tahrip edilmesiyle, bütün verilerin kaybolmasına sebebiyet verecek risk kategorisi.

B. Yazılımsal ve İşletim Sistemleri Riskler

Bulut sistemini oluşturan yazılım ve işletim sistemlerinin güvenilir, minimum açıkları olan ve sürekli geliştirilebilen yazılımlar olmaması durumunda oluşabilecek risk kategorisi.

C. Kullanıcı Tarafından Meydana Gelen Riskler

Bilinçsiz kullanıcılar tarafından bulut sistemini zayıflatılacak ya da veri kaybına neden olabilecek siber saldırı girişleri yapılmasına müsaade edebilecek risk kategorisi.

II. BULUT SİSTEMİNİN TANIMI VE KAPSAMI

Bulut sistemi net bir tanımı bulunmamakla birlikte; uzak bir sunucu tarafından uygulamaların çalıştırılması ya da kullanıcı verilerinin sunucu tarafından her zaman ulaşılabilir şekilde bulundurulmasını sağlayan bir servis sistemi olarak tanımlayabiliriz. Bulut sistemi; basit ve kullanışlı ara yüzleri ile bilgiyi istenilen her yerde, istenilen zamanda ulaşılabilir ve kullanılabilir hale getirmiştir. 2000'li yılların başından itibaren, bilgilerin yerel bilgisayar diskinde bulundurularak yapılan uzak erişimler ve uygulamaların kullanıcı bilgisayarı üzerinden çalıştırılması ile merkezi bilgisayar ve ona bağlı terminal yapısı kullanılmaya başlanmıştır [2]. Bu yönüyle bulut sistemi; geçmişte kullanılmış bir yöntemin günümüzün ekonomik şartlarına uyarlanarak ve geliştirilerek, tüm ağ kullanıcılarının erişimine olanak sağlayacak şekilde yeniden sunulmasıdır [3].

Bulut sistemi ile bilgiye istenilen her yerden ve her türlü bilgi iletişim cihazı (PC, Mac, iPhone, Android veya BlackBerry) kullanarak ulaşmak mümkün olabilmektedir. Konuya askerî açıdan incelendiğinde daha çok ülkelerin kendi geliştirdikleri cihaz ve sistemlerle bilgiye ulaştıkları ve depoladıkları görülmektedir.

Yüksek erişilebilirlik imkânının sunulması, bellek ve disk değişikliği gerektirmeyen esnek yapının kullanılması ve doğa dostu (elektrik ve yer tasarrufu) olması, bulut sisteminin ilk bakışta dikkati çeken avantajları arasında görülmektedir.

İsmail AYDIN, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100/0100, İstanbul-Turkey, e-mail: iaydin2004@gmail.com.

Recep KILIÇ, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100/0100, İstanbul-Turkey, e-mail: rkilic40@gmail.com.

Ahmet Zeki GEREHAN, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100/0100, İstanbul-Turkey, e-mail: azgerehan@hotmail.com.

Bu avantajlı yönleri dikkate alındığında; bilgi iletişim teknolojilerindeki gelişimin yansıması olan bulut sistemiden uzak durmak ya da alternatif yöntemlerde ısrarcı olmak akılcı bir çözüm olarak görülmemektedir. Bulut sistemi beraberinde getirdiği avantajlar ile birlikte riskleri de unutulmamalı ve hassasiyetle üzerinde durulmalıdır.

A. Bulut Sistemi Modelleri ve Kullanım Biçimleri

Kullanım biçimine göre bulut sistemi üç sınıfta toplanmaktadır [4]. Bunlar (Şekil 1);

1. Genel Bulut (Public Cloud)

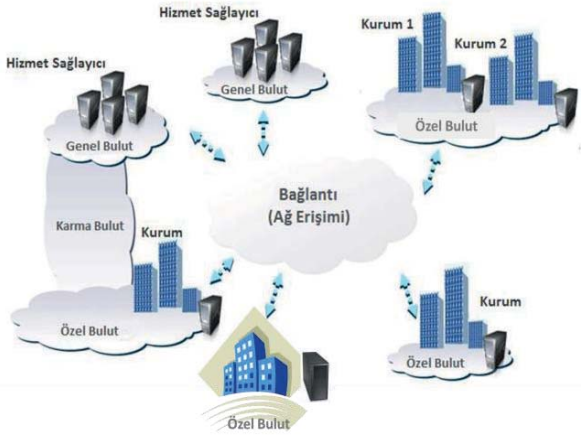
Web ara yüzü aracılığıyla internet üzerinden genel kullanıma sunulan hizmetlerdir (Google Apps, Amazon, Windows Azure) [5].

2. Özel Bulut (Private Cloud)

Belirli bir kurum ya da kuruluşa sunulan bulut hizmetidir. Bulut sistemini sağlayan, kurumun kendisi olabileceği gibi, başka bir bulut sistemi sağlayıcı da olabilir. Bu bulut sisteminde sadece kurum içi hizmet verilir.

3. Melez Bulut (Hybrid Cloud)

Genel ve özel bulut sistemlerinin birlikte kullanımasıdır. Bir kurumun verileri özel bulut içinde yer alırken, bazı servisleri genel bulut üzerinden halkın kullanımına açılabilir. Günümüzdeki askeri bulut sistemleri melez buluta örnek verilebilir.



Şekil 1. Bulut Sistemi Yapısı [6]

Bulut sistemi hizmet sağlayıcıları, bulut hizmetini sağlarken yazılım, platform ve alt yapı hizmet modellerinden birini ya da aynı anda birkaçını kullanmak zorundadır. Bulut Hizmet Modelleri aşağıda açıklanacaktır.

B. Bulut Sistem Hizmet Modelleri

1. Yazılım Hizmetleri (SaaS - Software as a Service)

Uygulama bulutudur. Bulut sistemi alt yapısı kullanılarak, web tabanlı çeşitli uygulama ve yazılımların (örneğin e-Posta, ağda konferans) bulut sistemi kullanıcısına sağlanmasıdır. Kullanıcı, bulut hizmeti almakta olduğu sunucu bilgisayar üzerindeki yazılımı çalıştırmak suretiyle istediği dosyaları üzerinde çalışabilmektedir. Kullanıcının; sunucu, işletim sistemi, veri depolama alanı üzerinde yönetim işlevi bulunmamaktadır.

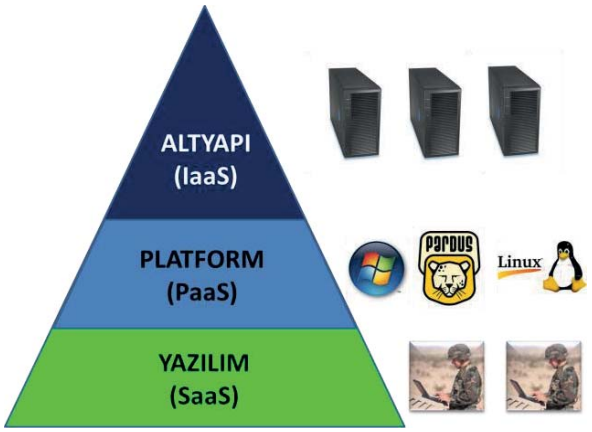
2. Platform Hizmetleri (PaaS - Platform as a Service)

Kullanıcıya kullanabileceği uygulamaları geliştirmesi ve sunabilmesi için uygun servis ortamı sağlanmasıdır. Geliştirilen uygulama ile ilgili alt yapı, ortam ve diğer servisler bulut hizmet sağlayıcı tarafından sağlanır [7]. Kullanıcının işletim sistemi, sunucu, veri depolama alanı üzerinde yönetim işlevi bulunmamaktadır. Kullanıcı ancak geliştirilen uygulamalar üzerinde kontrol sağlayabilmektedir. Bir bulut hizmet sağlayıcısı tarafından (Windows Azure v.b) üzerinde geliştirilen uygulamalarda herhangi bir standartın bulunmaması nedeniyle sadece geliştirilen platform üzerinde kullanılabilmektedir.

3. Altyapı Hizmetleri (IaaS - Infrastructure as a Service)

Bulut sisteminin kaynağı olarak da ifade edilmektedir. Ağ üzerinden güvenli erişim imkânı sunan dinamik veri depolama alanı (Amazon S3 v.b), işlemci kaynaklarının sanal olarak sunulması (Amazon EC2 v.b) ve ağ hizmetleri gibi servisler, bulut sistemi alt yapı servisi örnekleridir. Kullanıcının bulut alt yapısında yönetim işlevi bulunmamaktadır [8]. Fakat işletim sistemi, veri depolama alanı ve sınırlı olarak ağ bileşenleri (güvenlik duvarı gibi) üzerinde kontrol sağlayabilmektedir.

Bulut sistemi hizmetleri tabanını altyapı hizmeti ve bunun üzerine platform ve yazılım hizmetleri gelse de kullanıcı açısında bakıldığında piramit tam tersi şekilde olmaktadır. (Şekil 2).



Şekil 2. Bulut Sistemi Hizmetleri

III. BULUT SİSTEMİNİN ASKERÎ ALANLARDAKİ KULLANIMLARI

Bulut sistemi; karmaşık harekât ortamında taktik resmin oluşturulması için gerekli verilerin güvenilir ve zamanında işlenebilmesi maksadıyla gelişmiş bütün ordu ve askerî organizasyonlar tarafından kullanılmaktadır.

Taktik resim cereyan eden harekâtın istenilen anki fotoğrafıdır. Doğru karar verilmesi için bu fotoğrafta kara, deniz, hava kuvvetleri, insansız hava ve uzay sistemleri, coğrafi bilgi sistem sistemleri, sağlık ve lojistik konularından gelen tüm veriler bulunmak zorundadır (Şekil 3).

Taktik resim oluşturmak için çok fazla veriye ihtiyaç duyulması, bu toplanan verilerin istenen yer ve zamanda hazır bulundurulması gerekliliği bulut sisteminin kullanımını zorunlu kılmaktadır. Ayrıca anlık oluşan ani durumlar ve

rutin faaliyetlerde de bulut sistemi günümüzün olmazsa olmaz bir sistemi haline gelmiştir.



Şekil 3. Taktik resim bileşenleri

IV. Bulut Sisteminin Sağladığı Teknik Faydalar

A. *Erişimde Esneklik*

Bulut sisteminin ana görevi, kullanıcıya ait verilerin ağ üzerindeki bir sunucuya yüklenmesi, depolanması ve gerektiğinde erişilerek bilgiler üzerinde değişikliğin yapılmasını sağlamaktır. Bu nedenle taktik resmin oluşturulmasında mutlaka olması gereken bir sistemdir. Bulut sisteminin en önemli özelliliği her an kullanıcının isteklerine cevap verecek durumda ve yeterlilikte olmasıdır. Bu özelliği ile bulut sistemi, taktik durumun güncellenmesi ve istenen verilere ulaşılabilmesinde en önemli bilgi ve iletişim teknolojileri hizmetlerinden biri haline gelmiştir. Bulut sistemi ile ağ erişimi sağlanabilen her noktadan bilgilere ve uygulama programlarını kullanma imkânına sahip olunabilmektedir. Uzaktan erişim kolaylığı; harekât alanından yapılabilecek bir hırsızlık ya da fiziksel disk problemleri gibi nedenlerle verinin kaybedilme riskini azaltmaktadır.

B. *Kaynak Paylaşımı ve Maliyet*

Bulut sisteminde; kullanıcı sayısı ve sunulan hizmetin niteliğine bağlı olarak maliyetler değişmekte ve yönetilebilmektedir. Hizmet sunmak için kullanılan tüm donanım, bakım ve güncellemeleri hizmet sağlayıcı tarafından yapılmaktadır. Kullanıcı tarafından herhangi bir yazılım ücreti ödenmemektedir. Yazılım maliyeti kullanıcı sayısına bağlı olarak hizmet sağlayıcı tarafından karşılanır. Kullanıcı tarafından veri depolamak için yüksek kapasiteli veri depolama birimlerine ihtiyaç yoktur. Bu sebeple harekâtın hızla geliştiği bir ortamda mobiliteyi artırma adına çok önemli bir hususdur.

C. *Depolama için Kapasite Sınırlamalarının Ortadan Kalkması*

Bulut sisteminde; kullanıcılara tahsisli özel bir disk alanı bulunmamaktadır. Bundan dolayı veri depolama alanının yönetimi daha etkin olarak yapılabilmektedir. Kullanıcılar, depolama alanı kullanımı konusunda, sanal disk üzerinde yazılım ile kısıtlanırlar ve tüm kullanıcılara ait veriler aynı ortamda bulunmaktadır[9]. Kullanıcı bilgisayarında veri depolamak için yüksek kapasiteli veri depolama birimlerine ihtiyaç duyulmamaktadır. Bulut sisteminde kullanılan bilgi ve veri alanı yönetim araçları, eşit seviyede maliyet ile daha geniş veri alanında daha güçlü veri koruma imkânı sunar ki bu husus harekât ortamındaki yoğunluk ve karmaşa düşünüldüğünde en önemli konulardan biridir. Ancak bulut teknolojisinin bu kolaylıklarının yanında bazı risklerde bulunmaktadır. [10]. Bu riskleri üç başlık altında toplayabiliriz:

V. Bulut Sisteminin Oluşturduğu Riskler

A. *Donanım Riskleri*

Bulut teknolojisinde kullanılan alt yapı donanımlarının ve yedeklerinin hasım güçler tarafından imha edilmesi çok ama çok önemli verilerin kaybolmasına ve taktik resmin elde edilememesine neden olabilecektir [11]. Bu durum kolayca onarılamayacak ve olumlu giden bir harekâtın seyrini olumsuz yönde değiştirebilecektir. Bundan dolayı bu alt yapıların fiziki güvenlik risklerinden söz etmek mümkündür. Muharebe esnasında bu sistemlerin çok iyi bir şekilde korunması kesin sonuçlu bir muharebe için şarttır.

B. *Yazılım ve İşletim Sistemleri Riskleri*

Bulut sistemini oluşturan yazılım ve işletim sistemlerinin güvenilir, minimum açıkları olan ve sürekli geliştirilebilir olması çok önemli bir hususdur [12]. Dünyadaki bütün ordu ya da askerî organizasyonlar kendi yazılım ve işletim sistemlerini üretip kullanmaya doğru bir eğilim içerisindedir. Yazılım ve işletim sistemlerinin yanında kriptoloji hususları da veri aktarımında son zamanlarda oldukça önemli ve popüler bir hale gelmiştir.

C. *Kullanıcı Tarafından Oluşturulan Riskler*

Bilinçsiz kullanıcılar tarafından bulut sistemini zayıflatılacak ya da veri kaybına neden olabilecek siber saldırı girişleri yapılmasına müsaade etmesi çok önemli bir risk kategorisidir.

VI. Risklere Karşı Çözüm Önerileri

1) Sistemlerin Milli bir işletim sistemi üzerine inşa edilmesi,
2) Saldırı tespit sistemlerine yönelik milli yazılım ve donanımlar geliştirilmesi ve milli kriptolama sistemlerinin oluşturulması,
3) Operatörlerin ve kullanıcıların bulut sisteme karşı yapılacak saldırılara karşı farkındalığı artırıcı eğitim ve seminerlerin düzenlenmesi,
4) Yine bu kapsamda kurulacak Eğitim Laboratuvar'ları ile kullanıcı ve operatörlerin bir rotasyon dahilinde simülasyon ortamında eğitim ve durum tespitlerinin yapılması,
5) Kullanıcı ve operatörlerin kullandıkları sistemlerde meydana gelebilecek olağandışı tüm olayları uzman personele rapor etmesi,
6) Bulut Sisteminin, yapılacak saldırılardan korunmasına yönelik olarak aynı ünite içerisinde bilgi sistem güvenlik personeli kadroları tesis edilmesi,

7) Periyodik ya da zamansız olarak bilgi sistem güvenlik personeli tarafından öncelikle sistemlerin ve yazılımların, müteakiben kullanıcıların test edilmesini ve bilinçli ya da bilinçsiz olarak sistemin hatalı kullanılımının engellenebilmesi,
8) Sistem alt yapısını oluşturan donanımın bulunduğu bölgelerde emniyet önlemlerinin arttırılması ve yedekleme mekanizmasının çalışmasının uygun olacağı değerlendirilmektedir.

VII. SONUÇ

Harekât Ortamının çok hızlı gelişmesi ve teknolojinin yardımıyla değişmesi bulut teknolojisini zorunlu kılmıştır. Gelişen bu teknoloji ile birlikte risk ve fırsat dengesini göz önüne alarak bulut sisteminin tüm ordu ve askerî organizasyonlarca kriptoloji ile birlikte kullanılması, kullanıcılara etkinlik, maliyet, güvenlik konularında fayda sağlayacağı değerlendirilmektedir.

VIII. KAYNAKLAR

[1] N. Türkay, Bilişim Zemininde Etnik Milliyetçiliğe Dayalı Terörist Faaliyetler, 1st International Symposium on Digital Forensics and Security (ISDFS'13),283.
[2] S.D. Chi, J.S Park, K.C. Jung, and J.S. Lee, Network security modeling and cyber attack simulation methodology. In Information Security and Privacy, pp. 320-333. Springer Berlin Heidelberg, 2001.
[3] A. Lin, N-C. Chen, Cloud computing as an innovation: Percepetion, attitude, and adoption. International Journal of Information Management, , s.533-540.,2012.
[4] T. Henkoğlu, Ö. Külcü, Bilgi Erişim Platformu Olarak Bulut sistemi: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme Cloud Computing as an Information Access Platform: A Study on Threats and Legal Requirements, Bilgi Dünyası, s. 62-86, 2013.
[5] R.Madhubala, An Illustrative study on Cloud Computing, , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, s. 286-290, 2012.
[6] http://www.hakanuzuner.com/index.php/cloud-computing-risk-and-security-assesment-bulut-bilisim-risk-ve-gvenlik-degerlendirmesi.html erişim zamanı: 11.07.2013 23.26.
[7] L. Schubert, The Future Of Cloud Computing: Opportunities for European Cloud Computing, s. 9-11, 2010.
[8] L. Youseff, M. Butrico, D. Da Silva, Toward a unified ontology of cloud computing. In: Grid Computing Environments Workshop, 2008. GCE'08. IEEE, p. 1-10,2008.
[9] T. Velte, A. Velte, R. Elsenpeter, Cloud computing, a practical approach. McGraw-Hill, Inc., 2009.
[10] D. Catteddu, Cloud Computing: benefits, risks and recommendations for information security. Springer Berlin Heidelberg, 2010.
[11] M. Carroll, A. Van Der We, P. Kotze, Secure cloud computing: Benefits, risks and controls. In: Information Security South Africa (ISSA), 2011. IEEE, p. 1-9, 2011.
[12] K. Goztepe, A Study on OS Selection Using ANP Based Choquet Integral in Terms of Cyber Threats. International Journal of Information Security Science, 2012, 1.2: pp.67-78.

Siber Güvenlik Konusunda Kurumsal Farkındalık ve Entegre Çözüm Altyapısı

İbrahim Dinçer

***Özet*—Siber Güvenlik Saldırılarının çeşit ve miktarının artmasına karşın, kurum ve kuruluşların gündeminde uygun güvenlik politikalarının belirlenmesi, güvenlik yamalarının zamanında yapılması, güvenlik uzmanı istihdamı gibi konular hala önemli bir sorun olarak yer işgal etmektedir. Bu sorunların çözülmesinin sonrasında da yoğun siber saldırılar karşısında daha etkin önlemler alabilmek için bilişim alt yapısının on-line dinlenerek, elde edilen verilerden olayları analiz edip, çözüm yolarının belirleneceği bir otomasyon alt yapısının tesis edilmesine ihtiyaç bulunmaktadır. Bu alt yapının güvene dayalı işbirliği esaslı bir portal yapısı içinde de işbirliği ile desteklenmesi durumunda etkinliği arttırılmış olacaktır.**

***Anahtar Kelimeler*—Siber Güvenlik, Tümleşik Siber Güvenlik İzleme Sistemi, Siber Güvenlik Analisti, Durumsal Farkındalık**

Abstract—Despite increased number of cyber-attacks, security policy issues, security patch management, allocation of security analyst for organizations are still live challenges. Even all those issues have been resolved effective hassling for cyber-attacks is only possible via on line cyber defense analysis infrastructure. Having the result of analysis in hand, the precautions for future attacks will be employed and will be shared with trusted shareholders.

***Index Terms*—Cyber Security, Integrated Cyber Security Monitoring System, Cyber Security Analyst, Situation Awareness**

I. GİRİŞ

SON dönemlerde kurum ve şirketlerin hizmetlerini internet üzerinden sunmalarına bağlı olarak, internet kullanımında da bir artış gözlenmektedir. İnternet kullanımındaki bu artış da; son yıllarda siber saldırıların da sayısı ve niteliklerinde bir atışa sebep olmaktadır. Bu bağlamda siber güvenlik olarak adlandırılan, bilgi uzayı (siber ortam) güvenliği; hem ulusal güvenliğimiz hem de ticaret ve rekabet gücümüz açısından büyük önem taşımaktadır. Bu kadar hassas ve önemli konuda bakanlar kurulu 20 Ekim 2012 tarihinde ve 28447 Resmi Gazetede yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonu " konusunda bir karar alarak yürürlüğe koymuştur. Kurum ve şirketlerin güvenlik konusundaki genel yaklaşımı ise önceden riskleri analiz edip, değerlendiren ve önleyici tedbirler alan bir yapıyı tesis ederek proaktif olmak yerine; bir olay sonrası sorunu çözmeye yönelik reaktif olmaktadır. Çoğu zaman güvenlik konusunda ayrı bir insan kaynağı bile ayrılmaz; Bilgi Teknolojileri (BT) alt yapısının yönetim sorumluluğu verilen kişilerin bu görevi de yerine getirmesi beklenir. Esasen bir kurum ve kuruluşta kesintisiz bilişim hizmeti sunmak, hizmet sunulan kullanıcı sayısı ile doğru orantılı olarak her bir kullanıcıya zaman ayırmak; kullanıcıların sorunları için zaman harcamak demektir. Çoğu kere böyle yoğun bir hizmet için bile yeterli insan kaynağı tahsis edilmezken, üstüne bu kişilere bir de süreklilik isteyen siber güvenlik konusunda bir sorumluluk yüklemek, olası tehlikeleri ve sonuçlarını baştan kabullenmek anlamına gelebilir.

Manuscript received March 01, 2013.
İbrahim Dinçer, BİTES Savunma Havacılık ve Uzay Teknolojileri

II. MEVCUT DURUM

Günümüzde küçük firmalardan büyük holdinglere kadar birçok kurum/kuruluş BT alt yapısını kendi bünyesinde kurar ve işletir. Bu durum, mali olarak her birimin benzer mali yatırımı yapmasının yanında, sistemin kesintisiz çalışması için uzman insan kaynağının temini ve idamesi; sitem yönetim personelinin yeterli uzmanlık eğitimleri ve sayısı, uzman personelin sıkça sirkülasyonu, sistem yönetim ve güvenlik politikalarının belirlenip uygulanması, işletme ve idame maliyetleri gibi zorlukları da beraberinde getirmektedir.

Özellikle güvenlik, birçok kurum/kuruluşta ayrıca bir uzman insan kaynağı istihdam edilmeyen, ihmal edilen ve ancak bir sorun yaşandığında bir süre üzerinde durulan ve olayın sıcaklığı geçtikten sonra da gene eski akışına bırakılan bir konu olarak karşımıza çıkmaktadır. Dünyada günlük 77,000 terabayt verinin [1] dolaştığı yoğun Internet kullanımı dikkate alındığında, her saat binlercesinin geçekleştiği güvenlik ihlallerini tamamen izleme ve kontrol altına almak imkansız hale gelmektedir. Kurumlar ve şirketler her geçen gün artan siber tehlikelerin etkilerini azaltmak üzere, Bilgisayar Acil Müdahale Ekipleri (CERTS) ve Farkındalık Oluşturma (Situation Awareness) arttırıcı Siber Güvenlik Uzmanlığı gibi yapıların oluşturulmasına katkı sağlamaktadır. Siber Güvenlik, bilginin çalınmasını, riske edilmesini veya saldırıya uğramasını önleyici yöntemler olarak tanımlanabilir. Siber strateji kimlik, risk ve vaka yönetimlerini kapsar [2]. Bu görevi yapan kişi veya kişilere de "Siber Güvenlik Savunma Uzmanı" denilmektedir.

Siber Güvenlik Savunma Uzmanları, hızla çeşidi ve miktarı artan siber güvenlik saldırılarına karşı çeşitli yazılım araçları kullanmaktadırlar. Genel olarak güvenlik araçları *Düşük Seviyeli Durum* verisi sağladıklarından, analizlerin

yapılabilmesi için insanın algılamasını kolaylaştırıcı *Yüksek Seviyeli Durum* bilgisine dönüştürmek için çok büyük hacimli bu verilerden ayıklama yapmak gerekir. Bu da Siber Güvenlik Savunma Uzmanının iş yükünün artmasına ve dolayısı ile de performans kaybına sebep olmaktadır. Ayrıca bu tür araçların çoğu da farkındalık yaratma (SA-Situation Awareness) konusunda yeterli değildir. "**Farkındalık Oluşturma**yı" da tanımlamak gerekirse, çevrede olup bitenleri algılama zamanında, anlamlandırma ve yakın geleceğe yansımasını tahmin etme olarak ifade edilebilir.

III. SORUN ALANLARI

a. Güvenlik Politikaları Açısından Kurumsal Farkındalık ve Kurum Kültürü:

Siber Güvenlik araştırma anket sonuçlarına göre [3], 2010 yılında kurum ve kuruluşların %43'ü kendi kullanıcıları tarafından saldırıya uğramışlar ve bu saldırıların da % 46'sı dışarıdan gelenlere göre daha fazla zarar vermişlerdir. Bu saldırılar da kendi içinde gruplandırılırsa; Yetkisiz kurum verisine erişim %63, Kasıtsız olarak hassas veriye erişim %57, Virüs ve Zararlı kodlar %37, Fikri mülkiyet çalma %32 şeklinde olduğu gözlenebilir. Bu durum açıkça göstermektedir ki kurum/şirket içi tehdit tehlikenin yarısını oluşturmaktadır. Dolayısı öncelikle iç tehdit için çözüm üretmek, tehlikenin yarısını bertaraf etmek demektir. Güvenlik politikalarının kurumsal kültür ve kurumsal farkındalık oluşturacak şekilde benimsetilmeden politikanın sağlıklı ve uzun soluklu olması mümkün değildir. Bunun için üst yönetim zamanında bilgilendirip, problem doğru tanımlanmalı, kullanıcılar mutlaka bilgilendirilmeli, önlemler abartılmadan alınmalı, uygulamaya geçmeden önce kullanıcıdan geri besleme almayı müteakip uygulamaya konulmalıdır. Kullanıcıdan hiçbir şey saklanmamalı ve güvenlik politikaları bir ceza uygulamasına dönüştürülmemelidir. Kurum kültürü oluşturabilmek için de güvenlik politikası belirleyici ve uygulayıcıları mutlaka kurum çalışanları ile sıcak temaslarda bulunmak suretiyle kişisel/ kurumsal beklentilerin nabzını tutmaları gerekir.

b. Siber Güvenlik Uzmanlığı

Genel olarak kurum ve kuruluşlarda güvenlik konuları bir olay vuku bulduğunda gündeme gelir, olayın sıcaklığı geçince işler normal seyrinde devam eder. Bazı kurumlar hariç, güvenlik konusunda ayrı bir personel ayrılmaz; bilişim hizmetlerinin sürdürülmesini sağlayan sistem yönetim personeline personele ek sorumluluk olarak verilir. Dolayısı ile Siber Güvenlik Uzmanlığı gibi bir uzmanlık birçok kurum ve kuruluşta henüz benimsenip istihdam alanı haline dönüşmemiştir.

c. Siber Güvenlik Uzmanlık Eğitim İhtiyacı

Siber Güvenlik Uzmanlığı henüz tam bir istihdam alanına dönüşemediği; siber saldırı tekniklerinin her geçen gün artmasına bağlı olarak siber güvenlik tehditleri için çözüm yolları ve bilgi birikimi ile eğitim alt yapısı istenilen seviyeye gelememiştir. Her kurum/kuruluş karşılaştığı sorunları kendi iç dinamikleri ile çözmeye çalıştığı ve sertifika eğitimi tarzındaki bazı eğitimlerin yaygınlaşıp, kurumsal hale gelmediği için de bu sorunların büyük bir kısmı hemen her gün farklı yerlerde yaşanmaya devam edecek gibi görünüyor.

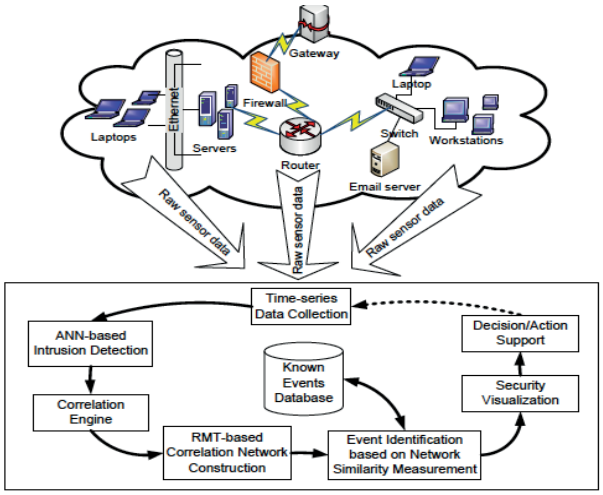
d. Siber Güvenlik Konusunda İşbirliği

Siber Güvenlik saldırısı yaşayan kurum ve kuruluşlar bunları, kendi özeli olarak gördüklerinden ve bir zafiyet algısı içinde başkaları tarafından bilinmesini istemediklerinden, çevre ile paylaşmazlar. Bu da işbirliklerini azaltır ve potansiyel tehditler için bir zafiyet oluşturur. Halbuki en azından benzer iş kollarındaki kurum ve kuruluşlar kontrollü erişimle bir portal yapısı ile bu tür bilgileri ve çıkarılan dersleri paylaşmış olsalar, hem kurumsal kazanımlar artar hem de potansiyel tehlikelere karşı önceden önlem alma imkanı olabilir.

IV. SİBER GÜVENLİKTE ÇÖZÜM ÖNERİLERİ

Siber Güvenlik konusunda, kurum ve kuruluşlarda hizmet sunan bilişim alt yapısı için (yazılım/donanım) güncel güvenlik yamalarının zamanında yapılması, virüs koruma gibi koruma yazılım araçlarının kurulması; kurumsal farkındalığı arttırıcı on-line ve off-line eğitimlerin düzenli olarak verilmesi, kullanıcılarca benimsenmiş uygulanabilir güvenlik politikalarının hayata geçirilmesi gibi önlemler yeterli olmayabilir.

Farkındalık Oluşturma konusunda sorumluluğu olan, Siber Güvenlik Uzmanlarının günlük iş yoğunluğu nedeniyle bu işi bir otomasyon yardımıyla yapmaları halinde sonuçların olumlu olması söz konusudur. Bu durumda ilk akla gelen, kurum ve kuruluşun büyüklüğüne göre kendi bünyesinde veya bulut bilişim hizmeti gibi hizmet alımı söz konusu ise hizmet sağlayıcı seviyesinde bir "Entegre Siber Güvenlik İzleme Sistemi" [4] şeklinde bir yapının kurulması, siber güvenlik analizlerinin hızla yapılmasını sağlayarak, alınacak önlemleri etkinleştirmektir. Muhtemel bir **E**ntegre **S**iber **G**üvenlik **İ**zleme **S**istemini (**ESGİS**) kavramsal tasarımı aşağıdaki şemada gösterilmiştir. Şekildeki ağ yapısı içinde yer alan Sensörler, sunucu, kişisel bilgisayar, ağ cihazı ve Router'lara takılan yazılım/donanım unsurlarıdır ve zaman içinde rastlanan olaylara ait verileri toplarlar. Bu toplanan veriler, *Düşük Seviyeli Durum verisidir* ancak Farkındalık Oluşturmada kritik bir öneme sahiptir. Sensörlerden toplanan bu durum verisi ön uç veri merkezine gönderilir. Burada saldırı tespit edici Yapay Sinir Ağı (ANN- Artificial Neural Network) esasına [5] göre çalışarak bir karar verir. Daha sonra "**Korelasyon Motoru**", *Düşük Seviyeli Durum verisinden,* olay gösterge korelasyon matrisini oluşturur.



Şekil 1. Entegre Siber Güvenlik İzleme Sistemi Kavramsal Tasarımı [4]

Korelasyon matrisi, en son iki olay gösterge çifti arasında ilişki kurar. Daha sonra da RMT (Random Matrix Theory) esasına göre korelasyon ağı oluşturulur. Bir sonraki aşamada ise bilinen olaylar veri tabanı ile benzerlik esasına göre kıyaslama yapılarak olay tipi belirlenir. Bu maksatla SOFM denilen(Self Organizing Featuring Map) Sanal Sinir Ağlarının insan beyninin öğrenme süreçlerini taklit ettiği bir yöntem kullanılmaktadır. SOFM insan beyninde olduğu gibi, eğitildiği ilgili örneklerin ortak özellikleri ile kavrama ve ezberleme yapar.

Burada da iki temel ölçüt uygulanır:

a. Bir olay "Bilinen Olay Veri Tabanındaki"lerden biri ile yüksek benzerliği belirlenebiliyorsa; hassasiyeti gidermek, saldırıyı yok etmek veya etkisini azaltmak için gerekli koruma mekanizması devreye hemen sokulur.
b. Şayet veri tabanında benzer bir olay yoksa "Bilinen Olay Veri Tabanı"na mevcut olay gelecekte dikkate alınmak üzere eklenir.

Bu izleme belli bir zaman aralığında devam ettirilir. Zaman içinde veri tabanında daha çok olay biriktikçe, daha doğru olay tanıma ve teşhis yapılabilir hale gelinecektir. Korelasyon ağındaki benzerlikleri ölçmede kullanılan kıyaslama yöntemlerindeki iyileşme, olayların teşhis edilmesini daha sağlıklı hale getirecektir.
Olaylar teşhis edildikten sonra, "**Görselleştirme Motoru**"na gönderilir ve orada ağ konum bilgisi ile birleştirilerek gösterge panosunda yer alır. Burada maksat, güvenlik ihlallerini görselleştirecek bir yapı oluşturmaktır. Bir ağ bölgesinde oluşan olayların sayısı, cereyan eden olayın şiddetini gösterir.

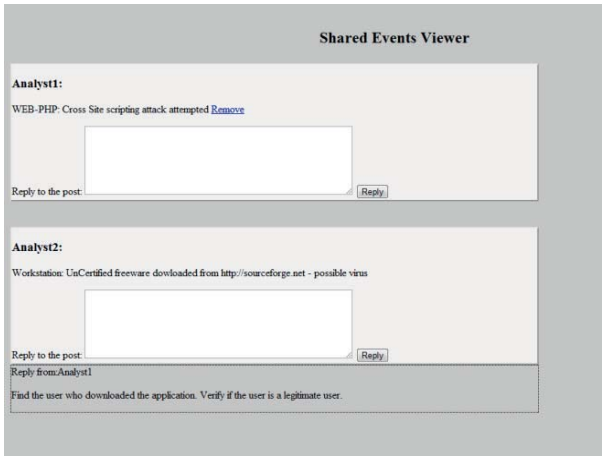
Olay tanıma ve teşhisini kolaylaştırmak için, Bilinen Olay Veri Tabanındaki olay benzeşmesi olmayan durumlarda, belli kurum/kuruluşlar ve servis sağlayıcılar gibi paydaşlar arasında bir portal üzerinden olay paylaşımı yapılarak işbirliğine gidilebilir. Portal üzerinden yapılacak böyle bir işbirliği ile hem Bilinen Olay Veri Tabanı zenginliğini kısa sürede arttırmak hem de saldırı ile ilgili koruma mekanizmalarını bir an önce devreye sokarak saldırıyı yok etmek veya etkisini azaltmak mümkün olabilecektir. Portal için 3 ara yüz [6] oluşturulabilir:

a. Olay Paylaşım Ara Yüzü:
Bu ara yüz vasıtasıyla paydaşlar arasında bilinirliği olmayan olaylar paylaşılır ve olaylarla ilgili yardım almak mümkün olacaktır. Paylaşılan olaylar "Paylaşılmış Olaylar Ara Yüzü" vasıtasıyla diğer paydaşların görmesi sağlanacaktır.



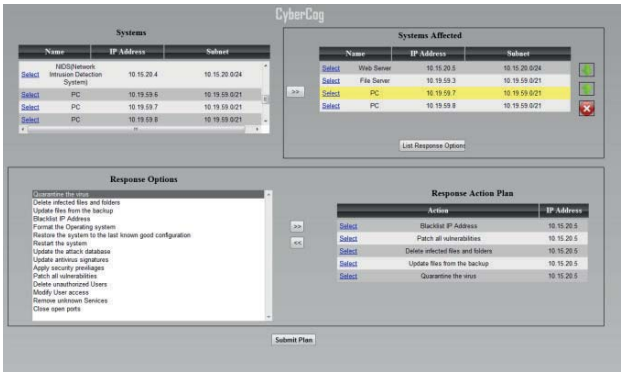
Şekil 2. Olay Paylaşım Ara Yüzü [6]

b. Paylaşılmış Olaylar Ara Yüzü:
Bu akranda diğer paydaşlar tarafından daha önce veri tabanında olmayan paylaşılmış olaylar görüntülenebilecektir. Her bir paydaş kendine göre çözüm önerisi veya hareket tarzını olayı yayımlayan paydaşa gönderebilecektir. Olayın olduğu konumdaki paydaş da bu çözüm önerilerinden bir veya birkaçını seçip uygulayabilecektir.



Şekil 3. Paylaşılmış Olaylar Ara Yüzü [6]

c. Çözüm Seçenekleri Ara Yüzü:
Bu ara yüzde de olayların listesi, etkilenen sistemler ve muhtemel çözüm yolları paydaşlarla paylaşılabilir. Böylece kurumsal olarak daha kısa sürede "Bilinen Olay Veri Tabanı" zenginleşmiş olacaktır.



Şekil 4. Çözüm Seçenekleri Ara Yüzü [6]

V. SONUÇ VE DEĞERLENDİRME

Siber güvenlik kapsamında her kurum/kuruluş büyüklüğüne göre bir veya birkaç Siber Güvenlik Uzmanı istihdam etmelidir. Buna ilave olarak (yazılım/donanım) güncel güvenlik yamalarının zamanında yapılması, virüs koruma gibi koruma yazılım araçlarının kurulması; kurumsal farkındalığı arttırıcı online ve offline eğitimlerin düzenli olarak verilmesi, kullanıcılarca benimsenmiş uygulanabilir güvenlik politikalarının hayata geçirilmesi en başta yapılması gereken ön koşullar arasında yer almaktadır.

Bütün bu ön koşullar yerine getirildikten sonra da sistemi on-line olarak izleyip, sensörlerden alınan düşük seviyeli durum verisi ile olayları analiz eden; "Bilinen Olay Veri Tabanı"na çözüm seçenekleri ile kaydedebilen **E**ntegre **S**iber **G**üvenlik **İ**zleme **S**istemi (ESGİS)'ne ihtiyaç olacaktır. Bu sistemin etkinliğini arttırmak üzere, olay veri tabanındaki olaylarla eşleşmeyen, güvene dayalı işbirliği esasına dayalı olarak, yeni olayların paydaşlar arasında paylaşılıp, süratle analiz edilmesini sağlayacak bir portal yapısı ile desteklenmesi ile hem olaylara süratle müdahale edilebilir hale gelecek hem de ESGİS'in etkinliği arttırılacaktır.

KAYNAKLAR

[1] Cisco. (2011). Cisco Visual Networking Index: Forecast and Methodology: 2010 – 2015. [White Paper]. Retrieved from: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525 /ns537/ns705/n s827/white_paper_c11-481360.pdf
[2] http://www.techopedia.com/definition/24747/cybersecurity
[3] 2011 CyberSecurityWatch Survey How Bad Is the Insider Threat?
[4] Visualization of Security Events Using an Efficient Correlation Technique by Qishi Wu, Denise Ferebee, Yunyue Lin, Dipankar Dasgupta
[5] Yapay Sinir ağları,www.ube.ege.edu.tr
[6] CyberCog A Synthetic Task Environment for Measuring Cyber Situation Awareness by Prashanth Rajivan

Disaster Readiness of Hospital Information Systems: A Case Study from a Turkish University Hospital

Elif Çalık, Hilal Kaya, Abdullah Çavuşoğlu, Selami Akkuş, and Baha Şen

Abstract— **One of the crucial points for information systems is to guarantee security of the produced data and the data production process as well as designing information systems in order to serve humanity. At this point of view, concept of disaster refers to the unplanned loss or interruption of the data that has been achieved. All data generated by hospital information systems are kept in databases, stored in data warehouses and protected in data centers. Causes of disasters are mainly classified into two groups as natural and human-based. These causes that often threatening information technologies are earthquakes, floods, staff's faults, fire, virus attacks etc. According to these reasons, data centers or communication through the data infrastructure elements can be affected in an unplanned way. Therefore, it's possible to lose data completely; even data cannot be delivered or cannot be stored properly. Earthquake-resistant buildings, fire early alarm systems, backup power providers, protection measures against virus attacks, staff training programs, software and hardware supports etc. are considered in the context of preparing hospital information systems in case of disasters.**

In this study, importance of storing data and its daily backups in the centers far from local if possible, supporting infrastructure components, taking hardware and software safety precautions, supporting staff training programs and keeping the hardware and software support up to date is emphasized within the framework of disaster plans in the hospital information systems.

Index Terms— **Disaster plan, Hospital information systems, data recovery systems**

I. Introduction

Effectiveness of disaster management depends on disaster plans that were previously prepared by the coordination of all units, drills are performed at specific intervals and as a result of these drills, improvements on the plans were made. Disaster plans include taking measures, advance preparation, disaster response, recovery, documentation and steps of drills. From the perspective of hospital information systems, to back up the vital data, updating and recovery will be an important contribution to prevent the interruption of availability and business continuity of 365 days-7/24 serving health institutions. To prepare effective disaster recovery plans, identification of the risks, making definitions, creation of the procedures, review of backup plans and performing innovations and arrangements are needed to be made.

Elif Çalık Karabuk University, Health School, elifcalik@karabuk.edu.tr
Hilal Kaya, Ministry of National Education, hilalkaya@meb.gov.tr
Abdullah Çavuşoğlu, Yıldırım Beyazıt University, Faculty of Engineering and Natural Sciences, abdullah.cavusoglu@ybu.edu.tr,
Selami Akkuş, Yıldırım Beyazıt University, School of Medicine, selamiakkus@ybu.edu.tr
Baha Şen, Yıldırım Beyazıt University, Faculty of Engineering and Natural Sciences, bsen@ybu.edu.tr

II. Basic Information

Basic components of the hospital information systems are technical requirements of computer hardware (database servers, application servers, desktop computers, monitors, laptops, tablet computers and their processors, main memory, disk units, input/output processing units, backup units, keyboard, display card, network card etc.), uninterruptible power supply, network switches, security products (firewall, anti-virus gateway, anti-spyware, content filtering, intrusion detection and prevention), data cabling (fiber optic cabling, UTP cabling, cable trays, telephone cabling, rack cabinet etc.). These components may differ in conjunction with the hospital may be large or small. Hospital information system is one of the major units of general hospital disaster plan [1].

Disaster preparedness exercises of the hospital information systems are monitored by a team that is working under control of head of the hospital disaster plan. Disaster preparedness measures which start with buying an information system should continue during the installation and operation processes. In the United States, by the study on disaster recovery preparation for electronic data, importance of being prepared for disasters is emphasized although data recovery is not possible during disaster and disaster is not avoidable [2].

In a study that is related with management of health information during disasters in Australia, need for taking electronic health records in a pre-planned manner during disaster, allocating new data and having a disaster strategy plan about management of health-related records is mentioned [3]. For the design of hospitals' data backup systems, establishment of a center that has automatic and efficient backup system by the support of policy-based management is proposed [4]. In the study that was carried out on 36 hospitals in Australia and examined system failures of hospital information technologies and preparations in case of disasters, hospitals were evaluated in terms of presence of internal disaster plans and installation of data backup infrastructure of hospital information services. According to the results that they obtained about backup systems, 82% of large-scale hospitals, 73% of

medium-scale hospitals and 63% of small-scale hospitals have backup systems [5].

In the study conducted on the necessity of being prepared for disasters and examining data of institutions that use information systems for disaster preparation in USA, it has been concluded that 1429 administrators fullfilled the questionnaire sent by e-mail and backup strategies are significant components of disaster recovery plans [6]. It's emphasized in the study that is conducted in the United States on the issue of data disaster prevention; data backup and data storage options, objectives of data recovery points, data recovery times and determination of the budget have high importance [7].

In another practice made in China, structure of data recovery system in the disaster situation was evaluated. In this study, hospitals that have information systems in international standards are examined and published articles studied on the issue of data recovery during disaster are reviewed. In addition, under the content of hospital information system, disaster recovery of information system is defined and establishment of disaster recovery mode and a three-level structure is proposed for hospital information systems. They define the first level of this structure as establishment of a center that store the data stable; the second level as setting a secure data backup system and finally the third level as creating a quick-response remote disaster recovery system [8]. Also it's one of the most important points that health care institutions should improve data backup plan and maintain the plan up to date with exercises [9]. Ensuring data security and business continuity in any case in order to prevent interruption of hospital information systems with critical data and applications, backups should be kept in an appropriate location.

When analyzing the studies under the guarantee of the state in our country, the circulars issued by the Ministry of Health and the document "Hospital Information Systems Procurement Framework Principles" prepared by the Department of Information Technologies in the Ministry of Health are found. For the purchase process of Hospital Information Systems (HIS) realized by the State Hospitals belongs to Ministry of Health, a framework is drawn for technological infrastructure and other requirements by the document prepared in February 2008 and also this document covers relevant technical recommendations. In the document, issues on information recovery from disasters are given under the title of "extraordinary circumstances". It's determined that an open-ended statement as "In extraordinary circumstances, tenderers should also indicate how they will provide the continuity of the solutions (on issues of fire, flood, earthquake, etc.) they suggested by which technological measures and how the information in the system can be rescued." is used [1].

In order to generate disaster plans for hospital information systems, need to determine the types of internal and external disasters is one of the important steps to ensure data security. Types of internal disasters (computer system failure, power failure, fire, flood, personnel errors, virus attack, unexpected increase in patient population etc.) against the information system in the hospital disaster plan may vary according to the physical layout and architectural features of the hospital [5]. Likewise, in the hospital disaster plan, types of external disasters for information systems (earthquakes, floods, landslides, etc.) may vary depending on the region of the hospital. Taking measures and making expenditures with the disaster plan that was generated according to the type of the disaster (internal or external) will be more meaningful. Disaster recovery plans in the content of the hospital information systems should be practical, complete, consistent and reliable.

Information security is the protection of technological methods and knowledge in the process of knowledge generation and storage. The main objectives of information security can be grouped as confidentiality, integrity, availability, nonrepudiation and monitoring. International standards and guidelines that must be followed as information technology security evaluation criteria [10], information security management system standard [11], and information and communications technology disaster recovery services manual [12] play a guiding role in the development and provision of information security.

In order to maintain the sustainability of health care services aftermath a disaster, determination of critical services and basic materials and developing alternative support plans, in other words business continuity plans, are required. Matters require attention in the business continuity plan are listed below:

- Evaluation of the potential impact on life and property in the analysis of the hospital's unpreparedness for damages,
- Developing procedures for the replacement of equipment and materials, ensuring adequate staffing levels and overcoming the physical and psychological needs of the staff within the organization,
- Labeling of important records, ensuring the computer backups and facilitating the preparation of payrolls,
- Determining the alternatives that will be launched in case of hospital suppliers fail to deliver on their promises,
- Backing-up and caring the generator system regularly and periodically [13].

Interrupts on the functioning of the system room due to disasters will result in the interruption of the availability and business continuity of the health care institution. The system rooms should be resistant to environmental hazards, accidents and deliberate attacks as detailed below:

- Necessary measures should be taken for the protection of environmental factors such as fire, smoke, dust, earthquake, explosion, extreme temperatures, insects, electrical noise, lightning, vibration, humidity, water and the instructions should be established, warning signs must be posted.
- The personnel should be avoided to enter the system room with food and drink.
- Measures should be taken as card and/or fingerprint door control in order to monitor the entry/exit of the personnel and closed circuit camera systems in

order to ensure controlling the ventilation holes, doors and windows if they are closed or not [14].

Data center should be located far from the central system room where data was primarily saved in order to ensure data availability uninterrupted and avoid data loss in unusal circumstances. The establishment of two separate data centers and direct link between these centers should be provided with fiber optic cables. Performing ground survey of data center buildings, testing of load-carrying capacity per square meter, building energy and telecommunications infrastructure in accordance with regulations of structures to be built in disaster areas should be provided. In data centers, measures mentioned below should be taken;

- Taking measures against energy disruptions (battery, generator support),
- Establishing cooling and air-conditioning systems; for unusual circumstances, taking measures such as fresh air fun,
- Taking measures such as indoor and outdoor closed-circuit security camera system, card for entrance and exit of personnel and / or fingerprint-controlled doors, alarm systems, motion-flooding, combined heat and humidity sensors,
- Choosing most effective fire extinguishing system possibilities that don't damage the personnel and the equipment,
- Optimizing telecommunications infrastructure with fiber-optic cables, robust and resistant to abnormal conditions.

To provide the business continuity of 7/24 service units such as hospitals, they are more sensitive about data recovery as well as they need continuous availability. As considering all of the unusual circumstances, disaster recovery scenarios should be created and applied in order to ensure the hospital information systems continue the applications and not to lose the stored data. Also studies should be focused on improvement process. Within the hospital information system and the disaster recovery work, the data backup type of the hospital should be determined. Appropriate method for the hospital should be selected from full, differential and incremential backup methods. Comparison of data backup types is shown in Table 1:

Table 1. Comparison of data backup types **[15]**

Backup Type	Back Recovery Speed	Backup Speed	Storage Space Usage
Full	Highest	Lowest	Highest
Differential	Medium	Medium	Medium
Incremential	Lowest	Highest	Lowest

III. RECOMMENDED MEASURES IN THE HOSPITAL DISASTER PLANS RELATED TO THE INFORMATION SYSTEMS

Unusual situations that may occur in hospital information systems, measures that are related with hospital information systems disaster plan;

- Provision of disaster early notification,
- Provision and updating of the hardware and software-based security measures about the local data center and the distant data center,
- Provision of information security,
- Analysing cost-benefit situation of the measures,
- Establishing the institutional backup policies,
- Personnel planning for the disaster situation,
- Provision of training programs for staff,
- Establishment of distant data centers in different location with the local data center for data backups,
- Backing up critical information on a daily basis,
- Identifying data backup type,
- Selection of data backup software,
- Determining the frequency of data backup,
- Determination of storing period of the backup data,
- Monitoring and solving the analysis of backup errors,
- Ensuring the security of backup data,
- Testing the data backup process,
- Keeping and labeling the data backup records,
- Preparation and updating of the instruction to the return of the backup data,
- Ensuring transfer of the records that are manually saved in the situation of system interrupts to the hospital information system,
- Checking up to date status of the transactions [14,15,16].

IV. METHOD

System room of Yıldırım Beyazıt University Hospital has been examined by the researchers on 03/22/2013 and the checklist prepared in line with the literature is used as data collection tool. Check list of the system room is applied for the research tool by using the methods of face-to-face interview with the staff and the observation technique.

Table2. Check List of the System Room

	Check Digits	**Yes**	**No**	**Explanations**
1	**Physical infrastructure of the system room**			
a.	Environmental Precautions (fire, smoke, dust, earthquake, explosion, extreme temperatures, insects, electrical noise, lightning, vibration, humidity, water, etc.).	✓		-Located on the ground floor of the hospital, -Platform 35 cm raised from the floor, -Suspended ceiling, -One fire extinguisher, -2 air conditioning units, -A window made of pimapen
b.	Instruction and warning signs		✓	-Despite the lack of the instructions and warning signs in the system room, it's declared by the officials that instructions have been prepared and stored in the folders.
2	**Entrance measures of the system room (ventilation holes, windows and control of the doors)**			
a.	Windows and ventilation holes		✓	-Window facing the ventilation cavity does not have iron bars.
b.	Door control of fingerprint and password	✓		-Actively not in use (door is opened manually with the key)
c.	Closed circuit camera system		✓	-Closed circuit camera system is not available at the system room entrance or in the room.
3	**Data Center**			
a.	Local	✓		-One data center in the system room on the ground floor of the hospital
b.	Distant center	✓		-One distant data center on the ground floor of the hospital (Clear information is not available about the location because of the security measures)
4	**System Room: Hardware**			
a.	Measures against power failure (battery, generator support)	✓		-Central generator of the hospital (activated in 1 min. in case of power outage) -2 uninterruptible power supply (UPS) -One electrical control panel of the system room
b.	Cooling and air-conditioning systems	✓		-2 air conditioning units (+18°C)
c.	Telecommunications infrastructure	✓		-Fiber optic cabling
d.	1st cabinet	✓		-Fiber optic cabling providing connection of the blocks of the hospital and the system room
e.	2nd cabinet	✓		-Fiber optic cabling providing the integration of the systems (administrative procedures and the hospital information management system)
f.	3rd cabinet	✓		-2 own servers and processors of the hospital (For administration of financial transactions) -One of these devices each is used for backup procedure.
g.	4th cabinet	✓		-Hospital Information Management System -2 servers and 2 processors belongs to a private company by the service purchasing method (Hospital Information System) -One of these devices each is used for backup procedure.
h.	Control panel of the system room	✓		-3 monitors and 2 processors
5	**System Room: Software**			
	Software	✓		-Because the system room was established with service procurement method, detailed information about the software could not be taken due to data security measures.
6	**Data Backup and Security**			

a.	Institution's backup policy	✓		-Backup policy of the institution is on the direction of backing up all data.
b.	Data backup types: full data backup	✓		-All the data produced through the hospital procedures is backed up.
c.	Data backup frequency	✓		-Data backup is made between 01:00 a.m. and 04:00 a.m. every day and data backup is recorded to DVD once a week (about 20 GB).
d.	Storage of backup data	✓		-DVDs having backed up data are stored in a locked safe in a separate location. -The backup data is labeled.
e.	The storage time of data backed up		✓	-There is no policy of the hospital on the duration of storage.
f.	Data recovery instructions	✓		-Data recovery instructions are present but responsibility is on the contractor firm.
g.	Data backup tests		✓	-An application about the data backup tests is not available.
7	**Strategies in case of disaster**			
a.	Manual registration procedure	✓		-Manual registration procedures and forms are available for each unit of the hospital in case of an unusual interruption of the system, until the backed up data will be in use.
b.	Transfer of the manual records to the hospital information system	✓		-It has been declared that manual entries are made to the hospital information system by the secretaries in each unit.
c.	Cost-benefit analysis of the measures		✓	-There are no cost-benefit analyses in written sources.
d.	Staff scheduling in case of disaster	✓		-Staff planning is made within the framework of the hospital disaster plan.
e.	Staff training		✓	-Except from in-service training routines, on the issue of data security in case of disaster, no specific in-service training has been performed.

V. EVIDENCES

In the sampling assessment study of system room performed at a university hospital, presented data in the Table 2 is achieved.

As analyzing the data in Table 2, it's seen that while a part of the measures are taken, some of them are not provided yet. Measures on the hardware systems and the data backup and security measures in the system room are provided and have no problem. Manual registration procedures are ready for using in case of disaster and these measures are very important for the continuity of the system. On the other side, it's seen that the security measures for the entrance of the system room are not enough; local data center is located inside the system room on the base floor of the hospital and the far data center is also on the same floor and there is no data center outside the hospital. Because software infrastructure is under the responsibility of the contractor's company and the company has the details, information about which programs are used couldn't be reached. Disaster strategies and the measures taken within the plans depend on procurement strategies, because of these cost-benefit analyses are not made by the institution itself. Finally, staff training programs on the disaster issue are not scheduled.

Entrance security measures of the system room and the physical infrastructure are seen in Figure 1 and Figure 2, respectively:



Figure1. Entrance measures of the system room



Figure 2. System room **a)** Placement of cabinets

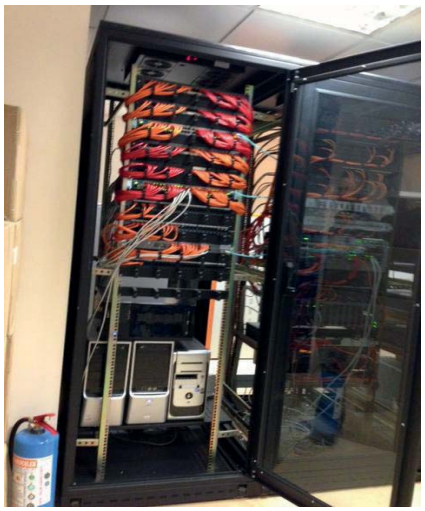


Figure 2. System room **b)** Wiring

VI. CONCLUSIONS AND RECOMMENDATIONS

In our country, there are often the earthquake-based scenarios on disaster planning. Official data about manual sustainable business processes related to the unusual situations that information systems remain out of service and re-integration of these processes with the hospital information systems. As examining a University Hospital as an instance in this study, in accordance with the data obtained, although the hardware and software elements are enough, to reach the adequate level of corporate awareness about disaster readiness is more important than the infrastructure. An in-service training requirement is stipulated on testing and using the hardware and software components of the system room and the data center on the suitable time and situation; and also on the issue of data input and security of personal information in case of disaster due to the level of the authorization of the end-user. Also in connection with strategic planning for disaster readiness of the hospital information systems and hospital disaster plans, need for including this issue in more detail is determined.

As a result of this study, importance of establishing data centers (that data is stored and backed up) far from the system room if possible, supporting infrastructure components, hardware and software security measures, ensuring staff training programs and keeping hardware and software support up to date is emphasized.

REFERENCES

[1] Internet: http://www.saglik.gov.tr/TR/dosya/1-53183/h/ Access Date: 26.05.2013.

[2] Hanauer D., "Disaster Recovery for Electronic Data: Are You Prepared?", J. Med Pract. Manage., 20(2):82-7, 2004.

[3] Smith E., Macdonald R., "Managing Health Information During Disasters", Health Information Management Journal, 35(2):1833-3583, 2006.

[4] Zhou Q., Qian B., "A Scheme for Solution of Hospital's Data Backup System", Sheng Wu Yi Xue Gong Cheng Xue Za Zhi, Jun;21(3):453-5, 2004.

[5] Lee C., Robinson K.M., Wendt K., Williamson D., "The Preparedness of Hospital Health Information Services for System Failures due to Internal Disasters", The Journal of Health Information Management, 38(2):18-25, 2009.

[6] Nelson K., "Examining Factors Associated with IT Disaster Preparedness", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006.

[7] Repasky L., Heard S., "Preventing Data Disasters: Helpful Tips on Data Backup and Storage Options", MGMA Connex, 10(5):46-9, 1, 2010.

[8] Xu J., "Construction of Information Disaster Recovery for Hospitals", Computer and Information Science, 2(4):148-152, 2009.

[9] Halpert A.M., "Complying with the Privacy Rule During a Disaster-Part 1. An Overview of Plan Development, Data Backup and Recovery", JAHIMA, 79(4):60-1, 2008.

[10] ISO/IEC 15408-1:2009, Information Technology -- Security Techniques -- Evaluation Criteria for IT Security -- Part 1: Introduction and General Model.

[11] ISO/IEC 27001:2005, Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements.

[12] ISO/IEC 24762:2008, Information Technology -- Security Techniques -- Guidelines for Information and Communications Technology Disaster Recovery Services.

[13] B.Ü. Kandilli Rasathanesi ve Deprem Araştırma Enstitüsü, Hastaneler İçin Afete Hazırlıklı Olma Kılavuzu, *http://www.koeri.boun.edu.tr/aheb/pdf%20dokumanlar/hastane_2010.pdf* Access Date: 23.11.2012.

[14] TBD/Kamu-BİB/2009-ÇG2, TBD Kamu-BİB, Kamu Bilişim Platformu XI, Felaketten Kurtarma ve Depolama Final Raporu.

[15] Dinçkan A., "Veri Yedekleme Kılavuzu", Ulusal Veri Yedekleme ve Kriptoloji Araştırma Enstitüsü, BGYS-0010, Sürüm 1.00, 2008.

[16] Oğuz B., Gülkesen H.K., Saka O., "Sağlık Bilgi Sistemlerinde Maliyet-Fayda Analizi", Akademik Bilişim, Dumlupınar Üniversitesi, Kütahya, 2007.

Identity Management Based Security Architecture of Cloud Computing on Multi-Agent Systems

Alguliev Rasim, and Abdullayeva Fargana

***Abstract*—In traditional identity management systems user authentication is usually carried out on the basis of management list, previously defined in a system. But with the increasing number of users in such environment as a cloud the management of this list becomes more difficult. For this purpose, in this paper the model supplying the dynamic management of the users' identity federation was introduced. With the implementation of multi-agent systems and the decision making solutions the identity federation dynamization was ensured.**

***Index Terms*—Cloud computing, federated identity management, provider, single sign-on.**

I. Introduction

THE emergence of cloud computing has recently caused a revolutionary coup in the Internet. However, main abstacle to wide range application of this technology is information security.

In the majority of cloud computing security investigations and standardization documents the identity management, risk assessment and trust management are considered as the key issues.

In the guideline published by the ENISA (European Network and Information Security Agency) [1] the establishment of trust relationship in the cloud infrastructure is defined as an important research area.

Also in the recommendations prepared by the NIST (National Institute of Standards and Technology) [2] and the CSA (Cloud Security Alliance) [3] the identity management and trust management are highlighted as an important issue.

In addition, in a number of other documents published by the standardization organizations and research institutions the identity federation is considered as an invaluable mechanism [4,5].

There is a wide rang of research works lead in the area of federated identity management problems in the cloud computing environments.

Among these studies, the approaches devoted to the federation of the clouds [6], as well as the identity management integration approaches [7] draw more attention.

Rasim Alguliev is with the Institute of Information Technology, Azerbaijan National Academy of Sciences, Azerbaijan, Baku (e-mail: director@iit.ab.az).

Fargana Abdullaeva is with the Institute of Information Technology, Azerbaijan National Academy of Sciences, Azerbaijan, Baku (e-mail: farqana@iit.ab.az).

Lack of these approaches is that the identity management architectures are constructed on the basis of pre-existing trust relationships between providers and are based only on the static technologies such as digital certificates, PKI (Public Key Infrastructure).

At present, by series of the world leading organizations there has been developed a number of identity management systems. An example of these systems can be shown as McAfee Cloud Identity Manager, Microsoft Identity & Access, Novell Identity Manager, EmpowerID SSO Manager, Symplified Trust Cloud, OneLogin, IdM4Cloud etc. The functioning of these systems within certain limitations is one of the biggest drawbacks. The integration means of these systems are not constructed sufficiently, therefore they do not allow us to expand the scope of the systems rapidly. In other words, the increasing number of the providers makes the integration functions of the systems unable to integrate.

In this paper we offered a dynamic federated identity management model that allows us to rapidly decrease and increase the scope of the cloud. For this reason, we applied the multi-agent systems. One of the functions of the multi-agent systems is to perform the collection of necessary information about the user, which allows us to make dynamic decisions in the real-time system.

In such uncertain environment as a cloud the assessement of the subject's trust degree is considered to be an important means of realization of the decision-making process.

On the basis of the trust degree calculated by the number of metrics we can construct a dynamic trust relationship between cloud providers. And this trust value may be the best tool in the federation prosess among clouds.

II. IDENTITY MANAGEMENT

Digital identity is the representation of an entity (or group of entities) in the form of one or more elements of information (attributes) that enable the entity to be recognized only within a context [8,9,10].

Identity Management (IdM) is a set of functions and capabilities, such as administration, management and maintenance, discovery, information exchange, policy enforcement and authentication, used to ensure identity information, thus assuring security. An identity management system (IMS) provides tools for managing individual identities in a digital environment [10].

The main functions of an IMS are follows [10]:

- *Provisioning:* the practice of provisioning of identities within an organization addresses the provisioning and deprovisioning of several types of user accounts (e.g. end user, the application administrator, IT administrator, supervisor, developer, etc.).
- *Authentication:* the process of ensuring that the individual is who he claims to be, and is identified through various mechanisms, such as login, password, biometrics, token, etc.
- *Authorization:* a common need in security to provide different access levels (e.g. deny/allow) for different parts or operations within a computing system. This need is called authorization.
- *Federation:* a group of organizations or SPs that establish a circle of trust that allows the sharing of information of user identities to each other.

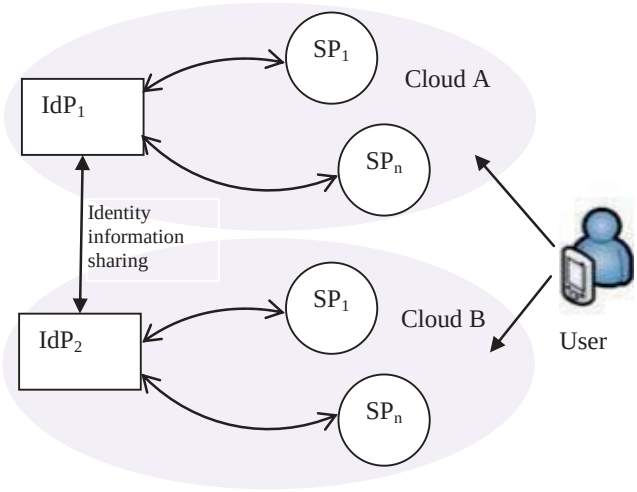


Figure 1. Identity federation prosess

III. SINGLE SIGN ON AND FEDERATED IDENTITY MANAGEMENT

In the Internet users obtain access to the resources belonging to the different service providers by using different accounts. Passwords and user names generated in these accounts are different from each other. For this reason, the vast majority of the network users tries to use the same password in each possible place. This leads to serious security risks. The repeated authentication of the users causes the troubles among them, and beside that it also strongly increases the series of the administrative expenses. Nowdays, the majority of the world global organizations, in order to struggle with passwords, try to use SSO (Single Sign On) technologies as these technologies allow to replace a number of network passwords with a single password.

Single Sign On − is the technology that allows the users to authenticate at a single IdP and gain access to all SPs in a federation with IdPs without providing any additional information.

Identity Federation − is the one of the identity management concepts [11], that share and distribute attributes and identity information across different administrative domains according to certain established policies.

Following three actors are forms the identity federation model (Figure 1):

- *Service Providers (SPs).* Actors which consume user's identity data. They rely on the user authentication made by a third party. SP are also called Relying Parties (RP).
- *Identity Providers (IdPs).* Actors that assert information about a subject. IdP are also called Asserting Parties (AP). IdPs focus on the authentication of the users as well as on the management of identity information, which can be shared with various SP.
- *Users.* Actors which interact (usually via the user agent, e.g. web browser) with SPs. They are the subject of the assertions.

As shown in the figure 1, the share of the identity information between the two providers (IdP1 and IdP2) allows a user to log in only once and gain a seamless access to services and applications offered in different domains.

Identity federation can be accomplished by means of formal Internet standards, such as the OASIS SAML specification, or by using open source technologies and other openly published specifications, like the Liberty Alliance Identity Federation Framework (ID-FF), Shibboleth, OpenID or WS-Federation.

SAML (Security Assertion Markup Language). It is an XML-based protocol which provides the exchange of security returns between the subjects. In this model trust relations between IDPs and SPs are defined in advance. Trust establishment is based on PKI technology [12]. It is founded in 2005 by the organization OASIS.

Shibboleth. It is a system based on SAML technology and is a project of "Internet2 Middleware Initiative" consortium. The world's most widely used federated identity management mechanism, allows users to gain access to the resources whitin and out of organization. In this model the federation process between the providers is conducted on the base of the list containing the names of the providers. This list allows to use common rules between the providers. One of the shortcomings of this model is the complexity of the management of the providers' list.

OpenID. This is a user-centric protocol. This means that the user chooses the IdP for authentication by himself. The trust model is not used there.

Identity Federation Framework (ID-FF). It is the Liberty Alliance organization's project. In this model the federation between the subjects is provided on the basis of the "Circle of Trust" (COT) concept.

WS-Federation. In this model the federation between the subjects is provided on the basis of the WS-Trust (Web service) concept.

The conducted researches show that the organization of the federation prosess is accomplished between the providers on the basis of current technologies known in advance as static trust relationships. This approachs is not

suitable in such dynamic environment as a cloud. For this reason, there arises the necessity to develop a new kind of dynamic federated management model, which takes into account the main characteristics of the cloud.

IV. FEDERATED IDENTITY MANAGEMENT MODEL FOR CLOUD COMPUTING

The model presented in Figure 2 provides the dynamical management of the user identity federation process and is based on authentication and authorization tasks.

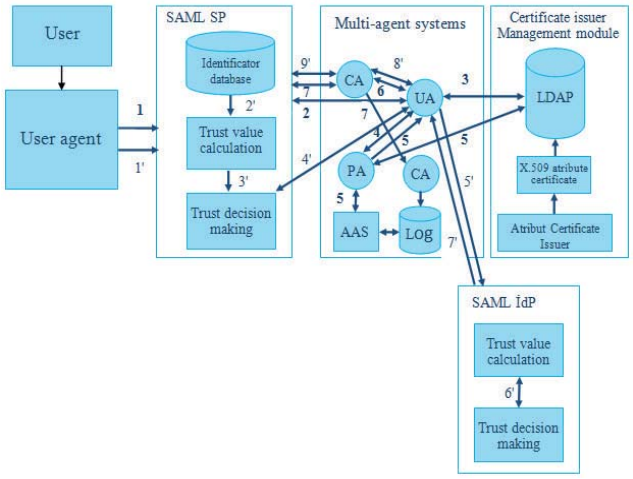


Figure 2. Identity federation dynamic management architecture

Here for providing a user's single access to cloud infrastructure the protocol SAML is used. The users' dynamic federated identity management process is based on PKI technology and the calculation of trust value. The user's access to the cloud infrastructure is provided on the basis of their attribute certificates, also the privileges to each user are given by the role based on the access control mechanisms. Cloud environments are dynamic. Because of that statically the determination of the users' roles only by certificates has lost its actuality. In this case, the dinamic management of roles becomes necessary. The application of multi-agent systems in architecture allows the dinamic determination of users' roles. The content of these roles also contains behavioral characteristics of the users.

For the maintenance of the architecture as a single sisytem the following components are used:

Multi-agent system (MAS). Provides the authentication, authorization and audit operations within the cloud environment. The trust degree of the MAS module is defined by the Public Key İnfrastructure (PKI). MAS contains the following agents:

- *User agent (UA).* Provides the validation of user certificates, the verification of user requests, acquires the authorization of the information from the policy agent (PA), presenting a list of privileges for the user.
- *Collecting agent (TA).* The agent which generates the interface with a log server. Each component of the architecture sends the users' log records to this agent. This agent plays an interface role between the log server and another components of an architecture. All records to the log server are added via this interface.
- *Policy agent (PA).* Combines the roles obtained from the user's attribute certificate with DPL created in AAS and on the basis of this generates a single privilege list (SPL) for the user.
- *Contact agent (CA).* Agent which provides the communication with SP.

Activity Analyzer Server (AAS). Performs two functions: analyses the log files and generates a Dynamic Privileges List (DPL) for the user. This list is called DPL, because it comprises the data associated with the users' behavior.

Log server. Collects log records associated with the activity of each entity in the system.

Certificate Issuer Management Module. It is a component which produces X.509 type attribute certificate. This certificate is physically stored in the catalog LDAP (Lightweight Directory Access Protocol).

Attribute Certificate (AC). The management of the users' privileges is carried out in accordance with the roles included in AC. Attribute Certificate contains version, holder, issuer, signature, serial number, validity period, and attributes. In the attributes field the user's roles can be assigned.

V. INFORMATION FLOW IN FEDERATED IDENTITY MANAGEMENT MODEL

In the given architecture the information flow is implemented in two phases (Figure 2). These phases are based on the circle of trust which may be known or unknown for the providers.

Federated identity management with a known circle of trust

1. User sends a request to SP to authenticate himself by using smart card or tokens (which contains certificates).
2. If the user signed up in the SP identifiers database, the SP sends a request to the MAS module. This module on the basis of this request creates a UA for the user. The purpose of the UA is to manage all user requests. MAS creates UA only for the users which are verified by the SP and this new UA is automatically accepted as a trusted subject.
3. The UA looking for the LDAP directory, confirms the authenticity of the user certificate and verifies it in conformity with systems' predefined security policy.
4. Here the creation of the user privilege list is carried out on the basis of these privileges the users gain the ability to implement any transactions in cloud infrastructure. For this purpose the UA creates a privilege list for a certified user by sending a request to the PA.
5. The PA obtains user static roles contained in certificates by addressing LDAP directory and combines them with a dynamic privilege list greated in AAS and sends them to the UA. The privilege list created in AAS contains information

associated with the user activity, therefore its structure is dynamically changeable.

6. The users' query shipped to the UA is compared with his privilege list. If the user is an authorized user, the UA sends a request to the CA for starting a new session.
7. The CA signs the request and sends it to the SP. The SP accepts the request, checks the signature signed by the CA in the previous stage, determines the trust degree of the request and on the basis of this allows to start the session.

In the above described process on the basis of pre-determined contracts there is a certain trust relationship between the SP and the IdP. Previously registration of the user in IdPs allows him to gain access to the SP infrastructure, without any additional registration process.

Assume that the user does not have the registration in the SP infrastructure, and he wants to use SP recources by authenticating himself in his own IdP. And these providers (SP and IdP) are unknown to each other, in other words the pre-determined static trust relationship is not established between these providers and their circles of trust are different. In this case, it is becoming necessary to ensure the identity management prosess in a federation. This prosess can be described as follows.

The federated identity management with the unknown circle of trust

1. For the using of SP resources the user sends a request to the SP.
2. The *identifier database* discovers that the user is not registered, and then it automaticaly sends the query to the trust value calculation block. On the basis of some metrics (for example, the IdP reputation, data on the service level agreements etc.) it calculates the trust value of the IdP belonging to the user.
3. The trust value is sent to the decision making block, and if the calculated trust value is not greater than that of the threshold adopted by the SP, then the SP evaluates the IdP as a trusted subject.
4. In order to create the federation, decision making block sends a request to the MAS module and on the basis of this request the MAS sets the UA for the user.
5. The UA sends this request to the IdP.
6. For the establishment of the federation process between the providers, their trust value should be known to each other. Therefore, to build a trust relationship and to start the federation prosess with the SP the IdP also calculates the trust value of the SP and sends it to the decision making block.
7. If the calculated trust value is not greater than that of the threshold adopted by the IdP, then the IdP evaluates the SP as a trusted subject and in order to create the federation, it sends a request to the UA block.
8. On the basis of this information the UA sends a request to the CA.
9. The CA signes the request and sends it to the SP. The SP checks the signature of the CA, ensures that the request is trusted and then provides the starting of the new session.

REFERENCES

[1] D. Catteddu, G. Hogben, "Cloud computing: benefits, risks and recommendations for Information security," European Network and Information Security Agency Technical Report, 2009, 125 p.

[2] SP 800-144. "Guidelines on Security and Privacy in Public Cloud Computing," National Institute of Standards and Technology Special Publication, 2011, 70 p.

[3] "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, 2011, 176 p.

[4] "Identity in the Cloud−Use Cases," Organization for the Advancement of Structured Information Standards, 2012, 111 p.

[5] "Moving to the Cloud," Cloud Computing Use Case Discussion Group, 2011, 11 p.

[6] V. Casola, M. Rak, U. Villano, "Identity federation in cloud computing," In Proc. of the IEEE 6th International Conference on Information Assurance and Security, 2010, pp. 253–259.

[7] A. Celesti, F. Tusa, F.M. Villari, A. Puliafito, "Security and cloud computing: Intercloud identity management infrastructure," In proc. of the 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, 2010, pp. 263–265.

[8] ITU-T X.1250, "Baseline capabilities for enhanced global identity management trust and interoperability," Draft New Recommendation ITU-T (X.idmreq), February 2009.

[9] D.W. Chadwick, "Federated identity management," Springer Verlag: Berlin, Heidelberg, 2009, pp. 96–120.

[10] M.A. Leandro, T.J. Nascimento, D.R. Santos, C.M. Westphall, C.B. Westphall, "Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth," The Eleventh International Conference on Networks (ICN), 2012, pp. 88-93.

[11] R.M. Əliquliyev, F.C. Abdullayeva, "Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi," İnformasiya Texnologiyaları Problemləri, 2013, to be published.

[12] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL)," RFC 5280, 2008, 151 pp.

Zararlı Yazılım Tespit, Takip ve Analiz Yöntemleri Geliştirilmesi

Mustafa ALKAN, Burak ÇİFTER ve Elif Tuğba KILIÇ

***Özet*—Gelişen teknolojiyle birlikte siber saldırıların artması, hem kamu kurumlarının hem de özel kuruluşların daha güvenli sistemler kullanmasını zorunlu hale getirmektedir. Bu çalışmada sistemleri tehdit eden zararlı yazılımların tespit edilmesi, takip edilmesi ve müdahale edilmesi yöntemi geliştirilmeye çalışılmıştır. WEB sitelerinin takibini anlık yapan ve tamamen merkezi bulut tabanlı (Software as a Service-SaaS) olarak çalışan ve WEB tabanlı olarak platform bağımsız kullanılıp yönetilebilen bir yazılım sistemi geliştirilmeye çalışılmıştır. WEB sitelerini, sistemlerin DNS altyapılarını, SSL sertifikalarını, ağ erişim adımlarını, hem içeriğini hem de yapısal durumunu sürekli takip ederek "hack" edilip edilmediğini, güvenlik zafiyeti barındırıp barındırmadığını, özellikle zararlı yazılım yayıp yapmadığını analiz edecek olan bu uygulama ile zararlı yazılımlar tespit edilerek anlık (real time) bilgi ve alarm sağlayacaktır. Bu uygulama ile sisteme kullanıcı tarafından girilen WEB sitelerini, yine kullanıcının belirlediği aralıklarla kontrolü gerçekleştirip güvenlik problemlerini tespit ederek ve bununla ilgili yetkili yöneticileri uyararak acilen müdahale edilmesine destek vermektedir.**

Anahtar Kelimeler— Bilgi güvenliği, siber güvenlik, tehdit analizi, zararlı yazılım

***Abstract*—The increase of cyber attacks along with the developing technology makes it imperative to utilize more secure systems for both public and private organizations. In this study, the method of detection, monitoring, and intervention of the malicious software that threatens the systems has been tried to be developed. A software system implementing instantly the follow-up of WEB sites, running completely as centralized cloud-based (Software as a Service-SaaS), and able to use and manage the platform based on WEB has been tried to be developed. With this application that will analyze WEB sites, DNS infrastructure of the systems, SSL certificates, network access steps, whether it is hacked by continuously monitoring both its content and structural condition, whether it includes security weakness, and especially whether it spreads malicious software, real time information and alarm will be provided by detecting the malicious software. Moreover, with this application, by performing the control of the WEB sites entered by the user within the user-defined intervals, it identifies the security problems and gives support to intervene urgently by alerting the authorized managers.**

Index Terms— Information security, cyber security, threat analysis, malicious software

I. GİRİŞ

Türkiye'de de, dünyada olduğu gibi siber saldırılar ve siber güvenlik hassasiyeti son yıllarda artmıştır. Bunun sebebi ise artan iletişim kaynakları ve gelişen internet servisleri sayesinde hedef olmaya müsait sistemlerin atmasıdır.

Saldırıların dünya ve Türkiye gündemlerine hemen hemen eş zamanda girmeleri ise artık saldırıların ülke ve sınır tanımaması ve dünya gündeminde olan herhangi bir organize saldırının aynı anda Türkiye'yi de etkilemesinden kaynaklanmaktadır. Yani siber güvenlik gündemimiz sadece bizim tarafımızdan oluşturulmamakta, dünyadaki gelişmelerle aynı doğrultuda ilerlemektedir.

Bu durum çerçevesinde hem kamunun hem de özel kuruluşların bilgi güvenliği çalışmaları yapmaları kaçınılmazdır. Bilgi güvenliği tesis ve sistemlerinin hemen hepsi yurtdışı menşeilidir. Türkiye'de siber güvenlik alanında her alana uyarlanabilecek bir ürünün geliştirilmesi, ülke ekonomisi açısından yurtdışına yönelebilecek kaynağın yurtiçinde kalmasını sağlayacaktır.

Bununla birlikte, güvenlik yatırımlarının temel gerekçesi, tehdit durumunun ölçümlenmesidir. Türkiye'de hali hazırda güvenlik ihlal durumlarının kayıtlarının tutulduğu ve yıllık olarak yayınlanabilecek bir veri havuzu bulunmamaktadır. Bu uygulama sayesinde tüm kamu kurumlarının WEB altyapıları takip edilerek otomatik olarak hack edilen sistemler kayıt altına alınacak böylelikle resmi olarak her yıl yaşanan güvenlik ihlalleri ile ilgili rapor üretilebilecektir.

Söz konusu uygulama aynı zamanda kullanan kurumlara da ekonomik fayda sağlayacaktır. Özellikle veri çalınması veya web sitesinin hack edilmesi neticesinde yaşadıkları itibar kaybı, kurumlara doğrudan ve dolaylı ekonomik kayıp olarak dönmektedir. Bu sayede kurumların hem zafiyetleri proaktif olarak saldırganlardan önce tespit edilerek hem de saldırı durumunda yetkililere derhal haber verip müdahale etmeleri sağlanarak veri sızıntısı ve prestij kaybının önlenmesi sağlanacaktır. Aynı zamanda sosyal olarak uygulamayı kullanan özellikle merkezi takip yapan kurumların diğer kurumlardaki bilgi güvenliği ekipleri ile koordineli

Mustafa ALKAN Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği Bölümünde Bölüm Başkanı olarak görev yapmaktadır (Telefon: 0534 438 383 8, e-mail: malkan@gazi.edu.tr).

Burak ÇİFTER , BOA Bilgi Teknolojileri ve Güvenliği şirketinde güvenlik alaninda projelerde fiilen görev yapmaya devam etmektedir (Telefon: 0532 790 13 94, e-mail: burak@burakcifter.com).

Elif Tuğba KILIÇ Gazi Üniversitesi Fen Bilimleri Enstitüsü Kazaların Çevresel ve Teknik Araştırılması Bölümünde Yüksek Lisans eğitimine devam etmektedir (Telefon: 0537 931 90 66, e-mail: elif_tugba_kilic@hotmail.com).

çalışmasını sağlayacak bu sayede hem sosyal hem de organizasyonel anlamda fayda sağlayacaktır.

Ayrıca kullanıcıların da takip edilen sitelerde (özellikle e-devlet uygulamalarında) kendini daha güvende hissetmesini sağlayacak ve internet üzerinden hizmet kullanımına güvenlik kaygısı sebebiyle yanaşmayan insanların da bu mecraya taşınmasına yardımcı olacaktır.

II. SİBER GÜVENLİK

Siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür[1].

Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır[2].

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefleri erişilebilirlik, bütünlük (aslına uygunluk ve inkâr edilemezliği de kapsar) ve gizliliktir. Siber güvenliğin temel hedefleri, 10. Ulaştırma şurasında; erişilebilirlik, bütünlük ve gizlilik olarak ifade edilmiştir [3].

Bilgi güvenliği, bilginin ve bilgi teknolojileri altyapısının bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlemektir. Buna uygun tanımı: elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için duruma uygun güvenlik politikasının belirlenmesi ve uygulanması gereklidir.

A. Siber Güvenlik Politikaları

- Faaliyetlerin sorgulanması,
- Erişimlerin izlenmesi,
- Değişikliklerin kayıtlarının tutulup değerlendirilmesi,

Silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir.

Bilgisayar teknolojilerinde yer alan bilgisayar güvenliğinin amacı ise; kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır[4].

Güvenlik açıkları, gelişen teknolojiyle birlikte tüm firmalar tarafından çok ciddi para, zaman, kritik bilgi ve itibar gibi maddi ve manevi kayıplara sebep olmaktadır. Firmalar bilgi ve sistem güvenliği için astronomik rakamlar ödemekle beraber, buna rağmen hala ciddi kayıplar yaşamaktadır.

Bu çalışmada kullanılan yöntem ile WEB sitelerinin ve hizmet vermesi için kullandığı DNS sistemleri gibi bileşenlerin takibinin anlık yapılması sağlanarak, sistemlerin hack edilip edilmediğini, zararlı yazılım (malware) yayılıp yayılmadığını, güvenlik açıklarının olup olmadığı, sisteme DDOS (Distributed denial of service attack) saldırılarının olup olmadığının, SSL sertifikalarının doğruluğu ve güvenilirliğinin kontrol edilerek anlık (real time) bilgi sağlayacak siber saldırı takip ve uyarı sistemi geliştirililmiştir.

III. SİBER SALDIRILAR

Güvenlik açıkları, gelişen teknolojiyle birlikte tüm kamu kurumları ve özel şirketler tarafından çok ciddi para, zaman, kritik bilgi ve itibar gibi maddi ve manevi kayıplara sebep olmaktadır. Firmalar bilgi ve sistem güvenliği için astronomik rakamlar ödemekle beraber, buna rağmen hala ciddi kayıplar yaşamaktadır. Bunlara örnek olarak ünlü aktivist hacker gruplarından Anonymous, LuLzSec, Syrian Electronic Army, RedHack'in, devlet kurumları başta olmak üzere, birçok ülke, kurum ve firmalara karşı yaptığı saldırıları gösterebiliriz. Dünyaca ünlü elektronik devi SONY, uğradığı saldırı sonucu 600.000 USD zarar ettiğini ve bunun yanında müşterilerinin kredi kartı bilgilerinin çalındığını açıklamıştır. Saldırı sonrasında hacker grubu ise: "Çok basit bir yöntemle SONY 'nin tüm bilgilerine ulaştık. Bu kadar kolay ulaşılabilen bir şirkete neden güveniyorsunuz?" şeklinde bir açıklamada bulunmuştur[5].

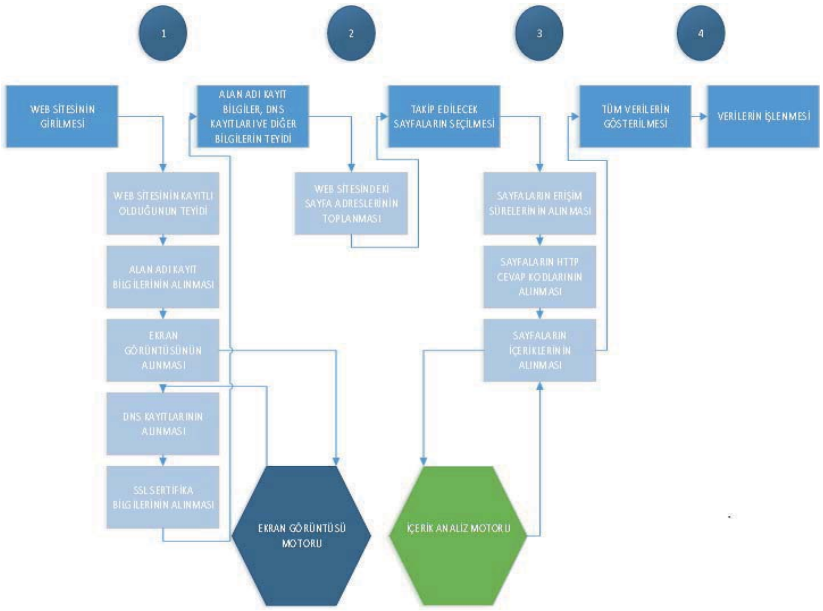
Ülkemizdeki WEB sistemlerinin birçoğunda tehdit durumunu takip edecek bir sistem olmamakla birlikte kritik altyapıların güncel takip edilememesinden kaynaklı siber saldırıların takibi yapılamamaktadır. Birçok kamu kurum ve kuruluşların "gov.tr" uzantılı siteleri son yıllarda hack olayları ile sıkça gündemde yer edinmiştir bunun en önemli sebebi sistemlerin siber saldırılara karşı zayıf olmasının yanı sıra anlık tehdit takibinin yapılmamasından kaynaklanmaktadır.

Bunun yanı sıra, ülkemizde en azından devlet sitelerini takip ederek karşılaştıkları hack saldırılarına ait kayıtları tutan bir sistem bulunmamakta, bu sebeple şu anda dahi kaç saldırı gerçekleştiği veya kaç kamu sitesinin hack edildiği, nasıl ve hangi yollarla saldırıların gerçekleştirildiği bilinememektedir.

Gelişen teknolojiyle birlikte siber saldırıların artması, kurumların ve şahısların daha güvenli sistemler kullanmasını zorunlu hale getirmektedir. e-devlet uygulamaları devlet politikası olarak desteklenmektedir ve devlet web sitelerinin güvenliği, güvenliğinin takibi, halkın bu sistemleri kullanmaya teşvik edilmesi için de oldukça önemlidir.

Bu gerekçeyle yola çıkılarak yapılan bu çalışma sayesinde;

- Öncelikle kritik altyapıya sahip kurumların siber güvenlik tehditlerine karşı uyarı/alarm alabilmeleri sağlanacak,
- Kritik altyapılara yapılacak olası siber saldırıların tespitinin yapılarak takip edilmesi,
- Web sayfaları üzerinden yayılan zararlı yazılım (Malware) ve gelişmiş kalıcı tehditler (APT – Advanced Persistent Threat) tespit edilecek ve yayılmasına izin verilmeden önlem alınması,
- Dijital sosyal medya ortamlarında ve saldırganların



Şekil. 1. Takip edilecek sistem girişi süreç akışı

kullandıkları paylaşım platformlarında kurumlarla ilgili bir ifşa veya ön hazırlık durumunun hemen tespit edilmesi

- Tespiti yapılan siber saldırılarla ilgili olarak yetkili birimlere alarm vermek ve gerekli ilk önlemlerin alınması sağlanabilecektir.

Bu çalışma ile Yazılım sisteminin software as a service (servis olarak yazılım hizmeti) amaçlı sistem tasarımı gerçekleştirilerek, sistemin kullanıma hazır hale getirilmesi ile internet servis sağlayıcılarının gereksinimleri karşılanabilecektir. Ayrıca devlet kurumlarının siber saldırılara karşı korunması hızlı, güvenilir ve doğru şekilde gerçekleştirilmiş olacaktır.

IV. WEB SİTESİNİN GİRİLMESİ VE İLK VERİLERİN TOPLANMASI

- WEB sitesi yöneticisi WEB alan adını websitesi.com sisteme kayıt eder.
- Alan adının kayıtlı olduğunun teyidi yapılır
- Alan adına ait kayıt bilgileri (WHOIS) sorgulanıp ilgili alanlar normalize/standardize edilir.
- WEB sitesinin son kullanıcı tarafından görüntülendiği şekilde ekran görüntüsü alınması için ekran görüntüsü alma motoru çalıştırılır.
- Alan adına ait DNS kayıtları (A, CNAME, PTR, MX, PTR, vb) alınır.
- WEB sitesinin eğer SSL sertifikası varsa bu sertifikaya ve sertifika sağlayıcısına ait bilgiler alınır.
- Bilgiler yönetici tarafından doğrulanmak üzere gösteriliyor ve doğruluğunun onaylanması istenir.

A. Sayfa Adresleri (URL) Ayıklama ve Adres Seçimi

WEB sitesi üzerindeki sayfaların adresleri (URL) link ayıklama motoru tarafından alınır; elde edilen URL'ler üzerinde takip edilmesi istenen URL'ler için ekleme ve çıkartma yapılmak üzere yöneticiye gösteriliyor ve onayı talep edilir.

B. İçerik ve Eğitim Verilerinin Oluşturulması

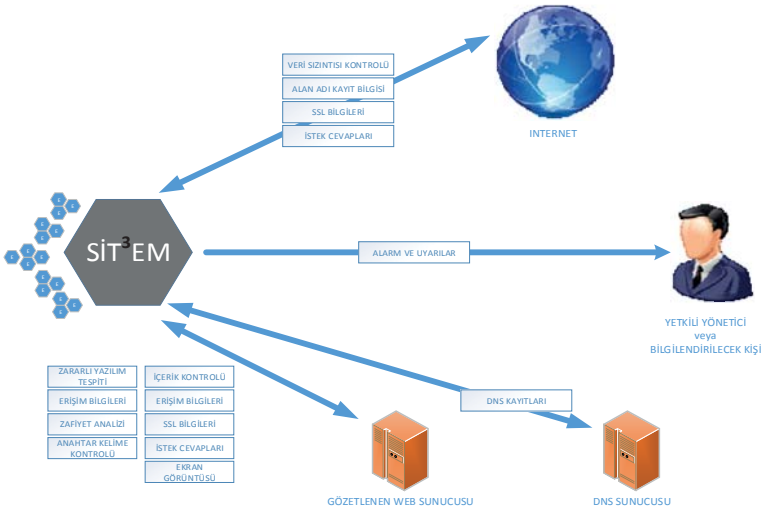
- Onay verilen sayfa adresleri (URL), sayfa motoruna iletilir
- URL'lere erişim süreleri alınır
- URL'lerin cevaben döndüğü HTTP hata kodları alınır (HTTP 10x, 20x, 30x, 40x, 50x gibi)
- URL'lerin içerikleri alınır ve içerik analiz motoruna gönderilir. İçerik analiz motoru sayfa içerikleri ile ilgili veri madenciliği (data mining), veri analizi (data analysis) ve metin madenciliği (text mining) yaparak içerik ile ilgili standart değerleri oluşturulur.

C. Onay ve Kayıt

Tüm veriler yönetici tarafından doğrulanmak üzere gösterilir. Onay verildiğinde veriler sisteme işleniyor ve sistem yeni eklenen siteyi analiz etmeye başlar.

Uygulama düzenli olarak verilen aralıklarla takip edilmesi istenen siteye normal bir ziyaretçi olarak girmektedir. Her girişinde ve siteyi normal bir ziyaretçi gibi gezmesi esnasında elde ettiği verileri analiz edip yorumlar ve daha önceki verileri ile karşılaştırır. Bu veriler ile ilişkili çeşitli diğer verileri ise internet üzerindeki veri kaynaklarından (DNS sunucuları, WHOIS kayıt sorgulama sunucuları gibi) kontrol eder.

İzlenen sitenin erişim bilgileri, sayfaların erişim süreleri ve erişilebilirlikleri, sayfaların içeriğindeki kritik HTML kodları



Şekil. 2. Genel çalışma düzeni

istenmeyen anahtar kelimeler ve sistemin hack edildiğine işaret eden imzalar, alan adı ile ilgili DNS sunucusundaki kayıt değişiklikleri ve alan adı kayıt (WHOIS) bilgilerinin değişiklikleri, SSL sertifikası verileri uygulama tarafından incelenir. Sayfalarda ve sitedeki dosyalarda zararlı yazılım taraması yapılır. Uygulama aynı zamanda WEB sitesinin ekran görüntüsünü alır ve ekran görüntüsü üzerinde resim işleme yaparak sitenin görsel değişiklik oranını hesaplar, eşik değerlerin üzerinde olup olmadığını kontrol eder. Bu uygulama sayesinde web sitesi üzerinde normalin üzerinde bir değişiklik varsa ve bunu anahtar kelimeleri kontrol ederek yakalayamasa dâhi, görsel değişiklik analizi tabanlı anormallik kontrolü ile sitenin hack edilip edilmediğini tespit ederek uyarı verir.

Sayfayla ilgili elde ettiği içeriği analiz ederek, içerikten XHTML iskeletini ve okunabilir içeriği (Human Readable) ayıklar, ayıkladığı XHTML içerisinde yapısal değişiklik olup olmadığını kontrol eder. Ayrıca XHTML içerisinde tehlikeli kabul edilen XHTML etiketlerini takip eder ve sitede tehlikeli kabul edilen XHTML etiketleri eklenmiş ise bunları bildirir.

Bu çalışmada WEB sayfasını ve WEB sitesi içerisindeki dosyaları zararlı yazılım analizi motorundan geçirir, böylelikle WEB sayfaları üzerinden yayılan zararlı yazılımlar ile APT ataklarının gerçekleştirilmesini engeller.

WEB sayfasının kullanıcıya gönderdiği SSL sertifikasını kontrol eden uygulama, bu sertifikanın doğruluğunu ve tutarlılığını kontrol ederek, sertifikanın gerçekten doğru sistem tarafından mı üretildiğini yoksa SSL araya-girme saldırısı mı gerçekleştirilmeye çalışıldığını tespit eder ve uyarı verir.

Bu çalışma çoklu dil desteği ve rol tabanlı kullanıcı erişimi (RBAC – Role Based Access Control) ile tasarlanmıştır. Kullanıcılar yönetici seviyesinde (Administrator) veya sadece takip edecek operatör seviyesinde (View Only Operator) yetkilendirilebilmektedir[6].

Uygulama sistem üzerinde aktif olarak gerçekleştirdiği bu analizlerin yanı sıra, takip ettiği web sitelerinden saldırganlar tarafından yaygın olarak kullanılan platformlarda bahsedilip bahsedilmediğini kontrol eder. Bu sayede, organize bir saldırı için birbiriyle iletişim kurmaya çalışan saldırganların iletişimleri yakalanarak, siber saldırıyla ilgili erken uyarı ve tehdit istihbaratı gerçekleştirilir. Aynı zamanda internet üzerinde WEB sitesi ile ilgili veri sızıntısı/ifşası bulunuyorsa bununla ilgili yöneticiye alarm verir.



Şekil. 3. Birbirini tamamlayan motorlar

Çalışma kapsamında geliştirilen, sisteminin içeriği Web sitelerinin takibini anlık yapan ve tamamen WEB tabanlı (SaaS) olarak çalışan bir yazılımdır. WEB sitelerini sürekli takip ederek hack edilip edilmediğini, güvenlik açıklarını tespit eder. Takip edilen site üzerinden herhangi bir zararlı yazılım (malware) yayılıp yayılmadığını kontrol ederek anlık (real time) bilgi sağlar ve alarm üretir.

Uygulama, sisteme kullanıcı tarafından girilen WEB sitelerini yine kullanıcının belirlediği aralıklarla sürekli ziyaret ederek güvenlik problemlerini tespit eder ve bununla ilgili yöneticileri uyarır.

Uygulamanın ana modülleri aşağıda açıklanmıştır:

1. Erişim Kontrol Modülü

Günümüzde en çok karşılaşılan problemlerden biri sistemlerin servislerini durdurmaya veya aksatmaya yönelik saldırılardır. Servis aksatma (Denial of Service) saldırıları olarak isimlendirilen bu saldırıların mümkün olabilecek en kısa sürede bildirilmesi ve önlenmesi önemlidir. Bu çalışmada, bu tür atakların bildirilmesi ve önlenebilmesi için bir takım önlemler geliştirilmiştir. Periyodik aralıklarla alan adı cevap süreleri ve URL kontrolleri gibi unsurlara bakarak sunucuya yapılacak olan herhangi bir atağın önceden belirlenmesi sağlanmıştır.

2. Anahtar Kelime Kontrol Modülü

WEB uygulamaları veya WEB siteleri saldırganlar tarafından ele geçirildikten sonra içerikleri değiştirilmektedir. Bu değişiklikler genelde sitenin ele geçirildiğine dair ibarelerden oluşmaktadır. Bu modül sayesinde bu tip içerik değişikliklerine karşı web sitelerini periyodik aralıklarla takip ederek olası değişiklikler tesbit edilebilmektedir.

Bu takip süreçlerini gerçekleştirmek ve saldırı tespiti yapabilmek için sadece içerik değişikliklerine değil, URL tabanlı kontroller uygulayarak farklı vektörlerde değişiklik tespiti yapabilmektir.

3. Zararlı HTML Kod Tespit Modülü

Saldırganlar, gelişmiş kalıcı saldırılar olarak adlandırılan organize ataklar gerçekleştirdiklerinde ele geçirilen web siteleri üzerinden zararlı yazılım dağıtımı yapmaktadır. Bu modül saldırganlar tarafından ele geçirilen web siteleri üzerinden herhangi bir zararlı yazılım dağıtımı yapılıp yapılmadığını kontrol etmektedir.

Ayrıca bu tip saldırıların tespit edilebilmesi için site içerisinde bulunan ve saldırganlar tarafından eklenmiş olabilecek iframe, javascript, embedded gibi içerik kodlarına bakarak bildirim yapabilmektedir[7].

4. İçerik Değişiklik Modülü

Bu modül ile takibini gerçekleştirmek istediğiniz WEB uygulamasını veya WEB sitesini, uygulama veri tabanına ekledikten sonra eklediğiniz sitenin anlık görüntüsü veri tabanına kaydedilir. Bu işlemden sonra içerik değişimleri statik ve dinamik kodlar karşılaştırılarak bildirim sağlanır.

Ayrıca bu karşılaştırılmanın yapılabilmesi için gerekli periyodik aralıkların belirlenebilmesi noktasında esneklik sağlamaktadır. Statik ve dinamik karşılaştırma sonucunda şüpheli durumları tespit ederek doğruluk oranıyla birlikte bildirim gerçekleştirilmektedir.

5. Yapısal Değişiklik Kontrol Modülü

Bu modülde statik içeriğe ait değişimlerin belirlenebilmesi için birden fazla yöntem kullanmaktadır. İçerik Değişim kontrollerine benzer olarak sitenin sisteme bildiriminden sonra anlık XHTML içeriği alınarak statik içerik içerisinde dinamik analizler gerçekleştirilmektedir. Site içerisinde kullanılan, değiştirilen veya eklenen HTML etiketlerinin dahi belirlenerek kullanım oranlarının çıkarılması ve şüpheli durumların bildirilmesi sağlanmaktadır.

6. SQL Sızıntısı Zafiyeti Kontrol Modülü

Günümüzde web sitesi saldırılarının büyük bir bölümü SQL Enjeksiyon sayesinde gerçekleştirilmektedir.[8] WEB sitelerinin dinamik, değişken ve modüler yapılarından dolayı güvenlik kontrollerinin sürekli olarak gerçekleştirilmesi oldukça zordur.

Bu modül web sitelerini periyodik aralıklarla tarayarak SQL Enjeksiyon kaynaklı kritik güvenlik açıklarını tespit etmektedir. Aynı zamanda güvenlik açıklarını kritiklik düzeylerine göre sınıflandırabilmektedir.

Bunun yanında, periyodik aralıklarla sistemi taramasının yanı sıra güvenlik açıklarına dair detaylı rapor sunabilmekte ve sunduğu rapor içerisinde tespit edilen her güvenlik açığına dair detaylı bilgi barındırmaktadır.

7. WEB Ekran Görüntüsü Analiz Modülü

Bu modül veri tabanına herhangi bir WEB sitesi dâhil edildikten sonra alan adı bazlı ekran görüntülerini periyodik aralıklarla almaya başlayacaktır. Uygulama periyodik olarak aldığı ekran görüntülerini piksel tabanlı karşılaştırarak değişim oranlarına göre bildirim yapacaktır.[9]

8. DNS Kayıt Kontrol Modülü

Uygulama ilk kurulum esnasında WEB sitesine ait DNS kayıtlarını veri tabanı üzerinde saklamakta. Olası DNS değişikliklerine veya şüpheli işlemlere karşı periyodik olarak tarama yapmaktadır. Bunun yanında tüm DNS kayıtlarını tek tek inceleyerek değişiklikleri tespit etmekte, değişikliğin yapıldığı andan itibaren bildirim sağlayarak sitenin istenmeyen durumlarda servis dışı kalmasını önlemektedir[10].

9. Alan Adı Kayıtları Kontrol Modülü

Bu modül sitelere ait whois bilgilerinde saldırılardan kaynaklı olabilecek değişiklikleri tespit ederek bildirmeyi amaçlamaktadır. Hizmet alınan firmaya veya sunucuya ait isim sunucuları, kayıtlı elektronik posta adresleri gibi birçok farklı unsura bakarak sitenin risk altında olup olmadığını belirlemektedir. Ayrıca olası atakları ve belirlediği değişiklikleri doğruluk oranlarına göre bildirerek, olası bir saldırıdan kaynaklı oluşabilecek hasarı en az kayıpla sonlandırılmasına ve önlem alınmasına yardımcı olmaktadır.

10. Ağ Yolu Kontrol Modülü

Bu modül web sitesine erişim esnasında kullanıcının hangi olağan yollardan geçtiğini öğrenerek bunun dışında erişimde geçilen yolları tespit etmekte. Trafiğin saldırgan tarafından yönlendirildiği durumlarda siteye erişim engellenebilmekte veya değiştirilebilmektedir. Bu gibi durumlara karşı, uygulama bu iletişim yollarını sürekli takip ederek, gerçekleşen değişiklikleri anında bildirmektedir. Düzenlenen saldırılara karşı anında aksiyon alınabilmesi için uygulama kullanıcılarını bildirim yapılmaktadır

11. SSL Sertifikası Kontrol Modülü

Uygulama kontrol ettiği WEB siteleri üzerinde SSL Sertifikalarının doğruluğunu teyit etmek için bir takım kontroller gerçekleştirmektedir. SSL sertifikasının doğrulanmış bitiş tarihi, seri numarası ve imza algoritması gibi kontroller gerçekleştirilmesi oldukça önemlidir. Bu modülle doğrulama işlemlerini gerçekleştirememesi durumunda kontrol paneli üzerinden anında bildirim gerçekleştilmesi sağlanmaktadır.

12. Zararlı Yazılım Kontrol Modülü

Bu modül sayesinde gelişmiş kalıcı tehditler adı verilen organize ve ısrarlı düzenlenen saldırılara karşı güvenlik çözümleri geliştirilmiştir. Zararlı yazılım analizi ve kontrolü bu süreçlerden sadece bir tanesidir. Bu modül web siteleri üzerinde bulunan zararlı yazılım yayılması amacıyla yaygın olarak kullanılan PDF, HTML/JS, EXE, DLL ve benzeri uzantılardaki dosyaları anti-virüs taramasından geçirerek zararlı içeriklere sahip dosyaları listeleyebilmektedir.

Bunun yanında site üzerinde belli uzantılarda tespit edilen dosyaları birden fazla anti-virüs ile tarayarak ve aynı zamanda statik analiz süreçlerine tabii tutarak zararlı olabilecek dosyaları belirlemektedir. WEB siteleri üzerinden zararlı yazılım dağıtımı yapıldığını tespit etmesi durumunda anında bildirim sağlamaktadır. Tüm tarama süreçleri uygulama üzerinden ve periyodik aralıklarla gerçekleştirilmektedir.

13. Veri Sızıntısı Takip Modülü

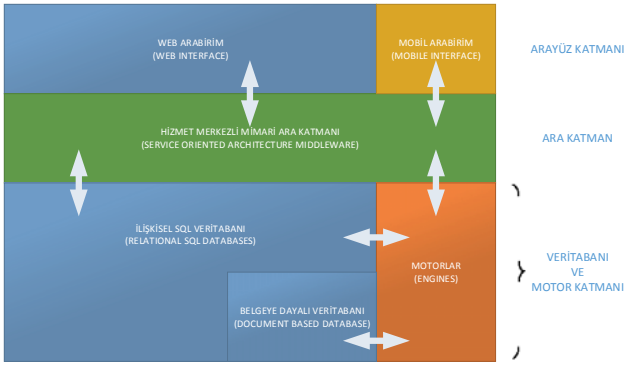
Veri sızıntıları günümüzde birçok kuruluşun en büyük problemlerinden biridir. Saldırganlar ele geçirdikleri sistemlere ait gizli/önemli bilgileri kurumlardan çalarak çoğu zaman internet üzerinden yayınlamaktadır. [11]

Bu modül ile benzeri durumlara karşı veri sızıntısını önlemek adına çözümler geliştirilmiştir. Bir çok veriyi sosyal medya platformları, IRC benzeri sohbet ortamları, web tabanlı metin saklama alanları gibi birçok platformu sürekli tarayarak takip etmektedir. Ayrıca muhtemel veri sızıntılarına karşı tespit ettiği bilgileri site/içerik sahipleri ile paylaşarak anında bildirim sağlamaktadır.

V.BU ÇALIŞMADA İZLENECEK YÖNTEM VE TEKNİKLER

Çalışma kapsamında öncelikle Şekil 2'de geliştirilen kavramlar, Şekil 3'te gösterilen uygulamanın içeriğinde bahsedilen modüler motorlar ile ilgili akademik araştırmalar, daha önce geliştirilmiş teknikler incelenecek olup buna gore yeni yaklaşımlar ve çalışmalar gerçekleştirilebilecektir. Çalışma kapsamında nesne tabanlı ve katmanlı yapı olarak geliştirilecek sistem, temelde üç ana kısımdan oluşmaktadır:

- Ara Yüz Katmanı
- İş Katmanı
- Veri Tabanı ve Motor Katmanı



Şekil. 4. Yazılım mimarisi-katmanlar

A. Arayüz Katmanı

Web ve Mobil arabirim, ara katman üzerinden verileri alacak ve yönetici veya kullanıcılara gösterecektir. Ara katman kullanımı sayesinde hiçbir şekilde uygulamaların doğrudan veritabanına erişmemesi sağlanacak böylelikle güvenlik ihlallerinin önüne geçilecektir. Zira ara katman, sadece kendisi üzerinde tanımlanan komutlara cevap veren ve sadece belirli sorguları veritabanında çalıştırmak üzere tasarlanmaktadır.

B. İş Katmanı

Kurumlar veya kullanıcılar, kendi geliştirdikleri uygulamalar veya farklı programlar üzerinden de kendi sistemlerine ait verileri almak ve görüntülemek istedikleri durumda buna cevap verebilmek amacıyla ara katman tamamen API ve SOAP yaklaşımıyla tasarlanmıştır. Ara katman erişimleri temin edilen API-KEY ile PKI ile gerçekleştirilerek ve trafik SSL üzerinden gerçekleştirilerek güvenliği sağlanmaya çalışılmıştır.

C. Veri Tabanı ve Motor Katmanı

Motorlar topladıkları verileri ve yaptıkları analiz sonuçlarını iki farklı mimarideki veri tabanına doğrudan kaydedetmektedir. İlişkisel verilerden oluşan verileri SQL tabanlı veri tabanına, belgeye dayalı verileri ise NoSQL veri tabanına işlenmektedir.

Site kurulumu safhasında sitelerle ilgili temel bilgilerin toplanarak kaydedilmesi için, ara katman (iş katmanı) sadece kendine ayrılmış alandaki motora istek göndererek gerekli verileri alıp temel değerler olarak veri tabanına işlenmektedir.

Bu çalışmada çeşitli dilleri en uygun oldukları alanlarda kullanarak ve kesinlikle bir dil bağımlılığı olmadan geliştirilmeye çalışılmıştır.

VI. SONUÇ

Sonuç olarak: Öncelikle kritik altyapıya sahip kurumların siber güvenlik tehditlerine karşı uyarı/alarm alabilmeleri sağlanmıştır. Yazılım sisteminin Software as a Service Servis olarak yazılım hizmeti amaçlı sistem tasarımının gerçekleştirilerek, sistemin kullanıma hazır hale getirilmesi ile internet servis sağlayıcılarının gereksinimleri karşılanacaktır. Ayrıca devlet kurumlarının siber saldırılara karşı korunması hızlı, güvenilir ve doğru şekilde gerçekleştirilebilecektir.

Geliştirilecek ürün, WEB sitelerinin ve bağlı oldukları DNS servislerinin güvenlik durumlarını sürekli takip edecek, sitelere karşı gerçekleştirilen bir siber saldırıyı tespit ettiği anda ilgili kişilere alarm vererek derhal müdahale edilmesini sağlayacaktır.

Siber saldırı gözlem ve kayıt ürünü olarak; özellikle kamu sitelerinin siber saldırı sebebiyle erişilmez duruma gelmeleri, siteye propaganda mesajı bırakılması, siteye bir zararlı yazılım/virus/solucan bulaşması veya bulaştırılması, sitelerin güvenli iletişim kurmalarını sağlayan SSL sertifikalarında bozulma gerçekleştirilmesi durumunda derhal uyarı verecek ve bu saldırıyla ilgili bilgileri, saldırı sonucundaki durumu daha sonradan incelenebilmesi için kayıt altına alacaktır. Bunun yanında;

- Kritik altyapılara yapılacak olası siber saldırıların tespitinin yapılarak takip edilmesi sağlanacak,
- WEB sayfaları üzerinden yayılan zararlı yazılım (Malware) ve gelişmiş kalıcı tehditler (APT – Advanced Persistent Threat) tespit edilecek ve yayılmasına izin verilmeden önlem alınması sağlanabilecek,
- Dijital sosyal medya ortamlarında ve saldırganların kullandıkları paylaşım platformlarında kurumlarla ilgili bir ifşa veya ön hazırlık durumu hemen tespit edilebilecek ve gerekli tedbir alınabilecek,
- Tespiti yapılan siber saldırılarla ilgili olarak yetkili birimlere alarm vermek ve gerekli ilk önlemleri alması sağlanacaktır.

KAYNAKÇA

[1] Bilgi Güvenliği Derneği Siber Güvenlik Ulusal Strateji Belgesi
[2] http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php
[3] http://www.ubak.gov.tr/BLSM_WIYS/HGB/tr/Belgelik/20130430_162338_10472_1_66697.pdf
[4] http://tr.wikipedia.org/wiki/Bilgisayar_g%C3%BCvenli%C4%9Fi
[5] http://www.turk-internet.com/portal/yazigoster.php?yaziid=31969
[6] Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (August 1996). "Role-Based Access Control Models" (PDF). IEEE Computer (IEEE Press) 29 (2): 38–47.
[7] http://www.w3.org/TR/html-markup/syntax.html#doctype-syntax (Haziran 2013)
[8] www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet (Haziran 2013)
[9] Deltchev, Krassen. "Yeni Web 2.0 Saldırıları" . Lisans Tez . Ruhr-University Bochum . 18 Şubat 2010
[10] http://www.icann.org/en/news/announcements/announcement-23aug13-en.htm
[11] http://wikileaks.org/syria-files/ Ağustos2013



Mustafa ALKAN Erciyes Üniversitesi Mühendislik Fakültesi, Elektronik Mühendisliği Bölümünden mezun olan Alkan, Aynı Fakültede Araştırma Görevlisi olarak göreve başladı. Yüksel Lisans ve Doktora eğitimini Erciyes Üniversitesinde tamamladı. 1994-2001 Yıllarında Elektronik Bölüm Başkanlığı, Meslek Yüksekokulu Müdürlüğü görevlerinde bulundu. 1998 Yılında Doçent oldu. 2001-2012 Yıllarında Bilgi Teknolojileri ve İletişim Kurumunda Kurum Başkan yardımcısı olarak görev yaptı. 2012 Yılında Prof. oldu. Halen Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği Bölümünde Bölüm Başkanı olarak görev yapmaktadır.
Elektronik ve Bilişim alanında ulusal ve uluslar arası dergi ve sempozyumlar da yayınlanmış 100 den fazla eseri bulunmaktadır. Bilgi Güvenliği, Kriptoloji, İnternet Alan Adları, IPv6, Siber Güvenlik, Elektronik İmza, Kayıtlı Elektronik Posta Sistemleri, gibi konularda proje çalışmaları bulunmaktadır. Dünya Bilgi Toplumu Zirvesi Ulusal Koordinasyon Kurulu Başkanlığı, Elektronik İmza Koordinasyon Kurulu Başkanlıkları gibi görevleri yürütmüştür. Bilişim alanında yapılan birçok Ulusal ve Uluslararası Konferansın eş başkanlığını yapmaktadır.



Burak ÇİFTER 2000'lerin başından beri bilgi güvenliği alanında denetmen ve danışman ünvanlarıyla görev aldı. Yerli ve yabancı bir çok finans kurumuna, telekom servis sağlayıcısına ve kamu kurumlarına hizmet ve destek verdi.
Özellikle uygulama ve ağ güvenliği alanında yaptığı çalışmalarda yaygın kullanılan bir çok ticari ve açık kaynak kodlu yazılımda güvenlik açıkları buldu. Çoğunlukla yabancı güvenlik komünitelerinde faliyet gösterdi.
2010 yılında BOA Bilgi Teknolojileri ve Güvenliği şirketini kurdu ve güvenlik alanındaki çalışmalarını bu çatı altına topladı. Halen güvenlik alaninda projelerde fiilen görev yapmaya devam eden Burak Çifter, artan ulusal risk ve milli çozüm ihtiyacı sebebiyle çalışmalarını ulusal kritik altyapılar ve milli siber güvenlik üzerine yoğunlaştırdı. Bilgi Güvenliği Derneği'nin aktif üyesi olan Burak Çifter, siber güvenlik ile ilgili fikirlerini ve güncel olayları blog'unda (http://www.burakcifter.com/) paylaşmaktadır."



Elif Tuğba KILIÇ 05 Aralık 1987 yılında Ankara'da doğdu. 2001-2005 yılları arasında lise eğitimini yabancı dil ağırlıklı eğitim almak suretiyle Antalya Atatürk Lisesi'nde tamamladı. 2005-2009 yılları arasında Kara Harp Okulu'nda lisans eğitimini tamamladı ve 2009 yılında Muhabere Teğmen olarak mezun oldu. 2009-2010 yılları arasında MEBS Okulu ve Eğitim Merkezi Komutanlığı (ANKARA)'nda icra edilen 56'ncı Dönem Muhabere Sınıfı Subay Temel Kursu'nu 2'ncilikle bitirdi. Subay Temel Kursu'nu tamamlamayı müteakip 2010-2012 yılları arasında GES K.lığı (ANKARA)'nda görev yaptı. K.K.K.lığının 2012 Yılı Genel Atamaları ile MEBS Okl.ve Eğt.Mrk.K.lığı (ANKARA)'na atanmıştır. 2012 Yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü Kazaların Çevresel ve Teknik Araştırılması Bölümünde Yüksek Lisans eğitimine başlamıştır ve hali hazırda eğitim süreci devam etmektedir. bekar olup, İngilizce bilmektedir.

Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler

Uğur Akyazı

***Özet*—Siber uzay artık çoğu ülkede kara, deniz, hava ve uzay gibi bir askeri harekât alanı olarak değerlendirilmektedir. Diğer çatışma alanlarından farklı olarak siber uzay ulusal güç unsurlarının herbirisi üzerinde etkinlik sağlamaktadır. Bu çalışmada siber harekât ortamı tarif edilmiş, NATO'nun siber güvenlik politikası, ülkelerin stratejileri ve ilgili ABD doktrinleri incelenmiştir. Bu kapsamda alınması gereken önlemler ortaya konmuştur.**

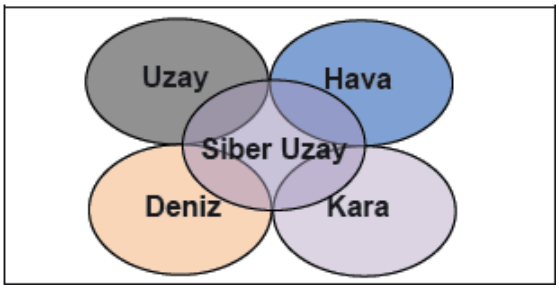
***Anahtar Kelimeler*—Siber güvenlik stratejileri, siber güvenlik doktrinleri**

***Abstract*—Cyber space is considered to be a military operational environment as land, sea, air and space by many countries. Unlike other conflict areas, cyber space affects each one of the elements of the national power. In this study, operational environment of cyber space is described and cyber security policy of NATO, strategies of other developed countries and related U.S. doctrines are examined. In this context, measures to be taken are put forward.**

***Index Terms*—Cyber security policy, strategy and doctrine**

I. GİRİŞ

SİBER güç, tüm harekât alanları ve güç unsurları üzerindeki olayları etkileyerek avantaj sağlamak için siber uzayı kullanma kabiliyetidir. Bu tanımdan da anlaşılacağı gibi siber uzay artık çoğu ülkede kara, deniz, hava ve uzay gibi bir askeri harekât alanı olarak değerlendirilmektedir. Diğer çatışma alanlarından farklı olarak siber uzay ulusal güç unsurlarının herbirisi üzerinde etkinlik sağlamaktadır (Şekil-1).



Şekil-1: Beşinci Harekât Alanı olarak "Siber Uzay"

ABD Hava Kuvvetleri Temel Doktrininde hava gücü artık "stratejik, operasyonel veya taktik hedeflere ulaşmak için hava, uzay ve siber uzayın kullanılması ve kontrolü yoluyla askeri gücü veya etkiyi yöneltme yeteneği" olarak tanımlanmakta ve siber uzay bir savaş alanı olarak algılanmaktadır. Bu tanımın yakın zamanda diğer uluslarla beraber kendi doktrinlerimizde de yer bulacağını tahmin etmek zor değildir. Siber uzay hava, kara, deniz ve uzay olan diğer etki alanları arasında bulunmakta ve saklanan, değiştirilen ya da aktarılan verileri kullanan bilişsel süreçler ile bu fiziksel etki alanlarını birbirine bağlamaktadır.

Uğur Akyazı, Hava Kuvvetleri Komutanlığı, uakyazi99@yahoo.com

İnternet, siber uzayı oluşturan en önemli unsurlardan biri olmakla birlikte, siber uzay sadece internet ile sınırlı değildir. Tanımından da anlaşılacağı üzere, iletişim ağları, dış dünyaya kapalı askeri ağlar, enerji dağıtım ağları, cep telefonları, yazılım tabanlı telsizler, elektronik komuta sistemleri, uydu sistemleri, insansız hava araçları gibi birçok sistem ve donanım siber uzayın elemanlarıdır.

Siber savaş geleneksel savaşa benzemez, ama hava bombardımanı, denizaltı savaşı, özel harekât güçleri ve hatta suikastçıların tarihsel rolü ile bazı özellikleri paylaşır. Özellikle, uzak mesafelerden veya baskın prensibini istismar ederek bir düşmana ciddi düzeyde asimetrik hasar verebilir. Siber saldırıların en azından yakın gelecekte, stratejik bir bombardımandan daha ölümcül olması beklenmemektedir. Ama sonuçta, askeri operasyonların başarısı etki temellidir. Eğer bir hedefi hem bir balistik füze hem de bir bilgisayar solucanı yok edebiliyor veya devre dışı bırakabiliyorsa, doğal seçim solucan olacaktır [1].

II. NATO SİBER GÜVENLİK POLİTİKASI

8 Haziran 2011 tarihinde revize edilen NATO Siber Savunma Politikası, NATO'yu İttifak'ın temel görevleri olan kollektif savunma ve kriz yönetimini gerçekleştirmek amacıyla kendi iletişim ve bilgi sistemlerinin korunmasına odaklamaktadır. Ancak, siber tehditler ittifakın ve devletin sınırlarını aştığı için, İttifak'ın NATO ortağı ülkeler, özel sektör ve akademik çevreler ile işbirliği ihtiyacı da ifade edilmektedir. NATO üyesi devletler uluslararası işbirliğinin önemini Mayıs 2012'deki Chicago Zirvesi Bildirgesi'ndeki şu ifadelerle pekiştirmişlerdir: "Siber güvenlik tehditlerini belirlemek ve ortak güvenliğimizi geliştirmek için somut işbirliğini artırmak amacıyla ilgili ortak ülkelerle ve uluslararası kuruluşlarla beraber çalışmaya kararlıyız." [2]

NATO Siber Savunma Politikası'nın kavramsal temelini oluşturan NATO Siber Savunma Konsepti Mart 2011 tarihinde hazırlandı ve 8 Haziran'da NATO Savunma Bakanları tarafından onaylandı. Konseptle beraber NATO'nun kendi yapıları ve Müttefiklerin savunma kuvvetleri için özel görevler ve faaliyetleri içeren ayrıntılı bir belge olan Eylem Planı yayımlanmıştır. Siber Savunma Politikası'na göre:

a. NATO'nun temel görevleri olan kollektif savunma ve kriz yönetimini gerçekleştirmek için NATO yapılarına ve planlama süreçlerine siber savunma hususları entegre edilecek,

b. NATO ve müttefikleri için kritik olan siber varlıkların korunması ve savunmasına odaklanılacak,

c. Güçlü siber savunma yetenekleri geliştirilecek ve NATO'nun kendi ağlarının korunmasını merkezileştirilecek,

ç. NATO'nun temel görevleri için kritik olan ulusal ağların siber savunması için minimum gereksinimler geliştirilecek,

d. Ulusal kritik altyapılarının güvenlik açıklarını azaltmak için Müttefiklere yardım sağlanacak,

e. Ortaklar, uluslararası kuruluşlar, özel sektör ve akademik çevreler ile birlikte çalışılacak,

f. İlgili siber savunma gereksinimlerinin tespit edilerek NDPP (NATO Defence Planning Process) yoluyla öncelik verilecek,

g. NATO Askeri Yetkilileri siber savunmanın NATO'nun temel görevleri yerine getirmesini, askeri görevler için planlamayı ve bu görevlerin yürütülmesini nasıl desteklediğini değerlendirecek,

ğ. Farkındalık programları geliştirilecek ve NATO tatbikatlarına siber bileşenler eklenecek,

h. NATO ve müttefikleri Tallinn'deki Kooperatif Siber Savunma Mükemmeliyet Merkezi'nden uzmanlık ve destek almak için teşvik edilecektir [3].

NATO ülkeleri Ulusal Siber Güvenlik ve (kollektif) siber savunmanın yakın bağlantı içerisinde olması gerektiği görüşünde olduklarını giderek daha açıkça ifade etmektedirler. Bu durumu en doğrudan açıklayan Beyaz Saray olmuştur: "Bütün devletler doğal olarak kendini savunma hakkına sahiptirler ve siber uzay yoluyla yapılan bazı düşmanca eylemler askeri ortaklarımız ile olan taahhütlerimiz gereği olan eylemleri mecbur kılabilir." "Müttefikler arasındaki güçlü ilişkiler etkili bir siber savunma politikasının temelini oluşturmaktadır" şeklinde olan Fransız Ulusal Siber Güvenlik Stratejisinde olduğu gibi diğer bazı ulusal stratejiler doğrudan kollektif savunmayı değil ama NATO taahhütlerini öne çıkarmaktadır. "Kollektif siber savunma"nın tam olarak ne gerektirdiği açık değildir ve çok geniş bir aralıktaki siber eylemleri kapsayabilir. Bunlar:

a. Etkilenen bir ülkedeki kritik altyapıların savunmasına yardımcı olması için asker ya da sivillerin kullanılması,

b. Kayıt tutma ve çağrı yönetimi gibi en kolay işlerden, olaylara müdahaleyi yönetme gibi profesyonel görevlere kadar askerlerin ya da sivillerin kriz yönetim görevlerinde kullanılması,

c. Soruşturmalara yardımcı olmaları için adli müfettişlerin görevlendirilmesi,

ç. NATO ya da diğer ülkeler veya sektörlerle koordinasyona yardımcı olmaları için ekiplerin görevlendirilmesi. Örneğin, finans sektörüne yapılan bir saldırı üzerine bilgi akışında yardımcı olmak için ilgili ülkeye bir finans temsilcisi gidebilir, ya da askeri bir irtibat ekibi aynı şeyleri askeri koordinasyon için yapabilir.

d. İnternet Servis Sağlayıcılarına, saldırı altındaki ülkeye giden saldırı trafiğini engellemeleri direktifinin verilmesi (veya ikna edilmesi),

e. İnternet Servis Sağlayıcılarına, saldırıları sona erdirmede yardımcı olmak için işbirliğinde bulunana kadar saldırının arkasında olduğundan şüphelenilen ülkenin trafiğini kısma direktifinin verilmesi (veya ikna edilmesi),

f. Saldırının arkasındaki Komuta Kontrol altyapısını bozmaya yönelik seçici aktif savunmanın yapılması,

g. Saldırıları kurutmak ve savunma seçeneklerini artırmak için ilave yerel Internet Değişim Noktaları ve diğer yerel altyapıların kurulması,

ğ. Saldırı altındaki ülkenin ek kapasite geliştirmesine yardım etmek için ağ teknolojisi üreticilerinin sipariş önceliğini bu ülkeye vermelerinin sağlanması,

h. İttifak üyesi bir ülkenin kendi siber saldırı kuvvetlerini İttifak adına karşı atak yapmak için konuşlandırması [2].

III. ULUSAL SİBER GÜVENLİK STRATEJİLERİ

Yüzden fazla ülkenin devlete ait siber yetenekleri bulunmakta olup bunların en az elli tanesi gelecekteki ulusal ve ekonomik güvenlik girişimleri için siber güvenliğin önemini vurgulayan bir çeşit siber strateji yayınlamıştır. Bu ülkelerden öne çıkanlar Tablo-1'de görülmektedir. Türkiye'nin "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinesinde 20 Haziran 2013 tarihinde yayınlanmıştır.

ABD Ulusal Siber uzay Güvenliği Stratejisi beş ulusal önceliği dile getirmektedir:

a. Ulusal Siber Uzay Güvenliği Yanıt Sistemi;

b. Ulusal Siber Uzay Güvenliği Tehdit ve Güvenlik Açığı Azaltma Programı;

c. Ulusal Siber Uzay Güvenliği Farkındalığı ve Eğitim Programı;

ç. Devletin Siber Uzay Güvenliğini sağlamak ve

d. Ulusal Güvenlik ve Uluslararası Siber Uzay Güvenlik İşbirliği.

İlk öncelik siber olaylara karşı verilecek tepkileri geliştirmeye ve bu tür olaylardan gelecek potansiyel zararı azaltmaya odaklanır. Ikinci, üçüncü ve dördüncü önceliklerin amacı siber saldırılardan gelecek tehditleri ve kendi güvenlik açıklarını azaltmaktır. Beşinci öncelik ise, ulusal güvenlik varlıklarını etkileyebilecek siber saldırıları önlemek ve bu tür saldırılara karşı uluslararası tepkiler geliştirmek ve yönetmektir [5].

Tablo-1: Siber Güvenlik Stratejisi sahibi ülkeler [4]

Ulusal Siber Güvenlik Stratejileri	
ABD	Savunma Bakanlığı, "Siber Uzayda Harekât Stratejisi" (2011)
	Beyaz Saray, "Uluslararası Siber Uzay Stratejisi: Ağlarla Birleştirilmiş Dünyada Refah, Güvenlik ve Şeffaflık" (2011)
	İç Güvenlik Bakanlığı, "Güvenli Siber Gelecek Planı: İç Güvenlik Kuruluşları Siber Güvenlik Stratejisi" (2011)
İngiltere	"İngiltere Siber Güvenlik Stratejisi: Dijital Dünyada İngiltereyi Korumak ve Yükseltmek" (2011)
Fransa	İç İşleri Bakanlığı, "Fransa Stratejisi: Bilişim Sistemlerinin Güvenliği ve Savunması" (2011)
Almanya	Federal İç İşleri Bakanlığı, "Almanya Siber Güvenlik Stratejisi" (2011)
Hollanda	"Ulusal Siber Güvenlik Stratejisi: İşbirliği ile Başarı" (2011)
Hindistan	Bilişim Teknolojileri Bakanlığı, "Siber Güvenlik Stratejisi" (2011)
Türkiye	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, "Ulusal Siber Güvenlik Stratejisi" (2013)

IV. ABD DOKTRİNLERİ

ABD Hava Kuvvetleri Temel Doktrininde [6] hava gücü artık "stratejik, operatif veya taktik hedeflere ulaşmak için hava, uzay ve siber uzayın kullanılması ve kontrolü yoluyla askeri gücü veya etkiyi yöneltme yeteneği" olarak tanımlanmaktadır. Hava Kuvvetleri temel fonksiyonlarından olan Siber Uzay Üstünlüğü ise "engelleyici bir müdahale olmaksızın belirlenen zaman ve etki alanında harekât icra edebilmek amacıyla siber uzaydaki harekât avantajı" olarak ifade edilmektedir [7]. Bu işlevin alt öğeleri: Siber uzay Kuvvetlerini Kullanma, Siber uzay Savunması, Siber uzay Desteğidir.

ABD Savunma Bakanlığı, "Siber Uzay Harekâtları için Ulusal Askeri Stratejisi"ni yayınlayarak siber uzayı bir savaş alanı olarak algıladığını resmen belirtmiştir. Bu belgede, siber uzay veri saklamak, değiştirmek, ağ sistemleri ve ilgili fiziksel altyapılar sayesinde veri akışını sağlamak için elektronik ve elektromanyetik spektrumun kullanıldığı bir alan olarak tanımlanmaktadır. Bu tanıma göre, siber uzay elektronik ve elektromanyetik enerji kullanan ağ sistemlerinden oluşan gerçek bir fiziksel etki alanıdır.

ABD Silahlı Kuvvetlerin siber uzay tanımı, siber uzayın bilgisayar ağlarından daha fazla şeyler içerdiğini göstermektedir. Daha da önemlisi, ağ sistemlerinin elektromanyetik enerji kullanılarak oluşturulmuş olmasından dolayı, siber uzaydaki savaşlar hâlihazırda elektronik harp olarak kabul edilen yetenekleri de içerecektir. Elektromanyetik enerji kullanarak bir ağın elektronik bileşenlerini sorgulamak veya bozmak için doğrudan internete bağlı olmayan ağlara bile erişilebilinecek veya saldırılabilinecektir. Bu silahlı kuvvetler için önemli bir tehdittir.

Çoğu askeri komuta ve kontrol ağları ve hava savunma sistemleri silahlı kuvvetler dışındakilerce doğrudan erişilemeyen izole ya da kapalı ağlardır. Siber uzay elektromanyetik ortamda fiziksel bir etki alanı olarak tanımlandığından dolayı, siber uzayda fiziksel harekât ile savaşılacaktır. Bu, sanal etkiler yaratmak veya düşmanlara sanal gerçeklik ortamında saldırmak değildir. Bu nedenle, siber uzaya bir harekât alanı olarak yaklaşmak, bu etki alanının sürekli kullanılabilmesini sağlamak için bazı yetenekleri geliştirmek gerekmektedir. Dokümanda, etkiler oluşturmak için siber yeteneklerden bazılarını geçmişte kullandıkları belirtilirken, bu kabiliyetlerin siber uzayda eylem özgürlüğünü sağlamak için henüz kullanılmadıkları ifade edilmektedir. Siber uzayda hareket serbestîsi elde ettikten sonra müşterek kuvvet komutanının stratejik, operasyonel ve taktik hedeflerine ulaşmak için diğer işlemleri gerçekleştirebileceği anlatılmaktadır.

Hava Kuvvetleri'nin yeteneklerinden yararlanmak için siber uzayda harekât icra edebilmek amacıyla ABD Hava Kuvvetleri Siber Komutanlığı kurulmuştur. Hava Kuvvetleri, müşterek savaşta düşmanın kuvvetlerini yönlendirme, komuta ve kontrol etme, hatta silahlarını ateşleme kabiliyetini etkileyecek şekilde siber uzayda gerçek etkiler oluşturma imkânı sağlamayı hedeflemektedir. Bu etkiler kolayca düşmanın zihninde oluşacak etkiler değildir. Diğer bir deyişle, bunlar sanal ya da hayali etkiler değildir - düşman siber uzaydaki savaşta gerçekten ölebilir veya zarar görebilir [8].

Siber uzay, insan yapımı bir harekât alanıdır ve doğal harekât alanları olan kara, deniz, hava ve uzaya benzememektedir. Siber uzayın düğümleri fiziksel olarak diğer harekât alanlarının içerisinde bulunur. Siber uzaydaki etkinlikler diğer harekât alanlarındaki faaliyetler için hareket serbestîsi sağlayabilirken diğer harekât alanlarındaki faaliyetler de siber uzay içerisinde etkiler oluşturabilir. Siber uzay fiziki altyapı, elektronik sistemler ve elektromanyetik spektrumun (EMS) bölümleri ile desteklenmektedir. Yeni sistemler ve altyapılar geliştirildikçe, yüksek EMS frekanslarını kullanabilir, daha yüksek veri işleme kapasitesi ve hızına sahip olabilir ve daha büyük bant genişliği kullanabilir. Sistemler verileri değiştirdiği gibi aynı zamanda frekansları değiştirmek için de tasarlanmış olabilir. Bu nedenle, siber uzayda fiziksel manevra alanı bulunmaktadır.

Siber uzayda mantıksal manevra kabiliyeti genellikle konakçı bilgisayar sistemleri tarafından kullanılan güvenlik protokollerinin bir fonksiyonudur. İstenmeyen sistemlerin girişine karşı savunma, konakçı bilgisayar sisteminin kodunda ya da mantığında yer almaktadır. Sistemler arasında

bir bağlantı kurulduktan sonra, potansiyel bir saldırganın sisteme girmesi için mantıksal bir hatadan faydalanması gerekir. Bu nedenle, siber uzayda mantıksal manevra biçimi kod yazmadır.

Saldırgan, hedeflenen sistemlere karşı manevra kabiliyeti kazanmak için kötü amaçlı kod yazar. Sistem içinde istenmeyen bir varlığın farkına varıldığında, savunma sistemi girişi engellemek için sistemin kodunu değiştirecektir. Hedef sistem içinde kalmak isteyen saldırgan, kötü amaçlı kodunu buna göre uyarlar. Bu süreç geleneksel hava, kara, uzay ve deniz alanlarında avantajlı pozisyonlar elde etmek için manevra yapan güçlere eşdeğerdir. Mantıksal ve fiziksel manevra alanlarının her ikisi de gereklidir – genelde biri olmadan diğeri işe yaramaz. Tablo-2'de ABD Doktrinlerinde yer alan Harp Prensiplerinin Siber uzay Harekâtında uygulamalarına örnekler verilmiştir.

ABD'nin Siber Güvenlik Ulusal Stratejisi kapsamlı bir stratejidir. Üç adet stratejik önceliği vardır:

a. Amerika'nın kritik altyapılarına karşı siber saldırıları önlemek,

b. Siber saldırılara karşı ulusal güvenlik açıklarını azaltmak,

c. Siber saldırılardan gelecek zararı ve toparlanma süresini en aza indirmek.

Siber uzay Harekâtları için Ulusal Askeri Strateji (NMS-CO) siber uzayda ABD üstünlüğünü sağlamak amacıyla ABD Silahlı Kuvvetleri için hazırlanmış olan kapsamlı bir stratejidir. NMS-CO'nun dört stratejik önceliği bulunmaktadır:

a. Düşman karar döngüleri içinde harekât icra edebilmek için inisiyatif kazanmak ve korumak,

b. Askeri harekâtlar arasındaki siber yetenekleri entegre etmek,

c. Siber uzay harekâtları için yetenek geliştirmek,

ç. Siber uzay harekâtlarındaki riski yönetmek.

Halkın bilgi ve becerisi ile birlikte taarruzi ve müdafi siber harekâtların entegrasyonu, bu yaklaşım için temel esastır.

Siber harekâtlar stratejik, operasyonel ve taktik seviyedeki birden çok etki alanında aynı anda etkiler oluşturabildiği için devam eden harekâtlar için bile stratejik düzeyde planlama yapmak zorunludur. Plancıların kamu kuruluşları ve ortak ülkelerdeki uygun istihbarat ve hedefleme kuruluşlarına girdi sağlamaları ve geri bildirim almaları gerekmektedir. Siber uzayın benzersiz özellikleri ve hız potansiyeli hızla değişen durumlara tepki verme yeteneği gerektirir.

Tablo-2: Harp Prensiplerinin Siber Harekât Uygulamaları

PRENSİP	AMAÇ	ÖRNEK SİBER UZAY HAREKÂTI
Hedef	Her askeri operasyonu açık bir şekilde tanımlanmış, kararlı, ulaşılabilir bir hedefe doğru yöneltmek	Müşterek Komutanın yönettiği siber uzay saldırıları ile düşmanın önemli enerji ağlarının elektrik gücünü kapatmak
Taarruz	Bozmak, zayıflatmak, engel olmak, caydırmak, ele geçirmek, korumak ve istismar etmek	2007 yılında yapılan Dağıtık Hizmetin Engellenmesi Saldırısı ile Estonya ağ sistemine aşırı yüklenme olmuştur
Sıklet Merkezi	Etkileri en avantajlı yer ve zamanda yoğunlaştırmak	2008 işgali sırasında Rus aktörlerin Gürcistan güçlerinin koordinasyonu bozmak için Gürcü ağlarda önleyici siber saldırı yapması
Kuvvet Tasarrufu	İkincil çabalara minimum gerekli güç tahsis etmek	"Kinetik" varlıkları diğer harekâtlar için serbest bırakabilmek amacıyla düşmanın önemli düğüm noktalarına siber saldırı yapılması
Manevra	Düşmanı dezavantajlı bir konuma sokmak	Bir siber saldırı sırasında çok sayıda IP kullanarak kimliğinin belirlenmesini önlemek
Emir ve Komuta Birliği	Bir sorumlu komutan altında kuvvet birliğini sağlamak	24'üncü Hava Kuvveti ile Hava Kuvvetleri küresel bilgi şebekesinin kontrolü
Emniyet	Müdahalesiz erişim sağlamak	Katmanlı savunma, kendi kendini düzeltme ve yeniden yapılandırılmalarla Komuta Kontrol ağlarının işlerliğini sağlamak ve korumak
Baskın	Düşmanı hazırlıksız olduğu bir zamanda, yerde veya şekilde vurmak	Savunmasız veya önceden ele geçirilmiş sistemlere habersiz yapılan siber saldırılar
Sadelik	Anlaşılmayı sağlamak için açık ve öz yönlendirme yapmak	Kuvvetin her düzeydeki veri ve ağ yapılarına kullanıcı dostu erişim sağlamak
Sınırlama	Gereksiz güç kullanımını önlemek, yan hasarı sınırlamak	Hedefleri yok etmeden etki oluşturarak, komutanlara tek başına icra edilebilen, kinetik olmayan seçenekler sağlamak
Sebat	Ulusal stratejik nihai durumu gerçekleştirene kadar savaşa devam etmek	Sistemlerin sürekli güvende çalışmasını sağlamak; ortak ülkelerde güçlü siber yetenekler oluşturmak
Meşruiyet	Hedef toplum ve ortakların gözünde, eylemlerin yasal, ve meşru göründüğünden emin olmak	Kinetik saldırıların avantajlı olmadığı şartlarda düşmana karşı istenilen etkiyi elde etmek için kinetik olmayan siber yetenekleri kullanmak

Plancılar siber uzayda artan güvenliğin harekâtlar üzerindeki etkisini göz önünde bulundurmalıdır. Bilgi harekâtlarının koşullarını değiştirmek veya ağları analiz etmek için ek araçlar kullanmak düşük ağ çalışma hızına

neden olabilir. Bant genişliği sınırlı olan veya kuvvetlerin çok dağınık olduğu bir ortamda, plancılar siber savunma geliştirmek için alınan önlemlerin aslında harekâtları engelleyebileceği veya uyumlarını bozabileceğini dikkate almalıdırlar.

Askeri operasyonların yürütülmesi aşamasında, Harekât Merkezi içindeki siber uzay operatörleri siber etkileri komutanın niyeti, istenilen etkiler, dost ve düşman kuvvetlerin yetenekleri temelindeki zaman aşamalı manevra ve vuruş düzeni içine entegre edecektir.

Görev döngüsünün önemli bir ürünü olan Hava Kuvvetleri Siber Görev Emri (CTO), siber uzay kuvvetlerinin görevlerini alması ve uygulaması için kullanılır. Hava görev döngüsünü temel alan siber görev döngüsü, siber uzay harekâtlarının etkinliğinin planlaması, koordinasyonu, uygulanması ve değerlendirilmesi için kullanılan iteratif bir süreçtir. Krizleri desteklemek için döngünün süresi savaş temposuna göre uzatılabilir veya kısaltılabilir. Durumsal farkındalık ve çakışmaların önlenmesi amacıyla siber harekâtların tamamı CTO'da yer almalıdır. Planlama aşamasında, 624'üncü Harekât Merkezi CTO'yu tamamlamak için COMAFFOR / JFACC direktifini, angajman kurallarını (ROE), müşterek öncelikli hedef listesini, aday hedef listesini ve onaylı ana hava taarruz planını (MAAP) kullanır.

Yasal hususlar ve uluslararası yasal yükümlülükler siber yeteneklerin kullanılmasında da geçerlidir. Uluslararası hukuk, iç hukuk ve politika kararları, silahlı çatışma hukuku, angajman kuralları harekât faaliyetlerinin değerlendirildiği yasal çerçeveyi oluşturmaktadır. Genellikle, komutanın karargâhındaki askeri hukukçu siber uzay harekâtlarını hukuka uygun olarak yapması konusunda, Askeri Harekâtlara Hukuki Destek (JP 1-04) [9] dokümanına göre ilgili komutana tavsiyelerde bulunur. Hukuki destek personelinin siber uzay harekâtlarında kullanılan bilgi, süreç ve programlara erişimi ve temel siber teknolojilerine hâkimiyeti olmalıdır [7].

V. SONUÇ

Günümüzde belli bir artış trendi izlese de hayatın akışını çok ciddi biçimde olumsuz etkileyecek siber saldırılar henüz gerçekleşmemiştir. Ancak gelecek yıllarda, dünyamız büyük oranda e-dünyaya dönüştüğünde gerçekleştirilecek siber saldırıların hayal dahi edilemeyecek boyutta cana ve mala zarar vermesi kuvvetli bir olasılık olarak görülmektedir. Bu itibarla, gelecekte kıyamet senaryosu benzeri kötü durumlarla karşılaşmamak için bugünden siber güvenlik konusunda tedbirlerin alınmasında yarar görülmektedir.

Alınacak tedbirlerin başarılı olabilmesi için bunların küresel çapta olması gerekmektedir. Küresel çapta işbirliği ve koordinasyon sağlanarak ortak algı, anlayış ve kabullerin oluşturulması, sorunların önlenmesi, önlenemese dahi ortaya çıktıktan sonra hızla ve asgari zararla çözülebilmesi noktasında büyük önem arz etmektedir. Bu itibarla, tüm ülkelerin taraf olacağı sözleşmeler marifetiyle küresel bir hukuki çerçeve geliştirilmesi, bu hukuki çerçeve içinde yargı ve kolluk birimlerinin hızlı ve etkin çalışabilmelerinin temin edilmesi hayati önem taşımaktadır. Bunların yanında, siber alan da diğer alanlarda olduğu gibi silahlı çatışma hukukuna uygun davranış standartlarına sahip olması gerekmektedir. Uluslararası siber uzay düzenlemeleri için diğer ortak alan düzenlemeleri örnek alınabilir. 150 ülkenin katkısıyla 14 yılda ancak oluşturulabilen BM Deniz Hukuku Sözleşmesi'nde olduğu gibi, eğer ülkeler ısrarla takip etmezse kapsamlı bir çerçevenin geliştirilmesi çok zordur.

NATO Siber Savunma Politikasında yer aldığı gibi Silahlı Kuvvetler yapımıza ve planlama süreçlerine siber savunma hususları entegre edilmeli, farkındalık programları geliştirilerek tüm tatbikatlara siber bileşenler eklenmelidir. Siber uzay harekâtlarının planlaması, koordinasyonu, uygulanması ve değerlendirilmesi için hava görev döngüsünü temel alan bir siber görev döngüsü kullanılabilir. Harekât merkezlerine siber güvenlik hücreleri eklenmeli ve harekâtı destekleyen siber harekât merkezleri kurulmalıdır. Siber güvenlik teşkilatı içerisinde bilgi sistemleri güvenliği, iletişim ağı güvenliği, adli analiz gibi teknik unsurlara ilave olarak; istihbarat, harekât ve adli konularda görev yapacak icracı veya danışman statüsünde personelin görevlendirilmesi sağlanmalıdır.

KAYNAKLAR

1. K. Geers, "Strategic Cyber Security", NATO Cooperative Cyber Defence Centre of Excellence, 2011
2. *National Cyber Security Framework Manual*, Talinn, NATO CCDCOE Publication, 2012
3. *Defending the Networks, The NATO Policy on Cyber Defence*, 2011
4. M.D. Cavelty, "The Militarizatin of Cyber Security as a source of global tension", Strategic Trends 2012, Chapter 5, Center for Security Studies, Zurich
5. E. Tıkk, "Frameworks for International Cyber Security", NATO Cooperative Cyber Defence Centre of Excellence, Talinn, 2011
6. *Air Force Doctrine Document (AFDD)-1, Hava Kuvvetleri Temel Doktrini*, ABD Hava Kuvvetleri, 2011
7. *Air Force Doctrine Document (AFDD) 3-12, Siber Uzay Operasyonları*, ABD Hava Kuvvetleri, 2011
8. D.T. Fahrenkrug, "Cyberspace Defined", The Wright Stuff, Air University, 17 Mayıs 2007
9. *Joint Publication (JP) 1-04, Legal Support to Military Operations*, ABD Genelkurmay Başkanlığı, 2011

Uğur AKYAZI. 1978 yılında Çankırı'da dünyaya gelmiştir. İlk ve ortaokulu Kırıkkale'de, liseyi Kuleli Askeri Lisesi'nde okumuş ve Hava Harp Okulundan 1999 yılında mezun olmuştur. 1999-2011 yılları arasında Hava Harp Okulu Dekanlığı Bilgisayar Mühendisliği Bölümü Yazılım A.B.D. Bşk.lığı Öğretim Elemanlığı görevini yapmıştır. 2011-2013 yılları arasında Hava Harp Akademisi öğrenimini tamamlamıştır. 2002 yılında ABD Hava Kuvvetleri Teknoloji Enstitüsü'nde (AFIT) Sistem Mühendisliği dalında yüksek lisans, 2011 yılında İstanbul Teknik Üniversitesi'nde Bilgisayar Mühendisliği dalında doktora eğitimi almış olup 2008-2011 yılları arasında yayımlanmış 3 adet uluslararası konferans makalesi ve 1 adet uluslararası dergi makalesi bulunmaktadır.

Bulut Bilişim Kapsamında Ortaya Çıkabilecek Hukukî Sorunlar

M. Mürsel Başgül, Oumout Chouseinoglou

***Özet*—Bulut Bilişim (BB), sağladığı hizmetler ile işletme ve bireylerin iş yapma ve bilgi paylaşma modeline yeni bir boyut getirmektedir. BB'in sağladığı fayda ve fırsatlardan dolayı, bu teknolojiye geçiş kaçınılmazdır. Fakat bu geçiş, BB hizmet sağlayıcıları ve kullanıcılar yönünden, çözümlenmesi gereken çok ciddi sorunları da beraberinde getirmektedir. Bunlar arasında, BB'in hukukî boyutu ve ortaya çıkan ve çıkabilecek hukukî sorunlar gelmektedir. Bu bildiride öncelikle, BB sözleşmelerinin yapılması aşamasında karşılaşılan hukukî sorunlar ele alınmaktadır. Daha sonra ise, BB sözleşmelerinin hukukî niteliği ve uygulanması aşamasında ortaya çıkan hukukî sorunlar incelenmektedir. Sözleşmenin sona ermesi aşamasında verilerin geri verilmesi ile ilgili ihtimaller ve BB sözleşmelerine hangi hukukun uygulanacağı konuları ise son bölümde tartışılmaktadır.**

***Anahtar Kelimeler*— Bulut bilişim hukuku, Bulut bilişim sözleşmeleri, Bulut bilişim genel işlem koşulları, Yasal düzenleme ihtiyaçları**

***Abstract*— Cloud Computing (CC) with the services that it offers brings a new dimension to the business conducting and information sharing model of businesses and individuals. Considering the advantages and opportunities that CC provides the transition to this technology is inevitable. However, this transition, with respect to CC service providers and users, brings many important complications that need to be resolved. Among these, the legal dimension of CC and the legal problems that exist and may arise in CC can be listed. This paper firstly addresses the legal issues that are encountered while forming CC contracts, followed by the legal character of CC contracts and the legal issues that arise during their execution. The paper concludes with discussions on the possibilities regarding the return of data at the termination of CC contracts and the conflict of laws.**

***Index Terms*— Cloud computing law, Cloud computing contracts, Standardized terms of contract in cloud computing**

I. GİRİŞ

BULUT bilişim (BB), ortaya yeni çıkmakta olan bir teknoloji olarak, şirketlerin ve bireylerin iş yapmasına, kaynak ve sermayelerinin korunması ve saklanması alanlarına yeni boyutlar getirmekte olup, dünya çapında ticareti ve ticarî işletmeleri tekrar şekillendirecek araçlardan biri olduğu iddia edilmektedir [1]. BB hizmetini sunan ve alan kuruluşların ölçek ekonomilerinden faydalanması ve bu sayede şirketlerin temel yetkinliklerine odaklanmalarını sağlamasından dolayı, yakın gelecekte kuruluşların büyük oranda BB'e geçiş yapacağı öngörülmektedir [2]. Fakat bu yeni yapı ve hizmet anlayışına geçiş, üstünde düşünülmesi ve çözümlenmesi gereken birçok konuyu beraberinde getirmektedir. Bunlardan bir tanesi de BB'in hukukî boyutudur.

BB'in kabul görmekte olan genel hizmet yapısı katmanlı bir mimari olup, bu katmanlarının tamamı *hizmet* olarak kabul edilmektedir (XaaS) ve sırası ile Hizmet olarak Yazılımlar (Saas), Hizmet olarak Platform (PaaS) ve Hizmet olarak Altyapı (IaaS) şeklinde sıralanmaktadırlar [3, 4, 5]. IaaS tüm bulut hizmetlerinin temeli olup, PaaS onun, SaaS de PaaS'ın üstüne kuruludur [4]. *SaaS* birden fazla müşteriye aynı anda destek verebilecek şekilde, ortak kaynaklar, yazılımların ve altta yatan veritabanının bir gerçekleşiminin çalışması şeklinde tanımlanmaktadır. *PaaS* hizmet yapısı ile, BB hizmet sunucuları uygulama geliştiricilere, geliştirme sürecinin yaşam döngüsü sistemlerini ve ortamlarını (geliştirme, test etme, kurulum, vb.) sunmaktadır. *IaaS* hizmet yapısı, kullanıcıların kullandıkça ödediği bir ödeme şekli sunmakta olup, hizmet alan işletmelerin kendi bilgi teknolojileri sistemlerini kurmak ve bakımını yapmak için yatırım yapma ihtiyacını ortadan kaldırmaktadır. Böylelikle, hizmet alımının başlamasından sonraki teknolojik gelişmelerin de kullanılabilmesi sağlanmaktadır.

BB hizmetleri ve hizmet yapıları, dört farklı kurulum ve dağıtım modeli ile sunulmaktadır [5]. Sadece bir organizasyon için işletilip, bir kuruluş ya da bir üçüncü şahıs tarafından yönetilmekte olan *Özel BB*, altyapının birçok organizasyon tarafından paylaşıldığı ve güvenlik gereksinimleri, kurallar, hedefler vb. ortak endişelerin özel bir topluluk tarafından desteklendiği *Topluluk BB*, kişiler veya işletmelere açık olup, bir kurum tarafından hizmet ticareti yapılmakta olan *Halk BB*, ve yukarıda bahsedilmekte olan iki veya daha fazla dağıtım alt yapısının beraber kullanılması şeklinde tanımlanan *Melez BB*.

Rimal vd'nin [4] tanımladığı üzere, BB'de *mimari gereksinimler* temel olarak; BB sağlayıcıları, BB hizmeti alan işletmeler ve BB kullanıcıları şeklinde üçe ayrılmaktadır. Hizmet sağlayıcı açısından, sanallaştırılmış ve dinamik hizmetler sunabilmek için, altyapı ve hizmetleri destekleyecek nitelikte üst seviyede etkin bir hizmet altyapısına ihtiyaç duyulmaktadır. BB hizmeti alan işletmeler bedelini ödedikleri hizmetleri; hizmet kalitesi, hizmet seviyeleri, mahremiyet, uyumluluklar, veri mülkiyeti ve veri mobilitesi gibi konularla değerlendirmektedirler. Kullanıcı gereksinimleri, başarılı bir BB benimsenmesi için önemli başka bir önkoşuldur. Ayrıca, BB'in güven-temelli olması zorunlu bir özellik olarak tanımlanmaktadır. Üçüncü kişiler veya kurumlar tarafından yönetilen ve coğrafi olarak uzak sunucularda bulunan bilişim sistemlerine, çoğunlukla şirket, müşteri ve çalışan verilerinden, iş ile ilgili bil-

M. M. Başgül, Başkent Üniversitesi Hukuk Fakültesi, Ankara, Türkiye (tel: +90 312 246 66 66; e-posta: mbasgul@baskent.edu.tr).

O. Chouseinoglou, Başkent Üniversitesi, İstatistik ve Bilgisayar Bilimleri Bölümü, Ankara, Türkiye (e-posta: umuth@baskent.edu.tr).

yaplardan ve fikrî mülkiyet haklarından oluşan bilgi yığınlarını emanet etmek, bunlar üzerinde menfaatleri bulunanlar yönünden değişik boyutlarda kaygıların ortaya çıkmasına neden olmaktadır [4]. Bundan dolayı SaaS, PaaS ve IaaS hizmet yapıları, farklı nitelikte güvenlik önlemlerine ihtiyaç duymaktadırlar.

BB'nin hukuki boyutu ile ilgili yayınlar sınırlı sayıda olup, bu konuda mevcut olan az sayıdaki araştırmalar konu hakkında daha fazla çalışma yapılması gerektiğini açıkça ortaya koymaktadır. Subashini ve Kavitha [6], SaaS hizmet yapısında oluşabilecek veri ihlalleri ve uygulama problemlerinin yol açabileceği hukuki sorunlardan, yasal belirsizliklerin hizmet sağlayıcıların hizmet alıcılara sağladığı güvenlik boyutunun ve şeklinin tam anlaşılamadığından bahsetmektedirler. Kerr ve Teng [7] ABD ve Avrupa Birliği hukukunu temel alarak, özel hukuk hükümleri kapsamında, BB sözleşmelerine uygulanabilecek sözleşmeden doğan sorumluluk ve hakları kısaca incelemekte, hizmet seviyesi anlaşmalarında açık olmayan hukukî ve ahlakî konulara değinmektedirler. Çalışmalarının sonucu olarak, sözleşme ve hizmet seviyesi anlaşmalarının tek tip olmamasından dolayı, BB hizmeti alanların, sözleşme yükümlülük zincirinde BB hizmet sağlayıcılarının ve diğer tedarikçilerin ne kadar sorumluluk üstlendikleri doğrultusunda riske maruz kaldıklarını belirtmektedirler. Yazarlara [7] göre BB hizmet sağlayıcıları, sözleşme ve hizmet seviyesi anlaşmalarında üstün konumda oldukları için, büyük işletmeler gibi pazarlık gücü olmayan KOBİ'lerin yapılacak sözleşmelerde dezavantajlı konumda olacaklarını iddia etmektedirler. İsviçre Mühendislik Bilimleri Akademisi tarafından yayınlanmış olan 2012 tarihli raporda [8], İsviçre kanunları çerçevesinde BB incelenmekte, BB sözleşmeleri ile ilgili hukukî konuların sistematik bir şekilde, hizmet yapısına, dağıtım modeline ve emanet edilmiş bilginin nitelikleri gibi noktalara odaklanan özelleştirilmiş bir bakış açısı ile ele alınması gerektiği belirtilmektedir. Yazarlar [8] yapılan sözleşmelerin "*müzakereye kapalı yığın standart şartlar*" olduğunu, ancak belli bir işlem hacminin üstünde olan sözleşmelerde hizmet alanların özelleştirilmiş maddeler isteyebildiklerinden bahsedip, yasal düzenlemelerin BB hizmet alıcılarını koruyacak nitelikte olması gerektiğine değinmektedirler. Bu çalışmalar haricinde Avustralya hükümeti Bilgi Yönetim Ofisi'nin 2013 yılında yayımlamış olduğu raporda [9], BB ile ilgili hukuki konular bilginin saklanması ve mahremiyeti, yasal yükümlülükler, performans yönetimi, sözleşmenin sonlandırılması ve ihtilaf çözümleme ana başlıkları altında incelenmekte, taraflar arasında yapılacak olan sözleşmelerin önemine özellikle değinilmektedir.

Bu çalışmada, hizmet sağlayıcılar ile kullanıcılar arasındaki hukukî ilişki, konularına göre değerlendirilmektedir. Bu yaklaşımda, faaliyetin kapsamının çoğunlukla bir ülke ile sınırlı olmaması, daha doğru bir ifade ile faaliyet alanı sınırlarının coğrafi yönden tam olarak tanımlanamaması etkili olmuştur. Bu durumda taraflar arasındaki sözleşmeye uygulanacak hukukun belirlenmesi önem taşımaktadır. Öte yandan taraflar arasındaki sözleşmenin hukukî niteliğinin belirlenmesi, klasik sözleşme tiplerinin unsurlarına tam olarak uymadığı için, sorun yaratabilmektedir. Farklı BB hizmet yapıları göz önünde tutulduğunda ise, birden çok sözleşmenin veya birden çok sözleşme tipine ait özelliklerin, taraflar arasında var olduğu gözlemlenmektedir.

BB ilişkisi, taraflar arasında yapılan bir sözleşmeye dayanır. Her sözleşmede olduğu gibi, BB sözleşmeleri de geçerlilik şartları yerine getirilerek kurulmalıdır. BB yapısı gereği belirli bir süre için varlığını sürdürür ve genellikle sürekli borç ilişkisi niteliğindedir. Bu yüzden tarafların sözleşmeden kaynaklanan somut borçları dışında, hukuk anlamında "iyiniyetli" olmaları, dürüstlük kuralına uygun davranmaları yasal bir yükümlülüktür, bu yükümlülük özellikle sözleşme ile açıkça düzenlenmeyen konularda önem taşımaktadır. Yine, sözleşmenin sona ermesinde tarafların durumu, özellikle saklanan verilerin iadesi borcunda olduğu gibi, maddi mallardan tamamen farklı bir yapı göstermektedir. 1 Temmuz 2012 tarihinde yürürlüğe giren Türk Borçlar Kanunu (TBK) [10] ve Türk Ticaret Kanunu (TTK) [11], BB sözleşmelerine de uygulanabilecek önemli kurallara yer vermiştir.

Bildirinin ikinci bölümünde, BB sözleşmelerinin yapılması aşamasında karşılaşılan hukukî sorunlar ele alınmakta ve temel özellikleri ile incelenmektedir. Üçüncü bölümde BB sözleşmelerinin hukukî niteliği ve uygulanması aşamasında ortaya çıkan hukukî sorunlara, dördüncü bölümde ise sözleşmenin sona ermesi aşamasındaki sorunlara değinilmektedir. Beşinci bölümde BB sözleşmelerine hangi hukukun uygulanacağı konusu tartışılmaktadır. Son bölümde çalışmada varılmış olan sonuçlar bir bütün olarak değerlendirilmektedir.

II. BB SÖZLEŞMESİNİN YAPILMASI AŞAMASINDAKİ HUKUKİ SORUNLAR

Sözleşme özgürlüğü ilkesi uyarınca, sözleşmenin içeriğini ve süresini taraflar istedikleri gibi belirleyebilirler. Şekil yönünden ise, ancak Kanunda öngörülen şekle uyulmamasının yaptırımı "kesin hükümsüzlük"tür (TBK.m.12) [10]. BB sözleşmesi ise kanunla özel olarak düzenlenmemiştir, teknolojik olarak "katmanlardan oluşan bir hizmet yapısı" özelliği göstermesine karşılık, salt "hizmet sözleşmesi" olarak da nitelendirilemez. Birden çok sözleşmenin unsurlarını taşıyan, kendine özgü yapısı olan bir hukukî ilişki olduğu ifade edilebilir. Yazılı olarak yapılan sözleşmede imza öncelikle el yazısı ile atılan imzadır, yani "ıslak imza"dır. Öte yandan, "güvenli elektronik imza", el yazısı ile atılmış imzanın bütün hukukî sonuçlarını doğurur (TBK.m.15) [10] (EİK) [12]. Bir sözleşmenin geçerli olarak kurulması yanında, sözleşmeden kaynaklanan bir hakkın ispat edilmesi de büyük önem taşır. Bu yüzden, yasal zorunluluk olmasa bile, BB sözleşmesinin yazılı olarak yapılması, basiretli bir davranıştır ve kanaatimizce özen yükümlülüğünün yerine getirilmiş sayılabilmesi açısından önemlidir [13]. Sözleşmenin yazılı olarak yapılması şartıyla, sözleşme ile ilgili belgeler elektronik ortamda saklanabilir. Elektronik ortamdaki veriler Hukuk Muhakemeleri Kanunu (HMK) anlamında "Belge"dir. Her belge "senet" niteliğinde olmamakla birlikte, hakların ispatı yönünden önem taşımaktadır [13, 14].

Ancak özellikle BB sözleşmelerinde, başlangıçtaki çerçeve anlaşma dışında kalan çok sayıda sözleşmenin elektronik ortamda, sadece "kabul et (accept)" tuşuna tıklayarak yapıldığı bir gerçektir. İşte bu noktada, yeni

yasalar açısından iki temel sorun ortaya çıkmaktadır:

a) Çoğunlukla hizmet sağlayıcının önceden hazırladığı, tıklama aşamasında fiilen okunup anlaşılma imkânı bulunmayan metinler, çerçeve sözleşmenin bir parçasını oluştururlar mı?
b) İlk soruya "evet" denebilirse, bu metinlerde yazan şartlar, karşılıklı olarak görüşülüp kabul edilmeden, mutlak olarak kullanıcıları bağlar mı?

Yeni kanunlarda "genel işlem koşulları" olarak nitelendirilen sözleşme hükümleri ile ilgili olarak özel denetim kuralları getirilmiştir [15, 16, 17]. Denetim süzgecinden geçemeyen hükümler "***yazılmamış***" sayılır (TBK.m.21) [10]. BB sözleşmesinin niteliğine yabancı şartlara aynı yaptırım uygulanır. Ayrıca, bu tür sözleşme şartları, düzenleyenin (hizmet sağlayıcının) aleyhine, kullanıcıların lehine yorumlanır. Türk hukuku yönünden, bu kuralların, her iki tarafı tacir olan sözleşmelerde de uygulanacağı kabul edilmektedir. Hatta ticaret hukukunda, dürüstlük kuralına aykırı işlem şartları kullanılması, haksız rekabet halleri arasında sayılmıştır (TTK.m.55) [11].

BB işlemlerinde çok sayıda, "model sözleşme" adı altında önceden hazırlanmış işlem şartları kullanılmaktadır. Örnek olarak "Office 365" uygulamasında, bu hükümler firmanın internet sitesinde önceden ilan edilmektedir. Her ülkenin dilinde sözleşmeler bulunmaktadır, ancak ayrıntılara ulaşılmak istendiğinde çoğunlukla bu durum değişmekte, farklı dilde ve farklı ülke hukukuna göre hazırlanmış (İngilizce, ABD hukuku) metinlere ulaşılmaktadır. Model sözleşmeler daha sonra, fiilen tek taraflı olarak değiştirilebilmektedir. Buna örnek olarak da, Microsoft hizmet sağlayıcısının 2011 yılı sonunda, sözleşme şartlarını yenilediğine, şartları Avrupa Birliği normlarına uygun duruma getirdiğine ilişkin duyurusu gösterilebilir. Ancak önemle belirtilmelidir ki, sadece duyuru ile, yeni sözleşme imzalanmadan, bu şartlar sözleşme içeriğine girmiş olmaz. Ancak, kullanıcının hizmet sağlanması talebi karşısında, kabul ettiğine ilişkin bir kutucuğu tıklatması istenerek amaca ulaşılırsa, bunun geçerliliği tartışılmalı olacak, hizmetten yararlanan aleyhindeki değişikliklerin "yazılmamış" sayılması gerektiği, yani sözleşme içeriği kapsamında olmadığı ileri sürebilecektir.

Avrupa Birliği BB stratejisinde "Güvenli ve adil sözleşme şartları" hazırlanması öngörülmektedir [18]. Bu strateji kapsamında, genel işlem şartlarının BB sözleşmesinde kullanılmasına karşı çıkılmamakta, ancak bu şartların belirli içerikte olması ve taraflar arasındaki menfaat dengesini gerçekleştirebilmesinin sağlanması amaçlanmaktadır. Bu kapsamda özellikle şu hususların düzenlenmesi öngörülmüştür [18]:

- Sözleşmenin sona ermesi aşamasında verilerin korunması,
- Verilerin gizliliği ve bütünlüğü,
- Veri yeri ve transferi,
- Veri mülkiyeti
- BB sağlayıcısı ve alt hizmet sağlayıcılar arasında doğrudan doğruya ve dolaylı sorumluluk ilişkisinin belirlenmesi.

III. BB Sözleşmesinin Hukukî Niteliği ve Uygulanması Aşamasında Ortaya Çıkan Hukukî Sorunlar

BB sözleşmesinin konusu çoğunlukla, sadece verilerin saklanabileceği ve istenildiğinde ulaşılabilecek elektronik bir ortam sağlamakla sınırlı kalmamaktadır. Bu durumda öncelikle, uygulanacak kurallar yönünden sözleşmenin niteliğinin belirlenmesi önem taşımaktadır.

BB sözleşmesi, borçlar hukuku açısından, taraflarını "hizmet sağlayıcı" ve "kullanıcı"nın oluşturduğu bir hukukî ilişkidir. Uluslararası alanda faaliyet gösteren hizmet sağlayıcılara örnek olarak "Apple", "iWork", "Google", "Microsoft", "Salesforce", "Amazon" ve "Zoho" gösterilebilir. Sözleşmenin konusunu oluşturan işgörme edimi, sanallaştırılmış verilerin işlenmeye hazır olarak saklanması faaliyetine dayanmaktadır. Verilerin tevdi edildiği yer kesin olarak belirlenemez veya ifade edilmez, tam olarak bilinmesi veri güvenliği açısından doğru da değildir; bu yüzden soyut bir kavram olarak "bulut" (cloud) terimi ile ifade edilmiştir. "Bulut" terimi, sözleşmenin uygulama alanı olarak coğrafi sınırların öneminin (fiilen) kalmadığını da ifade etmektedir. Aslında, verileri saklamaya ve işlemeye uygun, donanımın ön planda olduğu bir altyapı, vazgeçilmez bir unsur niteliğindedir. Ancak verilerin dinamik olarak dağıtıldığı mantıksal bir yapının varlığı nedeniyle, sözleşmenin tarafları, verilerin hangi cihazda saklandığını ve işlendiğini tam olarak bilemezler. Bu yüzden kullanıcının borcu olan ve kural olarak düzenli aralıklarla ödenen "ücret" bir cihazın kira bedelinden çok, hizmet sağlayıcının işgörme ediminin karşılığını oluşturmaktadır.

"***Genel saklama sözleşmesi***" bir taşınırın güvenli bir yerde korunmasının üstlenildiği sözleşmedir (TBK m.561) [10]. Taşınır kavramı, saklanan verileri kapsayacak şekilde yorumlansa bile, tek başına BB sözleşmesinin özelliklerini karşılayamayacaktır. Çünkü BB kapsamında donanım, yazılım, bakım ve çeşitli hizmetleri kapsayan edimler topluluğu bulunmaktadır. Bu konuda Alman hukukunda bir olayda [19] "kira sözleşmesi" hükümlerinin uygulanması gerektiği yönünde karar verilmiştir. Eser (yapıt) ve vekâlet sözleşmeleri de BB kapsamı içerisinde yer alabilir, genellikle işgörme sözleşmelerine ait unsurların ağırlıkta olduğu ifade edilebilir. Bu durumda, birden fazla sözleşmenin veya birden fazla sözleşmeye ait unsurların BB ilişkisinde tarafların iradesi ile bir araya getirilmesi söz konusu olacaktır. Böylece, "birleşik" veya "karma" sözleşme niteliğindeki hukukî ilişkilere özgü, kolay olmayan çözüm yolları aranacaktır [20]. Örnek olarak, işgörenin "özen ve sadakat borcu"nun kapsamı ve ağırlığı; sözleşmenin hizmet, eser veya genel vekâlet sözleşmesi hükümlerinin uygulanması ihtimallerinde farklı olacaktır. Yine BB sözleşmelerinde çok sayıda bulunan ve hizmet sağlayıcının sorumluluğunu kaldıran veya sınırlandıran "sorumsuzluk anlaşmaları" yeni kurallar karşısında geçersiz (hükümsüz) sayılabilecektir (TBK m.115, m.116) [10].

Genel saklama sözleşmesine ilişkin klasik hukuk ilkelerinin, bilişim ortamında da uygulanabilecek evrensel kurallar olduğu, yaklaşık bir asır önce yazılmış bir eserde görülebilir: "Emanet sözleşmesinin konusu, emanet alan tarafından korumanın üstlenilmesidir. Koruma, sadece fiilen elde tutmadan daha fazlasını ifade eder. Koruma, diğer sözleşmelerle de birleşmiş olabilir. Koruma için ödevin

içeriği, her şeyden önce anlaşmaya göre belirlenir. Güven işi olmasının niteliğinden bir sır saklama ödevi doğabilir" [21]. BB sözleşmesinde yer alan, verilerin saklanması ile bağlantılı işgörme borcu ile ilgili sonuçlar alt başlıklarla incelenmiştir:

A. Haksız Rekabet Hukuku

Haksız rekabet hükümlerinin amacı bütün katılanların menfaatine, dürüst ve bozulmamış rekabetin sağlanmasıdır. Özellikle rakipler arasında veya tedarik edenlerle müşteriler arasındaki ilişkileri etkileyen aldatıcı veya dürüstlük kuralına diğer şekillerdeki aykırı davranışlar ile ticari uygulamalar haksız ve hukuka aykırıdır (TTK.m.54) [11].

Bu kapsamda, BB hizmeti sağlayan yönünden, "kendisine emanet edilmiş teklif, hesap veya plan gibi iş ürünlerinden yetkisiz yararlanmak", sözleşme kapsamındaki sorumluluğunun dışında, ayrı ve ağır bir sorumluluk doğurmaktadır (TTK. m.55) [11].

B. Kişisel Verilerin Korunması, Veri Güvenliği ve Şeffaflık

BB sözleşmesi kapsamında saklanılan verilerin güvenliği konusu, bu alandaki temel sorunlardan birisidir. Veri güvenliği; taraflar arasındaki sözleşme hükümleri dışında, özellikle kişisel verilerin korunmasına ilişkin hukukî düzenlemelerle de sağlanmaya çalışılmaktadır [22]. Ancak, özellikle verilerin saklandığı yer ve devletlerin ulusal güvenlik kaygıları göz önüne alındığında, mutlak bir korumanın bulunduğunu söylemek mümkün değildir. Bu noktada ise, hizmet sağlayıcıların ve alt hizmet sağlayıcıların birlikte sorumlulukları da söz konusu olacaktır.

Avrupa Birliği'nde bu konudaki temel düzenleme, gerçek kişilerin korunmasına yönelik olarak kişisel verilerin işlenmesi konusunda 1995 yılında çıkarılmış olan direktiftir [23]. Avrupa Komisyonu, 2012'de Avrupa'da BB potansiyelinin kullanılmasına yönelik bir strateji kabul etmiş ve ilkeleri belirlemiştir [24]. Ancak AB yönünden güncel sorunlardan birisi, özellikle ABD kaynaklı BB hizmet sağlayıcılar bünyesindeki verilere, ABD makamlarının ulaşabilmesi imkânıdır. AB düzenlemesine göre, üye ülkelerde yapılan BB sözleşmelerinde, sadece fiziksel olarak topluluk sınırları içerisinde bulunan teknik altyapı kullanılabilecektir, sınıraşan veri trafiği konusunda özel hükümler ve izin süreci öngörülmüştür. Bu konuda temel ölçüt, üçüncü ülkenin öngörülen teknik düzeye ulaşmış olmasıdır, sertifika tek başına yeterli değildir. Örneğin, BB hizmet sağlayıcısının ABD "Safe Harbor" sertifikasına [25] sahip olması tek başına sınıraşan veri trafiğini içeren sözleşmeleri yapabilmesi için yeterli olmayıp, ek denetim de gereklidir [26]. Ancak özellikle ABD açısından, belirli şartların varlığı halinde BB'de bulunan verileri izleyebilme imkânını tanıyan "Patriot Act" göz önünde tutulmalıdır [27]. "Patriot Act" uygulaması nedeniyle, merkezi ABD'de bulunan hiçbir hizmet sağlayıcısının, BB ortamındaki verilerin ulusal güvenlik kurumlarının denetimine tâbi olmayacağı garantisini veremeyeceği ifade edilmiştir [28]. 2013 Haziran ayında ortaya çıkan NSA gözetim programlarının varlığı, bu görüşün doğruluğunu ortaya koymuş, sektör bu nedenle önemli ekonomik zarara uğramıştır. Bu konu, Alman Parlamentosunda, 31.01.2013 tarihli soru önergesi ile açıklıkla ortaya konulmuş ve yedi sayfa tutan ayrıntılı sorularla problemin ulaştığı boyut sergilenmiş, ancak doyurucu cevaplar verilememiştir [29].

Hizmet sağlayıcıların, kullanıcılara şeffaflık yönünden maddi ve hukuki güvenlik sistemleri ile ilgili olarak ayrıntılı bilgi vermeleri gereklidir, soyut nitelikteki güvence yeterli değildir. Bu konuda kullanıcılara tanınacak denetim hakkının fiilen uygulanabilmesi ise çok zordur.

Türkiye'de 2008 yılında TBMM'ne sunulan ve Avrupa Birliği düzenlemelerinden esinlenen ***"Kişisel Verilerin Korunması Hakkında Kanun Tasarısı"*** bugüne kadar kanunlaşamamıştır. Yine 2008 yılında TBMM'ne sunulan "***Ticarî Sır, Banka Sırrı ve Müşteri Sırrı Hakkındaki Kanun Tasarısı***" kanunlaşmayı beklemektedir. 2010 yılında TBMM'ne sunulan "***Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı***" ise Genel Kurul gündemindedir, Tasarının 10. Maddesi ile "*Kişisel verilerin korunmasını*" aşağıda verildiği üzere kapsamlı bir şekilde düzenlenmektedir:

"Hizmet sağlayıcı;
a) Bu Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanmasından ve güvenliğinden sorumludur.
b) Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz"

Kişisel sağlık verileri ile ilgili olarak, "*Genel Sağlık Sigortası Verilerinin Güvenliği ve Paylaşımına İlişkin Yönetmelik*" 11.07.2012 tarihli Resmî Gazete'de yayımlanmıştır.

C. BB Sözleşmesinde Riziko Yönetimi ve Sorumluluk

Sistemin çökmesi veya performans kayıpları, sistemin yavaşlaması, erişilebilirlik, kalıcı nitelikteki veri kayıpları, verilerin değiştirilmesi, silinmesi veya çalınması; BB ortamında ortaya çıkabilecek risklerdir. Özel bir yasal düzenleme bulunmadığından, bu hususların sözleşme ile düzenlenmesinde yarar hatta zorunluluk bulunduğu ifade edilebilir. Riziko yönetiminde, maruz kalınabilecek tehlikeler için sigorta sözleşmesi yapılmasının önemli bir yeri vardır, sorumluluk sigortaları konusunda yeni Ticaret Kanunu'nda özel düzenlemeler getirilmiştir (TTK. m.1472 vd.) [11].

Riziko yönetimi ile ilgili olarak, hizmet sağlayıcısının sorumluluğunu sınırlandıran veya tamamen kaldıran sözleşme şartları çoğunluktadır. Ancak belirtilmelidir ki, yeni kurallar karşısında hizmet sağlayıcısının veya onun alt hizmet sağlayıcılarının fiillerinden doğan ve kusura dayanan sorumluluğu kaldıran hükümler ilke olarak geçersiz olacaktır (TBK. m.115, m.116) [10]. Örnek olarak, sistemin "hafif kusur" niteliğindeki bir davranış nedeniyle çökmesi halinde, hizmet sağlayıcısının sorumlu olmayacağına ilişkin şart geçerli olmayacaktır.

D. Şirketler Hukuku Yönünden Ortaya Çıkabilecek Hukukî Sorunlar

TTK, anonim şirket ve limited şirket yöneticileri yönünden "özen ve bağlılık yükümlülüğü" getirmiştir. Yöneticiler, görevlerini tedbirli bir yöneticinin özeniyle yerine getirmekle ve şirketin menfaatlerini dürüstlük kuralına uyarak gözetmekle yükümlüdürler (TTK. m.369, m.626) [11]. Bu özenin ölçüsü, tedbirli bir yöneticinin

göstermesi gereken özendir. Tedbirli yönetici ölçüsü, yönetim kurulu üyelerinin kurumsal yönetim ilkeleri kapsamında *"işadamı kararı"* niteliğinde karar alabilmeleri imkânını tanır. Buna göre, belirli bir konuda karar alınmadan önce, konunun uzmanlarının birikimlerimden yararlanılmış, yeterince araştırma ve değerlendirme yapılmışsa; alınan kararın şirket için belirli riskler taşıması halinde bile, özen yükümlülüğü ihlâl edilmiş sayılmayacaktır. Ancak bunun için kişisel ve yabancı menfaatler ön planda tutulmamalı, şirketin menfaatinin gözetilmesi asıl olmalıdır [30].

Bu durumda, şirket sırlarını içeren verilerin, çoğunlukla başka ülkelerde bulunması, özensiz ve şirket menfaatlerine aykırı bir davranış sayılabilecek midir? Şirketin işletme konusuna uygun olarak aynı anda farklı yerlerde faaliyetini sürdürmesi ihtiyacı karşısında, hızlı ve şirket verilerine ulaşılarak karar alma ihtiyacının karşılanması amacıyla BB sözleşmesi yapılmış olması, işadamı kararı kapsamında değerlendirilebilir Böylelikle şirket, yüksek maliyetli donanım, yazılım ve güncelleme gerektiren bir alanda kendi çözümlerini aramaktan kurtulabilecektir. Bu noktada işaret edilmesi gereken bir husus da, TTK'nun 361. maddesinde [11] yer verilen, yönetim kurulu üyelerinin sorumluluklarının sigortalanması hükmünün hayata geçirilmesinin, yöneticiler için basiretli bir davranış olacağı olgusudur.

Yeni TTK ***anonim şirketlerin denetimi*** konusunda da yeni bir sistem getirmiş, dış denetim ilkesini benimsemiştir. TTK'nun 401. maddesi [11] hükmüne göre; "*Denetçi, yönetim kurulundan, kanuna uygun ve özenli bir denetim için gerekli olan bütün bilgilerin kendisine verilmesini ve dayanak oluşturabilecek belgeleri sunmasını ister*". Bu durumda denetçilere, BB kapsamındaki "denetim için gerekli olan" verilere ulaşabilme yetkisinin verilmesi gerekecektir. Sadece yönetim kurulunun verdiği bilgi ve belgelerle yetinmek doğru olmayacaktır. Ama bu yetki, denetim dışındaki hususları kapsamayacaktır. Bu sınırın belirlenmesi büyük bir önem taşımaktadır.

IV. BB SÖZLEŞMESİNİN SONA ERME AŞAMASINDAKİ HUKUKİ SORUNLAR

BB kullanıcısı, çeşitli nedenlerle sözleşmeyi sona erdirmek isteyebilir: Kendisi daha güvenilir ve daha hızlı bir veri saklama ve işleme altyapısı kurabilir veya daha güçlü ve daha uygun şartlarla hizmet sunan bir hizmet sağlayıcı ile sözleşme yapmak isteyebilir.

Borçlar hukukunda *saklananın geri verilmesi* genel olarak düzenlenmiştir; sözleşmede süre belirlenmişse bu sürenin sonunda, sözleşmede bir süre belirlenmemiş olsa bile kullanıcının talebi üzerine, verilerin geri verilmesini istenebilir (TBK. m.564) [10]. BB sözleşmelerinde "geri verme" özel bir önem taşımaktadır; verilerin iadesi yanı sıra saklanan verilerin, sözleşmenin sona ermesinden sonra silinmesi de teminat altına alınmalıdır. Avrupa Birliği BB stratejisinde de [18], adil ve güvenli sözleşme şartları kapsamında, sözleşmenin sona ermesi aşamasında verilerin korunmasına özel bir önem verilmiştir. Özellikle ortak kaynakların, yazılımların ve veritabanının da hizmet edimi kapsamında olduğu SaaS yapısında, verilerin iadesinden sonra, yazılım desteği de sona ereceğinden; hizmet kullanıcısının kendi verilerini kullanamama, bilişim ortamında görüntüleyememe, işleyememe rizikosu ortaya çıkacaktır. BB sözleşmesi yapılırken, sözleşmenin bitiminde mevcut verilerin en azından görüntülenebilmesi, yeni dosyalar oluşturulmasa bile, bunların değiştirilebilmesi imkânını sağlayacak şartların sözleşmeye konulmasının sağlanması, kanaatimizce işletme açısından ihmal edilmemesi gereken bir husustur. Öte yandan, verilerin sözleşme süresinin bitmesinden sonra başka bir hizmet sağlayıcı platformunda saklanabilecek ve işlenebilecek formatta teslim edilmesine ilişkin düzenlemeler de sözleşmenin kurulması aşamasında yapılmalıdır.

V. BB SÖZLEŞMELERİNE UYGULANACAK HUKUK

Yabancılık unsuru taşıyan özel hukuka ilişkin işlemlere uygulanacak hukuk, 5718 sayılı "Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun" [31] ile düzenlenmiştir. Bu Kanun'un 24. maddesi uyarınca, sözleşmeden doğan borç ilişkileri tarafların açık olarak seçtikleri hukuka tâbidir, hukuk seçimi taraflarca her zaman yapılabilir; yeter ki kamu düzenine aykırı olmasın.

BB sözleşmelerinde, özellikle verilerin saklandığı yer unsuru, kendine özgü bir yapıdadır. Farklı coğrafi bölgelerde bulunan kişilerin verilere her zaman ulaşabilmesi gerekli olduğundan, birden fazla yer, yabancı unsur olarak ortaya çıkabilir. Örnek olarak, "Office 365" uygulamasında, Ortadoğu'da bulunan kullanıcılara ilişkin veri merkezlerinin, öncelikli olarak Hollanda ve İrlanda olduğu belirtilmektedir, yedekleme veri merkezi ise çoğunlukla ABD'de bulunmaktadır. Somut bir olayda, zarar gören verinin % 20'sinin Fransa'da, % 30'unun Arjantin'de ve % 50'sinin ise Yunanistan'da saklandığı ortaya çıkmıştır [22]. Görüldüğü gibi, BB ilişkilerin, yer yönünden somut bir bağlama noktasından bağımsız olması, bir başka ifade ile veri bulutlarının sınıraşan biçimde hareket etmesi karşısında, kanunlar ihtilâfı sorunları ortaya çıkmaktadır. BB sözleşmesinden kaynaklanan bir uyuşmazlığın, hangi devlet kuralları uygulanarak çözülmesi gerektiğinin belirlenmesi güçleşecektir. Bu yüzden sözleşme ile uygulanacak hukukun kararlaştırılması önem taşımaktadır.

"Bulut" ortamında verilerin özellikle hizmet sağlayıcı dışındaki kişilerin fiilleri ile zarar görmesi veya yok olması halinde ise, uygulanacak haksız fiil hukukunun tespiti gerekmektedir. 5718 sayılı Kanun'un 34. maddesi uyarınca [31], haksız fiilden doğan borçlar haksız fiilin işlendiği ülke hukukuna tâbidir. Haksız fiilin işlendiği yer ile zararın meydana geldiği yerin farklı ülkeler olması durumunda, zararın meydana geldiği ülke hukuku uygulanır. Kanunda, belirtilen objektif bağlama kuralının katılığını giderecek bir istisna hükmüne (escape clause) de yer verilmiştir [32, 22]. Buna göre, haksız fiilden doğan borç ilişkisinin başka bir ülke ile daha sıkı ilişkili olması halinde bu ülke hukuku uygulanacaktır. Öte yandan taraflar, haksız fiilin meydana gelmesinden sonra, uygulanacak hukuku açık olarak seçebilme imkânına da sahiptirler.

VI. SONUÇ

Bu çalışmada, BB sözleşmesi kapsamında ortaya çıkabilecek hukukî sorunlar, ana başlıklar halinde ve ancak temel çözümler üretilmeye çalışılarak incelenebilmiş ve aşağıdaki sonuçlara ulaşılmıştır:

1- BB'in hukukî boyutu konusundaki çalışmalar yetersizdir ve geliştirilmesi gerekmektedir.
2- BB sözleşmeleri "model sözleşme" olarak yapılmaktadır. Bunun yasadaki karşılığı "genel işlem koşulları"dır, kısa süre önce yürürlüğe giren kurallarla önemli düzenlemeler getirilmiştir. Bu kapsamda, özellikle hizmet sağlayıcıların sorumluluklarını kaldıran veya sınırlandıran şartların geçersiz sayılması söz konusu olacaktır.
3- BB sözleşmeleri, tek tip değildir, bu yüzden çok sayıda sözleşmeye özgü unsurları içermektedir (Saklama, hizmet, kira, eser, vekâlet, vb.). Hâkim olan sözleşme türüne göre, tarafların hak ve yükümlülükleri, bu arada "sadakat ve özen borcu"ndan doğan sorumluluklarının kapsamı değişecektir.
4- Kişisel verilerin korunması ve veri güvenliği, BB sözleşmesinin temelini oluşturmaktadır. Bu konuda gerek uluslararası alanda gerekse iç hukukta düzenleme boşlukları vardır. Öte yandan, var olan kuralların uygulanması ve yorumlanması da, hizmet sağlayıcıların sorumluluklarını artırıcı sonuçlar doğurmaktadır.
5- BB sözleşmesinin sona ermesi aşamasında, BB ortamındaki verilerin daha sonra da kullanılabilecek formatta geri verilmesinin sağlanması, büyük önem taşımaktadır.
6- BB sözleşmesi kapsamındaki verilerin saklandığı yerin, bilişim teknolojisinin gereği olarak, somut ve tek bir nokta olarak belirlenememesi karşısında, uyuşmazlık halinde uygulanacak devlet hukukunun, sözleşmenin kurulması aşamasında geçerli olacak biçimde, taraflarca belirlenmesi büyük önem taşımaktadır.

KAYNAKLAR

[1] J. Bughin, M. Chui ve J. Manyika, "Clouds, big data, and smart assets: Ten tech-enabled business trends to watch," *McKinsey Quarterly*, cilt 56, sayı 1, s. 75-86, 2010.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, L. Gunho, D. A. Patterson, A. Rabkin, I. Stoica ve M. Zaharia, "A view of cloud computing," *Communications of the ACM*, cilt 53, sayı 4, s. 50-58, 2010.

[3] X. Xu, "From cloud computing to cloud manufacturing," *Robotics and computer-integrated manufacturing*, cilt 28, sayı 1, s. 75-86, 2012.

[4] B. P. Rimal, A. Jukan, D. Katsaros ve Y. Goeleven, "Architectural requirements for cloud computing systems: an enterprise cloud approach," *Journal of Grid Computing*, cilt 9, sayı 1, s. 3-26, 2011.

[5] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger ve D. Leaf, "NIST cloud computing reference architecture," *NIST special publication*, cilt 500, sayı 292, 2011.

[6] S. Subashini ve V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, cilt 34, sayı 1, s. 1-11, 2011.

[7] J. Kerr ve K. Teng, "Cloud computing: legal and privacy issues," *Proceedings of the Academy of Business Disciplines Conference*, 2010.

[8] O. Brian vd., "Cloud Computing - White Paper," Swiss Academy of Engineering Sciences, Zürich, 2012.

[9] "Negotiating the cloud- legal issues in cloud computing agreements," Australian Government - Information Management Office, 2013.

[10] "Türk Borçlar Kanunu," 11 Ocak 2011. Çevrimiçi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6098.pdf.

[11] "Türk Ticaret Kanunu," 13 Ocak 2011. Çevrimiçi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6102.pdf.

[12] "Elektronik İmza Kanunu," 23 Ocak 2004. Çevrimiçi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf.

[13] E. Yılmaz, Hukuk Muhakemeleri Kanunu Şerhi, Ankara, 2012.

[14] "Hukuk Muhakemeleri Kanunu," 4 Şubat 2011. Çevrimiçi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6100.pdf.

[15] F. Eren, Borçlar Hukuku (Genel Hükümler), Ankara, 2012, s. 215-223.

[16] G. Antalya, Borçlar Hukuku (Genel Hükümler), İstanbul, 2012, s. 285-343.

[17] Y. Atamer, Sözleşme Özgürlüğünün Sınırlandırılması Sorunu Çerçevesinde Genel İşlem Şartlarının Denetlenmesi, İstanbul, 1999.

[18] "European Cloud Computing Strategy," Çevrimiçi: https://ec.europa.eu/digital-agenda/. 14.7.2013 tarihinde erişilmiştir.

[19] "Der Bundesgerichtshof, XII ZR 120/04," 15 11 2006. Çevrimiçi: http://www.bundesgerichtshof.de/EN/Home/home_node.html.

[20] C. Yavuz, Borçlar Hukuku Dersleri (Özel Hükümler), İstanbul, 2012, s. 11-13.

[21] H. Becker, İsviçre Borçlar Kanunu Şerhi, Bern, 1934.

[22] A. Leupold ve S. Glosner, IT-Recht, Münchener Anwalts Handbuch, 2 dü., München, 2011, s. 97.

[23] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Official Journal L 281, 23/11/1995.

[24] "Unleashing the Potential of Cloud Computing in Europe, Text with EEA relevance SWD-2012-271 Final," 2012.

[25] "Main Safe Harbor Page," Çevrimiçi: http://www.export.gov/safeharbor/ 15.7.2013 tarihinde erişilmiştir.

[26] M. Borgmann, T. Hahn, M. Herfert, T. Kunz, M. Richter, U. Viebeg ve S. Vowe, On the Security of Cloud Storage Services, Darmstadt: Fraunhofer Institute for Secure, 2012.

[27] J. Billings, "European protectionism in cloud computing: addressing concerns over the Patriot Act," *CommLaw*, cilt 21, s. 211, 2012.

[28] Z. Wittaker, "Microsoft admits Patriot Act can access EU-based cloud data," 28 6 2011. Çevrimiçi: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225. 1.7.2013 tarihinde erişilmiştir.

[29] "Deutscher Bundestag, 17. Wahlperiode, 17/12259 Sicherheit, Datenschutz und Überwachung von Cloud-Daten," 2013.

[30] F. Bilgili ve E. Demirkapı, Şirketler Hukuku, Bursa, 2013.

[31] "Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun," 12 Aralık 2007. Çevrimiçi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5718.pdf.

[32] F. B. Tanrıbilir, "Akit dışı Borçlara Uygulanacak Hukuka İlişkin Tüzükte (Roma II) Ürün Sorumluluğu," *Gazi Üniversitesi Hukuk Fakültesi Dergisi,* cilt XIV, sayı. 2, s. 131, 2010.

Mobile Cloud Authentication and Secure Communication

R. Gokaj, M. Ali Aydın, R. Selami Özbey

***Abstract*—The secure communication of today's mobile devices is of high interest because the threats have increased and it is now not easy to handle the billions of devices securely. With the ongoing developments of huge systems being transformed into cloud systems, we have the need to provide an easy to use, simple, flexible and robust mobile client platform to be used in the cloud environments. One of the most important challenges that we face is the way to secure the environment. The first step is to secure the authentication, and after that to secure the application communication and file transfer. Here we present a way, by using nowadays technologies like Mobile Signature, SSL, SOA, SFTP and combine them to provide a complete solution for a mobile cloud environment.**

***Index Terms*—About authentication, cloud, mobile, secure communication.**

I. INTRODUCTION

NOWADAYS, mobile devices are being of high interest because of all the actions they can perform. We can say that nearly all the PC operations have been to transferred to mobile devices. So, basically every daily action previously performed only on our PCs can now be performed in mobile devices.

People always feel the need to have with themselves their personal data on which we can give as an example photos, emails, work files, reminders, calendar, music, etc. In order to make this possible for all people all around everywhere, cloud solutions come up for this. In order to have a brief description for cloud computing, we can tell that this is a group of web solutions which offers services that can be accessed through internet.

Manuscript received September 2, 2013. This work was supported in part by the Istanbul University Scientific Research Projects Department with project number 28489.

R. Gokaj, is with the Computer Engineering , Istanbul University, Istanbul, Turkey (e-mail: redigokaj@gmail.com).

M. Ali Aydın, is with the Computer Engineering , Istanbul University, Istanbul, Turkey (e-mail: aydinali@istanbul.edu.tr).

R. Selami Özbey, is with the TUBITAK-BILGEM-UEKAE, Kocaeli, Turkey (e-mail: selami.ozbey@tubitak.gov.tr).

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Storage as a Service (STaaS)

The one which is part of our concept, related with the mobile devices, is the "Software as a Service". So, a shared software will be running on the cloud and make it possible for all clients to use it in a secure way.

When thinking about a cloud solution for the mobile devices, we refer to the term Mobile Cloud. In fact, this should not be confusing by thinking that the cloud environment will run on the mobile devices. The cloud distributed servers will be used as source when the mobile devices (considered as clients) can be connected and utilize the service or the platform. With mobile devices being part of the cloud environment, confidential data may be by mistake exposed to unauthorized people. This means that a security threat may be part of the system's solution. So a secure cloud environment should offer a reliable connection and operational process when dealing with mobile devices.

II. RELATED WORKS

As an example of current cloud authentications we can see Amazon EC2. It offers a public / private key authentication in order to connect with the server running on Amazon's cloud. Regarding the technical overview of implementing the cloud connections over a mobile device we have got a very detailed explanation in the manuscript "Mobile cloud computing: A survey" [1]. It is stated that limited resources from mobile devices make it obligatory to share common resources among cloud computing. The simplest example with a basic approach would be using the Gmail application on your mobile phone.

- In this case we face may problems like:
- Phishing attacks
- XML signature element wrapping
- Man-in-the-middle attack
- Eavesdropping
- Brower-based authentication weaknesses

These problems are specified in "Considerations for mobile authentication in the Cloud" [2] where general security issues are given as an example. The proposed security checks go deep into the SIM card on which we take guarantee that it is not corrupted or accessed without permission. That's why also in our proposed approach, the SIM card's digital signature operation helps us in the authentication stage.

In order to ensure the identity of a device user, the Digital ID term takes place [3]. In cooperation with the mobile line carrier, the new properties of 128 bit SIM cards are used. A special software runs on that SIM card. This software allows the user to sign information and send it back to the carrier line. Because the card is specially produced by the carrier, the carrier is able to know if the signature is correct or not.

Data theft [4] is another problem which should be considered to be solved inside the server side part of the cloud. Specific file organizations should be done in the part where users' data is stored. In this case, the cloud environment should protect each user's data and not allow unauthorized access.

Authentication modules [5] should be separated and considered as a standalone module which operates independently and securely. This shows the importance of the authentication process over a cloud environment.

By running mobile applications on a cloud [6] some other topics should be considered as very much important.

- Application re-design and deployment
- Network condition and service availability
- Control of applications
- Privacy of data
- Information security

Another approach of securing the authentication is TrustCube [7]. This consists of a collection of SMS and Call history and encrypt them with a hash algorithm. After that, check this data with the previous history stored in the cloud part. In this case, if authentication is done from another device, it would be noticed immediately.

Regarding the commercial applications used for cloud data synchronization we may consider DropBox and Google Drive. Basically, after a username/password authentication, a file sharing service is enabled. This makes possible for you to access your shared files in every device that you have setup with the cloud environment. If we have to specify the service that these two providers offer, we can tell it is STaaS (Storage as a Service).

III. THE PROPOSED METHOD

The main theme can be divided into some specific topics which can later be considered alone. We have to consider:

- Authentication
- Application Communication
- File transfer

As given in Fig. 1, we have the big picture which represents the mechanisms required for the full cycle to be implemented. In the proceeding sections the big picture will be divided in small parts and an explanation will be given for each part.

A. Authentication

1. The user makes a classic authentication with username & password.
2. The server generates a session key SKEY.
3. We need to be sure that this SKEY will be used from our trusted device which has the CA trusted identity.
4. So, Mobile Signature is used to check the session key if it is being used from the real trusted mobile device. This key maybe validated periodically during the mobile-cloud communication.

Part of the authentication mechanism is also the session handling. The provided SKEY will be binded with the session stored in the server for the current connected client. In order to protect the sequence of web service calls, we put a SEQUENCE_NUMBER and initialize it with 1 and after the after each request we increase it by one. If the sequence number's chronology is broken, then the authentication fails and is required to be done again. If in any case SKEY expires or there is a problem with the session, then the server informs the client that authentication should be refreshed and blocks in the server all the operations until the authentication is done again. Here SKEY should not be confused with SSL. The SKEY is only the representative of the client in the server instance.

B. Application Communication

The client will communicate with the server using a basic web service approach. In this case we say that we use SOA (Service Oriented Architecture) platform. In order to secure the communication we need to use SSL in order to encrypt the traffic. HTTPS protocol will be used in the cloud (server side) and the client will be able to connect by using the signed certificates.

C. File transfer

A very good way for file transfer is the SFTP protocol. Secure authentication and transfer take place in this protocol. A public / private key pair is generated from the server and the public one is given to the client. The client then, uses this public key to connect and make the file transfer (while the private key stays only on the server).

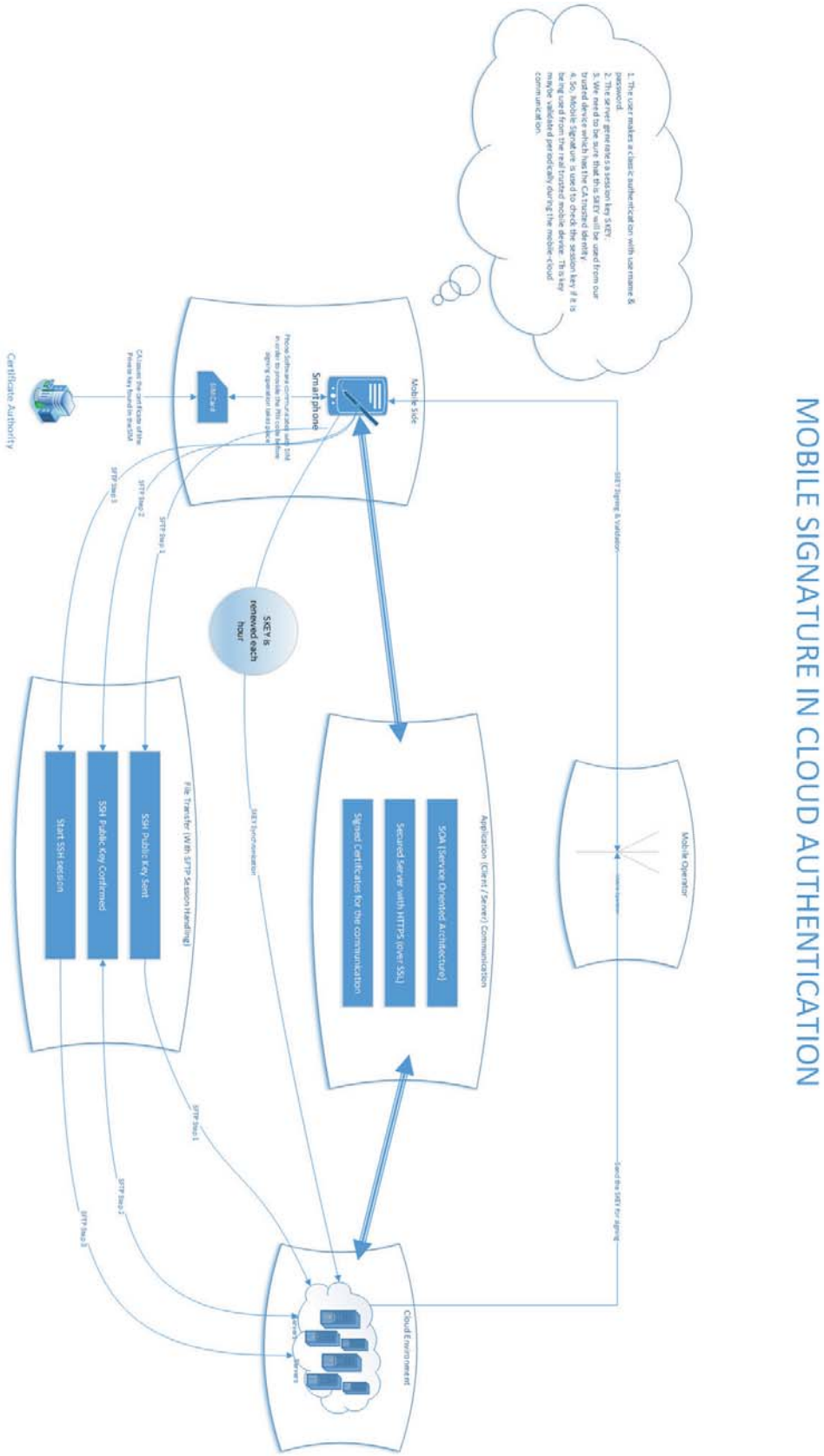


Fig. 1. Securing the authentication and file transfer in the mobile cloud

TABLE I
NOTATIONS

Notation	Explanation
AMO	Authorized mobile operator
MSgReq	Mobile signature request
MSsHash	Mobile signature hash key
SKEY	Session key
SN	Sequence number
WSReq	Webservice request
SSLe	SSL encryption
WSRes	Webservice response
SSs	SSH start session
SP_{KR}	SFTP public key request
SP_{KC}	SFTP private key check
FP	File transfer progress
SSe	SSH session end
MSpin	Mobile signature pin code check

D. Schema explanation

Fig. 1 is the overall system that shows how information travels from the mobile device to the cloud and vice versa.

In Fig. 2, we see the server side application structure. Application communication is done via HTTPS protocol, which has a SSL secured layer with a signed certificate. SOA architecture means a communication with web services. So, our mobile device will call web services found in the server side. Regarding file transfer, SFTP structure is given in the picture. By this way, the file transfer, which is an expensive network operation, will be handled by this protocol.

In the next picture, Fig. 3, we see the mobile phone and the SIM card which does the signature process by using the Digital ID information. The mobile device communicates with the carrier and via internet it communicates also with the

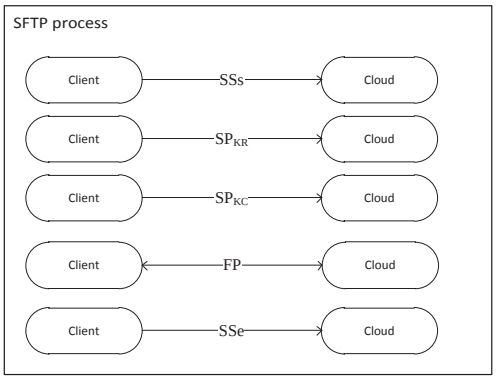


Fig. 4. The SFTP file transfer progress step by step

cloud environment by doing authentication, application access and file transfer. As the SIM Digital Signature is protected by law, it gains an official trust level.

The Fig. 4 shows our cloud environment which is a distributed system of servers that contain the SFTP module. All SFTP steps are described there where it is obvious that file transfer is totally independent from the application module.

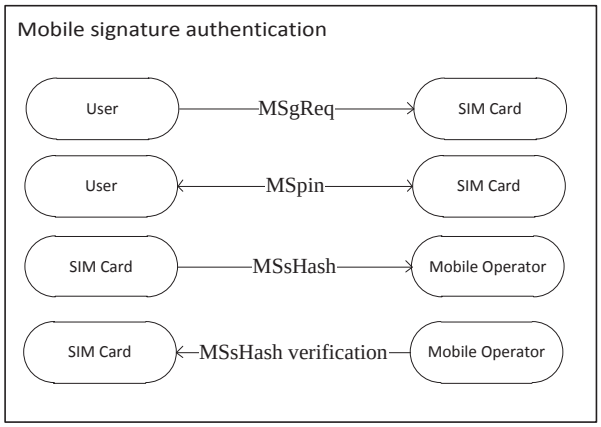


Fig. 2. Steps that a mobile device follows up in order to have a secure authentication via Mobile Signature

A key feature of this system should be the uptime guarantee

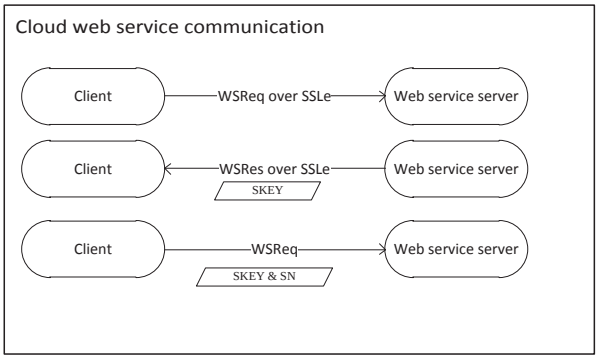


Fig. 3. The secured file transfer and application business communication

in any failure condition of one of the servers. So, the distributed application should work on all servers and if any of the servers goes down, another server should continue operating without interrupting. So, distributed session handling is present in this environment.

Creating this system in the real world is possible as the environments and tools below can be easily used. According to the researches done, the Amazon EC2 (offered by Amazon Inc.), is suitable as it offers: The Elastic Cloud, Virtual Load Balancers, Cloud Storage and Backup.

The Mobile Signature is officially offered by Turkcell in Turkey, and it is protected by electronic signature law number 5070. Another reason to use this Mobile Signature is that Turkcell is one of the first companies in the world that designed and developed the Mobile Signature.

As a comparison with the previous works done at [8], results are shown at Table II.

TABLE II
COMPARISON ACCORDING TO ATTACK TYPES

Attack	Proposed Model	Method at [8]
Man-In-The-Middle	Supported by sequence number	Not supported
Identity theft	Supported by Mobile signature	Not Supported
Phishing	Supported by Mobile Signature	Supported
Eavesdropping	Supported by Session Key and HTTPS	Supported

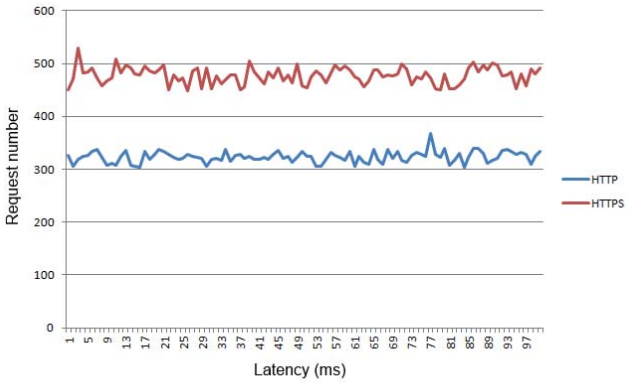


Fig. 5. The SFTP file transfer progress step by step

Also, a comparison graph is prepared in order to tell the difference of running an application over HTTP and HTTPS. In Fig. 5 the graph shows 100 requests made to a test server running firstly in HTTP and after that in HTTPS. There is a difference of about 150 milliseconds which in fact is not event distinguished by the user. In the other hand, this latency is related with the protection mechanisms running in the proposed model.

IV. CONCLUSION

By this material, we show how a secure authentication can be implemented on a real life platform currently supported by most of the mobile operators. We mentioned all types of required protocols in order to handle a complete infrastructure for an application to be connected to the cloud and operate. All the technologies gathered all together already exist, but in this platform all of them are combined in such a way that provides a secure and flexible operating environment.

The user identity is assured by the Mobile Signature. This makes possible to track the real person of each operation. By using SSL in the middle, the communication channel is secured. The session key and the sequence number make it impossible for a MAN-IN-THE-MIDDLE to replace or retry the network message.

REFERENCES

[1] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: a survey". Future Generation Computer Systems, May 2012.
[2] Z. Ahmad, K. E. Mayes, S. Dong, and K. Markantonakis, "Considerations for mobile authentication in the cloud". Information Security Technical Report 16, 2011, pp. 123 – 130.
[3] M. Whitehead, "GSMA Europe response to European Commission consultation on eSignatures and eIdentification", April 2011.
[4] D. Suna, G. Changb, L. Suna, and X. Wanga, "Surveying and analyzing security, privacy and trust issues in cloud computing environments". Procedia Engineering 15, 2011, pp. 2852 – 2856.
[5] W. Tang, J. Lee, B. Song, Md. M. Islam, S. Na, and E. Huh, "Multi-platform mobile thin client architecture in cloud environment". Procedia Environmental Sciences 11, 2011, pp. 499 – 504.
[6] S. Hung, C. Shih, J. Shieh, C. Lee, and Y. Huang, "Executing mobile applications on the cloud: framework and issues". Computers and Mathematics with Applications 63, 2012, pp. 573–587.
[7] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, and E. Shi, "Authentication in the clouds: a framework and its application to mobile users". Management of Computing and Information, October 2010.
[8] S.N. Hsueh, J.J. Lin, M.Y. Lin, "Secure Cloud Storate for Convenient Data Archive of Smart Phones", IEEE 15th International Symposium on Consumer Electronics, 2011, pp. 156-161.

Storage Free Basis Conversion over Composite Finite Fields of odd characteristics

M. Riaz Sial, Ersan Akyildiz

***Abstract*—We study the Finite Fields of type $F_q, q = p^{2pn}$ from the efficient implementation point of view. We found that we can represent these fields with irreducible polynomials in the form $f(x) = x^p - x - a$. By using this representation we have found a way of constructing normal basis for the field, together with transmission matrix between normal basis and algebraic basis (Polynomial Basis) of F_q and vice versa. The key point is that this matrix and its inverse can be computed very efficiently without any memory requirement.**

***Index Terms**:* finite fields,composite field, basis conversion,polynomial basis, normal basis, Vandermonde matrix, reciprocal polynomial.

I. Introduction

MOTIVATION of this work started from [2] and [3], in which authors have proposed efficient ways to compute pairing-based cryptographic protocols on hyperelliptic curves of genus 3 over finite fields of char 7, 3 respectively. Both authors used the same composite structure of finite fields of type $F_{p^{2pn}}$ for Tate-pairing computation. In [2] it is shown that using this structure as the value of prime p grows the complexity of the algorithm is reduced. Specially using $p = 7$ is more efficient as comparred to $p = 3$.

It is well known in the finite field arithmetic literature that multiplication in polynomial basis is much faster than in normal basis. On the other hand squaring in binary fields or exponentiation is much cheaper in the normal basis instead of polynomial basis as raising to the power p is just a shift operation. Normal basis are considered very attractive specially for hardware implementations due to the fact that shift operation is free to implement in hardware. To overcome the multiplication difficulty in normal basis many solutions are proposed to make it faster like Optimal normal basis(ONB) of type I and II have been introduced in many publications e.g [12] and [13]. So researchers had been always looking for the optimization of the algorithms using optimal choice of basis and algorithm. Conversion from one basis to other is a costly operation using matrix multiplication, generally requires $O(n^2)$ operations and $O(n^2)$ field elements storage [11]. Its hard specially for memory constrained devices, as one needs to store an (n x n) matrix for this operation.

Manuscript received July 17, 2013.
Riaz Sial is with the Institute of Applied Mathematics, Middle East Technical University Ankara, Turkey, e-mail: riazsial @gmail,com
Ersan Akyildiz is with the Institute of Applied Mathematics and Faculty of Arts and Sciences, Middle East Technical University Ankara, Turkey, e-mail: ersan@metu.edu.tr

In past there have been suggested solutions for this sake. In [12] Muchtadi-Alamsyah and F. Yuliawan focused on the basis conversion from polynomial to Optimal normal basis(ONB) and vice versa, in the finite fields of type $F_{2^{nm}}$, where $gcd(n, m) = 1$, $m + 1$ must be prime and 2 must be primitive in Z^*_{m+1}. OR for type 2 ONB $2m + 1$ must be prime and 2 is a primitive in Z_{2m+1}, or $2m + 1 \equiv 3 \mod 4$ and 2 generates the quadratic residues in Z_{2m+1}. They suggested way to covert basis with $O(m)$ memory complexity and $O(m)$ time complexity.

In [10] Authors have suggested its more efficient to work in composite fields instead of binary fields and have devised algorithm to construct composite field of type $F_{2^{nm}}$ from F_{2^k} where $k = mn$. In [9] authors have suggested algorithms to convert basis in the Finite Field of type F_{2^m} with the $O(m)$ memory complexity and $O(m)$ time complexity.

In the literature researchers have also used the hybrid approach for basis to benefit from both basis advantages. One such example is from Shokrollahi [8]. In this paper authors used hybrid basis system, say when multiplication is needed, two field elements are converted to polynomial basis and multiplication is carried out in polynomial basis, then the reduction is carried out in normal basis after converting back from polynomial basis. In [6] authors have demonstrated that using the hybrid type of basis representation for implementing elliptic curve protocol outperforms all existing FPGA set-up to break ECC-130 challenge.

In this paper we focused on the efficient basis conversion between polynomial and normal basis to expedite the computation of such algorithms based on composite finite fields. Here we noticed that due to Frobenius in F_{q^p} over F_q the computations can be much faster than the normal when p is an odd prime. Moreover same can be extended to p^{2pn} type of field for all n co-prime to p. During this work luckily the basis conversion matrix happened to be a special type of Vandermonde matrix which can be constructed very efficiently. All the computations in matrix format are in the characteristic field which we show is very easy to compute as compared to parent field. Hence we purpose a storage free basis conversion for the composite Finite Fields of type $F_{p^{2pn}}$ over $F_{p^{2n}}$ which efficiently computes the presentation of an element from one basis to other with little extra computation cost . we also analyse the Tate Pairing algorithm described in [2] and give an estimate for the hardware implementation improvement for the Tate Pairing computation using our approach.

II. PRELIMINARIES

In This part we will give an introduction to what are composite finite fields and what are the basis.

A. Finite Fields and their Presentation

In the study of abstract algebra, a finite field or Galois field is a field in which there are finite number of elements. Finite fields are of prime importance in number theory, cryptography, error correcting codes, algebraic geometry etc.
Elements of the finite fields are presented using different basis system, a basis for F_{p^n} of size p^n elements over F_p is a set of n elements of F_{p^n} which are linearly independent. Once the type of basis is chosen then one needs to set the rules for field operations e.g multiplication, addition etc. There are mainly two types of basis known as polynomial and normal basis.

1) Polynomial Basis: If an element α of finite field is the generator of the field F_{p^n} then $1, \alpha, \alpha^1, \alpha^2, ..., \alpha^{n-1}$ are called the polynomial basis. In these basis an element $A \in F_{p^n}$ can be written as

$$A = \sum_{i=0}^{n-1} a_i \alpha^i$$

, where $a_0, a_1, ..., a_{n-1} \in F_p$ are the coefficients .

2) Normal Basis: Let F_{p^n} be the field extension of F_p then a basis of F_{p^n} over F_p of the form $\beta, \beta^p, \beta^{p^2}, ..., \beta^{p^{n-1}}$, where β is a suitable element of F_{p^n} and other elements are its conjugates with respect to F_p are called Normal basis of F_{p^n} over F_p .

3) Composite Field: Composite Field can be defined as an extension field defined over a base field which is already an extension of some field. For instance if we want to construct a field of size P^{2pn}elements then there exist only one finite field of this size however its representations may vary depending upon the basis and structure of the field you choose. Now we may represent the same field using F_{p^m} structure, where $m = 2pn$ and the elements of the field can be represented as polynomials of degree $m-1$ whose coefficients belong to F_p. The same field can be represented using composite field structure $F_{P^{2pn}}$, then each element $A \in F_{P^{2pn}}$ can be represented as polynomials of degree $p-1$ whose coefficients belong to $F_{P^{2n}}$ provided p and n are co-prime. If $A \in F_{P^{2pn}}$ then

$$A = \sum_{i=0}^{p-1} a_i \alpha^i$$

, where $a_0, a_1, ..., a_{n-1} \in F_{P^{2n}}$ are the coefficients.

B. Basis Conversion

Basis conversion refers to change the presentation of a field element from one basis to other. For cost effective solutions, better performance and compatibility of different systems its necessary to convert from one type of basis presentation to other.

III. THEOREMS AND PROOFS

Lemma 3.1: $f(x) = x^p - x + 1$ is irreducible over any F_{p^n} where $\gcd(p, n) = 1$.

PROOF.
In [1] theorem (3.78) says $f(x) = x^p - x - a$,$a \in F_p^*$ is irreducible over F_q where $q = p^n$, if and only if it has no root $\in F_q$. Now [1] theorem (2.25) and [1] corollary (3.79) gives that $f(x) = x^p - x - a$ has a root in F_q if and only if absolute $Tr_{F_q}(a) = 0$.
Hence $f(x) = x^p - x - a$,$a \in F_p^*$ is irreducible over F_q if $Tr_{F_q}(a) \neq 0$. since according to [1] theorem 2.23, abs $Tr_{F_q}(a) = n * a$, so if $Tr_{F_q}(a) = 0$ then either a is zero or n is divisible by p. It completes the proof. ■

Lemma 3.2: Let $\beta = \alpha^{-1}$, where α is the root of $f(x) = x^p - x + 1$ and $F_{p^p} = F_p[x]/ < f(x) = x^p - x + 1 >$ then β generates a normal basis namely $\{\beta, \beta^p, \beta^{p^2}, ..., \beta^{p^{p-1}}\}$ of F_{p^p} over F_p.
PROOF.
Since reciprocal of an irreducible polynomial is also irreducible so the reciprocal of $f(x) = x^p - x + 1$ (which is irreducible over prime p from lemma 3.1) is $x^p(f(\beta)) = x^p - x^{p-1} + 1$ is also irreducible. Root of this polynomial generates normal basis. For proof reader is directed to corollary (2.6) in [4]. ■

Theorem 3.3: α be the root of irreducible polynomial $f(x) = x^p - x + 1$ over F_p and $\beta = \alpha^{-1}$ then $\beta^{p^i} = 1 - (\alpha - i)^{p-1}$, where $i = 0, 1, 2, \cdots, p-1$.
PROOF.
Since α is the root of $f(x) = x^p - x + 1$, we have $\alpha^p = \alpha - 1$ and

$$\begin{aligned}
\beta &= f(\alpha) = a_0 + a_1\alpha + \cdots + a_k\alpha^{p-1} \\
&= \frac{1}{\alpha} = 1 - \alpha^{p-1} \\
\beta^p &= f(\alpha)^p = f(\alpha^p) = f(\alpha - 1) = 1 - (\alpha - 1)^{p-1} \\
\beta^{p^2} &= (\beta^p)^p = f(\alpha - 1)^p = f(\alpha^p - (1)^p) \\
&\quad \text{due to Frobenius} \\
&= f(\alpha - 2) = 1 - (\alpha - 2)^{p-1} \\
&\downarrow \\
&\downarrow \\
(\beta^{p^{i-1}})^p &= f(\alpha - (i-2))^p = f(\alpha^p - (i-2)) \\
&= f(\alpha - 1 - i + 2) = 1 - (\alpha - (i-1))^{p-1} \\
&\quad \text{Hence by induction} \\
\beta^{p^i} &= f(\alpha - (i-1))^p = f(\alpha - i) = 1 - (\alpha - i)^{p-1}
\end{aligned} \tag{III.1}$$

■

Lemma 3.4:

$$\binom{p-1}{k} \equiv \frac{(p-1)!}{k!(p-1-k)!} \equiv (-1)^k \mod p$$

where $k = 0, 1, 2, ..., p-1$.

PROOF. Note that $(p-1)! = (-1) \mod p$ known as Wilson's Theorem.

$$\begin{aligned}
\text{Let } S_k &\equiv (k!(p-1-k)!) \mod p, \\
&\text{where } 0 \le k \le p-1 \\
s_0 &\equiv 0!(p-1)! \equiv (-1) \mod p \\
\text{since } S_{k+1} &= (k+1)!(p-1-k-1)! \\
&= \frac{(k+1)k!(p-1-k)!}{p-1-k} \\
S_{k+1}(p-1-k) &\equiv s_k(k+1) \mod p \\
S_{k+1}(-1-k) &\equiv (-1)(s_k)(-k-1) \mod p \\
S_{k+1} &\equiv (-1)(s_k) \mod p \\
&\text{From the above equality and} \\
\text{Since } s_0 &\equiv (-1) \mod p \\
&\text{we can write} \\
s_k &\equiv (-1)^{k+1} \mod p \\
so\frac{(p-1)!}{k!(p-1-k)!} &\equiv \frac{(p-1)!}{s_k} \mod p \\
&\equiv \frac{-1}{(-1)^{k+1}} \equiv (-1)^k \mod p
\end{aligned}$$

■

Theorem 3.5: The matrix

$$M = \begin{bmatrix} -1 & 0 & \dots & 0 & 1 \\ -(1)^0 & -(1)^1 & \dots & -(1)^{p-2} & 0 \\ -(2)^0 & -(2)^1 & \dots & -(2)^{p-2} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -(p-1)^0 & -(p-1)^1 & \dots & -(p-1)^{p-2} & 0 \end{bmatrix}$$

is transition matrix from polynomial basis of the form $\{1, \alpha, \alpha^2, \cdots, \alpha^{p-1}\}$ to normal basis of the form $\{\beta, \beta^p, \beta^{p^2}, \cdots, \beta^{p^{p-1}}\}$ of the space F_{p^p} over F_p, where α is the root of $f(x) = x^p - x + 1$ and $\beta = \frac{1}{\alpha}$

PROOF. Let

$$\begin{aligned}
F_{p^p} &= F_p[x]/ < f(x) = x^p - x + 1 > \\
&= F_p[\alpha]/ < f(\alpha) = \alpha^p - \alpha + 1 > \text{and let} \\
\beta &= \alpha^{-1}
\end{aligned} \tag{III.2}$$

From theorem (3.3) we know that:

$$\beta^{p^i} = 1 - (\alpha - i)^{p-1}$$

where
$\beta^{p^i} for\ 0 \le i \le p-1 = \{\beta, \beta^p, \beta^{p^2}, \cdots, \beta^{p^{p-1}}\}$ are the normal basis.

From above equation using binomial expansion formulae we get

$$\begin{aligned}
\beta^{p^i} &= 1 - (\alpha + (-i))^{p-1} \\
&= 1 - \sum_{k=0}^{p-1} \binom{p-1}{k} \alpha^{p-1-k}(-i)^k
\end{aligned} \tag{III.3}$$

From Lemma (3.4) and above Eqn. we can write

$$\begin{aligned}
(\alpha - i)^{p-1} &= \sum_{k=0}^{p-1} (-1)^k \alpha^{p-1-k}(-1)^k (i)^k \mod p \\
&= \sum_{k=0}^{p-1} (-1)^{2k} \alpha^{p-1-k} i^k \mod p \\
&= \sum_{k=0}^{p-1} \alpha^{(p-1-k)} i^k \mod p
\end{aligned} \tag{III.4}$$

From above equations we can easily conclude that,

$\beta^{p^0} = 1 - \alpha^{p-1}$, as when $i = 0$, eqn:(III.4) $= \alpha^{p-1}$

$$\beta_i = \beta^{p^i} = -\sum_{k=0}^{p-2} \alpha^{(p-1-k)} i^k \mod p, \text{ for } 1 \le i \le p-1 \tag{III.5}$$

Now if we compute the above equation for all β_i in the tabular form we get our desired matrix and hence normal basis can be computed from polynomial basis as below:

$$\begin{bmatrix} \beta \\ \beta^p \\ \beta^{p^2} \\ \dots \\ \beta^{p^{p-1}} \end{bmatrix} =$$

$$\begin{bmatrix} -1 & 0 & \dots & 0 & 1 \\ -(1)^0 & -(1)^1 & \dots & -(1)^{p-2} & 0 \\ -(2)^0 & -(2)^1 & \dots & -(2)^{p-2} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -(p-1)^0 & -(p-1)^1 & \dots & -(p-1)^{p-2} & 0 \end{bmatrix} * \begin{bmatrix} \alpha^{p-1} \\ \alpha^{p-2} \\ \vdots \\ \alpha \\ 1 \end{bmatrix}$$

As each row of the matrix is just raising the power of field element, so no need of memory to store the matrix. ■

Lemma 3.6:

$$\sum_{m=0}^{p-2} k^m \mod p, k \in F_{p^*} \equiv \begin{cases} -1 \mod p & \text{if } k = 1, \\ 0 \mod p & \text{otherwise.} \end{cases}$$

PROOF. For k = 1 its straight forward sum of $p-1$ number of 1 = -1 mod p
For $k \neq 1$ lets have

$$\sum_{m=0}^{p-2} k^m \mod p \equiv k^0 + k^1 + k^2 + \cdots + k^{p-2} \mod p \tag{III.6}$$

Since this is a simple geometric series
$a + ar + ar^2 + ... + ar^{n-1}$, where
$a = 1$
$r = k$,
$n = p - 1$.
Then we have

$$\sum_{m=0}^{p-2} k^m \mod p \equiv \frac{a(1 - r^{p-1})}{1 - r} \mod p$$

Since $r^{p-1} \equiv 1 \mod p$, for $r = k, k \neq 1, k \in F_{p^*}$ So

$$\sum_{m=0}^{p-2} k^m \mod p \equiv 0 \mod p$$

■

Theorem 3.7: If the matrix

$$M = \begin{bmatrix} -1 & 0 & \dots & 0 & 1 \\ -(1)^0 & -(1)^1 & \dots & -(1)^{p-2} & 0 \\ -(2)^0 & -(2)^1 & \dots & -(2)^{p-2} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -(p-1)^0 & -(p-1)^1 & \dots & -(p-1)^{p-2} & 0 \end{bmatrix}$$

The inverse of the matrix M $\mod p$ can be computed by simple transpose of the permuted rows of matrix M.

PROOF. If we analyse the matrix M of dim (p x p) contains a sub-matrix A of size (p-1) x (p-1) which is of special type known as Vandermonde matrix. This sub-matrix is shown below.

$$A = \begin{bmatrix} -(1)^0 & -(1)^1 & \dots & -(1)^{p-2} \\ -(2)^0 & -(2)^1 & \dots & -(2)^{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ -(p-1)^0 & -(p-1)^1 & \dots & -(p-1)^{p-2} \end{bmatrix}$$

This Vandermonde matrix is well known and is invertible.

Now if we look at each row then we observe that R_i is nothing but just powers of i from 0 to $p - 2$. then we can write corresponding rows and the scalar product of two rows as under:

$$\begin{aligned} -R_i &= i^0, i^1, i^2, ...i^{p-1} \\ -R_j &= j^0, j^1, j^2, ...j^{p-1} \\ R_i * R_j &= (i*j)^0 + (i*j)^1 + (i*j)^2 + ... + (i*j)^{p-2} \\ &= k^0 + k^1 + k^2 + \cdots + k^{p-2} \mod p \\ &= \sum_{m=0}^{p-2} k^m \mod p, k \in F_{p^*} \\ &= \begin{cases} -1 & \text{if } k = 1, \text{where } k = i*j \mod p \\ 0 & \text{otherwise: due to Lemma (3.6)} \end{cases} \end{aligned}$$

Mathematically: if $R_i * R_i = 1$ and $R_i * R_j = 0$ where $i \neq j$ then such matrix is called **orthogonal matrix** and inverse of such matrix is just the transpose of it.

However in our case matrix A from equation III.7 this is not true but $R_i * R_j = -1$ only if $i * j \mod p = 1$ else 0. So to get the inverse of matrix A such that

$$A^{-1} * A = I$$

we need to compute the transpose of the matrix A with permuted rows such that column(i) of A^{-1} = - $(Row(j)ofA)^t$, where $j = i^{-1} \mod p$. we can write as

$$C_i = -(R_{(\frac{1}{i} \mod p)})^t \quad \text{(III.7)}$$

where C is the column of A^{-1} and R is row of matrix A. ■

A. Algorithm to compute inverse of M

Inverse of the transition (p x p)matrix M is nothing but the permutation of the M as described below:
1. Column 1 = p^{th} column of M but upside down.
2. Last row of the matrix is all 1.
3. Rest of the (p-1)x(p-1)matrix = A^{-1} as discussed above

Example.
Here is an example for the case p=7.

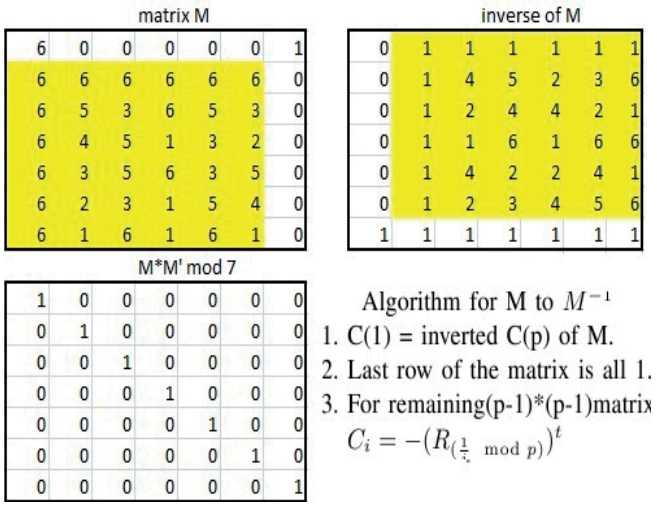


Fig. 1. Basis conversion matrix and its inverse

IV. BASIS CONVERSION

A. Polynomial to Normal Basis Conversion

Normal basis can be computed from polynomial basis using transition matrix as discussed in theorem (3.5). Where as the transition matrix is constructed using the algorithm given in IV-C with the time complexity of $\frac{p^2}{4}$. The equation is as shown below

$$\begin{bmatrix} \beta \\ \beta^p \\ \beta^{p^2} \\ \dots \\ \beta^{p^{p-1}} \end{bmatrix} =$$

$$\begin{bmatrix} -1 & 0 & \dots & 0 & 1 \\ -(1)^0 & -(1)^1 & \dots & -(1)^{p-2} & 0 \\ -(2)^0 & -(2)^1 & \dots & -(2)^{p-2} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -(p-1)^0 & -(p-1)^1 & \dots & -(p-1)^{p-2} & 0 \end{bmatrix} * \begin{bmatrix} \alpha^{p-1} \\ \alpha^{p-2} \\ \vdots \\ \alpha \\ 1 \end{bmatrix}$$

B. Normal to Polynomial Conversion

As inverse of conversion matrix discussed in theorem (3.2) above can be now used to compute polynomial basis from normal basis using the formulae below.

$$\begin{bmatrix} 0 & (1)^0 & \dots & (p-1)^0 \\ 0 & (1)^1 & \dots & (p-1)^1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & (1)^{p-2} & \dots & (p-1)^{p-2} \\ 1 & 1 & \dots & 1 \end{bmatrix} * \begin{bmatrix} \beta \\ \beta^p \\ \beta^{p^2} \\ \dots \\ \beta^{p^{p-1}} \end{bmatrix} = \begin{bmatrix} \alpha^{p-1} \\ \alpha^{p-2} \\ \vdots \\ \alpha \\ 1 \end{bmatrix}$$

Note: Its clear from the above conversion equations that there is no need of memory to store this matrix, as it can be computed with very little effort during basis computation.

C. Algorithm for PB-NB conversion

Input : alpha[$a_1, a_2, ...a_p$];
Output: beta [$b_1, b_2, ...b_p$];

Algorithm:
z = (p-1)/2 ;
prm = p
beta[1] = (alpha[prm] - alpha[1]) mod prm;
for i = 1 to z do
    x = 1; m = 1;
    y1 = 0; y2 = 0; x1 = 0; x2 = 0;
    for j = 1 to z do
        y1 = (y1 - x * alpha[j]) mod prm;
        y2 = (y2 - x * alpha[z+j]) mod prm;
        x = x*i mod prm;
        x1 = (x1 - m * alpha[j]) mod prm;
        x2 = (x2 - m * alpha[z+j]) mod prm;
        m = m*(-i) mod prm;
    end for;
    beta[i+1] := (y1+ x*y2) mod prm;
    beta[prm-i+1] := (x1+ m*x2) mod prm;
end for;
output = beta;

The above algorithm takes the coefficients of an element $A \in F_{p^p}$ in the polynomial basis representation as input and computes its coefficients in the normal basis. The time complexity of the algorithm can be seen as $p^2/4$ without any storage requirement. Same algorithm can be extended for the coefficients α_i if they belong to $F_{p^{2^n}}$.

Moreover Normal to polynomial basis conversion can be done using by using the algorithm as shown in figure 1.
Remarks:
1. It is important to highlight here that size of Finite field changes exponentially with the size of the prime p. For instance if we use the structure $F_{p^{2^{pn}}}$ and keeping the size of the n = 29 as in [2] constant then changing the size of the prime from 3 bit to 5 bit will result in changing the size of the finite field from 1000 to 9000 bits approximately. This shows that even at very high security level, the size of the p is not much so the conversion matrix cost will not be high as compared to multiplication in the field. 2. The matrix M and its inverse as discussed above are shown to prove the inversion, however for basis transition actually there is no matrix arithmetic involved because every row can be computed one by one for each basis element as shown in the algorithm IV-C
3. Since $f(x) = x^p - x - a$ is also irreducible over F_{p^2}, this work can be easily extended to the fields $F_{p^{2^{pn}}}$. From this, one can use generic algorithms e.g Montgomery, Karatsuba, algorithms to have efficient computation of field operations on $F_{p^{2^{pn}}}$, for any m, where $\gcd(p, n) = 1$. As authors in [2] suggested in their algorithm.

3. Algorithm for Tate Pairing as in [2].

Let $C_b = Y^2 = X^p - X + b, b = \mp 1$ and $\rho \in F_{p^p} \in F = F_{p^{p^n}}$ be a root of the polynomial $x^p - x + 2b$ over F_p *and* $\sigma \in F_{p^2} \in K = F_p^{2pn}$ be a root of the polynomial x^2+1. The polynomial x^p-x+2b is an irreducible polynomial over the field F_p. Hence all its roots belong to the field F_{p^p}. Simultaneously, the polynomial $x^p - x + 2b$ is also irreducible over the field F_{p^2} then,

Let the points $P = (\alpha, \beta) \in C_b(k)$ and
Q = $(\rho - x, \sigma y) \in F \times K$, $(x, y) \in C_b(k)$, where
$\sigma^2 = -1$, $\rho^p - \rho + 2b = 0$, $k = F_{p^n}, F = F_{p^{pn}}), and\ K = F_{p^{2^{pn}}}$, be given.

Initialization:
$f = 1$; $x = x^p$; $y = y^p$; $d = -(2n-1)b$ Calculation:
(1) for i = 1 to n,

$$\begin{aligned} \alpha &= (\alpha^p)^p \\ \beta &= (\beta^p)^p \\ g &= (\beta y\sigma - (\alpha + x + d - \rho)^{(p+1)/2} \\ f &= f^p g;\ y = -y;\ d = d + 2b \end{aligned} \tag{IV.1}$$

(2) $f = f^{p^{pn}-1}$
Return f.

As it is shown in algorithm above that there is p^{th} power computation in every round and the final exponentiation, so if we change normal basis instead of polynomial as used in [2] it will make the computation of the Tate Pairing approximately 2.7 times faster. Moreover for hardware implementations the cost of basis conversion will be negligible as from the algorithm for F_7 multiplication discussed in [2] is nothing but just the shift of the bits, and in conversion matrix all the multiplications are in F_7 field.

V. Conclusion

In this paper we proved the irreducibility of such polynomials over all primes, the normality of reciprocal polynomial, and the existence of such transition matrix for basis conversion. We give an algorithm to convert the basis with the time complexity of $\frac{p^2}{4}$ but without any storage requirement. Since we could not find any such work in odd primes characteristic composite field so its hard to compare with the binary extension fields. we have shown an important class of finite fields which can be used to benefit from the advantages of both types of basis, due to the fact that conversion cost is negligible as compared to exponentiation cost.

VI. Future Work

Further research in this area will explore the new possibilities of improvement, as to the best of our knowledge no previous such work exist in the literature. Its direct use can be seen in algorithm in [2], however it needs to be implemented and evaluated, Implementation of these fields and finding the optimal efficient algorithms is promising area to work on.

References

[1] Rudolf Lidl and Harald Niederreiter, *Book of Finite fields*, 2000

[2] S. B. Gashkov, A. A. Bolotov, A. A. Burtsev, S. Yu. Zhebet, and A. B. Frolov *On hardware and software implementation of arithmetic in finite fields of characteristic 7 for calculation of pairings*,journal of Mathematical Sciences, Vol. 168, No. 1, 2010.

[3] Eunjeong Lee, Hyang-Sook Lee and Yoonjin LeeFast,*computation of Tate pairing on general divisors of genus 3 hyperelliptic curves*,2006.

[4] Chih-Hua Chien, Trieu-Kien Truong, Yaotsu Chang and Chih-Hsuan Chen, *A Fast Algorithm to Determine Normal Polynomial over Finite Fields* ,IMECS 2007

[5] Kieren MacMillan and Jonathan Sondow, *Proofs of Power Sum and Binomial Coefficient Congruences Via Pascals Identity*,2010.

[6] Junfeng Fan , Daniel V. Bailey *Breaking Elliptic Curve Cryptosystems using Reconfigurable Hardware*,2010.

[7] Burton S. Kaliski Jr. and Moses Liskov, *Efficient Finite Field Basis Conversion Involving Dual Bases*,1999.

[8] J. v. z. Gathen, A. Shokrollahi, and J. Shokrollahi, *Efficient multiplication using type 2 optimal normal bases*,Lecture Notes in Computer Science,Springer, 2007.

[9] Burton S. Kaliski and yiqun Lisa Yin,1999 *storage efficient finite field basis conversion*, SAC 98, LNCS 156: 8193.

[10] Berk Sunar,Erkay Savas,Cetin K.Koc, *Constructing Composite Field Representations for Efficient Conversion*,2003.

[11] Burt Kaliski, Moses Liskov and Yiqun Lisa Yin, *Efficient Finite Field Basis Conversion Techniques*,1999.

[12] I.Muchtadi-Alamsyah and F.Yuliawan, *Basis Conversion in Composite Field*, International Journal of Mathematics and Computation vol 16 Issue 2 (2013).

[13] Berk Sunar, Cetin K. Koc,*Constructing Composite Field Representations for Efficient Conversion*, IEEE Transactions on computers, vol X, No. X, month 2003.

[14] Shigeki Kobayashi, Yasuyuki Nogami, Tatsuo Sugimura, *A Relation between SelfReciprocal Transformation and Normal Basis over Odd-Characteristic Field*, 4th ICCIT conferance 2009.

Recent attacks against HFE/Multi-HFE MQ cryptosystems and Connection with Ore's p-polynomial decomposition

Bilal Alam, Oğuz Yayla

***Abstract*—In this article we review some recent attacks against HFE and Multi-HFE cryptosystems and also a possible new direction proposed by Coulter et al. relating the security of HFE cryptosystems to the Ore's p-polynomial decomposition algorithm.**

***Index Terms*—HFE, multi-HFE, multivariate quadratic cryptosystems, Min-Rank problem, IP-problem, Ore's p-polynomial decomposition.**

I. Introduction

Hidden Field Equations (HFE) based Multivariate Quadratic (MQ) cryptosystems were proposed by Patarin [32] after he successfully attacked the MIA scheme [35]. HFE is a generalisation of the MIA scheme with the central trapdoor using a univariate quadratic polynomial over finite field $\mathbb{E}$ i.e. n degree extension of $\mathbb{F}$, instead of a monomial x^{q^h+1} used as a permutation map in MIA. There have been various practical attacks on this scheme, however some standard variations render those attacks in-efficient. Hence, we can consider HFE still a viable candidate with suitable parameter and variation choice. In this article, we review some recent cryptanalytic attacks on these HFE schemes and their relation to other mathematical problems.

The outline of the paper is as follows. In section II, we define HFE and multi-HFE multi-variate quadratic cryptosystems. Section III discusses some recent cryptanalytic structural attacks against HFE in which the problem is reduced to an instance of polynomial time solvable Min-Rank problem. In section IV, cryptanalytic attack by reduction to polynomial time solvable Isomorphism of Polynomials (IP) Problem is discussed. A new approach of analyzing the security of HFE while examining the significance of Ore's p-polynomial decompositions relevant to this case is discussed in section V followed by conclusion.

II. HFE and Multi-HFE

Patarin in [32] defined the basic HFE as follows.

Definition II.1. Let $\mathbb{F}$ be a finite field and $\mathbb{E}$ its n degree extension such that $|\mathbb{F}| := q$, then

$$P(X) = \sum_{0\leq i,j\leq D} A_{i,j} X^{q^i+q^j} + \sum_{0\leq k\leq D} B_k q^k + C \;\forall\; X \in \mathbb{E}$$

Bilal Alam and Oğuz Yayla: Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bul., No:1, 06800, Ankara, Turkey, e-posta: {e159447, yayla}@metu.edu.tr.

such that $q^i + q^j, q^k \leq D$ and co-efficients $A_{i,j}, B_i, C \in \mathbb{E}$ define the central quadratic polynomial map P for the HFE scheme. Using the canonical bijective map ϕ from $\mathbb{E}$ to $\mathbb{F}^n$ i.e. n-dimensional vector space over $\mathbb{F}$ and it's inverse we get the corresponding multivariate representation as $P' := \phi \circ P \circ \phi^{-1}(x)$ for $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$.

The degree of the polynomial P is upper bounded by D to allow efficient inversion of the equation $P(X) = Y$ for given $Y \in \mathbb{E}$. There are deterministic algorithms [32] for this inversion in time polynomial in D and the dimension n of extension field $\mathbb{E}$ over $\mathbb{F}$. HFE cryptosystems are susceptible to Gröbner bases attacks [20]. A thorough investigation of the Gröbner bases attack was given by Granboulan in [23] for HFE based MQ systems over finite fields of characteristic 2 and later by J.Ding and J.Hodges in [16] for those over finite fields of characteristic any prime p. The attack exploits the fact that the univariate equation in the extension field has a total degree that is much lower than the one for a randomly chosen equation. In order to improve upon this degree of the univariate polynomial representation over extension field $\mathbb{E}$, Patarin [2], [32] proposed a generalization of HFE that uses instead of a single univariate quadratic polynomial over extension field $\mathbb{E}$, a system of N quadratic polynomials in N variables over an extension field of degree d over $\mathbb{F}$. The basic HFE in Definition II.1 is an instance of Multi-HFE with $N = 1$, $d = n$.

Definition II.2. Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^d}$ its d degree extension. Let N be the number of variables and the number of secret quadratic polynomials in the polynomial ring $\mathbb{F}_{q^d}[X_1, \ldots, X_N]$ and D be their degree. Then the polynomial map $\mathcal{F} : (\mathbb{F}_{q^d})^N$ to $(\mathbb{F}_{q^d})^N$ given by

$$\mathcal{F} : (X_1, \ldots, X_N) \to (F_1(X_1, \ldots, X_N), \ldots, F_N(X_1, \ldots, X_N)$$

where

$$F_k = \sum_{1\leq i,j\leq N} \sum_{0\leq u,v<d} A_{k,i,j,u,v} X_i^{q^u} X_j^{q^v} + \sum_{1\leq i\leq N} \sum_{0\leq l<d} B_{k,i,l} X_i^{q^l} + C_k$$

such that $A_{k,i,j,u,v}, B_{k,i,u}, C_k \in \mathbb{F}_{q^d}$ for all $1 \leq i, j \leq N$, $0 \leq u, v, l < d$ and $q^l, q^u + q^v \leq D$ with $n = Nd$, defines the central quadratic polynomial map P for multi-HFE scheme.

III. Min-Rank Attacks against HFE

Min-Rank problem over finite field $\mathbb{F}$ is defined as

Definition III.1. Let $n, r, k \in \mathbb{N}$ and given matrices $M_0, M_1, \ldots, M_k \in \mathcal{M}_{n\times n}(\mathbb{F})$ where $\mathcal{M}_{n\times n}(\mathbb{F})$ denote the $n \times n$ matrices with co-efficients in $\mathbb{F}$. The (square) MinRank Problem relates to finding any k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}^k$ such that linear combination of the matrices M_i for $0 \leq i \leq k$ given as

$$\sum_{i=1}^{k} \lambda_i M_i - M_0$$

has rank $\leq r$.

A. Relinearization Attack

The attack was proposed by Kipnis and Shamir in [24] as the first key recover attack on the HFE systems. For private key central quadratic polynomial (cf. Definition II.1) over E i.e. n degree extension of finite field $\mathbb{F}$ given as

$$P(X) = \sum_{0\leq i\leq r-1} \sum_{0\leq j\leq r-1} p_{i,j} X^{q^i+q^j}$$

such that $q^i + q^j, q^k \leq D$ and co-efficients $p_{i,j} \in \mathbb{E}$, the corresponding public key polynomial map is $G(X) = \phi^{-1} \circ T \circ \phi \circ P \circ \phi^{-1} \circ S \circ \phi(X)$ with T, S as randomly chosen invertible linear transformations over $\mathbb{F}^n$. In matrix form over $\mathbb{E}$ this is equivalent to

$$G(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} g_{ij} X^{q^i+q^j} = \underline{X} G \underline{X}^t$$

with g_{ij} as the (i, j)-th entry and $\underline{X} = (X^{q^0}, X^{q^1}, \ldots, X^{q^{n-1}}) \in \mathbb{E}$ with $\underline{X}^t$ as its transpose. Thus, we can write

$$T^{-1}(G(X)) = \sum_{k=0}^{n-1} t_k \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (g_{i-k,j-k})^{q^k} X^{q^i+q^j}$$

and

$$P(S(X)) = \underline{X} W P W^t \underline{X}^t$$

where $P = [p_{ij}]$ and $W = [W_{ij}] = s_{j-i}^{q^i}$ are the matrices over $\mathbb{E}$. Let G^k denote the matrix over $\mathbb{E}$ obtained from G by raising all the entries of G to q^k-th power and cyclically rotating all rows and columns of G forward k times. Then $T^{-1}(G(X)) = \underline{X} G' \underline{X}^t$ where

$$G' = \sum_{k=0}^{n-1} t_k G^k = W P W^t \qquad \text{(III.1)}$$

The $n \times n$ matrix P can only have its top left $r \times r$ block as non-zero where $r << n$. Similarly the matrix $G' = WPW^t$ has each entry as the linear combination of the t_k variables. Thus, the rank of both P and G' cannot exceed r. The main principle of the attack is to express this rank condition of $r \approxeq log(D)$ as a large number of equations in small number of variables. Kipnis and Shamir observed that every correct choice for n variables $t_0, t_1, \ldots, t_{n-1}$ results in the rank of G' not more than r and any other random choice results in rank close to n.

Now, the matrix G can be easily obtained from the public key of the HFE cryptosystem and G^k is derived from G as explained earlier. Taking $t_0, t_1, \ldots, t_{n-1}$ as n variables and under the condition that its rank does not exceed r establishes the fact that its left kernel $\widetilde{X} : \widetilde{X} G' = 0$ is at least an $(n - r)$ dimensional vector subspace. Thus, there exist at least $\underbrace{n - r}$ linearly independent n-dimensional vectors $\widetilde{X_1}, \ldots, \widetilde{X_{n-r}}$ over $\mathbb{E}$ such that one can assign random values to their first $n-r$ entries still keeping them linearly independent. Assuming the remaining r entries as new variables overall we have $r(n-r)$ new variables added to the system. Each $\widetilde{X_i} G' = 0$ gives n scalar equations and in total, we have $n(n-r)$ equations in $n + r(n - r)$ variables. This gives an overdefined system of about n^2 equations in about rn variables where $r << n$ which is an instance of MinRank problem for a set of multivariate quadratic equations i.e.

$$\begin{pmatrix} 1 & & & X_{1,1} & \ldots & X_{1,r} \\ & \ddots & & \vdots & \ldots & \vdots \\ & & 1 & X_{n-r,1} & \ldots & X_{n-r,r} \end{pmatrix} \Big(\sum_{i=1}^{n} \lambda_i G^i - G^0 \Big) = 0_n$$

But these equations are quadratic and general technique to solve this system of equations by linearization is to replace any product of two variables $X_i X_j$ for $i \leq j$ by a new variable X_{ij} which are in total $n(n + 1)/2$. In general, the resultant system is no more overdefined and by normal linearization we are not expected to obtain a unique solution.

To filter the correct solutions from many parasitic solutions obtained by Gaussian elimination of linear system of equations obtained after linearization, Kipnis and Shamir performed the technique of relinearization. In relinearization technique, they add additional constraints to relate the new variable X_{ij} with each other and obtain additional equations. For example, in degree 4 relinearization any 4-tuple of indices $1 \leq i, j, k, l \leq m$, where m is the number of total variables, can be parenthesized as follows

$$(X_i X_j)(X_k X_l) = (X_i X_k)(X_j X_l) = (X_i X_l)(X_j X_k)$$
$$\Rightarrow X_{ij} X_{kl} = X_{ik} X_{jl} = X_{il} X_{jk}.$$

Hence, there are about $m^4/4!$ ways to choose 4-tuple of indices with each choice resulting in 2 quadratic equations in new variables introduced by re-linearization. Further optimization of the basic technique was also suggested by choosing degree 6 relinearization of indices and obtaining further set of equations. However in [6], it was pointed out by Curtois that degree 6 and higher relinearizations result in far less linearly independent equations and require far more computational power becoming less useful. The overall complexity of this attack was estimated by Curtois in [11] as $n^{log^2 d}$ where d is the degree of the central quadratic polynomial P over $\mathbb{E}$ of extension degree n.

B. Faugere Attack: Using Matrix/Vector Operations

To further improve the complexity of the attack in section III-A Faugere, Betttale and Perret [1] proposed to reduce this problem of computing Gröbner bases of a polynomial system to one with computations over smaller field $\mathbb{F}_q$ instead of $\mathbb{F}_{q^n}$. In order to achieve this they introduce the change of basis

matrix $M_n \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ where $\mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ is the set of $n \times n$ matrices with co-efficients in $\mathbb{F}_{q^n}$ such that

$$M_n = \begin{pmatrix} \theta_1 & \theta_1^q & \dots & \theta_1^{q^{n-1}} \\ \theta_2 & \theta_2^q & \dots & \theta_2^{q^{n-1}} \\ \vdots & & \ddots & \vdots \\ \theta_n & \theta_n^q & \dots & \theta_n^{q^{n-1}} \end{pmatrix}$$

and $(\theta_1, \dots, \theta_n) \in (\mathbb{F}_{q^n})^n$ is the vector basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Using M_n, one gets the following morphism $\phi_1 : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$

$$X \rightarrowtail (X, X^q, \dots, X^{q^{n-1}})M_n^{-1}$$

and its inverse $\phi_1^{-1} : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$

$$(x_1, \dots, x_n) \rightarrowtail ((x_1, \dots, x_n)M_n)[1]$$

where $((x_1, \dots, x_n)M_n)[1]$ denotes the first component of resultant vector $(x_1, \dots, x_n)M_n$. Using this change of basis matrix M_n, they obtained the following useful result.

Lemma III.2. *Let $M_n \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$. Let the symmetric matrices $(B_1, \dots, B_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ be associated to the multivariate secret central quadratic polynomials in the small field $(b_1, \dots, b_n) \in (\mathbb{F}_q[x_1, \dots, x_n])^n$ i.e. $b_i = \underline{x}B_i\underline{x}^t$ for $1 \le i \le n$. Then*

$$(B_1, \dots, B_n) = (M_nP^{*0}M_n^t, \dots, M_nP^{*n-1}M_n^t)M_n^{-1}$$

where $P = [p_{ij}] \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ is the matrix associated to the univariate secret central quadratic polynomial in the big field

$$P(X) = \sum_{0\le i\le r-1} \sum_{0\le j\le r-1} p_{i,j}X^{q^i+q^j} \in \mathbb{F}_{q^n}[X]$$

and

$$P^{*k} = p_{(i-k) mod\, n,(j-k) mod\, n}^{q^k} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})\ \forall k \in \mathbb{N}.$$

In order to relate the small field matrix representation of public key polynomial map in HFE to the big field matrix representation of private key, Lemma III.2 can be used. Let $G(\underline{x})$ and $(g_1(\underline{x}), \dots, g_n(\underline{x})$ be the univariate and multivariate small field representations of public key and $(b_1(\underline{x}), \dots, b_n(\underline{x}))$ as the corresponding multivariate small field representation of private key such that $\underline{x} = (x^{q^0}, x^{q^1}, \dots, x^{q^{n-1}})$ then we have

$$\begin{aligned} G(\underline{x}) &= T(P(S(\underline{x}))) \\ (g_1(\underline{x}), \dots, g_n(\underline{x})) &= (b_1(\underline{x}S), \dots, b_n(\underline{x}S))T \\ (\underline{x}G_1\underline{x}^t, \dots, \underline{x}G_n\underline{x}^t) &= (\underline{x}SB_1S^t\underline{x}^t, \dots, \underline{x}SB_nS^t\underline{x}^t)T \\ (G_1, \dots, G_n) &= (SB_1S^t, \dots, SB_nS^t)T \\ (G_1, \dots, G_n)U &= (WP^{*0}W^t, \dots, WP^{*n-1}W^t) \end{aligned}$$

for $T^{-1}M_n = U$ and $SM_n = W$ where the matrices $U = [u_{ij}], W = [w_{ij}] \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$. Let $(u_{0,0}, \dots, u_{n-1,0}) \in (\mathbb{F}_{q^n})^n$ represent the first column of matrix U, then this can be expressed as:

$$\sum_{i=0}^{n-1} u_{i,0}G_{i+1} = WP^{*0}W^t = WPW^t.$$

As observed by Kipnis and Shamir, the rank of the matrices on right hand side of equations is $\log(D)$ where D is the degree bound of the secret central quadratic polynomial P. This equation is very similar to Kipnis and Shamir equation in (III.1). However, the co-efficients of the quadratic equations originating from equation (III-B) are in small field $\mathbb{F}_q$ unlike equation (III.1) where the co-efficients are in the big field $\mathbb{F}_{q^n}$. Hence, they obtained the following result.

Theorem III.3. *[1, Theorem 2] In HFE cryptosystems, the problem of key recovery reduces to solution of MinRank problem with $k = n$ and $r = \lceil \log_q(D) \rceil$ on the public matrices $(G_1, \dots, G_n) \in \mathcal{M}_{n\times n}(\mathbb{F}_q)^n$. The solutions of this MinRank are in $(\mathbb{F}_{q^n})^n$.*

From here on, the attack proceeds by computing the gröbner bases of the system of quadratic equations and then its variety. However, the cost of operations compared to Kipnis-Shamir attack is reduced by an expected factor equivalent to the cost of multiplication of two univariate polynomials of degree n over big field.

In multi-HFE cryptosystems (cf. Definition II.2) a multivariate quadratic system of polynomials is used as the secret central private key P rather than a single univariate polynomial as in HFE. For $n = Nd$, the general form of this polynomial map $P : (\mathbb{F}_{q^d})^N$ to $(\mathbb{F}_{q^d})^N$ for homogeneous system is as follows

$$P : (X_1, \dots, X_N) \to (P_1(X_1, \dots, X_N), \dots, P_N(X_1, \dots, X_N)$$

where

$$P_k = \sum_{1\le i,j\le N} \sum_{0\le u,v<d} A_{k,i,j,u,v}X_i^{q^u}X_j^{q^v}$$

such that $A_{k,i,j,u,v} \in \mathbb{F}_{q^d}$ for all $1 \le i, j \le N$, $0 \le u, v, l < d$ and $q^u + q^v \le D$. In order to extend the attack to multi-HFE case the change of basis matrix is generalised to the following form

$$M_{N,d} = \begin{pmatrix} \theta_1 & \theta_1^q & \dots & \theta_1^{q^{d-1}} & & & \\ \theta_2 & \theta_2^q & \dots & \theta_2^{q^{d-1}} & & & \\ \vdots & & \ddots & \vdots & & & \\ \theta_d & \theta_d^q & \dots & \theta_d^{q^{d-1}} & & 0 & \\ & & & & & & \\ & & \ddots & & & & \\ & & & & \theta_1 & \theta_1^q & \dots & \theta_1^{q^{d-1}} \\ & & & & \theta_2 & \theta_2^q & \dots & \theta_2^{q^{d-1}} \\ & 0 & & & \vdots & & \ddots & \vdots \\ & & & & \theta_d & \theta_d^q & \dots & \theta_d^{q^{d-1}} \end{pmatrix}$$

Using $M_{N,d}$, one gets the following morphism $\phi_N : (\mathbb{F}_{q^d})^N \to \mathbb{F}_{q^n}$

$$(X_1, \dots, X_N) \to (V_1, V_1^q, \dots, V_N^{q^{d-1}}, \dots, V_N, V_N^q, \dots, V_N^{q^{d-1}})M_{N,d}^{-1}$$

and its inverse $\phi_N^{-1} : \mathbb{F}_{q^n} \to (\mathbb{F}_{q^d})^N$

$$(x_1, \dots, x_n) \rightarrowtail (X_1, X_{d+1}, \dots, X_{d(N-1)+1}) = (x_1, \dots, x_n)M_{N,d}$$

Lemma III.2 can be generalized using these morphisms as

Lemma III.4. *Let $M_{N,d} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^d})$. Let the symmetric matrices $(\mathbf{P_1},\ldots,\mathbf{P_N}) \in (\mathcal{M}_{n\times n}(\mathbb{F}_{q^d}))^n$ be associated to the multivariate secret central quadratic polynomials $(P_1,\ldots,P_N) \in (\mathbb{F}_{q^d}[x_1,\ldots,x_n])^N$ such that $P_i = \underline{X}\mathbf{P_i}\underline{X}^t$ where $\underline{X} = (X_1, X_1^q, \ldots, X_1^{q^{d-1}}, \ldots, X_N, X_N^q, \ldots, X_N^{q^{d-1}})$. Let ${\mathbf{P_i}}^{*d,k} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^d})$ be the matrix obtained from $\mathbf{P_i}$ by rotating the rows and columns of each $d\times d$ blocks by k positions and raising each entry in the matrix to the power q^k. Also, let the symmetric matrices $(B_1,\ldots,B_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ be associated to the multivariate secret central quadratic polynomials in the small field $(b_1,\ldots,b_n) \in (\mathbb{F}_q[x_1,\ldots,x_n])^n$ i.e. $b_i = \underline{x}B_i\underline{x}^t$ for $1\le i\le n$. Then*

$$\begin{aligned}(B_1,\ldots,B_n) = \\ (M_{N,d}{\mathbf{P_1}}^{*d,0}M_{N,d}^t,\ldots,M_{N,d}{\mathbf{P_1}}^{*d,d-1}M_{N,d}^t,\ldots\ldots \\ ,M_{N,d}{\mathbf{P_N}}^{*d,0}M_{N,d}^t,\ldots,M_{N,d}{\mathbf{P_N}}^{*d,d-1}M_{N,d}^t)M_{N,d}^{-1}.\end{aligned}$$

Thus, the relation among the small field public matrices $(G_1,\ldots,G_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ and the big field private matrices $(\mathbf{P_1},\ldots,\mathbf{P_N}) \in (\mathcal{M}_{n\times n}(\mathbb{F}_{q^d}))^N$ can be expressed using Lemma III.4 for multi-HFE systems using change of basis matrix $M_{N,d}$ as follows

$$\begin{aligned}(G_1,\ldots,G_n)T^{-1}M_{N,d} = \\ (SM_{N,d}{\mathbf{P_1}}^{*d,0}S^tM_{N,d}^t,\ldots,SM_{N,d}{\mathbf{P_1}}^{*d,d-1}S^tM_{N,d}^t,\ldots \\ ,SM_{N,d}{\mathbf{P_N}}^{*d,0}S^tM_{N,d}^t,\ldots,SM_{N,d}{\mathbf{P_N}}^{*d,d-1}S^tM_{N,d}^t) \\ (G_1,\ldots,G_n)U = \\ (W{\mathbf{P_1}}^{*d,0}W^t,\ldots,W{\mathbf{P_1}}^{*d,d-1}W^t,\ldots,W{\mathbf{P_N}}^{*d,0}W^t, \\ \ldots,W{\mathbf{P_N}}^{*d,d-1}W^t)\end{aligned}$$

where $U = T^{-1}M_{N,d}$ and $W = SM_{N,d}$. As a generalisation of MinRank problem in the HFE case this can be written as

$$\sum_{k=0}^{n-1} u_{k,0}G_{k+1} = W{\mathbf{P_1}}^{*d,0}W^t,$$

$$\ldots,\sum_{k=0}^{n-1} u_{k,0}G_{k+1} = W{\mathbf{P_N}}^{*d,0}W^t$$

The following result for multi-HFE is a generalization of Theorem III.3 in HFE case.

Theorem III.5. *[1, Theorem 2] In multi-HFE cryptosystems, the problem of key recovery reduces to solution of MinRank problem N times with $k = n$ and $r = N\lceil\log_q(D)\rceil$ on the public matrices $(G_1,\ldots,G_n) \in \mathcal{M}_{n\times n}(\mathbb{F}_q)^n$. The solutions of this MinRank are in $(\mathbb{F}_{q^d})$.*

IV. IP Attack against HFE

In general, to un-relate the IP problem from the secret key recovery in HFE, the central quadratic polynomial is kept secret in the design of HFE systems. However, Bouillaguet, Charles, et al in [4] proposed the framework under which equivalent polynomial P' of high degree can be used to recover the private key polynomial triple (S,P,T) by reducing the key recovery problem to an instance of IP problem. The concept of equivalent keys for multivariate public key cryptosystems has been discussed in detail in [39].

In [4], authors considered the usefulness of commutation of secret central polynomial with Frobenius map $F : X \to X^q$ over a finite field $\mathbb{F}$. They also observed that such property holds for certain instances of secret central polynomial $P(X) \in \mathbb{E}[X]$ of the form

$$P(X) = \sum_{0\le i,j\le D} Ai,jX^{q^i+q^j} + \sum_{0\le k\le D} B_kq^k + C\ \forall\ X \in \mathbb{E}$$

where $A_{i,j}, B_k, C \in \mathbb{F}$ such that $\mathbb{E}$ is the n-dimensional extension of $\mathbb{F}$. Equivalently if the secret central polynomial P can be written as the product of same element $\omega \in \mathbb{E}$ with some element of $\mathbb{F}$, then by employing the concept of equivalent keys, by considering equivalent affine transformations S', T' composed of original transformations S, T and the multiplication factor ω, the secret central polynomial can be considered as having co-efficients in $\mathbb{F}$. Such secret central polynomials P are observed to commute with Frobenius map F i.e.

$$P \circ F(X) = F \circ P(X).$$

Based on such commutation property, certain automorphisms among the public key $\mathcal{P} = T \circ P \circ S$ can be observed. Precisely, $\psi(F),\ldots,\psi(F^{n-1})$ are the only solutions of such automorphism where

$$\psi : F \rightarrowtail (T.F^{-1}.T^{-1}, S^{-1}.F.S)$$

such that

$$\mathcal{P} = (T \circ F^{-1} \circ T^{-1})^{-1} \circ \mathcal{P} \circ (S^{-1} \circ F \circ S).$$

We assume to have found such an automorphism $(V,W) = \psi(F^u)$ of the public key P for some $u \in [1, n-1]$. It is also observed [4, Preposition 3] that if $gcd(u,n) = 1$ (which holds if V and F are similar) then there exist equivalent linear transformations $\overline{S}, \overline{T} \in GL_n(\mathbb{F})$ such that $F = \overline{S} \circ W^k \circ \overline{S}^{-1}$ and $F = \overline{T}^{-1} \circ V^k \circ \overline{T}$ for $k := u^{-1} \bmod n$ and $\overline{S}.S^{-1}$ and $\overline{T}.T^{-1}$ commute with F. Also, in practice $\overline{S}, \overline{T}$ can be found efficiently using knowledge of u.

The relationship among $\overline{S}, \overline{T}$ and S, T can be used to neutralize the action of S, T on the public key $\mathcal{P}$. Considering the matrix representation of Frobenius map F it can be trivially observed that other matrices commuting with F over $\mathcal{M}_{n\times n}\mathbb{F}$ (set of $n\times n$ matrices over $\mathbb{F}$) form a vector space of dimension n generated by $(F^0, F, \ldots, F^{n-1})$. Hence, $F_1 = \overline{S}.S^{-1}$ and $F_2 = \overline{T}.T^{-1}$ are linear combinations of powers of F over $\mathbb{F}$. The composition of public key $\mathcal{P}$ as

$$\mathcal{P} = T \circ P \circ S$$

$$\overline{T}^{-1} \circ \mathcal{P} \circ \overline{S}^{-1} = F_2^{-1} \circ P \circ F_1^{-1}$$

results in the equivalent private key

$$P' = F_2^{-1} \circ P \circ F_1^{-1}.$$

Hence we get the following equations:

$$F_1(X) = \sum_{k=0}^{n-1} a_k X^{q^k} \qquad F_1^{-1} = \sum_{k=0}^{n-1} b_k X^{q^k}$$
$$F_2(X) = \sum_{k=0}^{n-1} c_k X^{q^k} \qquad F_2^{-1} = \sum_{k=0}^{n-1} d_k X^{q^k}$$
$$P'(X) = \sum_{0\le i,j\le D} A_{ij} X^{q^i+q^j} + \sum_{0\le i\le D} B_i X^{q^i} + C$$
$$P(X) = \sum_{0\le i,j\le D} e_{ij} X^{q^i+q^j} + \sum_{0\le i\le D} f_i X^{q^i} + g$$

with unknowns $a_k, b_k, c_k, d_k, e_{ij}, f_i, g$. Composing both sides of equation (IV) with F_1, we can write

$$F_1 \circ P' = F_2^{-1} \circ P.$$

This can be expressed as follows for left hand side

$$F_1 \circ P' = \sum_{0\le i,j\le D} A_{ij} (\sum_{k=0}^{n-1} a_k X^{q^k})^{q^i+q^j} + \sum_{0\le i\le D} B_i (\sum_{k=0}^{n-1} a_k X^{q^k})^{q^i} + C$$
$$= \sum_{i,j,k,l} A_{ij}.a_k.a_l.X^{q^{i+k}+q^{j+l}} + \sum_{i,k} B_i.a_k.X^{q^{i+k}} + C$$

and for right hand side

$$F_2^{-1} \circ P = \sum_{k=0}^{n-1} d_k (\sum_{0\le i,j\le D} e_{ij} X^{q^i+q^j} + \sum_{0\le i\le D} f_i X^{q^i} + g)^{q^k}$$
$$= \sum_{i,j,k} d_k.e_{ij}.X^{q^{i+k}+q^{j+k}} + \sum_{i,k} d_k.f_i.X^{q^{i+k}} + g.\sum_k d_k.$$

Finally, we have a system of $O(n^2)$ equations in $O(n + D^2)$ unknowns which is highly overdetermined system of equations and can be solved efficiently using fast Gröbner bases algorithms [19]. Based on their simulation results, authors in [4] also conjecture about the upper bound of complexity for their attack while using fast gröbner bases algorithm F_5 as $O(n^{21})$.

The attack returns the private key $(T, P, S) = (\overline{T}.F_2^{-1}, P, F_1^{-1}.\overline{S})$ using knowledge of public key $\mathcal{P}$ and determining an equivalent private polynomial P' but proceeds under the assumption that co-efficients of the actual central private polynomial P are in ground field $\mathbb{F}$ rather than $\mathbb{E}$ which is meaningful assumption by considering the concept of equivalent keys and sustaining transformation [39].

V. Ore's p-polynomials and security of HFE

Coulter, Havas and Henderson [7] gave an interesting insight into the security of HFE cryptosystems that have Dembowski Ostrom(DO) polynomials as the private key central polynomial. Their observation is based on the alternative definition of DO polynomials stated in [8] that establishes an important connection between p-polynomials and DO polynomials. Using this relation they propose a partial attack on HFE cryptosystems that tries to recover one of the secret linear map T in the private key tuple (S, P, T). Hence the corresponding pubic key $\mathcal{P} = T \circ P \circ S$ gets partially factored and the resultant (expected) low degree factors can be evaluated for their inverses using efficient root finding algorithm [36], [37]

HFE cryptosystem are designed by choosing a relatively low degree central polynomial P of the form

$$P(X) = \sum_{0\le i,j\le D} A_{ij} X^{q^i+q^j} \qquad \forall \quad X \in \mathbb{F}_q$$

where $A_{ij} \in \mathbb{F}_q$ i.e. n-degree extension of $\mathbb{F}_p$. Then this polynomial is mixed using right and left composition with two linear transformations S, T such that the resultant public key $\mathcal{P}$ is again a DO polynomial of reasonably high degree making it infeasible to compute the inverse. This was independently observed by Kipnis and Shamir [24] earlier and they also proved that any linear map can be expressed as a p-polynomial of the form

$$\sum_{i=0}^{n-1} a_i X^{p^i}.$$

It is not difficult to observe that DO polynomials are closed w.r.t left and right composition with p-polynomials. Hence the resultant public key $\mathcal{P}$ was proved [24] to have an equivalent univariate representation in the form of DO polynomial but it may have an exponential number of co-efficients and even if sparse it may have an exponentially high degree which makes inversion infeasible. However, being a DO polynomial it is bounded to have $O(n^2)$ terms.

Coulter et al.[7] observed that there could be a possible way to reduce the degree of this resultant public key $\mathcal{P}$. Their observation is based on the following result in [8].

Theorem V.1. *[7, Theorem 1][8, Theorem 3.2] For $f \in \mathbb{F}_q[X]$ with degree less than q the following statements are equivalent*

1) *f = DO + L_p where DO is a Dembowski Ostrom polynomial and L_p is p-polynomial.*
2) *The difference polynomial $\triangle_{f,a} = L_{p_a}$ for each $a \in \mathbb{F}_q^*$ where $\triangle_{f,a} := f(X+a) - f(X) - f(a)$ is the difference polynomial of f with respect to a and L_{p_a} is the p-polynomial depending on a.*

Considering the structure of public key $\mathcal{P} = T \circ P \circ S$, it can be considered as a left composition of $f = P \circ S$ (which is a DO polynomial itself) with T. The difference polynomial $\triangle_{\mathcal{P},a}$ can be evaluated as follows

$$\begin{aligned}\triangle_{\mathcal{P},a} &= \mathcal{P}(X+a) - \mathcal{P}(X) - \mathcal{P}(a)\\ &= T(f(X+a)) - T(f(X)) - T(f(a))\\ &= T(f(X+a) - f(X) - f(a))\\ &= T \circ \triangle_{f,a}\end{aligned}$$

$\triangle_{f,a}$ is a p-polynomial that follows from Theorem V.1 and $\triangle_{\mathcal{P},a}$ is a p-polynomial as p-polynomials are closed w.r.t polynomial composition [28]. Ore in [28] extending his work in [29] on non-commutative polynomial rings described the algorithm to compute left and right decompositional factors of p-polynomials. In [7] authors suggested to use Ore's ideas to develop a variant of famous Euclidean algorithm [26] and evaluate Greatest Common Left Decompositional Factor (GCLDF) of the p-polynomial composition. Their proposed attack on HFE cryptosystems works as follows

1) Randomly choose distinct $a_1, a_2 \in \mathbb{F}_q^*$.
2) Calculate $L(X) = GCLDF(\triangle_{\mathcal{P},a_1}, \triangle_{\mathcal{P},a_2})$.
3) Check whether L is the left decompositional factor of $\mathcal{P}$ i.e $L(X) = T(X)$. If this holds then we are done. This can be checked with complexity $O(\log_p(deg(\mathcal{P})))$ where $deg(\mathcal{P})$ is the degree of public key DO polynomial [7].
4) If L is not the left decompositional factor of $\mathcal{P}$ then choose a different $a \in \mathbb{F}_q^*$ and calculate $L(X) = GCLDF(L(X), \triangle_{\mathcal{P},a})$. Re-evaluate (3).

Since Ore's arguments are restricted to non-commutative rings and p-polynomials and not applicable directly on the DO polynomials, hence it is not possible to use them and compute $GCLDF(L(X), \mathcal{P}(X))$ to obtain T [7]. It was also observed that Giesbrecht algorithm in [22] cannot be used to obtain the left decompositional factor of public key polynomial $\mathcal{P}$ though it does claim to provide a probabilistic polynomial time algorithm to determine complete decomposition of p-polynomial. Based on Ritt's theorem [40] many such decompositions exist that have equivalent factors permuted and the resultant factors from Giesbrecht's algorithm may not all fall on the left. Finally the evaluation in (3) may not be successful as the difference polynomial $\triangle_{\mathcal{P},a}$ may or may not have a non-trivial left decompositional factor and the resultant factors may still have reasonably high degree making inversion infeasible.

Though the attack seems probabilistic in nature but it would be interesting to perform some simulations on practical HFE parameters and evaluate success probability of the stated attack for such parameters.

VI. Conclusion

In this article, we review few recent attacks against HFE and Multi-HFE MQ cryptosystems and review possible new direction proposed by Coulter et al.[7] that can be pursued in order to reassess the NP-hardness of the MQ-problem in general. Also certain simulation results can be obtained for practical parameters of HFE cryptosystems in order to prove the validity of the relation among decomposition of Ore's p-polynomial and security of HFE cryptosystems.

References

[1] Bettale, Luk, Faugére, Jean-Charles, and Ludovic Perret. *Cryptanalysis of HFE, multi-HFE and Variants for Odd and Even Characteristic*. Designs, Codes and Cryptography (2012): 1-52.

[2] Billet, Olivier, J. Patarin, and Yannick Seurin. *Analysis of intermediate field systems*. Proceedings of the First International Conference on Symbolic Computation and Cryptography, Beijing, China. 2008.

[3] Blake, Ian F. *Applications of finite fields.* Ed. Alfred J. Menezes. Vol. 199. Springer, 1993.

[4] Bouillaguet, C., Fouque, P. A., Joux, A., Treger, J. *A family of weak keys in HFE and the corresponding practical key-recovery.* Journal of Mathematical Cryptology, 5(3-4), (2012), 247-275.

[5] Chen, C. H. O., Chen, M. S., Ding, J., Werner, F., Yang, B. Y. *Odd-Char Multivariate Hidden Field Equations.* IACR Cryptology ePrint Archive, 2008, 543

[6] Courtois, N., Klimov, A., Patarin, J., Shamir, A. *Efficient algorithms for solving overdefined systems of multivariate polynomial equations.* In Advances in CryptologyEUROCRYPT 2000 (2000, January), (pp. 392-407). Springer Berlin Heidelberg.

[7] Coulter, Robert S., George Havas, and Marie Henderson. *Giesbrecht's algorithm, the HFE cryptosystem, and Ore's ps-polynomials*. Lecture Notes Series of Computing 9 (2001): 36-45.

[8] Coulter, Robert S., and Rex W. Matthews. *Planar functions and planes of Lenz-Barlotti class II*. Designs, Codes and Cryptography 10.2 (1997): 167-184.

[9] Courtois, Nicolas T. *Efficient zero-knowledge authentication based on a linear algebra problem MinRank*. Advances in Cryptology - ASIACRYPT 2001. Springer Berlin Heidelberg, 2001. 402-421.

[10] Courtois, Nicolas T., Magnus Daum, and Patrick Felke. *On the security of HFE, HFEv-and Quartz*. Public Key Cryptography - PKC 2003. Springer Berlin Heidelberg, 2002. 337 - 350.

[11] Courtois, Nicolas T. *The security of hidden field equations (HFE)*. Topics in Cryptology - CT - RSA 2001. Springer Berlin Heidelberg, 2001. 266 - 281.

[12] Courtois, Nicolas T. *Decoding Linear and Rank-Distance Codes, MinRank problem and Multivariate Cryptanalysis*. (2006).

[13] Cox, David A., John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Vol. 10. Springer Verlag, 2007.

[14] Ding, Jintai, Dieter Schmidt, and Fabian Werner. *Algebraic attack on HFE revisited*. Information Security. Springer Berlin Heidelberg, 2008. 215-227.

[15] Ding, Jintai, and Bo-Yin Yang. *Multivariate public key cryptography*. Post-Quantum Cryptography. Springer Berlin Heidelberg, 2009. 193-241.

[16] Ding, Jintai, and Timothy J. Hodges. *Inverting HFE systems is quasi-polynomial for all fields*. Advances in Cryptology - CRYPTO 2011. Springer Berlin Heidelberg, 2011. 724-742.

[17] Ding, Jintai, and Dieter Schmidt. *Cryptanalysis of HFEv and internal perturbation of HFE*. Public Key Cryptography-PKC 2005. Springer Berlin Heidelberg, 2005. 288-301.

[18] Faugére, Jean-Charles, Françoise Levy-Dit-Vehel, and Ludovic Perret. *Cryptanalysis of minrank*. Advances in Cryptology - CRYPTO 2008. Springer Berlin Heidelberg, 2008. 280-296.

[19] Faugére, Jean-Charles. *A new efficient algorithm for computing Gröbner bases without reduction to zero F5*. Proceedings of the 2002 international symposium on Symbolic and algebraic computation. ACM, 2002.

[20] Faugére, Jean-Charles, and Antoine Joux. *Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases*. Advances in Cryptology - CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729, pp. 44 - 60. Springer, Berlin (2003).

[21] Faugére, Jean-Charles, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. *Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity.* Journal of Symbolic Computation 46.4 (2011): 406-437.

[22] Giesbrecht, Mark. *Factoring in skew-polynomial rings over finite fields*. Journal of Symbolic Computation 26.4 (1998): 463-486.

[23] Granboulan, Louis, Antoine Joux, and Jacques Stern. *Inverting HFE is quasipolynomial*. Advances in Cryptology - CRYPTO 2006. Springer Berlin Heidelberg, 2006. 345-356.

[24] Kipnis, Aviad, and Adi Shamir. *Cryptanalysis of the HFE public key cryptosystem by relinearization*. Advances in cryptology - CRYPTO 99. Springer Berlin Heidelberg, 1999.

[25] Kipnis, Aviad, Jacques Patarin, and Louis Goubin. *Unbalanced oil and vinegar signature schemes*. Advances in Cryptology - EUROCRYPT 99. Springer Berlin Heidelberg, 1999.

[26] Lidl, Rudolf, Harald Niederreiter, and P. M. Cohn, *Finite Fields, second edition, Encyclopedia Math. Applications* Vol 20. Cambridge University Press. Cambridge 1997.

[27] Matsumoto, Tsutomu, and Hideki Imai. *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*. Advances in Cryptology - EUROCRYPT 88. Springer Berlin Heidelberg, 1988.

[28] Ore, Oystein. *On a special class of polynomials*. Transactions of the American Mathematical Society 35.3 (1933): 559-584.

[29] Ore, Oystein. *Theory of non-commutative polynomials*. The Annals of Mathematics 34.3 (1933): 480-508.

[30] Patarin, Jacques. *Asymmetric cryptography with a hidden monomial*. Advances in Cryptology - CRYPTO 96. Springer Berlin Heidelberg, 1996.

[31] Patarin, Jacques, and Louis Goubin. *Trapdoor one-way permutations and multivariate polynomials*. Information and Communications Security (1997): 356-368.

[32] Patarin, Jacques. *Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms*. In Advances in Cryptology - EUROCRYPT 1996, volume 1070 of Lecture Notes in Computer Science, pages 33 - 48. Ueli Maurer, editor, Springer, 1996.

[33] Patarin, Jacques, and Louis Goubin. *Trapdoor one-way permutations and multivariate polynomials*. Information and Communications Security (1997): 356-368.

[34] Patarin, Jacques. *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'98*. Designs, codes and cryptography 20.2 (2000): 175 - 209.

[35] Patarin, Jacques. *The oil and vinegar signature scheme* Dagstuhl Workshop on Cryptography, September 1997.

[36] Van Oorschot, Paul C., and Scott A. Vanstone. *A geometric approach to root finding in* $GF(q^m)$. Information Theory, IEEE Transactions on 35.2 (1989): 444-453.

[37] Von Zur Gathen, Joachim, and Victor Shoup. *Computing Frobenius maps and factoring polynomials*. Computational complexity 2.3 (1992): 187-224.

[38] Wolf, Christopher. *Multivariate quadratic polynomials in public key cryptography*. PhD thesis, Department Electrical Engineering, Katholieke Universiteit Leuven, 2005.

[39] Wolf, Christopher, and Bart Preneel. *Equivalent keys in Multivariate quadratic public key systems*. Journal of Mathematical Cryptology 4.4 (2011): 375-415.

[40] Ritt, Joseph Fels. *Prime and composite polynomials*. Transactions of the American Mathematical Society 23.1 (1922): 51-66.

[41] Shamir, Adi. *Efficient signature schemes based on birational permutations*. Advances in Cryptology CRYPTO 93. Springer Berlin Heidelberg, 1994.

A Novel Concept for Cybersecurity: Institutional Cybersecurity

İbrahim Şişaneci, Osman Akın, Muhammer Karaman, Mehmet Sağlam

Abstract—Broader use of digital technologies in all aspects of our lives, exponential expansion of cyberspace, along with complex and advanced cyber threats, lead us to reevaluate the cybersecurity concept that has been involved in our documents and directives differently or inadequately. One of the main issues in this evolving cyberspace is the perception of cybersecurity. Encapsulating a large scale of elements from individual to government level, cybersecurity approach particularly has two outstanding dimensions; national and institutional cybersecurity. Complicating, shape shifting and stretching the imagination, emerging cyber threats have demonstrated that traditional security needs and approaches do not fulfill cybersecurity requirements and can no longer withstand robustly to emerging cyber threats. In this study, a novel concept, "Institutional Cybersecurity", is suggested instead of information security (InfoSec) processes being used in present state by institutions.

***Index Terms*—Institutional Cybersecurity, Cyber risk, Dilemmas and Challenges of Cybersecurity, Evolution of Cybersecurity**

I. Introduction

Information technology has become widespread in our life that contains from cell phones and computers to more complex systems such as Information Technology (IT) infrastructures, power grids, air traffic management systems, industrial manufacturing, and banking sectors. It seems they will continue to be in upward trend in the future. Security of these IT components will be more important due to the increase of cyber attacks day by day. The more the critical infrastructures depend on the information system, the more cyber risks we have to expect.

Previous cyber attacks have showed that existing vulnerabilities in networks and information systems host serious damage risks [1]. In recent years, in addition to traditional cyber attacks, new attack techniques such as Advanced Persistent Threat (APT) related attacks, using zero-days, rootkit malwares and etc., have been used in many incidents that have a specific target to be attacked. Therefore, cyber attacks need to be handled comprehensively due to lack of attribution and geographical boundaries, low costs, low risk for the attacker, and a large scale of applicability. Hence, technical measures are not enough alone to cope with these kinds of complex cyber threats.

I.Şişaneci is with the Comp.Eng.Dept., Gebze Institute of Technology, Gebze-Kocaeli,Turkey, (e-mail: sisaneci@gyte.edu.tr).
O.Akın is with the Comp.Eng.Dept., Hacettepe University, Ankara,Turkey, (e-mail: oakin@hacettepe.edu.tr).
M.Karaman is a Cyber Security Expert, (e-mail: muammerkaraman29@gmail.com).
M.Sağlam is with the Comp.Science Dept., VirginiaTech, Virginia, USA, (e-mail: msaglam@vt.edu)

The terms as InfoSec, Information and Communication Technology (ICT) security, cybersecurity, etc. have utilized to define different concepts to address a wide variety of risks. In traditional cybersecurity perception, familiar terms are frequently used such as ICT security, InfoSec, information assurance, cybersecurity and so forth. By the dramatic up growth in the complexity of malwares and computer viruses, institutions could be vulnerable to cyber attacks due to the emerging cyber risks. Therefore, from now on emerging cyber risks should be elaborately redeemed and scrutinized in a new sense of cybersecurity awareness (c-saw). However, advanced multi-dimensional and complex cyber attacks necessitate and implicitly bring forth some other definitions and concepts like National Cybersecurity, Individual and Corporation-level InfoSec, and so on.

In this study, the evolution of cybersecurity is reviewed and the need of a new cybersecurity concept is emphasized. Besides, a new concept to provide institution-level cybersecurity is also proposed. The term "institution" is used for public/private companies that have infrastructures under potential cyber risks and critical services. This new concept enables us to understand cyber risks better than traditional approaches and basically contains cybersecurity challenges, components and main principles in institutional-level.

The organization of this study is as follows. In Section 2, we briefly define crucial terms as InfoSec, cyberspace and cyber threats. In Section 3, we briefly review InfoSec approach and evolution of cybersecurity, giving special emphasis on its challenges and dilemmas. Next, in Section 4, we propose a concept, "Institutional Cybersecurity", in particular the main features and principles of Institutional Cybersecurity, and components of institutional cybersecurity. Finally, the conclusions and future work are presented in Section 5.

II. Cyber Environment & Security Terms

A. Cyber Environment

Cyberspace: The cyberspace defined as "the notional environment in which communication over computer networks occurs." or "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" is growing rapidly [2].

Cyber Risk: Cyber risk, inherently exists in all IT assets, is a kind of risk which occurs in a variety that from individuals to international organizations that have critical IT assets. Cyber risk is specified as a group of risks, which differs in technology, attack vectors, means, etc., rather than one specific risk. The value of cyber risk is equal to

multiplication of probability and impact of cyber threats. Moreover, Cyber risks have two characteristics as having great potential impact and low probability (Fig. 1) [3]. Although traditional security focuses on many threats having high probability and average level impact on IT assets, cyber risk based security deals with cyber threats having low probability and very high impact on IT assets.

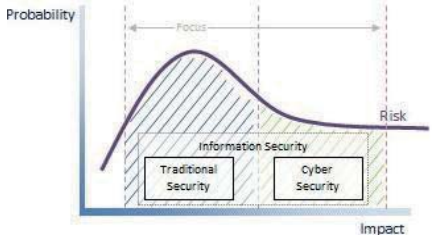


Fig. 1. Probability and Impact of Cyber Risk [3]

Cyber threats and attacks: After specifying the cyber risk, there is another crucial term, cyber threat. Cyber threat can be defined as a potential situation that covers the distortion of information, changing the information by unauthorized people, disclosing or stealing information or interrupting its accessibility. The source of cyber threat may be a single computer that is infected, or that may be a bot-net which could consist millions of computers. Therefore, even a single computer in the cyber environment, both with the information it contains and its connection the other systems, can be a source for hackers to reach critical systems. A list of cyber attack trends is presented (in Table I) conducted between 1990s and 2013. Briefly, cyber attacks can be vary from a dummy computer virus (Morris Worm) to an Advance Persistent Threat (APT), and they are evolving continuously and exponentially. These cyber attacks could be classified as: Cyber Crime, Hacktivisim, Cyber Terrorism, Cyber Espionage and Cyber Warfare [4].

B. Security Terms

The question "How can an IT asset get secured in this dangerous and complex cyberspace?" is origin of many security terms. The terms InfoSec, information assurance (IA), and computer security (CompuSec) are key cyber related security terms.

Information Security

Currently, the terms InfoSec and IA are frequently used. InfoSec is defined as protecting the information or information system from unauthorized access, modification or destruction in NIST Glossary of Key Information Security Terms [5]. According to the international standard ISO/IEC 27002:2005, Information Security is "preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved".

Information Assurance

A more comprehensive term than InfoSec is information assurance that includes practice of InfoSec. IA is "the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. IA includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data. It uses physical, technical and administrative controls to accomplish these tasks. While focused predominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form" [6].

TABLE I
CYBER ATTACK TRENDS

-Internet social engineering attacks	-Windows-based remote access trojans (Back Orifice)
-Network sniffers &Packet spoofing	-Email propagation of malicious code
-Analysis of vulnerabilities in compiled software without source code	-Wide-scale trojan distribution
-Cyber-threats & bullying (not illegal in all jurisdictions)	-Targeting of specific users
-Automated probes and scans	-Anti-forensic techniques
-GUI intrusion tools	-Wide-scale use of worms
-Automated widespread attacks	-Sophisticated botnet command and control attacks
-Widespread, distributed denial-of-service attacks	-Mobile device(phone) Android exploiting
-Industrial espionage	-Advance Persistent Threat (APT) [61]
-Executable code attacks (against browsers)	-Cloud Attacks
-Session-hijacking	-Embeded malwares
-Widespread attacks on DNS infrastructure & using NNTP to distribute attack	-Hardware based malicious components
-"Stealth" and other advanced scanning techniques	-Old school malwares for spying (MiniDuke)

Cybersecurity

As we come to cybersecurity term, there are many definitions in use, however we would present a couple of these: First, cybersecurity is "the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" [2] Second, "Cybersecurity is the sum of efforts invested in addressing cyber risk, much of which was, until recently, considered so improbable that it hardly required our attention" [3]. Third, from International Telecommunication Union's (ITU) point, it is "The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."

Institutional Cybersecurity

As a result of rapid changes in cyber environments, expansion of cloud computing, and residual use of mobile devices particularly in institutions, cybersecurity related terms should be re-handled with a broader line of sight. Therefore, in terms of institutional cybersecurity, a novel concept need has emerged. We suggested a new concept, Institutional Cybersecurity, to symbolize and fit for all institution-level cybersecurity issues. The Institutional Cybersecurity is the capability which consists of InfoSec components and cooperation with other cybersecurity partners and cybersecurity awareness from the cyber risk perspective.

III. INFORMATION SECURITY APPROACH AND EVOLUTION OF CYBERSECURITY

A. General Security Concept & Technological Developments

Security concept contains components that are assets, risks, threat, vulnerabilities and countermeasures. Generally,

security is a process of the selection and implementation of security controls (also called countermeasures) which help to reduce the risk posed via vulnerabilities [7]. The security process of information and elements that are related to information is evolving as the technology behind it. The motivations of this evolution are mainly changing assets and risks that have pose by the increase of dependency on Internet, the set of assets is growing every day as mentioned above. Unfortunately, variety of cyber risks is growing faster. Because of the highly interconnected nature of these assets, every vulnerability has impacts on the others that makes the evolution exponential. On the other hand, the change in security side is inherently behind this technological evolution. The new assets that are connected to the network and their vulnerabilities must be analyzed, or even in some cases they may get attacked by competitors to be understood what the real consequences could be. Then the solutions would be developed to address these emerged risks. However, conceptualization, developing strategies, and doctrines follow that.

B. Information Security Approach

Understanding Information Security approach and the evolution of cybersecurity requires analyzing the question that how/why the key concepts have emerged? The concepts that must be taken into account in this case are ICT security, InfoSec, and cybersecurity.

ICT security is the intersection area of InfoSec and cybersecurity. ICT security covers information technology infrastructure such as computers, computer networks, data centers as its assets. Furthermore, these assets could be extended in InfoSec to all sorts of information to be secured. By this definition, InfoSec covers not only the data in ICT but also the information which is not stored or transmitted via ICT (Fig.2). Nevertheless, as stated above, cybersecurity conceptually covers both information and non-information based assets that have posed risks via ICT. The types of these assets include a wide variety of what that also covers critical national infrastructures, household appliances, and even also human.

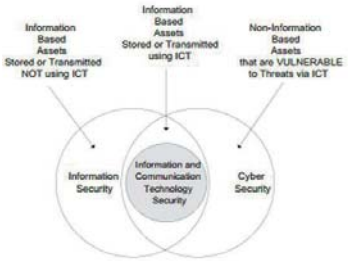


Fig. 2. Area of interest for Information and Cybersecurity [7]

As a matter of fact, in cyberspace, the assets need to take consideration could be anyone or anything that is accessible via cyberspace. Briefly, InfoSec intends to secure whole IT infrastructures and processes. But, due to its enormous size, that may not possible to secure cyberspace as a whole. Instead of this, cybersecurity focuses on eliminating vulnerabilities on IT assets.

C. Evolution of Cybersecurity

The concept of cybersecurity first appeared with cyber breaches. And then, it has taken the name of cybersecurity when cyber breaches damaged government networks. By the expansion of cyberspace, the concept of InfoSec becomes inadequate to address multi-dimensional and complex cyber attacks. For instance, one of the advanced cyber espionage malware, "Red October" targeted diplomatic and government institutions worldwide for at least five years which has been detected in January 2013 [8]. Another example is the Industrial Control Systems Computer Emergency Response Team (ICSCERT) report of the US Department of Homeland Security [9] has shown that; In the first half of the fiscal year 2013, (October 1, 2012–May 2013), the highest percentage of incidents reported to ICS-CERT occurred in the energy sector at 53%. For another example, as stated by Verizon 2013 security report [10], which reported 2012 alone consists of 47000 security incidents, show that the growth of recent data breaches alarm that the organizations to take new actions. These examples support the legitimacy of the new concepts such as National Cybersecurity, Individual and Corporational Information Security, Cyber Awareness (c-saw) and so forth. That is the current result of the ongoing evolution. The continuous national/international level InfoSec efforts or recommendation publications may not adequately address the risks of cyberspace. As the current situation, InfoSec efforts were limited to their InfoSec management systems which are developed in line with international standards such as ISO 27001, NIST-800 series and COBIT. The current versions of these international standards have failed to meet completely cybersecurity requirements. Many countries and international organizations have developed their cybersecurity strategies that mainly focus governance, cooperation and active defense. However, in institutional level, there is no international standard or guideline which consists cooperation, integration to national security and active defense to cope with cyber threats, such as APTs.

D. Challenges and Dilemmas of Cybersecurity

Due to the complex nature of cybersecurity, many challenges and dilemmas have been emerged from both national and institutional perspectives. For instance, in National cybersecurity Framework Manual, prepared by NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), dilemmas that nations face and have to deal with as establishing, maintaining and enforcing cybersecurity are stated that are stimulate the economy vs. improve national security, infrastructure modernization vs. infrastructure protection, private vs. public sector, data protection vs. information sharing, andfreedom of expression vs. political stability [11]. Similar to national level challenges, institutions also need to cope with some dilemmas that may be filtered from national challenges or may be localized version of national ones. The outstanding dilemmas of institutional cybersecurity are IT security cost vs. institutional cybersecurity, privacy vs. information sharing, homegrown human resource vs. outsourcing, open source vs. licensed software, and cooperation vs. loss of reputation [12]-[13]- [14]-[15].

Due to widely diverse cyber attacks, mentioned in Table I, sustainable cybersecurity is no longer a solely responsibility of cybersecurity personnel. But, it is a common

responsibility of all personnel, stakeholders and partners. For instance, an employee, without having enough cybersecurity knowledge and awareness or who underestimates cybersecurity regulations taken by the institution, may anytime cause deadly losses. Thus, this incident may result sometimes loss of reputation, economic assets, and so forth [1]. Along with national and institutional dilemmas, institutional cybersecurity challenges must be analyzed to understand the constraints. These challenges could be listed as; lack of broader perception of cybersecurity, information sharing, legal issues (legal suspense), leadership, cost, human resource, expansion of cyberspace, infrastructure insufficiency, standards addressing the majority, building common cybersecurity picture, lack of metrics of cybersecurity, lack of coordination and information sharing, security and usability issues, bureaucracy, insider threats, migration plan (unprotected systems to secure systems), technological backward compatibility and etc, [16].

E. Lack of broader perception of cybersecurity

The challenges of cybersecurity can be diversified endemically to nations and institutions according to their line of sight to cybersecurity. For example, according to Dmitriy Ayrapetov, Director, Product Management, Dell SonicWALL; the major cybersecurity challenges for businesses through 2013 will come from: increase in exploit kits, increase in mobile device security threats and increase in sophistication of threats [17]. But it may vary across analyses of experts on cybersecurity field; from our perspective, the number one cybersecurity challenge for both national and institutional level is lack of broader perception of cybersecurity. And to bring sectors and institutions to a level of security standard depends heavily on national perception of cybersecurity issues that also makes that the challenge number one. For instance, some governments may choose to centralize the majority of decision-making mechanisms, while others may devolve this to a lower level according to a particular need (e.g., to build resilience and responsiveness into highly decentralized and mostly privately-owned critical infrastructure) [11]-[18]. This decision would mainly effects the body of national cybersecurity issue. The cybersecurity burden on private sector may not desired but, even the government side of cybersecurity is tightened, it is just as easy for a terrorist organizations or other state-sponsored actors to take out a private-sector entity that will really impact the nation [19].

IV. AN EMERGING CONCEPT: INSTITUTIONAL CYBERSECURITY

With emerging new cyber risks and more complex malwares, countries and international organizations like NATO, ENISA, etc. have been looking for new ways to fight against challenging issues [16]-[20]. The essential step for countries is to form a national cybersecurity strategy. Generally, in that kind of strategies; the importance of policies, cybersecurity countermeasures and some action plans are taken into account at upper levels. Even though these strategies and policies cover intensively military, intelligence and critical infrastructures, the institution-level cybersecurity is ignored. In order to provide a robust national level cybersecurity, we believe that institution-level cybersecurity should be initial step to take forward. When we look at the whole cybersecurity organization structure (Fig. 3), institution-level cybersecurity forms the body part of cybersecurity organization which contains the entities as individuals, public/private institutions, military, government, and international organizations. Since the body part has a critical role to interact with all other entities, it affects the success of upper level cybersecurity.

While the weakest link in InfoSec is human being, in terms of national security the weakest link is the weakest institution having critical infrastructures or cyber risks. Unlike stated in national cybersecurity strategies, in terms of institutional cybersecurity, not only institutions which manages critical infrastructure but also other companies having cyber risk should be taken into account to ensure a robust cybersecurity. For example, a software company, without having any critical infrastructure, could be a target for cyber attacks due to stolen software code or root driver (SIEMENS & Stuxnet case)[21].

Current trends (Table I) including a complex attacks such as Stuxnet case make the need of a new concept inevitable. To address this need, our proposed concept, Institutional Cybersecurity could be defined as; A comprehensive concept for ensuring robust and resilient institution-level cybersecurity by; providing cyber situational awareness, addressing emerging cyber risks, encourage inter and intra institutional cooperation and coordination, and presenting a flexible framework for its applicability, for public/private institutions having critical infrastructures or having cyber risks for their business continuity.

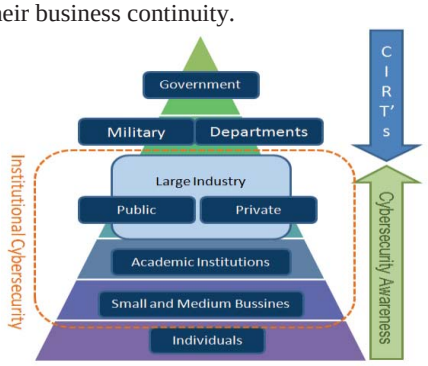


Fig. 3. Cybersecurity Organization Structure

Components and Principles of Institutional Cybersecurity

Our proposed concept provides a generic manner that every institution can adapt it for its own security needs to develop their institutional cybersecurity capability. To reach this goal, the main principles of Institutional Cybersecurity are presented as follows:

1-Cybersecurity approach must be holistic,

2-A flexible management style should be adopted,

3-Risk management-centered continuous improvement methods should be implemented,

4-In addition to coordination of public, private, academic, and non-governmental organization, international cooperation and information sharing should be bottom lines for security,

5- Transparency, accountability, ethical values, freedom of speech must be endorsed,

6-Setting balance between security and applicability is important.

In the light of these principles, in order to have efficient institutional cybersecurity, Institutional Cybersecurity should have fundamental components as presented (Fig. 4).

Policy, Strategy and Standards: Detailed cybersecurity policy, strategy and secure system management principles can help institutions to take the first step.

Cyber Risk Management: Cyber risks can be minimized and managed by utilizing efficient risk management mechanism to unveil all threats and vulnerabilities.

Vulnerability and Threat Management: According to advances in cyberspace, vulnerability and threat management could be handled under the cyber risk management. Vulnerability management should be supported by periodical vulnerability analysis/tests and penetration tests.

Central Incident Management: Efficient prevention, fast response and mitigation against to cyber attacks can be obtained by central incident management. And, active cooperation and collaboration to national cybersecurity can be achieved via the ability to central incident management including Institutional CIRT's.

Cybersecurity Awareness and Education: Human being is the weakest link in the security chain. Therefore, cybersecurity awareness and education programs must focus mainly human factor.

Log Management and Correlation: Possible attacks and data leakage could be detected in advance and preventive actions can be performed by utilizing efficient log management and correlation.

Secure Architecture: All institutional information technology infrastructures and architectures including business partners should be reviewed and questioned from the perspective of cybersecurity.

Legal Issues: The legal regulations always stand as the most important factor to enforce and ensure cybersecurity. To prevent privacy violation and to set liability processes, proper legal regulations must be set. Otherwise, countermeasures for providing cybersecurity such as monitoring personal information may pose risks for institutions.

Business Continuity: Business continuity plans must be harmonized with Institutional cybersecurity strategies and plans.

Technical Tools: Similar to ICT security, proper software and hardware including firewalls, IPDS, anti-virus software, etc. must be used to provide comprehensive cybersecurity.

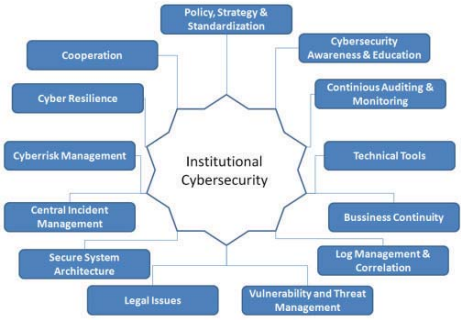


Fig. 4. Institutional Cybersecurity Components

Continuous Auditing and Monitoring: Auditing is a continuous process that contains audit tests or review procedures. Errors, policy violations, fraud, and misconducts should be audited in a timely manner to fill the control gaps and deficiencies. Monitoring is a mechanism that could be utilized to automate manual controls and processes or regular and frequent insights to avoid potential regulatory noncompliance, cyber attacks and malicious activities.

Cooperation: Cooperation with other cybersecurity partners and CIRT's are vital for institutions in order to set early warning mechanisms and effective resource sharing. Also, due to confronting asymmetric and organized cyber threats, government coordination with institutions and particularly with private sectors is inevitable.

Cyber Resilience: All efforts in the institutional cybersecurity management should be flexible enough to adapt to the dynamic developments in cyberspace. Cyber resilience can be defined in literature as "The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities conditions, stresses, or attacks on the supporting cyber resources it needs to function." [22]. A Resilient Enterprise is able to withstand systematic discontinuities and adapt to new risk environments [23] or dynamically reinvent business models and strategies as circumstances change [24]. According to [22] a Resilience framework is able to include anticipate, withstand, recover and evolve steps.

Reaching the goal of using all of these institutional securitycomponents efficiently requires achieving cybersecurity objectives in institutional level. Furthermore, main goal of Institutional cybersecurity is to cooperate these components into an integrated framework in a resilient perspective. While securing the whole system, availability and usability could be ignored unintentionally. In order to avoid this situation, resilient management model should be performed. In this perspective, our proposed institutional cybersecurity concept contains resilient solutions for challenges. Another point is to manage all these components as an integrated framework requires a leadership. Through the principles and components of proposed concept above, challenges and dilemmas for institutional cybersecurity can be resolved considerably.

V. Conclusion and Future Works

All institutions, regardless of being public or private, should definitely expect and envision emerging cyber threats. With the help of revitalized InfoSec processes to fit a holistic cybersecurity concept and high level cybersecurity awareness, assessing and analyzing the potential and possible effects of complex and advanced threats will get less hard.

As a result of this research, it can be expressed that unless cybersecurity for institutions are handled in a broader perception, professional manner and presented as an integrated solution, it will have a higher possibility to be exposured and damaged by a cyber attack at any moment.

To date, many companies and institutions have had only IT departments. However, now, institutions having cyber risks should set up a cybersecurity or CIRTs. Hereby, the

institutional cybersecurity could be taken up in a more generic manner and encapsulates above-mentioned issues.

With the establishment of an institutional cybersecurity organization; the exploitable points in the system can be corrected by performing vulnerability test, the abnormality can be detected in real-time by monitoring logs, the situational awareness can be improved by applying scenarios, the risk assessment can be carried out by establishing integrated systems and probably the cyber attacks can be prevented before they start.

Due to their field-based and structural differences, each institution can prepare and follow a different cybersecurity road map peculiar to itself. But, as a first step, the recommended concept can be evaluated as an inception guide for institutions willing to start building a new cybersecurity capability.

In this study, we handled the cybersecurity issue from a new perspective for institutions and discussed in details. This new cybersecurity concept has also contributed and filled the conceptual absence of lower-governmental levels in cybersecurity organization structure.

Institutional cybersecurity will be an emerging fertile research area. There are many ways to extend this work in the future. For instance, we are planning to propose a new road map for institutions which is going to contain a transforming guideline to set forward a new concept in cybersecurity management processes.

REFERENCES

[1] H. Senturk, Z. Çil, and Ş.Sağıroğlu, "Cyber security analysis of turkey", International Journal of Information Security Science, vol. 1, no. 4, pp.112–125, 2012.

[2] Oxford dictionaries. (2013, Jun.) [Online] Available: http://oxforddictionaries.com

[3] M. Barzilay. (2013, May) "A simple definition of cybersecurity", [Online]Available:http://www.isaca.org/KnowledgeCenter/Blog/Lists/Posts/Post.aspx?ID=296

[4] M. Clancy, "Arm yourself for cyber war-Are you next?" *in Sibos Conference Panel 2012*, 2012.

[5] R. Kissel, "Glossary of key information security terms". *DIANE Publishing*, 2011.

[6] N. Seddigh, P. Pieda, A. Matrawy, B. Nandy, I. Lambadaris, and A. Hatfield, "Current trends and advances in information assurance metrics." in *PST*, 2004, pp. 197–205.

[7] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, 2013.

[8] KasperskyLabratuaries. (2013, Jun.), "Red october an advanced cyber espionage campaign targeting diplomatic and government institutions worldwide", [Online] Available: http://www.kaspersky.com/about/news/virus/2013/

[9] ICS-CERT. (2013, Jun.) "Ics-cert monitor report between april-june 2013 of department of homeland security".[Online]. Available: http://icscert.uscert.gov/sites/default/files/ICx-CERT Monitor AprilJune2013 3.pdf

[10] (2013, Jun.) Verizon. [Online]. Available: http://www.verizon.com

[11] A. Klimburg, Ed., "National cyber security framework manual". *NATO CCD COE Publications*, 2012.

[12] B. Adelmann, "Cispa is big brother's friend," 2012.

[13] S. Alexander, "Rise of outsourcing poses new cybersecurity problems," 2011.

[14] B. Gourley, "Open source software and cyber defense," 2009.

[15] "Security task force: Public-private information sharing," 2012.

[16] NATO. (2013, Jun.) Nato web site. [Online]. Available: http://www.nato.int, June,2013

[17] Techrepublic. (2013, May) "Cybersecurity challenges in 2013". [Online].Available:http://www.techrepublic.com/blog/security/cybersecuritychallenges in-2013/9038

[18] B. Karabacak and S. OZKAN, "Critical infrastructure protection status and action items of turkey," 2009.

[19] APCOForum.com. (2013, Jun.) "The cyber security challenge: The risk of inaction". [Online]. Available: www.apcoforum.com

[20] ENISA. (2013, May) "European network and information security agency glossary". [Online]. Available: www.enisa.europa.eu/act/res/files/glossary

[21] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope," ESET LLC (September 2010), 2010.

[22] R. A. Caralli, J. H. Allen, and D. W. White, CERT "Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience". *Addison-Wesley Professional*, 2010.

[23] R. Starr, J. Newfrock, and M. Delurey, "Enterprise resilience: managing risk in the networked economy," *Strategy and Business*, pp. 70–79, 2003.

[24] L. Valikangas and G. Hamel, "The quest for resilience," 2009.

İbrahim Şişaneci is currently a PhD candidate in Comp.Eng.Dept., Gebze Institute of Technology (GIT). He received M.S. degree in Comp.Eng.Dept., GIT and BS degree in Comp.Eng.Dept. from Marmara University. His research interest are HCI, usability, InfoSec, Cybersecurity, data mining.

Osman Akın is currently a PhD student in Comp.Eng.Dept.,Hacettepe University. His research interest are cybersecurity, web based software, web based software security and computer vision.

Muhammer Karaman received his BS degree in Turkish Army Academy in 2005. His research interests are cyber war, cyber electronic war, cybersecurity.

Mehmet Sağlam received BS degree in Industrial Engineering from Turkish Naval Academy in 2009. He is currently a M.S. degree student in Department of Comp.Science, VirginiaTech. His research interests are Critical Infrastructure Protection and Cyber Warfare. In particular, his current research focuses on Power Grid Cyber Security.

Halk ve Özel Bulut Yapılarında Karşılaştırmalı Performans Ölçümleri

Hakan Aydın, Oumout Chouseinoglou

***Özetçe*— Bulut bilişim teknolojisinin hızla yaygınlaşmaya başlaması, bu sistemlerin performansları konusunda çalışmaların yapılması sonucunu doğal olarak ortaya koymaktadır. Bu çalışmada, Halk Bulut bilişimi farklı nedenlerden dolayı kullanmaktan çekinen kuruluşlara Özel Bulut yapıları bir alternatif olarak sunulmakta ve Özel Bulut Bilişim ile Halk Bulut Bilişim performansı karşılaştırmalı kıyaslama işlemi ile değerlendirilmektedir. Bunlara ek olarak gerçek bir organizasyon ortamında fiziksel sistemlerle, Özel Bulut Bilişim performans değerleri de bu çalışmada incelenmektedir.**

***Anahtar Kelimeler*— Bulut Bilişim, Özel Bulut, Karşılaştırmalı Sınama, Sanallaştırma**

***Abstract*— The rapid spread of cloud computing has resulted in the need of conducting benchmarking studies, particularly in performance related issues. In this study, Private Cloud Computing is proposed as an alternative for organizations which are not willing or are precluded to adopt Public Cloud Computing for numerous reasons and the performances of several Private and Public Cloud configurations are assessed with the use of benchmarking tests. Additionally, the performance capabilities of physical systems and Private Cloud Computing are compared in an actual organizational environment.**

***Index Terms*—Cloud Computing, Private Cloud Computing, Benchmarking, Virtualization**

I. GİRİŞ

Ekonomik krizlerin dolaylı bir sonucu olarak kurumlarda az, ancak etkili kaynak kullanımı önem kazanmış ve tüm iş gruplarının kendi içlerinde yeniden yapılanması gerekliliği ortaya çıkmıştır. Bilişim sektörü küresel düzeyde bu ihtiyaca ilk tepkiyi 2000 yılların sonlarına doğru [1], fiziksel sistemlerinin sanal ortamlara taşınması ve bir fiziksel sistemin üzerinde birçok sanal sistem kullandırılması ile göstermiştir. Bu çözüm, gerek elektrik harcamalarında, gerekse işgücü ve donanım boyutlarında kurumların maliyet kalemlerinde tasarruf etmesini sağlamıştır [1].

Bulut bilişim, minimal yönetim, iş gücü ve hizmet sağlayıcı etkileşimi ile uygun veya talep edilen bir ağ erişimi üzerinden hızla sağlanan ve uygulamaya geçen ortak bir havuzdaki yapılandırılabilir bilgisayar kaynaklarının olduğu bir hizmet modeli olarak tanımlanmakta [2] ve dört farklı dağıtım modeli ile açıklanmaktadır:

1-*Özel (yerel) bulut,* sadece bir organizasyon için işletilip, bir kuruluş ya da bir üçüncü şahıs tarafından yönetilmektedir.

2-*Topluluk bulut,* altyapının birçok organizasyon tarafından paylaşıldığı ve güvenlik gereksinimleri, kurallar, hedefler vb. ortak endişelerin özel bir topluluk tarafından desteklenmesidir.

3-*Halk (genel) bulut,* kişiler veya büyük sanayi şirketlerine açık olup, bir kurum tarafından hizmet ticareti yapılmaktadır.

4-*Melez bulut,* yukarıda bahsedilmekte olan iki veya daha fazla dağıtım alt yapısının beraber kullanılmasıdır.

Bulut bilişimin temel karakteristikleri; talebe göre kullanılması, müşterilerin kendi kendine bulut bilişim hizmeti kullanması, geniş ağ erişimine ve kaynak havuzuna göre esneklik hızına sahip olması ve son olarak ölçülenebilir bir hizmet olmasıdır. Hizmet olarak yazılım (SaaS), bir hizmet olarak platform (PaaS) ve bir hizmet olarak altyapı (IaaS) olmak üzere üç temel hizmet sunum modeli bulunmaktadır. Bu çalışmada yapılan performans testlerinde IaaS üzerine odaklanmış olup, bu hizmet modeli göz önüne alınarak sonuçlar elde edilmiştir.

Günümüzde bulut bilişim, donanım, depolama ve sunucu kaynaklarının internet üzerinden yönetilmesini sağlamak amaçlı yaygınlaşmaktadır. Halk ve topluluk bulut dağıtım modellerinde kullanıma göre bir ücret ödenmesi, devamlı kullanım masraflarının olması, kurumların özel ve gizli şirket bilgilerini kurum dışı sunucularda tutmak istememeleri ve en önemlisi performans açısından yeterli seviyede olup olmadıkları konusundaki endişeler, kurumların bu teknolojiye geçmeden önce onu çok boyutlu değerlendirme yapması gerekliliğini ortaya koymaktadır [3].

Bu çalışma iki temel kısımdan oluşmaktadır. Birinci kısımda, önde gelen halk bulut bilişim hizmeti sağlayıcılarından Amazon EC2, Flexiscale ve Rackspace platformlarında 2011 yılında yapılmış olan performans değerlendirmelerinin sonuçlarıyla, bu çalışma kapsamında bir kurum için kurulmuş olan özel bulut platformunda, aynı test araçlarıyla yapılmış performans testlerinin sonuçları kıyaslanmıştır. Özel bulut alt yapısı oluşturularak, halk bulut performansıyla özel bulutun performans değerlendirmesi Phoronix test [4] süiti kullanılarak yapılmış, sonuçlar üstünden çıkarımlarda bulunulmuştur. Çalışmanın ikinci kısmında, özel sektörde faaliyet gösteren bir bilgi teknolojileri kurumuna ait iki adet fiziksel sunucu (e-posta ve etki alanı sunucuları) Vmware Converter programı ile bire bir olarak sanallaştırılmış ve Passmark v7 performans ölçüm programı ile fiziksel sunucular ile performansları sınanmıştır. Gerek özel bulut yapısında çalışmakta olan

H. Aydın, Uluslararası bir enerji şirketinde Bilgi Teknolojileri Md.Yrd. olarak çalışmakta ve Başkent Üniversitesi, Bilgi Teknolojileri ve Sistem Yönetimi programında yüksek lisans çalışmalarına devam etmektedir (Tel: +90 312 291 7500; e-posta: hakan.aydin@kinesisenerji.com).

O. Chouseinoglou, İstatistik ve Bilgisayar Bilimleri, Başkent Üniversitesi (e-posta: umuth@baskent.edu.tr)

sunucular, gerekse fiziksel sunucuların merkezi işlemci birimi (MİB) ve disk performansı testleri yapılmıştır. Tüm bu performans testlerinin sonuçları kaydedilmiş ve yorumlanmıştır.

Bu bildirinin ikinci bölümünde bulut ve sanal sistemler üstünde yapılmış benzer performans ölçüm çalışmaları sunulmaktadır. Üçüncü bölümde çalışmada kullanılan test yazılımları ve donanımlar kısaca tanıtılmaktadır. Dördüncü bölümde gerçekleştirilen testler ve sonuçları verilmektedir. Son bölümde elde edilmiş sonuçlar doğrultusunda planlanan sonraki dönem çalışmaları kısaca gözden geçirilmektedir.

II. LİTERATÜR

Iosup vd. [5] bilimsel çalışmalar için kullanılan sistemler ile süper bilgisayarlara göre daha ucuz, dağıtımlı sistemlere göre de daha güvenilir olan bulut bilişim hizmetini araştırmak için IaaS hizmeti sunan farklı kurumlarda bulut bilişim sistemlerinin performans testlerini yapmışlardır. Çok Amaçlı İşlemler (ÇAİ) olarak tanımladıkları yöntemde, buluta ait çeşitli sistemler üzerinde ÇAİ gerçekleştirerek, elde ettikleri sonuçlar üzerinde çıkarımda bulunmuşlardır. Tüm testlerin sonunda mevcut bulut bilişim hizmetinin, ÇAİ merkezli bilimsel çalışmalar için ihtiyaç duyulan bilişim hizmetlerinin karakteristik özelliklerine benzemediği ve performansının yeterli düzeyde olmadığını belirtmişlerdir.

Cloud Analyst yazılımı ile yapılan kıyaslama testlerinden elde edilen verilerin çevrimsel sıralı bir algoritma ile analizi [6]'da verilmekte, mesafe, yazılım, donanım ve kullanıcı sayısının bulut bilişimde bulunan sunucuların performansı ile doğrudan ilişkili olduğu ve sabit bir performansın elde edilemediğini ortaya konmaktadır. Steinmetz vd. [7] aynı özelliklere sahip donanımlara Eucalyptus ve OpenStack yazılımlarının kurulumlarını yaparak, özel bulut performans testini gerçekleştirmişlerdir. Test aracı olarak Byte UNIX kullanılan bu çalışmada, Eucalyptus'un, Open Stack'a kıyasla daha yüksek performansa sahip olduğunu belirlemişlerdir. Ek olarak yazarlar, bulut bilişim ile yönetim sisteminin aynı donanım üzerinde olması nedeniyle kaynak kullanımında sorunlar yaşandığını tespit etmişlerdir. Bu çalışmanın sonucu olarak, iki bulut yazılımın test edilmesi ve arada performans farklarının görülmesi, özel bulut bilişimde donanım kadar yazılımın da önemli olduğu gerçeğini ortaya koymaktadır.

Yüksek performanslı dağıtımlı bilişim ve bulut bilişim sistemlerinin kıyaslaması ve bilimsel çalışmalar açısından performans değerlendirmesi Vecchiola vd. tarafından [8]'de verilmektedir. Çalışmalarında yazılım yükleme süresi, veri transfer süreleri vb. testler sonucunda, Amazon EC2'nin performansının, Grid 5000 dağıtımlı sisteme göre daha düşük olduğu sonucuna varmışlar, dolayısıyla şu anda bilimsel çalışmalar için yüksek performanslı bulut bilişim hizmetinin yeterli düzeyde olmadığını ortaya koymuşlardır. Gillam vd. [9] , Amazon EC2, Rackspace, IBM ve Openstack bulut bilişim hizmetlerini çeşitli düzeylerde LINPACK, MPPTEST ve Bzip2 gibi farklı performans test programları kullanarak kıyaslamışlardır. Genel olarak her bulut bilişim servis sağlayıcının farklı testlerde farklı tepkiler verdiği görülmüş, bunların içerisinde Rackspace en iyi performans değerine sahip olmuştur.

En yaygın kullanılmakta olan bulut bilişim hizmet sağlayıcıları olan Amazon, Rackspace ve Flexiscale şirketlerinin halk bulut bilişim performans testlerini Lenk vd. tarafından [10]'da yapılmıştır. Burada aynı özelliklere sahip, Ubuntu 32 bit ve 64 bit sunucular üzerinde Phoronix süiti kullanılmıştır. Yazarlar sonuçları değerlendirerek, bulut bilişim hizmet sağlayıcıların genel hizmet performansında değişiklikler nedeniyle fiyat/performans karşılaştırmasında istenilen sonuca ulaşamadıklarını belirtmişlerdir.

III. TESTLER VE KONFİGÜRASYONLAR

Lenk vd. [10] bulut bilişimin performans ve ücret karşılaştırmasını yapabilmek için, önde gelen bulut bilişim sağlayıcılarını ve uygun performans kıyaslama programlarını belirleyip, çeşitli konfigürasyonlardaki Linux sunucuların performans testlerini yapmışlar, bulut sağlayıcıları fiyat ve performans olarak değerlendirmişlerdir. İş süreçlerinin doğruluğu, önde gelen halk bulut platformları üzerinde çalışmış olmaları ve kullanmış oldukları testlerin bilimsel çalışmalarda kullanılmış olmasından dolayı Lenk vd.'nin [10] yaklaşımları bu çalışmanın birinci kısmındaki karşılaştırmalı sınamada kullanılmak için tercih edilmiş ve paralel olarak özel bulutta tekrarlanmıştır.

Özel bulut ile halk bulut karşılaştırmalı sınamasında, farklı akademik çalışmalarda [11] [12] kullanılan, Linux tabanlı bir karşılaştırmalı kıyaslama programı olan Phoronix test [4] süitinin 2.6.1 sürümü kullanılmıştır. Diğer yandan, özel bulut bilişim ile fiziksel sunucuların karşılaştırmalı sınama işlemi için, Vmware özel bulut performans testlerinde ve benzer akademik çalışmalarda [13] [14] kullanılan Passmark performans testi [15] kullanılmıştır.

Çalışmanın birinci aşaması olan, halk bulut IaaS hizmeti ile özel bulut karşılaştırmalı sınama işlemini yapabilmek için Intel i7 alt yapısına sahip sunucu ile Intel Xeon işlemci kullanan iki profesyonel donanım kullanılmıştır. Vmware Vsphere 5.0 ESXi yazılımı ana bilgisayar üzerine, bir adet 32 bit Ubuntu 10.04, 2GB bellek, 1 çekirdek ve 1 sanal çekirdek işlemciye sahip, Lenk vd. [10] yaptığı testler için kurdukları sunucu konfigürasyonlarının benzeri olan bir Linux dağıtımı kurulmuştur. i7-2700K, 3.5GHz işlemcili ESXi ana bilgisayarının disk yapısı SATA ve RAID 0 iken Xeon E5420, 2.50 GHz işlemcili ESXi ana bilgisayarının üzerinde bulunduğu sunucu SCSI ve RAID 5 disk alt yapısına sahiptir.

Lenk vd.'nin [10] ileri düzey olarak belirttikleri sistem değerlerini karşılaştırmak amacıyla, karşılaştırmalı sınama yapılan Vmware i7 işlemcili sunucuda bulunan Vsphere 5.0 ESXi ana bilgisayarının üzerine, 8 GB bellek, 4 çekirdek ve 2 sanal çekirdek donanıma sahip Ubuntu 64 bit 10.04 sunucu kurulmuştur. Xeon E5420, 2.50 GHz işlemcili sunucuya da aynı işletim sistemi kurulmuştur. Tüm sunuculara Phoronix test süit 2.6.1 yüklenmiştir. Buradaki donanım özellikleri ve yazılım sürümleri kıyaslama yapılacak olan halk bulut değerleriyle aynıdır. Özel buluta ait sunucu konfigürasyonunun, esas alınan çalışmanın [10] tarihine yakın olmasına dikkat edilmiştir. Xeon işlemcili özel bulut alt yapısı kurulurken, çalışmanın tarihinin 2011 olması nedeniyle, 2010 yılında satın alınmış bir sunucu kullanılmıştır.

Çalışmanın ikinci kısmında, fiziksel olarak çalışan Intel Xeon E5345, 2.33 GHz, işlemcili, 8 GB belleğe sahip 64-bit Windows Server 2003 R2, ***etki alanı sunucusu***, Vmware

Vsphere 5.1 ESXi ana bilgisayarının üzerine, Vmware Vconverter programı ile sanal sunucuya çevrilmiştir. Aynı şekilde, fiziksel donanım üzerinde Intel Xeon E5345, 2.33 GHz işlemcili, 8 GB bellek, 64 bit Windows Server 2003 R2 ***e-posta sunucusu***, Vmware Vconverter programı vasıtasıyla Xeon E5420, 2.50 GHz işlemcili Vmware vSphere, ESXi 5.1 yazılımına sahip ana bilgisayar üzerine sanallaştırılmıştır. Sanallaştırma işlemlerinin bire bir çeviri işlemi olması nedeniyle, sanal sunucular, fiziksel sunucular ile aynı özelliklere sahiptir. Sanallaştırma sırasında her iki özel bulut sistemin tüm ayarları aynı şekilde dönüştürülmüş, bellek yapısı ve disk boyutu gibi karşılaştırmalı sınama sonuçlarını etkileyecek herhangi bir değişiklik yapılmamıştır. Yapılan testte özel bulut ana bilgisayarının işlemcisi Xeon E5420, 2.50 GHz iken, fiziksel sunucuların işlemcisi Intel Xeon E5345, 2.33 GHz'dir.

İkinci çalışmada fiziksel olarak çalışmakta olan e-posta ve etki alanı sunucularının donanımları Intel Xeon E5345, 2,33GHz işlemcili, 8GB bellek ve 273 GB'lık RAID5 yapısında bir sabit disktir. İşletim sistemi Windows Server 2003 R2, SP2'dir. Özel bulut platformunda, Intel Xeon E5420, 2.5GHz özellikli ve RAID 5 disk yapısına sahip donanımın üzerinde Vmware 5.1 ESXi ana sunucu kurulmuştur. Ana sunucu üzerine ayrı ayrı 8GB bellek ve 273 GB sanal hard diske sahip e-posta ve etki alanı sunucuları, fiziksel sunucularla aynı özelliklere sahiptirler.

IV. TEST SONUÇLARI

A. Değerlendirmenin Yapılması

Karşılaştırmalı kıyaslama sonuçlarının değerlendirmesi yapılırken halk bulut sonuçlarının listesi Lenk vd.'nin [10] çalışmalarında kullandıkları tablolama biçimi kullanılarak tablo haline getirilmiştir. Yüzdesel olarak performans farklarının değerlendirmesi için, halk bulut karşılaştırmalı kıyaslama değerinin en iyisi olan değer ile bu çalışmadaki özel bulutta elde edilen en iyi değerin yüzde farkı alınarak hesaplanmıştır. Tablo 1'de testlerde kullanılan ölçü birimleri, açıklamaları ve yorumlama yöntemi verilmiştir. Phoronix test süitinde bulunan OFMM testi tüm karşılaştırmalı sınamalarda, Crafty testi de 32 bitlik sunucularda yapılan karşılaştırmalı sınamalarda kullanılmamıştır.

B. Başlangıç Düzey 32 Bit Ubuntu Karşılaştırmalı Sınaması

Xeon İşlemcili Sunucu

Lenk vd. [10] Phoronix testlerini Amazon'da 462, Flexiscale'de ise 49 defa çalıştırmışlardır. Çalışmamız kapsamında kurulan özel bulutta, tüm testler 50 defa çalıştırarak sonuçlar elde edilmiştir. Xeon işlemcili 32 bit Ubuntu sunucu özel bulut test sonuçları Tablo 2'de verilmektedir. Özel bulut ve halk bulut testlerinin karşılaştırmalı sınama sonuçları incelendiğinde John-the-ripper %16,42 ile ve OpenSSL ise %12,81 değerleriyle, halk bulutun performansının özel buluta göre daha iyi olduğu görülmektedir. Şekil 1 (a)'da yüzde miktarları verilen diğer 7 testte ise farklı oranlarda özel bulutun performansı daha iyidir. Genel olarak bakıldığında özel bulutun, halk buluta göre performansının daha iyi olduğu sonucuna varabiliriz. Özel bulut test sonuçlarındaki standart sapma değerleri, genel olarak halk buluta göre daha düşüktür (Opstone-Svd testi dışında). Standart sapmanın az olması, değerlerin kararlı olduğunu göstermektedir.

TABLO 1. PHORONIX KARŞILAŞTIRMALI SINAMA PARAMETRELERİ

Test	Kısa İsim	Açıklama	Ölçü Birimi	Küçük İyidir (Kİ)/ Büyük İyidir (Bİ)
Crafty	PT1	Açık kaynak kodlu satranç motoru performans testi	Saniye	Kİ
Dcraw	PT2	RAW'dan PPM'ye Dönüştürme	Saniye	Kİ
Espeak	PT3	eSpeak Konuşma Sentezleyicisi	Saniye	Kİ
Hmmer	PT4	Zaman ayarlı HMMER Arama	Saniye	Kİ
John-the-ripper	PT5	John the Ripper - Blowfish şifreleme	Saniyedeki kombinasyon , (Kullanıcı adı/Şifre)	Bİ
OpenSSL	PT6	OpenSSL RSA 4096-bit Şifreleme	Saniyedeki sinyal miktarı	Bİ
Opstone-SVD	PT7	Opstone Tekil Değer Ayrışımı	Mflops	Bİ
Opstone-SVSP	PT8	Opstone Seyrek-Vektör Ölçekleme Ürünü	Mflops	Bİ
Opstone-VSP	PT9	Opstone Vektör Skaler Ürün	Gflops	Bİ
Sudokut	PT10	Sudoku Çözücü	Saniye	Kİ

TABLO 2. XEON İŞLEMCİLİ ÖZEL BULUT BİLİŞİM, 2 GB BELLEK, 1 ÇEKİRDEK, 1 SANAL ÇEKİRDEK, TEST SAYISI: 50

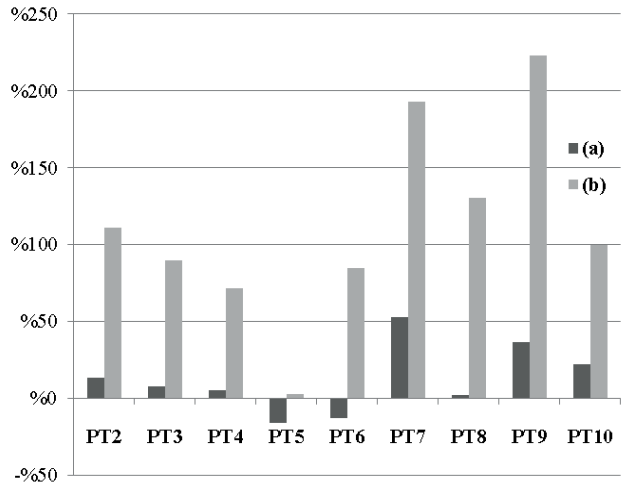
Test	Ortalama	Ortanca	Std. Sapma	En Yüksek	En Düşük
Dcraw	46,67	46,13	1,58	51,08	45,09
Espeak	100,43	100,32	0,36	102,08	100,07
Hmmer	145,54	145,47	0,31	147,33	145,24
John-the-ripper	415,12	418,00	14,30	419,00	317,00
OpenSSL	14,68	14,65	0,14	14,90	14,50
Opstone-SVD	372,14	411,50	66,86	430,00	244,00
Opstone-SVSP	379,24	378,50	10,18	405,00	362,00
Opstone-VSP	2,75	2,75	0,05	2,83	2,61
Sudokut	51,57	51,26	0,51	52,73	51,08

i7 İşlemcili Sunucu

Intel i7 işlemcili 32 bit Ubuntu sunucu özel bulut test sonuçları Tablo 3'te verilmektedir. Burada elde edilen kıyaslamalı sınama sonuçlarının, Xeon işlemcili halk buluta göre çok farklı olduğu görülmektedir. Şekil 1 (b)'de görüldüğü üzere %2,73 oranında daha iyi performans gösteren John-the-ripper testi dışında diğer tüm testlerde özel bulut performansının çok yukarılarda olduğu görülmektedir. Opstone-Vsp testinde, %223'lük yüksek bir değerle karşılaşılmıştır. Bu farklı sonuçlara verilebilecek bir açıklama, Xeon işlemci hızının 2.5GHz, i7 işlemcinin yeni nesil ve hızının ise 3.5 GHz olmasıdır. Standart sapma değerleri bu kıyaslamalı sınama sonuçlarında da çok düşüktür. Dolayısıyla, performans açısından özel bulutun, halk buluta göre daha istikrarlı çalıştığı yorumu yapılabilir.

TABLO 3. INTEL i7 İŞLEMCİLİ ÖZEL BULUT BİLİŞİM, 2 GB BELLEK, 1 ÇEKİRDEK, 1 SANAL ÇEKİRDEK TEST SAYISI: 50

Test	Ortalama	Ortanca	Std. Sapma	En Yüksek	En Düşük
Dcraw	24,34	24,29	0,09	25,51	24,15
Espeak	57,24	57,20	0,06	57,74	57,04
Hmmer	89,31	89,29	0,27	90,28	89,13
John-the-ripper	513,76	515,00	1,69	515,00	496,00
OpenSSL	30,45	30,40	1,42	30,70	29,50
Opstone-SVD	821,48	823,50	2,91	828,00	773,00
Opstone-SVSP	883,32	880,50	2,91	918,00	844,00
Opstone-VSP	6,13	6,14	0,05	6,17	6,07
Sudokut	31,21	31,20	0,07	31,50	31,13



Şekil 1. Başlangıç Düzeyi Özel Bulutun, Halk Bulut Performansına Göre Yüzde Değerleri: **(a)** Xeon İşlemcili Sunucu **(b)** Intel i7 İşlemcili Sunucu

C. İleri Düzey 64 bit Ubuntu Karşılaştırmalı Sınaması

Xeon İşlemcili Sunucu

Lenk vd. [10] 64 bit ileri düzey halk bulutu üzerinde yaptıkları Phoronix testlerini Amazon üzerinde 182, Flexiscale üzerinde 29, Rackspace üzerinde ise 34 kez çalıştırmışlardır. Bu çalışmada ise, 32 bit testlerinde olduğu gibi, Phoronix testleri 50 defa çalıştırarak sonuçlar elde edilmiştir. Performansların daha yüksek olduğu ileri düzey halk bulut ile özel bulut sunucuların karşılaştırmalı sınama değerleri bu bölümde incelenmektedir. Xeon işlemcili 64 bit Ubuntu sunucu özel bulut test sonuçları Tablo 4'te verilmektedir. Şekil 2 (a)'da görüldüğü üzere, toplam 10 testin 9'unda özel bulut performansının daha düşük olduğu, kalan bir test olan OpenSSL'de ise özel bulutun daha iyi sonuç verdiği görülmektedir. Özel bulutta çalışan birçok diğer sunucunun bu performans düşüklüğüne neden olduğunu, halk bulutta ise çok yüksek performanslı işlemcilere sahip alt yapılar kullanılmasının özel buluttaki performans değeri düşüklüğünün ana nedeni olarak açıklanabilir. Buna ek olarak halk bulut bilişim şirketlerinin kullandıkları alt yapı ve bulut programlarının, kendi içinde de çok değişik sonuçlar verdiğini Lenk vd. [10] çalışmalarında açıklamaktadırlar. Bu çalışmada da kullanılan halk bulut alt yapısının, sonuçlara olumsuz bir etkisinin olduğu söylenebilir.

TABLO4. XEON İŞLEMCİLİ ÖZEL BULUT BİLİŞİM, 8 GB BELLEK, 4 ÇEKİRDEK, X2 SANAL ÇEKİRDEK, TEST SAYISI: 50

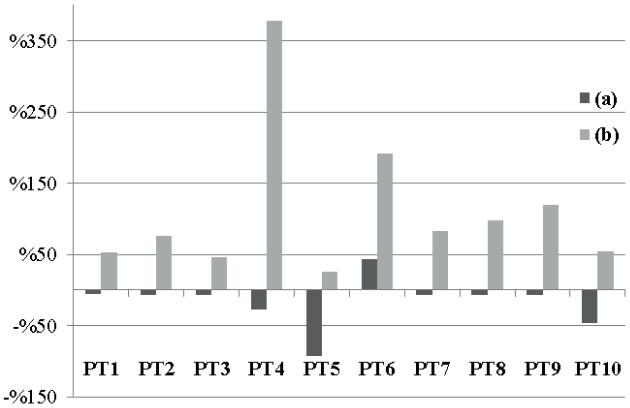
Test	Ortalama	Ortanca	Std. Sapma	En Yüksek	En Düşük
Crafty	147,56	147,06	1,37	150,91	145,67
Dcraw	36,65	36,66	0,35	37,59	36,03
Espeak	67,50	67,46	0,14	67,88	67,31
Hmmer	78,84	78,77	0,21	79,40	78,54
John-the-ripper	10669,20	10697,00	69,05	10717,00	10346,00
OpenSSL	251,73	270,50	37,40	279,30	155,60
Opstone-SVD	532,14	533,50	6,61	537,00	494,00
Opstone-SVSP	481,96	481,50	6,73	494,00	456,00
Opstone-VSP	2,87	2,88	0,04	2,92	2,66
Sudokut	38,58	38,55	0,23	39,26	37,95

i7 İşlemcili Sunucu

İleri düzey performanslı sanal sunucular için, i7 işlemcili alt yapıya sahip özel bulut platformunda yapılan test sonuçları Tablo 5'te verilmektedir ve karşılaştırmalı sınama sonuçları doğrultusunda halk bulut ve Xeon işlemcili özel buluta göre daha performanslı olarak ortaya çıkmaktadır. Özel bulut testinden elde edilen Hmmer değeri, halk bulutun sonucuna göre %377,6 gibi yüksek bir farka ulaşılmaktadır. Şekil 2 (b)'de görüldüğü üzere, birçok test sonucunun değeri, halk bulutun performansından daha yüksek olarak ortaya çıkmıştır. OpenSSL ise %191'lik değeriyle Hmmer test sonuçlarından sonra gelen ikinci yüksek değerdir. Karşılaştırmalı sınamada en düşük test değeri, %25 ile John-the ripper testine aittir. Burada bir başka önemli nokta özel buluta ait test sonuçlarının standart sapma değerlerinin çok düşük olması olarak görülebilir. Halk bulutta elde edilmiş büyük standart sapma değerleri, özel bulutun performansının halk buluta göre daha istikrarlı olduğunu işaret etmektedir.

TABLO5. i7 İŞLEMCİLİ ÖZEL BULUT BİLİŞİM, 8 GB BELLEK, 4 ÇEKİRDEK, X2 SANAL ÇEKİRDEK, TEST SAYISI: 50

Test	Ortalama	Ortanca	En Yüksek	En Düşük	Std. Sapma
Crafty	90,41	90,37	94,19	89,60	0,64
Dcraw	19,18	19,17	19,49	19,04	0,09
Espeak	43,28	43,27	43,54	43,21	0,06
Hmmer	12,11	12,07	14,00	12,01	0,27
John-the-ripper	867,40	868,00	870,00	863,00	1,69
OpenSSL	369,01	368,80	371,40	366,30	1,42
Opstone-SVD	1053,48	1053,50	1058,00	1044,00	2,91
Opstone-SVSP	1117,44	1117,71	1124,53	1107,11	3,49
Opstone-VSP	6,81	6,83	6,86	6,59	0,05
Sudokut	22,03	22,02	22,40	21,95	0,07



Şekil 2. İleri Düzey Özel Bulutun, Halk Bulut Performansına Göre Yüzde Değerleri: **(a)** Xeon İşlemcili Sunucu **(b)** Intel i7 İşlemcili Sunucu

D. Fiziksel Sunucu ile Özel Bulut Karşılaştırmalı Sınama

Çalışmanın ikinci aşamasında, özel sektörde faaliyet gösteren bir bilgi teknolojileri kurumunun bilişim hizmetlerine cevap vermek amacı ile çalışmakta olan e-posta ve etki alanı fiziksel sunucuları bire bir sanallaştırılarak özel bulut platformuna aktarılmış, devamında yapılan testler ile fiziksel sunucular ile özel buluttaki sanal sunucuların performans değerleri karşılaştırmalı sınama yöntemi ile incelenmiştir.

Bu bölümde kıyaslama sınama yazılımı olarak Passmark 7.0 [16] seçilmiştir. Bu yazılım ile bellek ve sabit disk testleri fiziksel sunucularda ve özel bulut üzerinde çalışan sunucularda gerçekleştirilmiştir. Tüm sunucularda testler 50 defa çalıştırılarak sonuçlar elde edilmiştir. Passmark 7.0'da mevcut olan tüm test sonuçlarında yüksek değer daha iyidir. Test sonuçları sırasıyla Tablo 6, 7, 8 ve 9'da verilmektedir.

İlk aşamada, e-posta ve etki alanı sunucusu üzerine yüklenen Passmark ile yapılan karşılaştırmalı sınamada fiziksel sunucuların değerleri birbirine yakın iken aynı şekilde özel buluttaki test sonuçları birbirine benzeyen değerler vermiştir. Passmark sonuçlarına göre, , her iki fiziksel sunucunun özel bulutta bulunan klonlarına göre çok daha performanslı olduğu gözükmektedir. Şekil 3 (a) ve (b)'de gözüktüğü gibi işlemci testinde, en düşük test değeri %5 ile "İlk Sayıyı Bulma", en yüksek test değeri ise %95 ile "SSE" testinde ortaya çıkmaktadır. Diğer yandan, sabit diskler için yapılan kıyaslamalı sınama sonuçlarında da dikkate değer sonuçlar elde edilmiştir. Test alt yapısı kurulurken tamamen standart donanım ve yazılımlar kullanılmış olup, özel bulut ile fiziksel sunucuların disk alt yapısı SCSI ve RAID 5 olarak birebir aynıdır. Buna karşın disklerin performansında, fiziksel sunucuların sonuçları ile özel buluttaki sunucuların sonuçları arasında büyük farklar oluşmuştur. "Rastgele Arama" ve "Okuma Yazma" testlerinde fiziksel e-posta sunucusu %688, etki alanı sunucusunda ise %4472 gibi özel buluttaki kopyalarına göre başarılı bir performans göstermişlerdir. Diğer disk testi sonuçları da fiziksel sistemler lehine yüksek değerler olarak ortaya çıkmaktadır. Standart sapmalara bakıldığında ise, fiziksel sistemlerin özel buluta göre daha kararlı çalıştığı söylenebilir. Fiziksel etki alanı sunucusunda "Dizi Sıralama" testinde standart sapma 51 iken, özel bulutta bu değer 468 olarak kaydedilmiştir. İki sunucu da bu testte kararlı bir tepki vermemiştir, ancak özel buluttaki sunucunun standart sapmasının çok yüksek olması dikkat çekicidir.

TABLO 6. FİZİKSEL E-POSTA SUNUCUSU PASSMARK SONUÇLARI

Test	Ortalama	Ortanca	En Yüksek	En Düşük	Std. Sapma
MİB – Tamsayı Matematiği	2219,48	2228,45	2238,90	2101,30	26,45
MİB – Gezer Nokta Matematiği	2949,29	2957,10	2971,90	2791,90	26,79
MİB – Asal Sayı Bulma	913,50	914,55	919,70	898,60	5,01
MİB – SSE	32,26	32,40	32,50	30,40	0,40
MİB – Sıkıştırma	9685,74	9693,60	9748,20	9511,50	45,93
MİB – Şifreleme	28,90	28,95	29,10	28,10	0,17
MİB – Fizik	359,02	359,45	370,20	343,60	6,41
MİB – Dize Sıralama	3846,34	3840,80	3990,20	3767,40	42,82
Disk – Sıralı Okuma (MB/s)	87,30	87,00	102,70	75,70	7,66
Disk – Sıralı Yazma (MB/s)	316,85	323,85	334,10	185,80	23,70
Disk – Rastgele Arama + OY (MB/s)	505,21	510,65	517,20	340,60	24,71

TABLO 7. SANAL E-POSTA SUNUCUSU PASSMARK SONUÇLARI

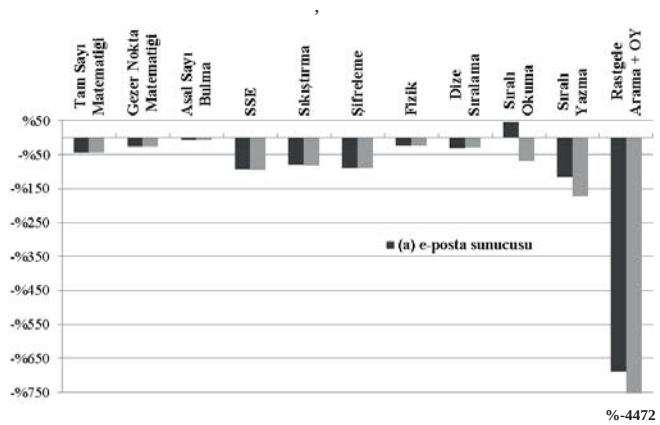
Test	Ortalama	Ortanca	En Yüksek	En Düşük	Std. Sapma
MİB – Tamsayı Matematiği	1475,94	1515,05	1542,90	1287,80	72,98
MİB – Gezer Nokta Matematiği	2236,97	2301,30	2366,10	1579,10	152,87
MİB – Asal Sayı Bulma	806,55	853,70	875,90	442,50	115,04
MİB – SSE	15,52	16,30	16,80	7,80	2,12
MİB – Sıkıştırma	4964,53	5282,90	5432,50	1693,90	853,34
MİB – Şifreleme	14,59	15,10	15,30	4,80	1,86
MİB – Fizik	250,66	266,30	296,00	94,50	47,69
MİB – Dize Sıralama	2758,85	2902,35	3055,50	1448,00	387,41
Disk – Sıralı Okuma (MB/s)	121,97	122,65	190,60	62,00	50,03
Disk – Sıralı Yazma (MB/s)	114,54	107,25	154,30	80,10	22,00
Disk – Rastgele Arama + OY (MB/s)	43,44	41,95	65,60	25,40	8,89

TABLO 8. FİZİKSEL ETKİ ALANI SUNUCUSU PASSMARK SONUÇLARI

Test	Ortalama	Ortanca	En Yüksek	En Düşük	Std. Sapma
MİB – Tamsayı Matematiği	2228,71	2228,20	2238,50	2217,30	5,89
MİB – Gezer Nokta Matematiği	2957,51	2956,70	2973,20	2937,90	8,10
MİB – Asal Sayı Bulma	916,44	916,40	919,40	911,50	2,05
MİB – SSE	32,45	32,40	32,60	32,20	0,10
MİB – Sıkıştırma	9707,13	9711,10	9744,40	9626,50	27,72
MİB – Şifreleme	28,99	29,00	29,10	28,80	0,08
MİB – Fizik	341,70	340,25	359,40	337,00	5,07
MİB – Dize Sıralama	3763,00	3756,50	3877,40	3669,10	51,74
Disk – Sıralı Okuma (MB/s)	90,93	90,15	132,60	49,60	13,40
Disk – Sıralı Yazma (MB/s)	260,06	274,65	311,70	162,10	48,46
Disk – Rastgele Arama + OY (MB/s)	499,85	503,45	516,70	473,60	12,26

TABLO 9. SANAL ETKİ ALANI SUNUCUSU PASSMARK SONUÇLARI

Test	Ortalama	Ortanca	En Yüksek	En Düşük	Std. Sapma
MİB – Tamsayı Matematiği	1500,71	1513,00	1549,80	1353,00	45,28
MİB – Gezer Nokta Matematiği	2291,16	2315,80	2368,50	1766,40	90,03
MİB – Asal Sayı Bulma	759,55	841,90	874,30	373,00	165,34
MİB – SSE	15,68	16,30	16,70	6,60	2,02
MİB – Sıkıştırma	5065,02	5281,35	5392,30	2215,20	651,15
MİB – Şifreleme	14,03	15,00	15,30	5,70	2,21
MİB – Fizik	231,29	261,70	291,60	81,90	64,41
MİB – Dize Sıralama	2667,13	2848,40	3038,30	882,20	468,41
Disk – Sıralı Okuma (MB/s)	56,18	57,55	78,00	10,80	12,85
Disk – Sıralı Yazma (MB/s)	89,60	82,55	114,80	74,60	13,18
Disk – Rastgele Arama + OY (MB/s)	8,01	7,85	11,30	4,80	1,93



Şekil 3. Özel buluta aktarılan sanal e-posta **(a)** ve sanal etki alanı **(b)** sunucularının, fiziksel sunuculara göre performans değerleri

V. SONUÇ VE GELECEK ÇALIŞMALAR

Bu çalışmada, farklı konfigürasyonlar kullanılarak, özel bulut ile halk bulut sistemleri üstünde karşılaştırmalı sınama testleri yapılmıştır. Intel i7 ve Intel Xeon işlemcili özel bulut yapılarının test sonuçları baz alınarak, işlemcilerinin hızları arttırıldığı veya yeni nesil işlemciler kullanıldığı takdirde özel bulut performansının istenilen düzeye yükseltilebileceği söylenebilmektedir. Ancak bilindiği üzere, kurumların bilişim altyapısındaki sunucularda Xeon işlemciler kullanılması, bu işlemcilerin özel bulutlarda istenilen performansa sahip olmadığı sonucunu bize göstermektedir. Birçok kurumun güvenlik ve benzer nedenlerden dolayı özel bulut kullanması, özel bulutlara uygun donanımların üretilmesi gerekliliğini ortaya koymaktadır. Özel bulut ile fiziksel sunucular üzerinde yapılan testlerde, fiziksel sunucuların karşılaştırmalı sınama test sonuçlarında daha iyi değerlere sahip olduğu ortaya çıkmıştır. Özel bulutta bulunan sunuculardaki sabit disk performansı, fiziksel sunuculara göre çok düşük kalmıştır.

Gelecek çalışma olarak, özel bulut bilişimin karşılaştırmalı sınama sonuçlarında düşük düzeyde olmasının nedenleri üzerinde bir çalışma yapılması planlanmaktadır. Bu çalışmadan elde edilen verilerle, özel bulut bilişimde performans arttırmak için halk bulutu kullanmak istemeyen kurum ve kuruluşların özel bulut bilişimi efektif olarak kullanmasını sağlayacak çözümlerin üretilmesi ve yöntemlerin önerilmesi amaçlanmaktadır.

KAYNAKÇA

[1] M. Uddin ve A. A. Rahman, "Virtualization Impplementation Model for Cost Effective & Efficient Data Centers", *International Journal of Advanced Computer Science and Applications,* cilt 2, sayı 1, 2011, s. 69-74.

[2] P. Mell ve T. Grance, "The NIST Definition of Cloud Computing, v15". http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf , Erişim tarihi: 10 Temmuz 2009.

[3] I. Foster, Y. Zhao ve S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", *Grid Computing Environments Workshop GCE '08*, Austin, 2008.

[4] Michael Larabel, "Phoronix Test Suite", 2013. http://www.phoronix-test-suite.com. Erişim tarihi: 30 Mayıs 2013.

[5] A. Iosup, S. Ostermann, M. N. Yigitbasi, R. Prodan, T. Fahringer ve D. H. Epema, "Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing", *IEEE Transactions on parallel and distributed systems,* cilt 22, sayı 6, 2011, s. 931-945.

[6] N. Bhargava, R. Bhargava, M. Mathuria ve R. Daima, "Performance Analysis of Cloud Computing for Distributed Client", *International Journal of Computer Science and Mobile Computing,* cilt 2, sayı 6, 2013, s. 97-104.

[7] D. Steinmetz, B. W. Perrault, R. Nordeen, J. Wilson ve X. Wang, "Cloud computing performance benchmarking and virtual machine launch time", *13th annual conference on Information technology education - SIGITE '12*, Calgary, 2012.

[8] C. Vecchiola, S. Pandey ve R. Buyya, "High-Performance Cloud Computing: A View of Scientific Applications", *10th International Symposium on Pervasive Systems, Algorithms, and Networks*, Melbourne, 2009, s. 4-16.

[9] L. Gillam, B. Li, J. O'Loughlin ve A. P. Singh Tomar, "Fair Benchmarking for Cloud Computing systems", *Journal of Cloud Computing: Advances, Systems and Applications,* cilt 2, sayı 6, 2013.

[10] A. Lenk, M. Menzel, J. Lipsky, S. Tai ve P. Offermann, "What Are You Paying For? Performance Benchmarking for Infrastructure-as-a-Service Offerings", *IEEE 4th International Conference on Cloud Computing*, 2011, s. 484-491.

[11] K. E. Stewart, J. W. Humphries ve T. R. Andel, "An Automated Virtualization Performance Analysis Platform", *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology,* cilt 9, sayı 3, 2012, s. 257-265.

[12] D. A. Dodge, B. E. Mullins, G. L. Peterson ve J. S. Okolica, "Simulating windows-based cyber attacks using live virtual machine introspection", *SCSC '10 Proceedings of the 2010 Summer Computer Simulation Conference* , San Diego, 2010.

[13] B. R. Chang, H.-F. Tsai ve C.-M. Chen, "Evaluation of Virtual Machine Performance and Virtualized Consolidation Ratio in Cloud Computing System", *Journal of Information Hiding and Multimedia Signal Processing,* cilt 4, sayı 3, 2013, s. 192-200.

[14] N. Huber, M. von Quast, M. Hauck ve S. Kounev, "Evaluating and Modeling Virtualization Performance Overhead for Cloud Environments", *1st International Conference on Cloud Computing and Services Science*, Noordwijkerhout, 2011, s. 563-573.

[15] "Vmware", 2007. http://www.vmware.com/resources/techresources/711. Erişim Tarihi: 10 Haziran 2013.

[16] "Passmmark Software", PassMark Software Pty Ltd., 2013. http://www.passmark.com/. 30 Mayıs 2013.

Kurumsal Elektronik Posta İletiminde Siber Güvenlik

Dr.Önder ŞAHİNASLAN, Dr.Ender ŞAHİNASLAN

***Özet*—Elektronik haberleşme kişi ve kurumların her an ihtiyaç duyduğu, fonksiyonel ve kanıt niteliği taşıyan hızlı bir haberleşme servisidir. Yaygın kullanımı, bilgilerin mahremiyeti ve değerli oluşu nedeniyle siber saldırganlar tarafından hedef seçilebilmektedir. Diğer taraftan bireysel ve kurumsal e-posta üzerindeki siber tehditler her geçen gün daha da artarak çeşitlenmektedir. Gerçek zamanlı olarak tehditleri engelleyebilmek optimize edilmiş sıkı bir güvenlik politikası ve aşamalı güvenlik yönetim süreciyle mümkündür. Zararlı etkileri olan, profesyonelce hazırlanmış yanıltıcı içerik ve yönlendirmeleri içeriklerden arındırılmış e-posta hizmetleri sunulmalıdır. Uzmanlaşan 'hacker' korsanlarına karşı uçtan uca siber güvenli mimarilerle desteklenerek maddi ve manevi kayıpların önüne geçilmelidir. Gönderici ve alıcı arasındaki iletilen özel bilgilerin mahremiyeti sağlanmalı, iletişim ve yedekleme şifreli(kripto) gerçekleştirilmelidir.**

Bu çalışma, siber saldırılara karşı daha güvenli bir elektronik haberleşme sisteminin nasıl yapılabileceğine dair kurumsal siber önlem ve çözümleri sunmayı amaçlar.

Anahtar Kelimeler: **E-Posta Yönetimi, Siber Saldırı ve Tehditler, Şifreleme, Bilgi Güvenliği, Spam Savunma**

CYBER SECURITY IN INSTITUTIONAL E-CORRESPONDENCE

Abstract **- Electronic communication, which is needed by both individuals and corporations at any moment bears legal quality of evidence, is a functional and quick correspondence. However, it may be exposed to Cyber attackers because of its widespread use, and secrecy and value of its data. Also, cyber threats to personal and institutional e-mail are variably increasing day by day. Yet, preventing the threats on a real time basis is possible with a strictly optimized security policy and a leveled security management. E-mail services, cleared of professionally produced misleading agents with malicious effects, must be offered. Those services must be protected with cyber-shielded architecture thoroughly against professional hacker pirates to prevent potential spiritual or material losses. Confidentiality of the data transferred between the sender and receiver should be secured; also correspondence and encrypted backup must be performed.**

The purpose of this study is to suggest institutional precautions and solutions for how a safer e-correspondence system against cyber attacks can be performed.

Keywords: **E-Mail Management, Cyber Attacks and Threats, Encryption, Information Security, Spam Defense**

I. GİRİŞ

İletişim çağı olan günümüzde saniyeler içerisinde elektronik haberleşme gerçekleşmektedir. Hızlı hayat akışı içerisinde yüz yüze görüşmelerin ve elden gönderilen iletiler yerini canlı ve kesintisiz bir dijital bilgi aktarım ortamına bırakmıştır. En popüler ve yaygın kullanım oranı bakımından e-posta ilk sıralarda yer almaktadır. Alman bilişim derneği Bitkom tarafından yaptırılan bir araştırmaya göre, kullanıcıların yüzde 88'i e-postanın yaşam kalitesini artırdığına inanıyor. Yüzde 89'u esnekliğe imkân tanıdığını, yüzde 84'ü ise bilgiye erişimini kolaylaştırdığını düşünüyor. Kullanıcıların yüzde 66'sı üretkenliğinin e-postayla arttığına inanırken, yüzde 61'i bu iletişim aracı sayesinde zamandan tasarruf ettiğini belirtmiştir[1].

İnternetin her alanında olduğu gibi e-posta kullanımında da siber saldırılara maruz kalınmaktadır. İstenmeyen eklenti, virüs ve içerik taşıyan e-postalar özellikle son kullanıcıları çok fazla mağdur etmektedir. Bu tür istenmeyen saldırılarla mücadeleyi sadece bireylere bırakmak sağlıklı bir çözüm değildir. E-posta sunucu hizmeti veren kurum veya kuruluşlar e-postalara gizlenmiş tehdit içerikli zararlılardan arındırılması için belli filtrelerden geçirmek durumundadırlar. Böyle yapılmadığı durumda hizmetten yararlanan üyeler spam tehditlerine maruz kalır. Sunucu üzerinde oluşan fazladan trafik oluşturma, posta kutularının gereksiz iletilerle aşırı büyümesi sonucu bakım ve yedekleme zorlaşır. Kullanıcı tarafında ise hem güvenlik riskine sebep olmakta hem de gereksiz zaman kayıplarına ve dikkat dağınıklılıklarına sebep olmaktadır.

Belli sayının üzerinde kullanıcısı olan ağlarda istemci ve internet güvenliği sağlanmak durumundadır. Kurum içi veya dışında bir kullanıcıya iletilen e-posta gönderildiği bilgisayarın güvenliği kadar güvenli olabilir. Eğer bilgisayar yeterli düzeyde güncel güvenlik yazılımları ile korunamamışsa zaman içersinde spam saldırı ve yayma aracı haline dönüşebilir.

Tablo-1. E-Postalar üzerindeki spam yoğunluğu

Sektör	Yoğunluk(%)
Finans Kuruluşları	% 83
Eğitim Kurumları	% 67,3
Kimya/İlaç Sanayi	% 65,8
Ticari Olmayan Kuruluşlar	% 65,4
Tatil ve Konaklama	% 65,2

Mayıs 2013 yayınlanan Tablo-1'deki Symantec güvenlik araştırma sonuçlarına göre e-postalar üzerindeki spam yoğunluğu finans kurumlarından sonra en fazla eğitim kurumlarında görülmektedir[2]. Kurumlar kullanıcı taleplerini karşılamanın yanı sıra sahip oldukları bilgilerin güvenliğini de sağlamak zorundadır. ISO 27001 Uluslar arası bilgi güvenliği standardında da bilginin temel nitelikleri olan "gizlilik", "bütünlük" ve "erişilebilirlik" açısından korunması gerekliliği belirtilmektedir[3].



Şekil 1- Bilgi Güvenliğinde Sağlanacak Nitelikler

Elektronik haberleşme de karşılıklı iletilen bilginin bu temel güvenlik döngüsü esasında değerlendirilmesi gerekir. Yetkisiz erişimlerin engellenmesinden, veri bütünlüğünün korunmasından ve kolay ulaşılabilir olması sağlanmalıdır. Güvenli internet ve haberleşme servis ağı oluşturmak kurumların markalaşmasına da katkı sağlayacaktır. Korumasız ve güvensiz bir ortam iş gücü, finans, imaj kaybına ve kaynak israfına sebep olur. Güvenlik bakımından oluşabilecek zayıflıklar önceden tespit edilerek gerekli kontroller yapılmalı ve siber önlemler alınmalıdır[4].

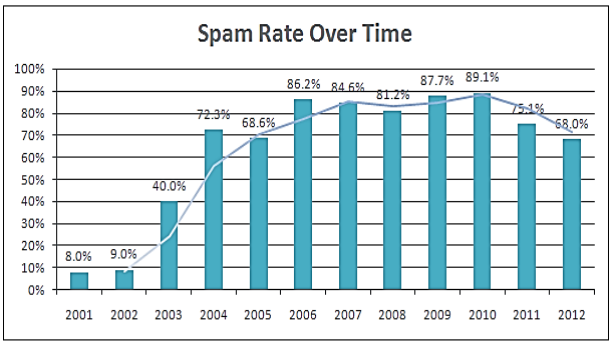
Özellikle elektronik posta iletimi üzerinden yayılımını gerçekleştirilen kötü amaçlı yazılımlar oldukça tehlikeli ve zararlı fonksiyonları içerir hale gelmiştir. Trend Micro firmasının 2012 güvenlik raporuna göre kötü amaçlı yazılımlar dünya üzerinde endişe verici büyüklüğe ulaşmıştır.



Şekil 2 – Zararlı yazılımlardaki artış oranı

Şekil-2 incelendiğinde 2011 yılı ikinci yarısından itibaren on aylık büyüme oranı %60'dan fazla gerçekleşmiştir[5]. Sürekli artış gösteren bu tehditlerin bilgi varlıklarına yönelik gerçekleşmemesi için risklerin önceden fark edilmesi ve kurum ve/veya birey bilgilerinin zarar görmeden korunması kaçınılmazdır. Phishing (e-dolandırıcılık) saldırılarındaki artış yasal e-mail adresleri ile sahte ve yanıltıcı e-posta adreslerinin ayırt edilmesi gerekmektedir. Kullanılacak yazılımlarla kullanıcılar kendilerine gelen bir e-postanın güvenilir adresinden gelip gelmediğini doğrudan ayırt edebilmelidir. Bu sayede phishing ve sahte e-posta ile oluşacak riskleri azaltmaya yardımcı olur.

Symantec Güvenlik araştırma firmasının spam kaynaklı saldırılar konusunda yaptığı analiz sonuçları şekil-3'de görülmektedir. Saldırılar, %89 oranla en fazla 2010 yılında artış göstermiştir.



Şekil-3 Son 10 Yıllık Spam Dağılım Oranı

Spam ile yapılan mücadele ve güvenlik tedbirleri geçtiğimiz 2 yılda etkisini göstermiştir [2]. Ancak belirgin bir düşüş olmasına rağmen pek çok şirketin ve bireylerin ciddi sorunu olmaya devam etmektedir. Mağdurların adres defterini, kimlik ve bankacılık bilgilerini karşı tarafa iletmekle kalmayıp, eklentilerindeki zararlı yazılımları kurdurarak bilgisayarı korumasız hale getirmektedirler. Yine 2012 Symantec raporuna göre dünyada her gün yaklaşık 100 milyar spam posta dolaşmaktadır. Siber saldırı araçlarını bu reklam postaları üzerinden gönderen spam tacirleri yılda 200 milyon dolar gelir elde etmektedirler. Mağdurlar ise milyar dolarlarca maddi kayıp ve işgücü israfına neden olmaktadır. Örneğin sadece Google, Microsoft ve Yahoo gibi şirketlerin sunucularına fazladan yüklenme ve bakım masrafı hariç kullandıkları anti-spam yazılımlarının toplam maliyeti 6.5 milyar dolardır[2]. Tüm bu artış rakamları bizlere kayıpları önleme adına e-posta yönetiminde bir takım siber güvenlik tedbirlerin alınması gerekliliğini göstermektedir. Sistemsel ve yazılımsal güvenlik çözümleri ile beraber son kullanıcı bilinçlendirme çalışmalarının yapılması gerekmektedir. Ayrıca e-posta iletiminde açık kaynak kodlu yazılım çözümleri üzerinden katmanlı yapıda, kurumsal siber güvenli uygulamalı güvenlik çözümleri anlatılmaktadır.

II. GÜVENLİ E-POSTA YÖNETİM SİSTEMİ

A. E-Posta Üzerinde Taşınan Siber Riskler

Günlük iş ve özel yaşantımızda sıklıkla kullandığımız e-posta hedef kişiye farklı veya aynı ağa ait sunucular üzerinden ulaşabilmektedir. İletilen postalar, güvensiz sunucularda okunma ve silinme riski taşıyabilir. Sunucular, günümüzde resmi geçerliliği de olan haberleşme

kanallarının dinlenmesi, taklit edilmesi, çoğaltılması gibi güvenlik açıklıklarına karşı güvenli olmak zorundadır. Çoğunlukla zararlı içerik taşıyan reklam türü spam postalar hem zaman ve kaynak israfına hem de zararlı eklentilerin taşınmasına neden olmaktadırlar[4]. Etkili bir siber güvenlik son kullanıcıya temiz bir posta kutusu iletişim hizmeti vermekle mümkündür. Güvensiz e-posta kullanıcıyı ve bağlı bulunduğu kuruluşu siber risk oluşturur. Kullanıcının da belli yükümlülükleri yerine getirmesinin yanı sıra asıl filtreleme ve risk önleme sunucu tarafında gerçekleştirilir.

1. İstenmeyen Elektronik Posta(spam)

Alıcı tarafın bilgisi ve talebi olmaksızın içeriğine çok fazla güvenilmeyen merak, korku, politik, reklam, kişisel veya ticari menfaat sağlamaya yönelik yüksek sayıda gönderilen ileti kopyalarıdır. Elektronik haberleşmede istenmeyen e-posta oranının arttığı bir dönemde spam saldırılarına karşı güvenli bir ağ trafiğinin olması gerekmektedir. Spam mesajlar internet üzerindeki trafiği arttırarak başta servis sağlayıcılar olmak üzere birçok internet servisi üzerinde gereksiz yük oluşturmaktadırlar

Spam iletilerinin masrafı gönderen açısından yok denecek kadar az olduğundan gönderilen iletilerde hedef kitle aranmaz ve bu tür mail'leri almak istemeyen binlerce kişi rahatsız edilir. Email spam listeleri gönderilerin taranması, sohbet gruplarının, üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur

Günümüzde e-uygulamaların hızla yaygınlaştığı e-devlet, e-kurum, e-bankacılık benzeri kimlik doğrulama ekran girişlerinin phishing türü yanlış yönlendirmelerde hesap ve şifre bilgilerinin elde edilmesi yöntemi sıklıkla kullanılmaktadır. Bu tür yöntemi kullanan kişiler öncelikle ilgili kurumdan geldiği izlenimini veren sahte spam mailler göndererek kişileri tuzaklarına düşürmektedirler. Bu nitelikteki e-posta içerisinde gönderdikleri sahte link benzeri yönlendirmelerle gerçeğinden farklı bilgi giriş ekranlarına girdirmektedirler veya sahte düzeltme formları göndererek gerçek bilgileri elde etmektedirler. Spam e-postalarla mücadele öncelikle sunucularda taratılarak ayıklanmalıdır. Kullanıcı tarafında ise akıllı öğrenme yeteneklerine sahip spam tarama yazılımları ve önemsiz posta klasörlerinin iyi yapılandırılması ile etkili siber tedbirler alınmalıdır.

2. Zararlı Eklenti ve Sahte Yönlendirmelere Sahip Elektronik Posta

Siber korsanların en belirgin phishing saldırı aracı haline gelmiştir. Posta gövde metninde gerçek kurum isim ve logoları üzerine verdikleri sahte tuzak adres linkleri ile yanıltılmaktadır. Özellikle spam postalarla birlikte taşınan virüs, trojan, worms benzeri gizli zararlı yazılımlar bilgisayarın kontrol dışı işlem yapmasından çok büyük bilgi kayıplarına kadar tehlikeli olabilmektedir. Çok değişik yöntem ve senaryolarla kişinin bilgisayarına gizli bir ajan yazılım olarak yerleşebilmektedir. Kendilerini faydalı bir program olarak göstererek kullanıcının onayını aldığından dolayı çoğu güvenlik önlemleri yetersiz kalabilmektedir.

Bilgisayara yerleşen zararlı bir yazılım kişinin Outlook'undan adres defterindeki tüm kullanıcılara kendi adında tuzak olabilecek zararlı eklentili ve yanıltıcı postalar gönderebilmektedir. Karşıdaki kişi gelen zararlı eklentiye sahip e-postanın tanıdığı ve güvendiği kişiden geldiği varsayımıyla rahatlıkla onay verebilmektedir. Bu şekilde bilgisayarlara yüklenebilen bir takım yazılımlar klavyeden girilen bilgileri, fare ve ekran görüntülerini saldırgan hedefe doğrudan göndermektedir. Zehirlenmiş PC olarak tariflenen bu bilgisayarlar üzerinden başkalarına ait binlerce reklam maili gönderilebilir. Uzak masaüstü servisini başlatarak saldırganın doğrudan erişmesini sağlar.

B. E-Posta Servis Hizmeti

Bilgi ve mesajların karşıdaki kullanıcıya elektronik iletişim araçları ile hızlı ve ucuz şekilde iletilmesidir. Oluşturulan bir e-postayı aynı anda çok fazla kişiye ulaştırmak mümkündür. İletilen mesajın ekinde doküman, ses, video gibi birden fazla dosya eki gönderilebilmektedir.

Kişilerin görsel ara yüzler kullanarak oluşturduğu elektronik bir mektubu bilgisayar ağları üzerinden taşınarak alıcı tarafa ulaşma işlemine e-posta denir. E-posta hizmeti sunucu ve istemci taraf olmak üzere iki bileşene sahiptir.

1. E- Posta Sunucusu

Bir ağ üzerinde çalışan bir veya birden fazla domain'e ait posta iletim ve dağıtım işlemini gerçekleştirebilen, çoklu kullanıcıya hizmet edebilen güçlü sistemleridir. Elektronik haberleşme servisleri üzerinden yapılan tüm iletim bilgilerini merkezi noktada toplar ve buradan ait olduğu hedef domainlere dağıtır. Hukuki durum ve bilgi güvenliği açısından yedekli bir yapıya sahiptir. Açık kaynak kodlu bazı e-posta sunucu yazılımları; Zimbra, Qmail, Send mail, Postfix

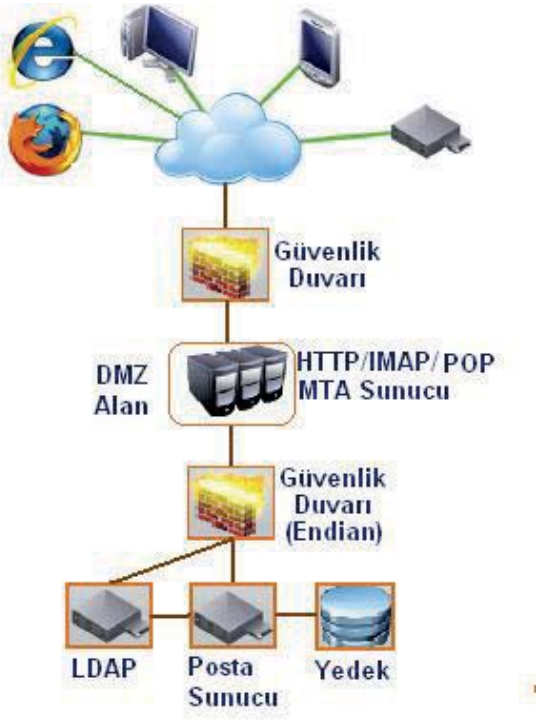
2. Elektronik Posta İstemcisi

İnternet kullanıcılarının e-posta yazma, gönderme, okuma ve silme işlemlerini gerçekleştirdikleri kullanıcı ara yüz servisleridir. Kullanıcılar bilgisayarlara kurulan yazımlar veya doğrudan browser üzerinden hesaplarına erişebilirler. Nestcape, k-mail, mozilla firefox, Thunderbird[3]

III. SİBER GÜVENLİ YAPILANDIRMA

A. Sistem Mimarisi

Bir kurumsal ağda, e-posta sunucusunun konumu, hangi kullanıcı grubunun izinli olacağı, merkezi yönetilebilir bir kimlik yetkilendirme ve trafik sınıflandırma sağlanmalıdır. Yeni nesil güvenlik cihazları kural ve politikalara bağlı izin tanımlarının yanı sıra saldırı önleme, virüs tarama, VPN bağlantı oluşturma, içerik filtreleme, spam ve virüs tarama gibi güvenlik fonksiyonları bütüncül şekilde konumlandırılmalıdır.



Şekil-4 Güvenli E-Posta Sunucu Yerleşimi

Sunucu ile istemci arasında uçtan uca şifreli mesajlaşma sağlanır. Proxy sunucu, DMZ bölge oluşturma, LDAP dizin erişim güvenlik doğrulaması, SSL/TLS Güvenli aktarım katmanı, SMTP/IMAP/POP vb. basit posta aktarım servisleri Şekil-4 de olduğu gibi güvenlik duvarı arkasında konumlandırılabilir.

1. Ağ Yapılandırması

Ağ üzerinde tek bir noktada güvenlik denetimi yapılması, günümüz siber saldırıları için oldukça yetersiz kalmaktadır. Farklı yöntemlerle savunma tedbirlerinin alınması, gelebilecek tehlikenin aşamalı olarak engellenmesini sağlar. Her kurumun kendi bilgi varlıkları ve e-posta sunucu uygulamaları risk düzeyine göre ağ güvenlik yaklaşımı farklılaşır. Aktif cihazlar, güvenlik duvarı, port yapılandırılması, IP-MAC filtreleme, log kayıtlarının tutulması gibi unsurlar sunucunun bağlı bulunduğu ağda denetim ve kontrol altında tutulmalıdır.

2. Sunucu Yapılandırması

E-posta domain, web, veritabanı, DNS, yedekleme gibi bir veya birçok uygulamayı aynı anda servis eden ve çok sayıda kullanıcıya 7x24 hizmet sağlayan sunucular siber tehditlere karşı korunaklı olmalıdır. Üzerindeki işletim sistemi ise sunucu yönetimi ile birlikte diğer uygulama ve servislere de yön veren siber güvenliğin sağlanmasında çok büyük fonksiyona sahiptir. İşletim sistemi kaynaklı açıklık ve açıklık için tedbir alınmadığı sürece bilgi varlıkları üzerinde siber güvenlik riski oluşturur. Yapılan çalışmada açık kaynak kodlu kolay kurulum ve yönetilebilirliği açısından Centos işletim sistemi tercih edilmiştir. Posta yönetim uygulama sunucu yazılımı olarak açık kaynak kodlu zimbra bütünleşik uygulama modülü tercih edilmiştir. Tümleşik uygulama olarak; Open Ldap Postfix, Apache-Tomcat, Mysql, Clamav, Spamassassin, Dspam uygulamalarını içerir[8]. Hazır Postfix MTA posta iletim aracı etkindir. Amavisd - Virüs ve spam koruması için güncel ve fonksiyonel bir içerik filtreleme aracıdır. Kurulum aşamasında tümleşik uygulamalar isteğe bağlı olarak doğrudan ücretsiz kurulumu gerçekleştirilebilir.

3. Spam ve Zararlı Eklentilerden Koruma

Kötü amaçlı yazılım ve phishing eklentilerle siber saldırı bugünün dijital ortamında oldukça yaygındır. Bu kuruluşların hassas bilgileri elde veya kötü amaçlı yazılım içeren girişiminde mesajlardan kullanıcıların koruması önemlidir.

ClamAV , ödüllü açık kaynak anti virüs sistemidir. Uygulamada açık kaynak kodlu Zimbra e-posta yönetim paketi kullanıldı. Siber tehdit zararlılarından(anti-virüs, anti-worm, anti-phishing) korumasını en üst düzeyde siber güvenlik oluşturmak için günde birden çok online güncelleme gerçekleştirmektedir.

Reklam ve tuzak olabilecek spam iletileri önlemede açık kaynak kodlu modül olan SpamAssassin ve DSPAM filtreleme araçları kullanılmalıdır. Zimbra açık kaynak posta sunucu kurulumunda bu modüllerde etkin hale gelmektedir. Bu araçlar posta sunucusu kullanıldıkça sürekli öğrenme yeteneğine bağlı olarak güvenlik performansı artmakta ve kendi veritabanlarını optimize etmektedirler. Ayrıca belli domainler veya spam kaynağı etki alanları tanımlanarak çok yetenekli spam kısıtlama ve ayıklama seçenekleri mevcuttur.

4. Ağ ve İnternet Trafiğini İzleme

Ağdaki paketlerin ileri düzey yönetilebilirliğini sağlayan Iptables, OpenBSD Paket Filter gibi açık kaynak yazılımları ile TCP/IP trafik routing, ethernet protokolü ve MAC filtreleme, bant genişliği yönetimi ile NAT işlemleri yapılmalıdır. Ağ paket trafik analizi ve çok özellikli saldırı tespiti engelleme yazılımı(Etherial, Ettercap), ağ güvenliği denetimi ve trafik dinleme amaçlı sniffer programı kullanımı ile olası siber saldırı durumlarına karşı denetlenmelidir. Ayrıca Nmap(Network Mapper) ile basit anlaşılır bir grafik arabirimi sayesinde çok amaçlı ağ araştırma ve port tarama gerçekleştirilmektedir. Uygulamada Squid proxy ve Dansguardian içerik filtreleme programını ile erişim iz kayıtları(log)'nı analiz etmek için sarg reports yazılım araçları kullanılmıştır.

5. Güvenlik Duvarı Yapılandırma

Dış ağlardan iç ağa gelecek veya içeriden dışarıya çıkacak IP'ler ve izin verilecek portlar, veri trafiğnin yönü tanımlanarak hedef sistemlere yönlendirilir. Domain, E-posta, Port veya IP bazında kısıtlamalar ve yasaklamalar getirilebilir. System Access kısmından interface'ler arasında hangi trafiklerin geçebileceği tariflenir. Uygulama da kullanılan Endian Firewall oldukça gelişmiş açık kaynak kodlu yazılımları bir araya getirerek bir paket çözümü sumaktadır. Kolay yönetilebilir web ara yüzünden DHCP, içerik filtreleme, anti spam, firewall, OpenVPN ve IDS gibi

bir yönetilebilir birçok bileşene sahiptir. Endian'da LAN, WAN, DMZ ve WIFI olmak üzere 4 ayrı ara yüz tanımı yapılabilmektedir[9]. Küçük ve orta ölçekli işletmelerde interneti kolayca dağıtıp paylaştırılabilecek ağın yanı sıra e-posta sunucusunu da kontrol altında tutabileceğimiz Linux tabanlı açık kaynak kodlu güvenlik duvarıdır. Dışarıdan gelebilecek saldırı ve botlara karşı etkin tarama modülleri ile tedbir niteliğidir. Veri iletişim sistemlerine karşı siber saldırıları en az indirebilecek güvenli, kullanımı ve sistem ayarları kolay yapılabilen bir sunucu tabanlı güvenlik yazılımdır.

B. E-Posta Mahremiyeti ve Gizlilik

E-posta hesabı pek çok üyeliklerde doğrulama ve aktivasyon aracı olarak kullanılmaktadır. Siber âlemde hesap bilgileri ve parolalar çok kıymetlidir. Sunucu ve bireysel posta kutularımız ile arada iletilen verinin gizlilik ve güvenliği oldukça önemlidir[10]. Aşağıda belirtilen hususlara dikkat etmek gerekmektedir.

1. Kimlik Doğrulama

Kişisel veya kurumsal mahremiyet gerektiren verilere erişim, izleme, kontrol ve düzenleme belli seviyelerde kimlik doğrulama gerektiren işlemlerdir. Günümüzde karmaşık yapıda şifre doğrulamanın yanı sıra iris, parmak izi gibi kişisel sağlık bilgilerine dayalı veya elektronik çipli doğrulama kullanılabilmektedir. E-posta servislerinde de LDAP benzeri yapılarla eşleme yapılabilmektedir[11].

2. Erişim ve Yetkilendirme

E-Posta uygulamaları içersinde bulunan bazı yan uygulamalar kullanıcının sahip olduğu yetkilere bağlı olarak işlem görürler. Yöneticiler belli posta gruplarına erişim ve yetkilendirme ayrıcalıkları tanıyabilmektedirler. Hesap geçerliyse ve bağlantı için yetki verilmişse, sunucu bağlantıyı posta erişim ilkelerine ve kullanıcı hesabı özelliklerine göre kabul eder. Yapılan uygulamada zimbra sunucusu içersinde class-of-service (COS) modülü üzerinden ayrıntılı ve güvenli yetkilendirme seçeneklerine sahip olduğu görülmüştür[8].

3. Şifreleme

Güvenli Sunucu Sertifikası (SSL - Secure Sockets Layer) ağ üzerindeki veri iletişiminde siber güvenliğin sağlanması amacıyla kullanılmaktadır[12]. Son yıllarda gelişmiş algılama ve yakalama teknikleri kullanılarak ağ trafiği üzerindeki değerli verilerin bilgisayar korsanları tarafından ele geçirmektedirler. E-posta iletişimine yönelik gerçekleşebilecek saldırılar ve ele geçirebilen verilerin maddi ve manevi değeri ölçülemez. O nedenle haberleşme iletileri başta olmak üzere kritik niteliklere sahip verilerin iletimi mutlaka şifreli mimari üzerine kurgulanmalıdır.

4. Dijital İmzalama

E-posta iletişiminde yüksek siber güvenlik sağlamak amacıyla kurumsal yapılarda kullanılmalıdır. Dijital imzalar göndereni doğrulamak ve iletilen mesajın bozulmamış olmadığını kanıtlar. Dolayısıyla bütünlük doğrulanır[13].

5. Yedekleme

E-posta sistem dosyaları ve posta kuruları yasalara uygun güvenli damgalama süreçleri kullanılarak kriptolu şekilde yedeklenir[14]. Kullanım yoğunluğu ve süreçlerin risk düzeyine bağlı olarak belli saatlerde günlük, haftalık ve birden fazla ortama, hızlı dönüş yapılabilecek şartları da sağlayacak şeklinde yedekleme yapılır.

C. Elektronik İletişimde Uygulanması Gereken Siber Güvenlik Politikaları

I. *E-Posta Politikası*

- Kurum e-postaları uygunsuz ve amaç dışı üyeliklerde kullanılamaz,
- Kurum saygınlığını zedeleyecek, taciz niteliğinde postalar için kullanamaz,
- Spam türü zincir e-postalar oluşturup, sahte ve zararlı eklentiler gönderemez,
- Kaynağından emin olunmayan e-postalar cevaplanmaz, başkasına gönderilmez,
- Kurumla ve işle bağdaşmayan uygunsuz iletiler kalıcı olarak silinir,
- Kullanıcı kendi e-postasından ve doğabilecek hukuki suçlardan sorumludur.
- Kullanıcılar, tanımadıkları kimselerden gelen, cazip öneriler içeren e-postaları açmamalı, gerektiğinde sistem ve güvenlik yöneticilerini vakit kaybetmeden konu hakkında bilgilendirmelidirler.

II. *Şifre Politikası*

- Ağda yetkilendirilmiş bir personelin e-Posta kullanıcı adı ve şifresi paylaşılamaz,
- Kullanıcı e-posta hesabının bilinçli amaç dışı kullanımdan doğabilecek zarardan sorumludur,
- Belli sürelerde şifre oluşturma kurallarına göre şifre değişmesi zorunludur,
- Bilgisayardan uzaklaşması halinde e-posta oturumu kapatma alışkanlığıdır,
- E-Posta kullanıcı adı ve şifreler üzerinden bazı program yetkilerinin verildiği ve sahipliğidir,
- Gizli belgelerin e-posta ortamlarında mutlaka şifreli şekilde iletilmesi gerekliliğinin önemli olduğu[15].

III. *Ağ ve İnternet Kullanım Politikaları*

- Kullanıcılar kurum internetini bilinçli kullanmalı, amaç dışı ve sistemlerin çalışmasını engelleyecek şekilde kullanmamalı,
- Kuruma ait bilgisayar, MAC ve IP adresi kullanılarak oluşturulan trafikten, o zaman dilimindeki kullanıcı olan kişi sorumludur,
- Kuruma ait sunucu sistemlerine karşı siber tehdit oluşturmamalıdır,
- Kurum ağından telif hakları ihlal edici yasal olmayan materyal edinmemek,
- Gerçek dışı endişe veren, yanıltıcı e-posta iletimde bulunmamak,
- Kullanılan cihazı ve ağa zarar verebilecek e-postaları açmamak, virüslü ve şüpheli iletilerden uzak durmak,
- Bilgi kaynaklarını yetkisiz ve izinsiz kullanmamak

IV. SONUÇ VE ÖNERİLER

Kurumları ve bireyleri sahte, spam, zararlı eklentiler yoluyla siber saldırılara neden olabilecek bilgi hırsızlığına karşı korumak için, sonuçta aşağıda belirtilen siber güvenlik önlemlerinin alınması gerekmektedir;

- E-posta kanalıyla hesap ayrıntılarını isteyen, kişisel ve gizli kalması gereken bilgiler asla verilmemelidir.
- Ağa bağlı son kullanıcıların e-postalarını takip ettiği bilgisayarda mutlaka güncel bir anti virüs olmalıdır.
- Bilgisayarın güvenlik duvarı uyarı konumunda etkin şekilde olmalıdır.
- İşletim sistemi yamaları yapılmış ve güncellenmiş olmalıdır.
- Son kullanıcıların spam, phishing, malware, worm türü zararlılar konusunda bilinçli olması için uyarı ve eğitimler düzenlenmelidir.
- Yazılım yüklenmesini gerektiren e-postalara karşı tedbirli ve bağlantılı ek kurulumlar iptal edilmelidir.
- İlginç ve beklenmedik e-postaların kendisi, eklentisi ve bağlantıları açılmamalıdır.
- E-posta isimleri veya listesi web sayfalarında açık ve doğrudan kullanılabilir şekilde yayınlanmamalı, en azından aradaki @ işareti resim veya at şeklinde değiştirilmeli.
- Posta sunucularında gelen giden veri trafiği ve posta kutuları üzerinde mutlaka anti-spam, anti-virüs, anti-worm, anti-phishing gibi yazılımlarla zararlılar ayıklanmalıdır.
- Posta sunucusu deneyimli personel tarafından sunucu işletim sistemi siber güvenliği eksiksiz sağlanmalıdır[16].
- Kullanıcılara ait posta kutuları, belli periyotlarda, kriptolu ve şifre korumalı şekilde yedeklenmelidir.
- Posta sunucusu SSL sertifikasına sahip olmalı, kullanıcılar web mail hizmetini https:// ile başlayan adres satırı kullanılarak veri trafiği kriptolu şeklide gerçekleşmelidir.
- Posta sunucusu üzerinde istem dışı aşırı posta gönderim trafiğine karşı uyarı ve koruma sistemi olmalıdır.
- İleti trafiği ve oturum açma bilgileri gerçek zamanlı kaydedilerek analizi yapılmalıdır.

Sonuç olarak elektronik posta iletiminde etkili bir siber güvenlik sunucunun doğru yapılandırılması ile başlar, son kullanıcının dikkat ve özenli kullanımı ile gerçek başarıya ulaşılabilir.

KAYNAKÇA

[1] http://www.bitkom.org/ - Mart-2012

[2] Symantec Intelligence Report, Symantec Corporation, http://www.symantec.com- Mayıs-2013

[3] E Şahinaslan, A Kantürk, Ö Şahinaslan, E Borandağ; Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, Akademik Bilişim 2009, Şanlıurfa, S.1

[4] The Horizon Scan 2013, "Council of Europe Recommendation" No. Rec (2006) 4 of the Committee of Ministers to memberstates on research on biologicalmaterials of humanorigin, https://wcd.coe.int/ViewDoc.jsp?id=977859

[5] http://www.trendmicro.com/how-big-will-the-android-malware-threat-be-in-2012/- Şubat 2013

[6] Ö Şahinaslan, E Şahinaslan M Razbonyalı, Open Source Administration Software and Implementation Results for ensuring Electronic Communication and Information Security Gediz University ISCSE 2010, Kuşadası, S.2

[7] National White Collar Crime Center, 2009 Internet Crime Report, US Department of Justice, http://www.ic3.gov - May 2010

[8] http://www.zimbra.com/- Mayıs 2013

[9] http://www.endian.com/en/community/ Nisan 2013

[10] TS ISO/IEC 17799, Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri - Kasım 2002, S.1.

[11] Ö Şahinaslan, E Şahinaslan, A Kantürk,; Kablosuz Ağlarda Bilgi Güvenliği ve Farkındalık, III. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu 2010, Ankara, S.4

[12] http://windows7news.com/2010/04/09/microsoft-security-intelligence-report-vol-7

[13] http://www.linuxhelp.net- Nisan 2013

[14] Ö Şahinaslan, E Borandağ, E Can, E Şahinaslan; Zibra Sunucu ile Birlikte Yönetim Sistemi, Akademik Bilişim 2009, Şanlıurfa, S.1

[15] http://www.howtoforge.com/- Nisan 2013

[16] Thomas R. Peltier, "Information Security Risk Analysis", Asset Protection and Security Management Handbook, Information Technology Control and Audit, CRC Press, London, 2005

BIYOGRAFILER

Dr. Önder Şahinaslan – Bilgi teknolojileri alanındaki yaklaşık 18 yıllık eğitim, birikim ve iş geliştirme becerilerine sahiptir. Bilgisayar Programcılığı ve Mühendislik eğitiminden sonra Bilgisayar Mühendisliği ve İşletme(MBA) alanında çift yüksek lisansın ardından Siber Güvenlik alanında Bilgisayar Mühendisliği doktora eğitimini tamamlamıştır. 1995 yılında bilgisayar sektöründe eğitmen ve teknik danışman olarak çalışma hayatına başladı. MEB'e bağlı özel öğretim kurumlarında uzman öğreticilik ve yöneticilikte bulundu. 2000 yılında katıldığı Maltepe Üniversitesi'nde sırayla Bilgisayar Mühendisliği Bölümünde Araştırma Görevlisi, Bilgi İşlem Daire Başkanı olarak çalıştı. Halen Bilişim Bölüm Başkanı ve Öğretim Görevlisi olarak görev yapmaktadır.

Bilgi ve bilgi teknolojileri, siber güvenlik, ağ ve sunucu sistem yönetimi, açık kaynak kodlu uygulama ve çözümler, sızma test ve denetleme araçlarının kullanımı, ağ ve sunucu güvenliği belli başlı çalışma alanlarını oluşturmaktadır.

1975 doğumlu evli ve 2 çocuk sahibi olan, özel yaşamında spora ve sosyal aktivitelere önem veren, ailesiyle birlikte vakit geçirmekten hoşlanan araştırmacı bir kişiliğe sahiptir.

Dr. Ender Şahinaslan - 1972 yılında Sivas ili Gürün ilçesinde doğdu, evli ve üç cocuk babasıdır. Trakya Üniversitesi Bilgisayar Mühendisliği Lisans, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği bölümünde 'Yazılımda Kalite Modellerinin Değerlendirilmesi' adlı çalışmayla Yüksek Lisans, Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünde 'Standartlara Dayalı Bilgi Güvenliği Risk Analiz ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi ve Uygulama Yazılımının Geliştirilmesi' adlı çalışmayla doktora programını tamamladı.
1996 yılında Gazi Üniversitesi'nde başladığı çalışma hayatına Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Araştırma Görevlisi, Maltepe Üniversitesi Öğretim Görevlisi, Sabancı Üniversitesi Bilgi Teknolojileri Birimi'nde Uygulama Sorumlusu olarak devam etti. 2004 yılında Bank Asya Yazılım Geliştirme Müdürlüğü'nde başladığı göreve, Organizasyon Kalite ve Sistem Geliştirme Müdürlüğünde devam etti halen Bilgi Güvenliği, BT Risk ve Uyum Müdürü olarak çalışmaktadır. ISO 27001 LA, ITIL Fv3 ve CRISC sertifikalarına sahiptir.

Yazılım Güvenliği Üzerine Bir İnceleme

Seda YILMAZ ve Şeref SAĞIROĞLU

***Özet*— Artık birçok şirket, kurumsal işlemlerini, diğer iş ortaklarıyla iletişimlerini ve yürüttükleri işlemleri web uygulamaları üzerinden geliştirmektedir. Hatta ülkeler e-devlet projelerini hızla devreye sokmakta ve hizmetlerini bu platform üzerinden vermektedir. Web uygulamalarının bu kadar aktif bir şekilde kullanılması işlemlerin güvenliğinin daha çok sağlanması ihtiyacını da beraberinde getirmiştir. Bu çalışmada web uygulamalarında güvenli yazılım geliştirme kuralları, modelleri, güvenli bir yazılımda olması gereken ilkeler, web yazılımlarına yönelik tehditler ile kurumsal olarak güvenli yazılım geliştirme döngüleri incelenmiş ve bunu arttırmaya yönelik çözüm önerileri sunulmuştur.**

***Anahtar Terimler*— Yazılım, web, yazılım güvenliği, tehdit modelleme**

***Abstract*— Many companies run their businesses, operations, branches and businesses with other partners, communications and transactions conducted over web applications. Even the countries involved into e-government projects and services over this platform is rapidly activated. Rapid grow within web application usage bring with the needs to ensure the safety and security of operations and information. In this paper, secure software development, web applications and their rules, models and principles in developing secure are reviewed and discussed in terms of threats and secure enterprise software development cycles. Some suggesstions are given in terms of security and safety of operations.**

***Index Terms*— Software, web applications, software security life cycle, threat modeling**

I. GİRİŞ

Bilgisayarın icat edilmesinin ardında onun yönetilmesi için bir dizi komuta ihtiyaç duyulmuştur. Başlangıçta bazı parçaların yerine yeni kodlu parçaların yerleştirilmesiyle yani fiziksel müdahale ile bu ihtiyaç giderilemeye çalışılmıştır. Zamanla işlemlerin ve ihtiyaçların artmasıyla bu fiziksel müdahalenin dışında bir sistem geliştirilmesi zaruri hale gelmiş ve yazılım geliştirme süreci 1956 yılında IBM tarafından Fortran programlama dilinin geliştirilmesiyle başlamıştır [3]. İnternetin temelinin atıldığı 1960'lı yıllardan sonra yazılım sektörü için yeni bir çağ başlamıştır. Yıllar içinde yaygınlaşan internet ağı zamanla yazılım uygulamalarını yerel bilgisayara bağımlı olmaktan çıkarmıştır. Firmalar, kurumlar ve hatta kişisel kullanıcılar internetten faydalandıkça, uygulamalar web ortamına taşınmaya başlamış, bu durum beraberinde web yazılımların güvenliği kavramını ortaya çıkarmıştır.

Yazılım mühendisliğinde, yapılan saldırılar karşısında karşı yazılımlar/programlar ile güvenlik duvarı uygulamalarının yetersiz kalmaya başlamasıyla, kod ile işlevselliğin ve güvenliğin arttırılması ihtiyacını doğurmuştur [6]. Yazılım güvenliği, yazılımın geliştirme sürecinden itibaren başlayan ve birbirini takip eden süreçlerde bir bütünlük içinde devam etmesi gereken bir kavramdır.

Bu çalışmada ikinci bölümde yazılım geliştirrme modelleri, üçüncü bölümde güvenlik ve güvenli kodlama teknikleri, dördüncü bölümünde tehdit modelleme, beşinci bölümünde kod injection, altıncı bölümünde kurumlarda güvenli yazılım geliştirme döngüsüne geçiş ve yedinci bölümünde yazılım güvenliğini etkileyen diğer hususlar konuları tartışılmış ve sonuç ve öneriler sunulmuştur.

II. YAZILIM GELİŞTİRME MODELLERİ

Yazılım, donanım ve sistem güvenliği açısından standart belirleme çalışmaları 1983 yılında ABD'de başlamış ve bunu Avrupa'daki çalışmalar takip etmiştir.Ülkeler bilgi sistem ürünleri için standartlar belirlemiş ve ürünlerini bu standartları dikkate alarak üretmeye, ithal ve ihraç etmeye başlamışlardır Bu durum zaman içinde ihraç edilen BT (Bilgi Teknolojileri) ürünlerini için farklı ülkelerde standart farklılıklarından dolayı güvenlik testlerinin başarılı olamasına neden olmuştur. Süreç içerisinde çeşitli çalışmalarda, ortak bir standart oluşturulmaya çalışılmıştır. Günümüzde 1996 yılında Kanada, Fransa, Almanya, İngiltere, Avustralya, Yeni Zelanda ve Amerika Birleşik Devletleri tarafından oluşturulan "Ortak Kriterler (Common Criteria)" temel alınmaktadır [3].

Yazılım geliştirme modellerine genel olarak bakıldığında aslında hepsinin temelinde, "Güvenli Yazılım Geliştirme Yaşam Döngüsü"nün yer aldığı görülmektedir.



Şekil 1. Güvenli Yazılım Geliştirme Yaşam Döngüsü [1].

Şekil 1'den de takip edilebileceği gibi *eğitim ve farkındalığın* geliştirilmesi, döngünün başlangıcı olup bütün süreç boyunca devam eden en önemli unsurdur [1]. Bu aşamada [1], tehditlerin belirlenmesi, güvenli tasarım ve güvenlik testleri konusunda geliştiriciler eğitilmediler. *İhtiyaç analizleri* aşamasında yazılımın geliştirilmesi, güvenlik ve test için kontroller yapılmalı ve sonuçları analiz edilmelidir. *Tasarım ve risk* analizinde güvenlik açısından belirlenen kriterler uygunluk, tehdit modelleme, gizlilik risk analizi gibi kontroller yapılır. *Geliştirme* sırasında belirlenen güvenlik kriterlerine uyulmalı, kaynak kod analizlerinden faydalanılmalıdır. *Doğrulama* aşamasında oluşturulmak istenen ürün/yazılım bütünlük, gizlilik ve erişilebilirlik yönlerinden bir takım testlere tabi tutularak kodun güvenilirliği sağlanmasına ve kod hatalarından oluşabilecek açıkların önlenmesine çalışılır. *Devreye alım* artık nihai ürünün piyasaya sürüldüğü ve kullanıcının bilgilendirildiği aşamadır. Yazılım geliştirme sürecinin güvenli bir şekilde yapılıp yapılmadığı bu aşamadan sonra gözlenebilmektedir. *Açıklık* yönetimi ve geri dönüş aşaması ise kullanıcılardan yapılan geri dönüşlerin değerlendirildiği ve bu değerlendirmelerden sonuç çıkarımlarının yapıldığı aşamadır. Bu sonuçlar farkındalık eğitimi için kaynak görevi gördüğünden döngü en başa dönmüştür [1].

Bu önemli alanın güvenli olarak geliştirilebilmesi ve denetlenebilmesi için geliştirilen modeller aşağıda farklı başlıklar altında açıklanmıştır.

A. Yetenek Olgunluk Modeli (CMM - Capability Maturity Model

1986 yılında ABD'de geliştirilmiştir. Bu model daha çok var olan uygulamaların geliştirilmesini hedefler. Bu modelde amaç, ürünün güvenlik standartlarına göre geliştirilmiş olmasını sağlamak değil daha çok özel bir inceleme alanındaki zayıflıkların giderilmesidir [9].

B. Tümleşik Yetenek Olgunluk Modeli (CMMI Capability Maturity Model Integration)

CMM modelini temel alan bu modellemede amaç, organizasyonun iyileştirilmesi, durumunun gözden geçirilmesi ve yönetimi ile ilgili çözümler sunmaktır [3]. Bu model büyük firmalar tarafından yazılım ihalelerinde firma seçme işlemi ve şirket yöneticilerinin şirketin durumunu analiz etmesini sağlamak için etkin olarak kullanılmaktadır. CMMI modeli, ürün/hizmetin oluşturulması, idame ve satış süreçlerinin iyileştirilmesi aşamalarına yöneliktir. Model temel alınarak şirketler için CMMI sertifikası verilmektedir. Bu sertifika, şirketlerin "neleri nasıl yaptığı" sorusuna cevap bulmayı hedefleyen ve üç seviyesi olan bir sertifikadır. En alt seviye olan C seviyesinde kağıt üzerinden şirket iş akışı veya iyileştirme planları incelenir. Varolan her şirketin C seviyesinde olduğu kabul edilir. B ve A seviyesi inceleme sırasında ise gerçek projeler üzerinden üretim sonuçlarının incelenmesi ile yapılır. Model, şirketlerin mutlaka sahip olması gereken ve sertifikada özellikle aranan genel ve özel amaçları içeren **temel bileşenler**, kuruma özgü ve/veya kurumlar arasında işletim farklılıkları gösterebilen uygulamaları içeren **beklenen bileşenler** ve bunların dışında kalan herşeyi kapsayan **açıklamalar**dan oluşur. CMMI modelinde yapılan kurumsal inceleme esnasında genel olarak gereksinimlerin belirlenmesi/ yönetimi/ geliştirilmesi, süreçlerin tanımlanması, proje planlanması/izlenmesi, ölçme/değerlendirme faaliyetleri, risk yönetimi ve çözüm üretme konularında şirketlerin durumları incelenmektedir [15].

C. Federal Havacılık Yönetim Tümleşik Yetenek Olgunluk Modeli (FAA-iCMM Federal Aviation integrated Maturity Model)

Federal havacılık sisteminde daha çok tercih edilen FAA-ICMM modeli, geniş kapsamlı projelerde kaynak kullanımı ve yönetimini kapsamaktadır. [3].

D. Güvenli CMM/Güvenli Yazılım Metodolojisi (Trusted CMM/Trusted Software Methodology (T-CMM, TSM))

Güvenli yazılım metodolojisi 1990'lı yıllarda geliştirilmiştir. Bu model yazılım geliştirme sürecinde geliştirme hatalarını bulma yöntemlerini, ürünün kullanıma sunulmasının ardından da ataklara karşı koyma tekniklerini içerir [3].

E. Sistem Güvenlik Mühendisliği Yetenek Olgunluk Modeli (SSE-CMM -- Systems Security Engineering Capability Maturity Model)

Organizasyonların güvenlik mühendisliği uygulamalarının iyileştirilmesini hedefleyen bir modeldir. Bu model, güvenlik prensipleri içermesine rağmen uygulama performansının ölçülmesi ve iyileştirilmesi üzerine çalışmaktadır. ISO/IEC 21827 standardı olarak yayınlanmış ve halen The International Systems Security Engineering Association (ISSEA) tarafından uygulanmaya devam etmektedir [3].

F. Microsoft Security Development Lifecycle (SDL)

Microsoft yazılım geliştiricileri, karşılaşılan problemlerden dolayı 2004 yılında güvenlik ve gizlilik için bütünleştirici bir model geliştirmeyi hedeflemişler ve bir yazılım güvenliği süreci olan SDL'yi tasarlamışlardır (Şekil 2). Bu süreç, temel yazılım güvenliği döngüsünü rol model olarak alan ve doğrudan proje yöneticisine bağımlı bir modeldir [7].

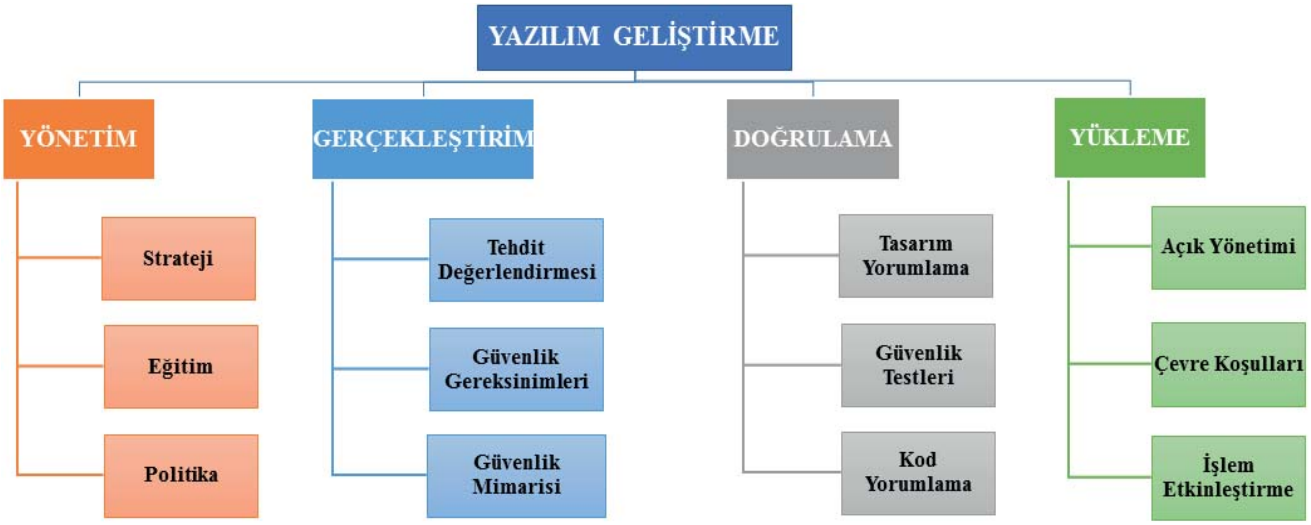


Şekil 2. Microsoft SDL Döngüsü [7].

Şekil 2'den de görülebileceği gibi [7], *Eğitim* aşamasında personele yazılım geliştirme modeli ve yazılım ihtiyaçları doğrultusunda temel eğitim verilmesi hedeflenir. *Analiz* aşamasında programın hedef kitlesi, içereceği özellikler, test için kullanılacak saldırı modelleri ve program maliyetinin belirlenmesi gibi ön planlama işlemleri gerçekleştirilir. *Tasarım* aşamasında analiz aşamasınından elde edilen sonuçlara göre program planlanır. Yapılacak saldırı teknikleri, karşı koyma yöntemleri kararlaştırılır ve risk analizi yapılır. *Gerçekleştirim* aşamasında kod geliştirilirken ve sonrasında kullanıcının isteyebileceği güvenlik tedbirleri de dikkate alınarak esnek bir yapı oluşturulmaya çalışılır. White-box Security, Code Review gibi yöntemlerle kodun güvenliği *Doğrulama* aşamasında test edilir. *Yayınlama* aşamasında uygulama tamamlanmış ve kullanıcıya sunulmuştur. Fakat bu aşamaya gelmeden yani son kullanıcıya ürün sunulmadan önce güvenlik kontrollerinin sonuçlarından emin olmak gerekir. Son aşama olan *Bilgi Toplama* aşamasında ise kullanıcıdan gelen geri bildirimler dikkate alınarak açıklar tespit edilip ilgili yamalar üretilerek kullanıcıya sunulur [4].

G. SAMM (Yazılım Garanti Olgunluk Modeli)

Open Web Application Security Platform (OWASP) tarafından desteklenen SAMM modeli bilgi güvenliği aktivitelerini yazılım geliştirme sürecine dâhil etmeyi hedefleyen bir modeldir [12]. Bu model organizasyonun büyüklüğünden bağımsız olup büyük bir proje için kullanılabileceği gibi organizasyonun tamamı ya da küçük bir kısmı içinde son derece uygundur [12].



Şekil 3. SAMM Genel Yapısı [12].

SAMM'a gore yazılım geliştirme süreci modellemesi katmanlı bir mimariye sahiptir. İş fonksiyonları ve bunların her birinin güvenlik araştırmaları farklı katmanlarda yer alır.Şekil 3'de verilen iş fonksiyonları katmanında yönetim, gerçekleştirme, doğrulama ve yükleme ana başlıkları bulunur. *Yönetim* fonksiyonunda yazılım geliştirme sırasındaki güvenlik süreçlerinin yönetiminin gerçekleştirilir. *Gerçekleştirme* fonksiyonu, güvenli yazılım gereksinimleri ve tasarım aşamaları üzerinde yoğunlaşan, tehdit değerlendirme, güvenlik gereksinimleri ve güvenli mimari aktivitelerini içerir. *Doğrulama* fonksiyonu tasarım, kodlama ve yazılım testlerinin gözden geçirilmesini ve güvenlik testlerini kapsamaktaolup tasarım, kod denetimi ve güvenlik testlerinden oluşur. Yükleme (*Kurulum)* fonksiyonu ürünün son kullanıcıya iletilmesi ve bakım, idame işlemlerini içerir. Bu fonksiyonun aktiviteleri ise güvenlik açığı yönetimi, platform farklılaştırması ve işletim kurulumudur [12].

III. GÜVENLİK VE GÜVENLİ KODLAMA İLKELERİ

Bu husular aşağıda verilen alt başlıklarda açıklanmış ve tartışılmıştır.

A.Güvenlik

Sahip olduğumuz maddi ve manevi varlıklarımıza doğrudan ve/veya dolaylı yönelen her tehdidin derecesi ve vereceği bir zarar vardır. Bu zararın önceden tahmin edilerek uygun tedbirlerin alınması işlemi "güvenlik" olarak tanımlanabilir [8]. Bilgi varlıklarımızın güvenliğinin tam olarak karşılanması için belgeleme, yetkilendirme, denetim, gizlilik, bütünlük ve uygunluk esalarının yerine getirilmiş olması gerekmektedir.

Belgeleme, sistemdeki ya da sistemden yararlanan son kullanıcı, bilgisayar ya da diğer servislerin "kim olduğu" sorusuna verilen cevap, her bir işlemin belgelenmesidir. *Yetkilendirme,* belgelenen kullanıcıların erişme izinlerinin olduğu her türlü kaynağın kontrol edildiği aşamadır. *Denetim*, kullanıcının yaptığı her çalışmanın kayıt altına alınmasıdır. Böylece inkar etmenin önüne geçilmiş olur.

Gizlilik, sistemin yabancı kullanıcılarca izlenmesi ve bilgilerin güvenliğinin sağlanması için önlem alınması sürecidir. Tam bir gizlilik esasına göre, ağdan yapılacak dinlemelere, monitör takiplerine v.b uygulamalara karşı olarak şifreleme ya da erişim kontrol listeleri oluşturmak gibi tedbirler alınabilir. *Bütünlük,* verinin bilinmeden ya da kötü niyetli yapılan değiştirmelerden korunmasını sağlar. *Gizlilik*te olduğu bir bütünlükte de ağlar üzerinden iletilen verinin korunması önemli bir unsurdur. Ağ üzerinden iletilen veriler için bütünlük, karma teknikler ve ileti kimlik doğrulama ile sağlanmaya çalışılır. *Uygunluk,* mevcut durumun meşru kullanıcılar için sabit kalması, meşru olmayan kullanıcılar ve saldırı atakları için erişiminin olup olmadığının kontrol edildiği durumdur [8].

B.Güvenli Kodlama İlkeleri

Bilgi güvenliği, kullanıcıya sadece izin verilen kısma erişim hakkı veren, *güvenlik* yetkisi olmayan kullanıcıya veri değiştirme izinin verilmediği, *bütünlük* ve ihtiyaç halinde yetkili kullanıcıya müdahale hakkı veren *kullanılabilirlik* prensiplerine dayanan bir işlemdir. Bu prensipler temel alınarak geliştirilen sistemde öncelikle dikkat edilmesi gereken unsurgüvenli bir mimarinin oluşturulmasıdır. Güvenli olmayan bir mimari kod ne kadar güçlü olursa olsun saldırılara açık bir haldedir. Yazılım geliştiricinin mimariyi oluştururken kendine sorması gereken soruların başında "kötü niyetli biri olsam…" gelmektedir. Bu bakış açısı Andrew van der Stock tarafından ileri sürülen "kötü düşünce" sistemidir. Bu sistemde kişi kendi açıklarını dışardan bakmaya çalışarak bulmayı ve düzeltmeyi hedefler [2]. 2'nolu kaynakta verilen bu hususlar aşağıda özetlenmiştir.

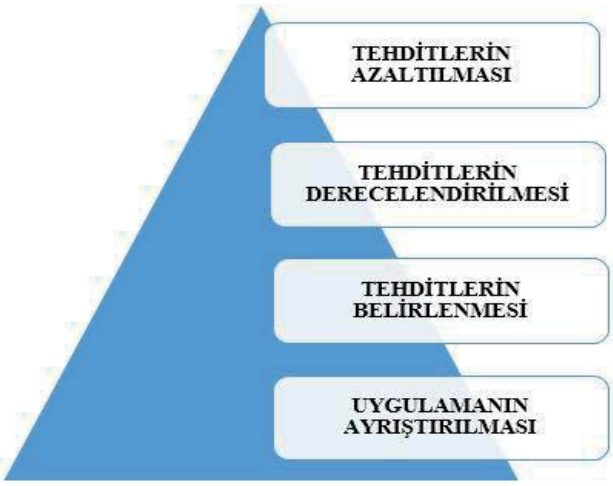
Saldırı yüzey alanını azaltmak kodlama işlemi sırasında dikkat edilecek en önemli ilkelerden biridir [2]. Böylelikle genel risk oranı azaltılmış olur. *Güvenli öntanımlar* yaparak kullanıcılar tarafından yapılacak bir çok işlem için önceden kurallar yaratma imkanı sağlanır. *En az öncelik* ilkesi ile kullanıcının hesap işlem süreçleri kontrol edilebilir. Sunuculara öncelik yetkisi verilmemelidir. *Kademeli savunma* ile koyulacak kontroller aşamalı olarak koyularak bir dizi kontrol elde edilmiş olur. *Güvenli aksama* ile kodda oluşacak aksamalar karşısında sistemin açık vermemesi sağlanmalıdır. Oluşan bu aksama kullanıcıya yetkisi olmayan hakların kapısını açmayacak şekilde kod düzenlenmelidir. *Dış sistemlerin güvenli olmadığı* akılda tutulması gereken bir ilkedir. Sistem sağlayıcılar her zaman kodunuz için gerekli güvenlik tedbirlerin tam olarak almamış olabilir. Farklı yetki sahiplerine farklı görevler vererek *görevlerin ayrımı* ile sistemde yapılan iş akışının kontrolü ve güvenliği sağlanış olur. *Belirsizlik yolu ile güvenliğe güvenmemek* gerektiği akıldan çıkarılmamalıdır. Güvenlik, tek bir sistemin kod içine gizlenmesiyle elde edilemez. Bunun yerine birbirini takip eden çok sayıda güvenlik kontrolü bulunmalıdır. *Basitlik*, kodun mümkün olan en basit şekilde yazılmasını öngörür zira kod karmaşıklaştıkça kontrolü de zorlaştıracaktır. *Güvenlik sorununun uygun şekilde ele alınması* ilkesinde ise yaşanabilecek sorunlar için test grupları oluşturulmalı ve yapılacak değişikliğin kodun ne kadarını etkileyeceğinin belirlenmesi için test süresi verilmelidir [2].

IV. TEHDİT MODELLEME

Yazılım tasarlarken karşılaşılabilecek tehditlere karşı model geliştirmek tehditlerin ve çeşitliğinin giderek arttığı bu dönemde daha da önemli olmaya başlamıştır. Tehdit modellemenin amacı, genel olarak sistemin güvenliğini tehlikeye atabilecek potansiyel durumları belirlemektir [8].

Tehdit modelleme, güvenlik tabanlı bir analiz sürecidir. Bu süreç uygulamanın anlaşılabilmesi, yeni gelen geliştiricilerin uygulama adaptasyonun hızlandırılması, tehditlerin belirlenmesi, kod hatalarının azaltılması gibi bir çok alanda faydalar sağlar [10,11]. Şekil 4'de tehdit modelleme aşamaları verilmiştir. Bu aşamalar aşağıda kısaca açıklanmıştır:

Uygulamanın Ayrıştırılması aşamasında uygulama alt alanlara ayrılır. Böylece hem uygulamanın anlaşılırlığı arttırılır hem de her bir alan için güvenlik profilleri oluşturulur. Her bir alt katmanın işlevleri bulunmaktadır. Bu işlevler aşağıda özetlenmiştir [10,11]:



Şekil 4. Tehdit Modelleme Aşamaları [10,11].

1) Güvenlik Çember: Sisteme giren ve sistemden çıkan bütün veriler kontrol altında tutulur.
2) Akış Diagramları: Sistemin genelinin modellemesi yapılır. Diagram hazırlanırken sisteme gelecek sorular ve bunların cevaplarının nasıl olacağı yüzeysel olarak ifade edilir.
3) Giriş Noktalarının Belirlenmesi: Her bir giriş noktası için yetkilendirme ve kimlik kontrolü yapılmalıdır.
4) Ayrıcalıklı kod Parçaları: Sistemde ayrıcalıklı ve korumalı bölgelere nüfuz edebildiği için bu alanlar özellikle dikkat edilerek geliştirilmelidir.
5) Güvenlik Profili Oluşturulması: Girdilere ne ölçüde izin verileceği, kimlik kontrolünün nasıl yapılacağı, kimlere yetki verileceği gibi sorular cevaplanmalı bu şekilde profil oluşturulmalıdır.

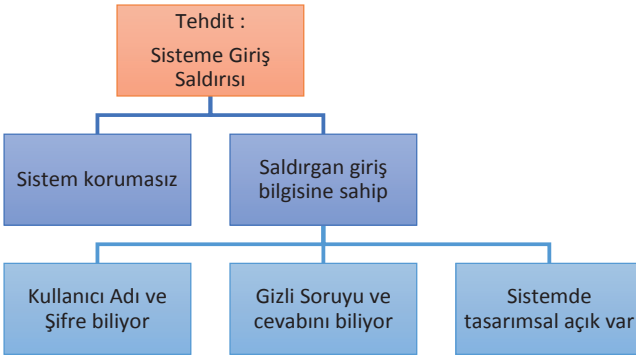
Tehditlerin Belirlenmesi aşamasında her bir kısım tehdit modeli olarak adlandırılmakta ve bunlardan oluşacak tehditler STRIDE modeline göre sınıflandırılmaktadır. Bu modeldeki sınıflar şunlardır [10,11]:

1) Kimlik Yanıltması (Spoofing Identity): Kayıtlı bir kullanıcı ya da geçerli bir sunucu gibi davranma yoluyla sistem için tehdit oluşturulmasıdır.
2) Verinin Değiştirilmesi (Tampering with Data): Verinin art niyet gözetilerek değiştirilmesidir.
3) Inkar (Repudiation): Yapılan işlemin ya da saldırının yapılmadığının iddaa edilmesidir.

4) Bilginin Açığa Çıkarılması (Information Disclosure): İzinsiz ve yetkisiz olarak sistemdeki veri ya da bilgilere ulaşılması ve bilmemesi gereken kişilere ifşa edilmesidir.

5) Hizmet Dışı Bırakma (Denial of Service): Sistemin hizmet veremez hale getirilmesidir.

6) **Yetki Kazanma (Elevation of Privilege):** Yetkisiz kullanıcının illegal yollarla sistemde yetki kazanmasıdır.



Şekil 5. Tehdit Ağacı Gösterimi [10,11].

Tehditlerin Derecelendirmesi aşamasında tehdit ağaçları oluşturulup durum değerlendirildikten sonra hangi tehdide öncelik verileceğini belirlenir. Her bir tehdit için tehdidin nasıl oluşacağı tehdit ağaçları ile gösterilir. Ağaçdaki kök tehdit kutusu, sonraki düğüm ve yapraklar ise tehdidin nasıl gerçekleşeceğini temsil eder Şekil 5'de tehdit ağacı sembolize edilmiştir [10,11]. Tehdit derecelendirilmesi işlemi için en çok tercih edilen yöntem DREAD yöntemidir. Yöntemin kriterleri aşağıda açıklanmıştır [10,11]:

1) Zarar Potansiyeli (Damage Potential): Tehdit gerçekleşirse oluşacak zararın büyüklüğü belirli aralıklar arasında derecelendirilir.

2) Uygulanabilirlik (Reproducibility): Saldırgan için bir tehdidin başarıya ulaşma ihtimali değerlendirilir.

3) Sömürülebilirlik (Exploitability): Tehdidi gerçekleştirmek için gereken bilgi ve süre değerlendirilir.

4) Etkilenen Kullanıcılar (Affected User): Tehdit gerçekleşirse nekadar kullanıcının zarar görebileceği değerlendirilir.

5) Keşfedilebilirlik (Discoverability): Açıkların hangi zorluk derecesinde bulunabileceği değerlendirilir.

Tehditlerin Azaltılması aşamasında bu işlem için dört farklı yaklaşım tercih edilebilir. Buna göre, tehdit konusunda tedbir alınmayabilir ki bu sonuçları ağır olabilecek bir seçenektir. Kullanıcılar tehdit konusunda bilgilendirilip kullanıcı bazlı tedbirler alınabilir (şifre derecesi zorlaştırma, şifreyi paylaşmama gibi). Tehdit konusu olan kısım sistemden çıkartılabilir ya da teknolojik önlemler alınarak tehdit için çözüm üretilebilir [10,11].

V. KOD ENJEKSİYONU

Kod enjeksiyonu, bilgisayar açıklarının (bugs) kötüye kullanımından kaynaklanan bir veri kaybı olarak nitelendirilebilir. Genel olarak enjeksiyon, kodlayıcının hatası sonucu oluşur. Kötü amaçlı enjeksiyon kullanımlarında, Sql enjeksiyon da olduğu gibi veri tabanındaki veriler değiştirilebilir, web uygulamasının kontrolü ele geçirilebilir, sunucuya erişilebilir, UNİX gibi işletim sistemlerinin çekirdekleri hedef alınabilir. İyi niyetli enjeksiyon kullanımlarında ise sayfanın düzenine geliştirme anlamında katkıda bulunulabilir, ihtiyaca uygun olarak verilerin filtrelenmesi için kullanılabilir ya da yazılımsal olarak bazı değişikliklerin daha az maliyetle yapılmasına olanak sağlayabilir [13,14].

Enjeksiyonları önlemek için girdilerin doğrulanması, girdi ve çıktıların kodlanması, program debuggerları için kilit olan kelimelerden kaçınılması, "store procedure" gibi ön derleme, değerlendirme mantığına dayalı kodlamaların tercih edilmesi gibi önlemler alınabilir [13,14].Bunlara ek olarak uygulamanın katmanlı mimariye sahip olması da önemli bir önlem olarak sayılabilir.

A. HTML Enjeksiyonu (XSS)

Bu açık, programcıların kodlama sırasında yaptığı hatalar sonucu oluşur. Web yazılımlarımda veri tabanına giren verilerin ya da çekilen verilerin bir kontrol mekanizmasından geçirilmemesi sebebidir. Bu açıktan faydalanılarak session ve cookie çalması yapılır. Korunmak için veriler sayfaya yüklenme aşamasında değil, veri tabanına gönderilirken ya da çekilirken bir filtrelemeden geçirilmelidirler [5].

B. SQL Enjeksiyonu (SQL Insertion Attacks)

SQL enjeksiyon, meta-karakter adı verilen ve derleyici için özel anlamları olan karakterlerin varlığına dayanan bir açıktır ve karakterlerin yanlış filtrelenmesinden kaynaklanır [14]. SQL enjeksiyon tipleri farklı şekillerde olabilir. Kullanıcıdan alınan kullanıcı adı ve şifre gibi giriş verileri bir filtrelemeye tabi tutulmadan SQL sorgusuna gönderildiğinde oluşan açıktan faydalanarak saldırı yapılabilir. Örneğin,bir web uygulamasının kullanıcı adı ve şifre ikilisi veri tabanına

"SELECT * FROM TABLE WHERE username = '" +Kullanıcı + "' AND password= '" +Şifre + "'"

şeklinde gönderildiğinde (" ") işaretleri içindeki veri bir filtrelemeye tabi tutulmazsa kullanıcının buraya yazacağı (OR "1=) şeklinde bir ifade sorguyu

"SELECT * FROM TABLE WHERE username = "OR"1=1" AND Password = " OR "1=1" "

haline getirir. Bu durum sorguda var olan bütün kayıtlar dönecektir. Böylece saldırgan bütün kullanıcı adı ve şifre bilgilerine sahip olacaktır [13,14].

Bir açık türü de tip kontrolü yapılmadığı durumlarda oluşur. Örneğin nümerik alana dair bir sorgu cümleciği gönderildiğini varsayalım.

"SELECT * FROM TABLE WHERE ID = '" +U_ID";'"

sorgusunu ele alırsak; burada programcı aslında sayısal bir alana ulaşmak istiyor ama gönderilen verinin(U_ID) string olarak gelip gelmediğini kontrol etmiyor. Bu durumda saldırgan tarafından bu sorguya "1;DROP TABLE `DBusers`" şeklinde bir ifade gönderilirse komut

"SELECT * FROM TABLE WHERE ID = '" 1;DROP TABLE `DBusers`';'"

olarak algılanacağından tablodaki kullanıcı bilgileri silinecektir [13,14].

Bir diğer durum ise Kör SQL Enjeksiyon denilen durumdur. Bu tür açık da, saldırgan tarafından sonuçlar veya veriler direk veritabanından görülmez. Bunun yerine gelen veriler farklı mantıksal ifadelerle elde edilir. Elde edilen bu sonuçlar sayfadaki var olan adımlarla elde edilmiş olur [13,14].

SQL enjeksiyonunu önlemek için uygulanabilecek yöntemlerde biri parametreli "store procedure" tekniğini kullanmaktır. Bu teknikte girdiler öncelikle derlendiği için açıklardan faydalanmak neredeyse imkânsızdır. Ayrıca uygulamalarda veri tabanından okuma için salt okunur yetkisi verilmesi de bir çözümdür. Oluşan hatalarda kullanıcıya dönen hata mesajlarında mümkün olduğunca az bilgi verilmesi de saldırganlara veri tabanı hakkında bilgi vermemek açısından önemlidir [13,14].

C. *Dinamik Değerlendirme Açıkları*

Bu açıklar daha çok PHP kodlarda karşılaşılan açıklardır. Saldırgan string değere karşılık sonuç gönderen fonksiyonları kullanır. Bu fonksiyonlara girdi olarak uygulamayı etkileyecek string komutlar göndererek istediği sonuçlara ulaşmayı hedefler [13,14].

D. *SHELL Enjeksiyon*

Bu enjeksiyon adını Unix'den almış olsa da komut satırı kullanan her uygulama için tehdit arz etmektedir. Alınan verinin komut satırı için özel komutlardan biri olup olmadığının kontrol edilmediği uygulamalarda saldırgan komut satırına ulaşarak amacını gerçekleştirmektedir [13,14].

VI. KURUMLARDA GÜVENLİ YAZILIM GELİŞTİRME DÖNGÜSÜNE GEÇİŞ

Kurumlarda karşılaşılabilecek güvenlik zafiyetlerini azaltmak için, [1] nolu kaynakta belirtilen ve aşağıdaki adımlarda özetlenen adımların hayata geçirilmeleri gereklidir.

1) *Kurumun Yazılım Geliştirme Yöntem ve Prosedürlerinin Araştırılması*

Yazılım geliştiren her kurum öncelikli olarak yazılım geliştirme konusunda mutlaka bir prosedürü veya yöntemi belirlemek için bir araştırma yapılmalı ve bir prosedür geliştirilmelidir. Bu prosedür projenin yönetim yaklaşımı, kuruma özel yöntemler ve yazılımlarla ilgili bağlayıcı hükümler içermelidir [1].

2) *Mevcut Modellerin İncelenmesi ve İhtiyaca Yönelik Eğitimler*

Güvenli yazılım geliştirmede kullanılan modeller incelenerek kurum, kurum içi ilişkiler ve etkileşimler, kurum kültürü ve modellerin her birinin kuruma uygun/uygun olmayan yönleri belirlenerek bir n-model seçilmeli ve personel için eğitimler yapılmalıdır [1].

3) *Kurum Şartlarına Uygun Güvenli Modelin Belirlenmesi*

Belirlenen model.kurumun ihtiyaçlarına göre revize edilerek güvenli ve başarılı yazılım geliştirme sürecine dahil edilmelidir. Gerekirse bir dönem belirlenen yapı test edilmeli, gerekli görüldüğünde modele ek tedbirler eklenebilmelidir [1].

4) *Politika ve Prosedür Dokümanlarının Hazırlanması*

Belirlenen modele ait politika ve prosedürlerin dökumante edilmesi, hem kuralların daha kolay anlaşılıp adapte edilmesini kolaylaştırır ve yanlış anlamaları önler hem de ortak bir çalışma yöntemi oluşturularak bu işin el kitabının hazırlanmasını sağlar. Bu yöntem, ekibe yeni katılan kişilerin de sisteme kolayca dahil olmasını sağlar ve sürecini hızlandırır [1].

5) *Eğitimlerin Hazırlanması ve İlgili Personele Eğitim Verilmesi*

Kullanılan Güvenli yazılım geliştirme döngüsü için kapsamlı bir eğitim programı hazırlanarak personelin eğitim alması sağlanmalıdır. Bu eğitimlerin gelişen teknolojiye paralel olarak düzenli olarak yapılması, hem teknolojiyi takip hem de karşıla-şılabilecek risklerin minimize edilmesini sağlayacaktır [1].

VII. YAZILIM GÜVENLİĞİNİ ETKİLEYEN DİĞER UNSURLAR

Yazılımların geliştirilmeleri kadar bu yazılımların işletildiği, barındırıldığı veya çalıştırıldığı ortamların da güvenliğinin sağlanması önemli bir husustur. "Ağdaki bir güvenlik açığı kötü niyetli bir kullanıcının host ya da uygulamayı istismar etmesine, hostdaki bir güvenlik açığı kötü niyetli bir kullanıcının ağ ya da uygulamayı istismar etmesine, uygulamadaki bir güvenlik açığı kötü niyetli bir kullanıcının host ya da ağı istismar etmesine izin verebilir" [7]. Belirtilen bu hususlar aşağıda başlıklarda kısaca açıklanmıştır.

A. *Ağ Güvenliği*

Güvenli bir yazılım ancak güvenli bir ağ yapısı üzerine çalıştırılabilir. Ağın korunması, TCP-IP ataklarına karşı korunmanın yanında güçlü şifreleme, güvenli erişim ve admin yapısıyla da desteklenmelidir. Güvenli bir ağ hem ağ trafiğini aksatmamalı hem de yönelen tehditleri geldiği katmanda kontrol altına almalıdır ki yazılım güvenliği yüksek oranda sağlanabilsin [8].

B. *Host Güvenliği*

Host güvenliğinde dikkat edilmesi gereken en önemli husus, web servisi, uygulama servisi ve veritabanı hizmetlerinin her birinin kendine has güvenlik protokollerinin olduğu ve her yeni gelen sistem için bu ayarların yapılması gerektiğidir [8].

C. *Uygulama Güvenliği*

Güvenlik konuları ile web uygulamaları karşılaştırılmaları analiz edildiğinde, güvenlik problemleri güvenlik açıkları olarak gruplanabilir. Bir uygulamanın güvenlik direncini ölçmek için güvenlik açıklarından elde edilen erişim doğrulama, belgelendirme, konfigürasyon yönetimi, oturum yönetimi, hassas veri şifreleme, parametre manipülasyonu, hata yönetimi, denetim ve log gibi güvenlik profilleri kullanılır [8]. *Erişim doğrulama,* uygulamanın giriş filtrelerini ifade eden bir profildir. *Bilgilendirme,* kullanıcının giriş verilerini ifade eder. *Yetkilendirme,* kullanıcının izinlerini ifade eder. *Konfigürasyon yönetimi,* uygulamanın nasıl çalışacağı hangi veritabanını kullanacağı bir operasyonel kavramları ifade eder. *Hassas veri,* uygulama verilerinin hafızada ya da korumalı diskte nerede tutulduğunu ifade eder. *Oturum yönetimi,* oturumda bir kullanıcı ve Web uygulaması arasında ilgili etkileşimlerin

nasıl olduğunu ifade eder. *Şifreleme,* gizli verilerin nasıl tutulduğu, şifrelemenin nasıl olduğunu ifade eder. *Parametre manipülasyonu,* parametrelerin nasıl işleyeceğini ifade eder. *Hata yönetimi,* uygulamada bir işlem başarısız olduğunda neler yapıldığını, nasıl bir hata döndürüldüğünü ifade eder. *Denetim ve log,* yapılan işlemlerin loglarını tutar. Yazılım geliştirilirken yukarıda belirtilen adımlara dikkat edilmiş ise uygulama katmanında güvenliğin büyük ölçüde sağlandığı anlamına gelmektedir [8].

VIII. SONUÇ

Web yazılım güvenliği, web uygulamalarının yaygınlaşmasıyla önem kazanmış bir alandır. Teknolojideki hızlı gelişmeye bağlı olarak uygulama alanı gelişmiş ve artık birçok işlem web üzerinden yapılabilir hale gelmiştir. Bankaların, kurumların ve hatta devletin hizmetlerini web uygulamaları şeklinde sunmaya başlamış olmaları bu alandaki saldırıları arttırmıştır. Yazılım geliştirilme aşamasında güvenli yazılım geliştirme modelleri referans alınarak güvenli kodlar yazılması, uygulamaların temellerinin sağlam oluşturulması, oluşabilecek tehditlerin analizi yapılarak gerekli tedbirlerin alınması, bunlara ek olarak ağ ve host üzerinde de ilave tedbirlerin alınması verilerin güvenliği açısından önem arz etmektedir. Web yazılım güvenliği, güvenlik standartlarına uygun ve risklerin göz önüne alınarak uygun yaklaşımlarla geliştirilen kodların ve sonrasında uygulandığı sistemdeki güvenlik tedbirlerinin bütünlüğü ile sağlanabilmektedir.

Yapılan inceleme çalışmasında, güvenli yazılım geliştirme modelleri, güvenli bir yazılımda olması gereken unsurlar, tehdit analizi ve web yazılım güvenliğinin sağlanabilmesi için ilave tedbirlerin neler olduğu araştırılmıştır. Ayrıca kurumsal olarak güvenli kod geliştirilmesi standardizasyonun nasıl yapılabileceği nelere dikkat edilmesi gerektiği üzerinde durulmuştur. Elde edilen veriler değerlendirilerek daha güvenli kod geliştirme uygulamaları gerçekleştirileceği düşünülmektedir.

Kurumsal bilgi güvenliği, web uygulama güvenliği, açık ve tehdit tespit yöntemleri üzerinde inceleme yapılabilecek kapsamlı konular olduğu, son dönemde meydana gelen açıkların/açıklıkların/saldırıların bu zafiyetlerden faydalanılarak yapıldığı tespit edildiğinden ülkemizde; bu alanda yapılan çalışmalara daha çok dikkat edilmesi, açık veya açıklıkların ana gerekçelerinin yazılımlarda meydana gelen güvenlik açıkları olduğu, gerekli tedbirlerin alınarak web yazılımlarının hizmete alınması gerektiği, mutlaka standartlara uygun yazılım geliştirilmesi gerektiği, ve en önemlisi de testlerin de prosedürlere uygun olarak yapılması gerektiği bir kez daha ortaya koyulmuştur.

Ülkemizde bu alanda eğitim-öğretim veren bölümlerin kurulmuş olması sevindirici bir unsur olsa da bu alanda çalışma yapan üniversitelerin müfredatlarında güvenlikle ilgili olarak derslerin ya hiç olmadığı veya çok üzerinde durulmadığı belirlenmiştir. Bu konuda eğitim veren üniversitelerin müfredatlarını yenilemeleri, ve bu bildiri kapsamında sunulan hususları dersler içerisinde mutlaka yer vermeleri, test ve standartları bilip uygulamaları gerekmektedir. Bunlara ilaveten, diğer önemli husus ise yazılım güvenliği gibi bölümlerin ülkemizde açılması bu alandaki uzman eksikliğinin kısa sürede tamamlanmasını da sağlayacaktır.

KAYNAKLAR

[1] ALPARSLAN Erdem, "Güvenli Yazılım Geliştirme Modelleri", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/guvenli-yazilim-gelistirme-modelleri.html, 2009

[2] AKANYILDIR Çiğdem , "Güvenli Kodlama İlkeleri", http://www.webguvenligi.org/wp-content/uploads/2007/08/Secure%20Coding%20 PrinciplesTRK.pdf ,2010

[3] BEYDAĞLI Erkut, KARA Mehmet, BAHŞİ Hayretdin, ALPARSLAN Erdem," Güvenli Yazılım Geliştirme Modelleri ve Ortak Kriterler Standardı", http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/guvenli-yazilim-gelistirme-modelleri-ve-ortak-kriterler-standardi.html, 2010

[4] BURAK Efe, "Microsoft'un Güvenli Geliştirme Süreci (SDL)", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/microsoftun-guvenlik-gelistirme-sureci-sdl.html, 2009

[5] ÇİTİL Ferhat, "HTML Injection Tehlikesi", http://www.cyber-security.org.tr/Madde/220/HTML-Injection-Tehlikesi- ,2009

[6] GÜMÜŞ Emine, "Yazılım Güvenliğine Genel Bakış", http://www.cyber-security.org.tr/Madde/182/Yazılım-Güvenliğine-Genel-Bakış,2009

[7] MİCROSOFT, "Microsoft Security Development Lifecycle(SDL)", http://msdn.microsoft.com, 2011

[8] MEİER J.D., MACKMAN Alex, DUNNER Michael, VASİREDDY Srinath, ESCAMİLLA Ray and MURUKAN Anandha, "Improving Web Application Security: Threats and Countermeasures", http://msdn.microsoft.com/en-us/library/ff648636.aspx, 2003

[9] REDWİNE, S. T. ve DAVİS, N., "Processes to Produce Secure Software.", http://www.cyberpartnership.org/init-soft.html ,2004.

[10] POŞUL Abdulkadir," Yazılım Geliştirmede Tehdit Modelleme I", http://www.bilgiguvenligi.gov.tr/yazilim-guvenligi/yazilim-gelistirmede-tehdit-modelleme-i.html, 2011

[11] POŞUL Abdulkadir," Yazılım Geliştirmede Tehdit Modelleme 2", http://www.bilgiguvenligi.gov.tr/yazilim-guvenligi/yazilim-gelistirmede-tehdit-modelleme-ii.html, 2011

[12] Dr. TATLI Emin İslam, "SAMM ile Güvenli Yazılım Geliştirme", http://dergi.webguvenligi.org/websec/57-samm-ile-guvenli-yazilim-gelistirme.wgt,2010

[13] Wikipedia, "Code injection", http://en.wikipedia.org/wiki/Code_injection,2010

[14] Wikipedia, "SQL Injection", http://en.wikipedia.org/wiki/SQL_injection, 2011

[15] KALAYCI Orhan,"CMMI-Yöneticiler İçin Doğru Sorular", Shamrock Süreç İyileştirme ve Yenilikçilik,2007

Seda YILMAZ Gazi Üniversitesi Bilgisayar Bilimleri Bölümünde yüksek lisans eğitimine devam etmektedir. Araştırma konuları arasında kablosuz sensor ağlarda güvenlik, web yazılım güvenliği, siber güvenlik, bilgi ve bilgisayar güvenliği yer almaktadır.

Şeref SAĞIROĞLU Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesidir. Zeki sistem kimliklendirme, tanıma ve modelleme, ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizi ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları; yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar gibi konularda çalışmaktadır. 50'nin üzerinde SCI tarafından taranan uluslar arası dergilerde yayınlanmış makalesi, 50' nin üzerinde ulusal dergilerde yayınlanmış makalesi, 100'ün üzerinde uluslar arası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş100'e yakın bildirisi bulunmaktadır. 3 adet alınmış patenti vardır. 5 adet yayınlanmış kitabı, 2 adet kitapta bölüm yazarlığı bulunmaktadır. 4 kitabın da editörlüğünü yapmıştır.
Ulusal ve uluslar arası pek çok proje yürütmüş ve konferanslar düzenlemiş olup akademik çalışmalarına devam etmektedir.

Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri

Seda YILMAZ ve Şeref SAĞIROĞLU

***Özet*—Bu çalışmada, siber güvenlik konusunda uygulanması önerilen evrensel kurallar, siber kaynakların risk analizi, tehdit ve hazırlık seviyelerinin neler olduğu ve siber tehdit araçları üzerine bir inceleme ve analiz sunulmuştur.**

***Anahtar Terimler*— Siber güvenlik, risk analizi, tehditler, inceleme**

***Abstract*— In this study suggested international rules and applications about cyber security, risc analysis of cyber resources, what are the levels of threats and readiness and tools for cyber threats are reviewed, anaylised and presented.**

***Index Terms*— Cyber security, risk analysis, threats, review**

I. GİRİŞ

Cambridge üniversitesinde 1837 yılında Profesör Charles Babbage tarafından "Akıllı Motor" adıyla ilk bilgisayar tasarlanırken bu denli büyük bir devrim yaratacağı belki de bugünkü savaşların eşiğine gelineceği düşünülmemişti. Zaman içinde hızla gelişen bu teknoloji, artık bilginin sadece saklandığı değil işlendiği, kullanıldığı ve geliştirildiği en önemli ortam haline gelmiştir.

Kişisel kullanıcıların yanı sıra kurumsal kullanıcılar tarafından da etkin şekilde kullanılan bu dijital bilgi dünyasının internet ortamına taşınması, erişilebilirliği kolaylaştırmakla birlikte bilgiyi daha çekici ve hedeflenebilir bir hale getirmiştir. Bugün dünyada yaklaşık 2.28 milyar internet kullanıcısı, 19,2 milyar internet sayfası, 1,6 milyar resim ve 50 milyon ses-görüntü dosyasının olduğu tahmin edilmektedir [1]. Hem kişiler hem de kurumlar tarafından çok etkin kullanılan bu siber dünya giderek daha tehlikeli bir yer olmaya başlamıştır. Siber güvenlik, siber saldırı, siber savaş sözcükleri hem bireylerin hem devletlerin kelime dağarcıklarına yerleşmiş, gün geçtikçe daha vahim anlamlar içermeye ve çağrışımlar yapmaya başlamıştır.

Siber güvenlik, "siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür" [1] şeklinde tarif edilebilir.

Siber saldırı, "hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır" [1].

Siber savaş, "Aynı saldırıların ülke veya ülkelere yönelik yapılmasıdır" [1]. Siber savaşta hedef ülkelerin güvenlik, sağlık, enerji, haberleşme, su ve kanalizasyon, bankacılık ve kamu hizmetleri gibi kritik altyapıları saldırı alanı olarak seçilmektedir [2].

Ülkeler siber güvenliklerini sağlamak için stratejiler ve politikalar belirlemektedirler. İngiltere Başbakanı Gordon Brown ülke güvenliği konusundaki anlayışın değiştiğini "19.yy da ulusal güvenliğimizi korumak için deniz ve hava güvenliğimizi sağlamak zorundayken 21.yy'da kamu kurum ve kuruluşlarımız ile işletmelerimizin sanal dünyadaki güvenliğini sağlamak zorundayız." sözleriyle ifade etmiştir [6].

Bu çalışmada ikinci bölümde siber güvenlik unsurları ve evrensel kurallar, üçüncü bölümde siber kaynak risk analizi, dördüncü bölümde siber tehdit ve hazırlık seviyeleri ile beşinci bölümde siber tehdit araçları konularından bahsedilmiştir.

II. SİBER GÜVENLİKTE EVRENSEL UNSURLAR VE KURALLAR

Bir ülkenin kurumlarına ya da ulusal güvenliğine yönelebilecek siber tehditlerin, dünya üzerindeki erişim kolaylıkları ve bağlantıları dikkate alındığında herhangi bir kaynaktan gelebileceği açıktır. Bu durum uluslar arası işbirliğini ve evrensel kuralların uygulanmasını zorunlu hale getirmektedir.

A. Siber Güvenlik Unsurları

Siber güvenliği sağlamak için alınacak her türlü tedbirde ve geliştirilecek uygulamalarda göz önünde bulundurulması gereken hususlar vardır. Bunlar hususlar [11]:

- Temel hak ve hürriyetlerinin korunması
- Demokratik toplum düzeninin gereklerine uyulması
- Ölçülülük İlkesine uyulması
- Karar alma süreçlerine tüm paydaşların katılımının sağlanması
- Bütüncül bir yaklaşımla hukuki, teknik, idari, ekonomik, politik ve sosyal boyutların ele alınması
- Güvenlik ile kullanılabilirlik arasında denge kurulması
- Diğer ülke mevzuatlarının göz önünde bulundurul-ması ve mümkün olabildiğince uyumluluğun sağlanması
- Uluslar arası işbirliğinin sağlanması

Bu hususların her yerde genel geçer önceliklere sahip olduğu bir gerçektir. Bunun yanı sıra siber güvenlik yaklaşımlarının belirlenmesinde dikkate alınması önerilen unsurlar aşağıda belirtilmiştir [11].

1) Ulusal Politika ve Stratejinin Geliştirilmesi: Siber saldırılar karşısında alınabilecek önlemlerin başarısı olması için ulusal politika ve stratejilerin geliştirilmesi gereklidir.

2) Yasal Çerçevenin Oluşturulması: Siber saldırılara karşı yüksek caydırıcılığı olan hukuki düzenlemelerin yapılması gereklidir.

3) Teknik Tedbirlerin Geliştirilmesi: Yazılım, donanım ve iş süreçlerinin güvenliğini arttırmak için güvenlik standartları dikkate alınarak teknik açıdan tedbirler geliştirilmelidir.

4) Kurumsal Yapılanmanın Belirlenmesi: Bireylerin, sivil toplum kuruluşları, özel sektör ile kamu kurum ve kuruluşlarının görev ve sorumluluklarının yasal çerçevesi belirlenmelidir.

5) Ulusal İşbirliği ve Koordinasyonun Sağlanması: Bütün sistem, şebeke ve altyapıların birbiriyle bağlantılı olduğu, her birinin güvenliğinin sağlanmadan tam bir güvenlikten bahsedilemeyeceği unutulmamalıdır. Bu nedenle belirlenen ulusal strateji ve politika çerçevesinde bütün unsurların tam bir koordinasyon ile çalışmasının sağlanması önemlidir.

6) Kapasitenin Geliştirilmesi: Teknolojinin sürekli gelişmesi siber tehdit araçlarının da değişmesine neden olmaktadır. Bu nedenle uygulama geliştirici teknik personel, yönetim birimleri, hukukçular ve kanun koyucuların teknolojiyi yakından takip ederek bu konudaki bilgi birikimlerini geliştirmeleri gerekmektedir.

7) Farkındalığın Artırılması: En zayıf halka olan kişisel kullanıcıların siber tehdit araçları ve korunma yolları konusunda bilgilendirilmesi gereklidir.

8) Uluslar Arası İşbirliği ve Uyumun Sağlanması: İnternet üzerinden bütün dünya ülkelerine rahatlıkla ulaşılabiliyor olması suç merkezlerinin farklı yerlerde olmasına imkan sağlamaktadır. Siber tehdidin bütün dünya için bir tehlike olduğu göz önünde bulundurularak hukuki mevzuatta uyum sağlanmalı ve bilgi paylaşımına önem verilmedir.

B. Evrensel Kurallar

2007 yılında Estonya'ya gerçekleştirilen siber saldırı, dünyanın siber tehdit efsanelerini dikkate almasını sağladı. 2010 yılında Çin'de Google ve diğer sitelere yapılan Aurora kod adlı saldırılar, 2008'de Microsoft ürünlerini hedefleyen Conficker adındaki solucan, İran nükleer programını hedefleyen Stuxnet solucanı ve daha birçok yeni saldırı yöntemi aslında soruna birkaç bilgisayar korsanının eğlence anlayışı olarak yaklaşmanın doğru olmadığını göstermiştir. 2007'de Estonya Siber Saldırılarından sonra ülkeler kendi varlıklarını ve vatandaşlarının bilgi güvenliğini korumak için daha etkin teknik ve hukuksal önlemler almaları gerektiğini görmüşlerdir. NATO, Birleşmiş Milletler, Avrupa Birliği, AGIT ve diğer birçok uluslar arası örgütün güvenlik politikaları bu sayede revize edilmeye başlanmıştır. Bu değişim sürecinde aşağıda belirtilen evrensel kurallar oluşmuştur [3]:

1) Bölgesellik Kuralı: Bir devletin toprakları içinde yer alan bilgi teknolojileri altyapısı devletin ulusal egemenlik unsurudur. Uluslar arası hukuk anlayışına göre; her devlet kendi ülkesinin bilgi teknoloji altyapısına karşı gerçekleştirilecek her türlü tehdit ve saldırıya karşı önlem almak ve bunlarla başa çıkabilmek için BT altyapısına yönelik her türlü iyileştirme yetkisine sahiptir [3].

2) Sorumluluk Kuralı: Bir devletin topraklarında bulunan bilgi sistem kaynağına düzenlenen siber saldırıların başka bir ülke kaynaklı olduğu varsayımı oluştuğunda sorumlu tutulan ülkenin konu ile ilgili soruşturma yapması, suçluların yakalanmasına yardımcı olması ve yargılanma sürecini desteklemesi beklenir [3].

3) İşbirliği Kuralı: Siber saldırı, bir devletin topraklarında bulunan bilgi sistemleri aracılığıyla başka bir ülkeyi hedef alarak gerçekleştirilmiş ise saldırı kaynakları kendi topraklarında olan devletin kurban devlet ile işbirliği yapma görevi vardır. Uluslar arası Siber Suçlar Sözleşmesine göre, tarafların cezai konularda uluslar arası araçlar ile hukuk kurallarının uygulanmasını ve elektronik kanıtların toplanmasını talep etme hakları vardır. Bunun yanı sıra Kuzey Atlantik Antlaşması uyarınca herhangi bir ülkenin toprak bütünlüğünü, siyasi bağımsızlığını ve güvenliği tehdit eden bir durum oluşması halinde diğer taraf ve müttefik ülkelerin işbirliği yapması zorunludur [3].

4) Öz-Savunma Kuralı: Uluslar arası ceza kanunlarına göre kişiler, yasaların kişisel özgürlüklerine karşı yasadışı olarak kullanıldığını düşündüğünde kendini korumak amacıyla gerçekleştirebilecekleri haksız eylemlerden sorumlu tutulamaz. Uluslar arası düzeyde eğer bir ülke bireysel ya da toplu olarak gerçekleştirilen bir saldırının güvenliğini tehdit ettiğini düşünürse silahlı güç de dahil olmak üzere belirlediği bir yöntemle saldırılara cevap verme hakkına sahiptir. Hatta NATO anlaşmasının 5.Maddesi uyarınca, NATO üyesi bir ülkeye gerçekleştirilen saldırıya karşı bütün üye ülkelerin cevap verme hakkı bulunmaktadır [3].

5) Veri Koruma Kuralı: Bir bireyin ağ üzerinde bulunan herhangi bir verisinin, verilerin gizliliği kapsamına girip girmediği hukuk uzmanları arasında halen bir inceleme ve tartışma konusudur. AB'nin Veri Koruma Yönergesi'ne göre tanımlanmış ya da tanımlanmamış gerçek kişilerin bilgileri kişisel veri olarak kabul edilir. Bu bakımdan bir kişinin ağ üzerindeki IP adresi yasa dışı yollardan elde edilirse hukuki olarak delil kabul edilemez. Yine aynı yönergeye göre bir kişi üçüncü bir ülkeye kişisel verilerini transfer ettiğinde ilgili ülkenin bu verileri koruma zorunluluğu vardır. Bu durumun suistimal edilmesi ihtimaline karşılık yasal mevzuatla ilgili olarak uluslar arası bir düzenlemeye ihtiyaç duyulmaktadır [3].

6) Bakım Kuralı: AB'nin Veri Koruma Yönergesi'ne göre, kişiler ağ üzerinden ya da yasal olmayan yollarla erişime karşı verilerin yanlışlıkla veya kasıtlı olarak yok edilmesini, değiştirilmesini, yetkisiz kişilere açıklanmasını önlemek amacıyla her türlü teknik ve organizasyonel önlemi almakla sorumludur. Aynı şekilde Avrupa Konseyi Sözleşmesi'nde (1981) kişilerin verilerini her türlü veri kaybı, yetkisiz kişilerin erişimi ve verilerin üçüncü kişilere açıklanması ile değiştirilmesini önlemek amacıyla gerekli önlemleri alması zorunluluğu hükmü 7.Maddede açıkça belirtilmiştir. Bu kapsamda siber saldırıların siyasi boyutları arttıkça toplumsal, askeri ve bilgi hizmetleri açısından verilerin bakım ve

korunmasına dair standartların geliştirilmesi gerekecektir [3].

7) Erken Uyarı Kuralı: Servis sağlayıcılar, e-Gizlilik Yönergesi EC/2002/58'e göre hizmetlerinin güvenliğini korumak için her türlü teknik ve organizasyonel önlemleri almakla yükümlüdür. Gerektiğinde kamu iletişim ağı sağlayıcısı ile benzer eylemleri koordine etmek yükümlülü-güne sahiptir. Ayrıca e-Ticaret Yönergesine göre servis sağlayıcılar yasadışı faaliyetleri üye devletlerin yetkililerine derhal bildirmek zorundadırlar [3].

8) Bilgileri Kuralı: Halkın yaşam, güvenlik ve refahına yönelik tehditler hakkında bilgi sahibi olma hakkı vardır. Avrupa'da toplumların kamusal yaşam ve refahlarına yönelik tehditleri ve bu tehditler karşısında alınan kararları öğrenmek konusunda devletlerin şeffaf olması gerektiğine dair bir yargı gün geçtikçe daha güçlü olarak varlığını hissettirmektedir. Tehditlerin ve bu durumlar karşısında alınan kararların erişime açık olması kamuoyunun bilgilen-dirilmesi ve siber güvenlik açısından bilinçlendirilmesini sağlarken istenmeyen bilgi ifşasına da neden olabilir. Buna rağmen yapılan saldırılar ve alınan tedbirlerin açıklaması yasal çerçevede stratejik iletişim ve kamu bilincinin arttırıl-ması bağlamında gereklidir [3].

9) Suçluluk Kuralı: Her ulusun kendi ceza hukukuna en yaygın siber suçları dâhil etme sorumluluğu vardır. Uluslar arası ceza kanuna göre bir durumun sonucu ulusal ya da uluslar arası yasalara göre bir suç sayılmadığı sürece siber saldırı yapan kişiye yönelik bir yaptırım uygulanması mümkün değildir. Bu durumlardaki anlaşmazlıkların giderilmesi ve bir uyum oluşturulması için esas alınabilecek olan Avrupa Birliği Siber Suçlar Sözleşmesi'ne göre bir bilgi-sayar sisteminin tamamına ya da herhangi bir parçasına haksız erişimler yasal yükümlülükler çerçevesinde değerlendirilmelidir [3].

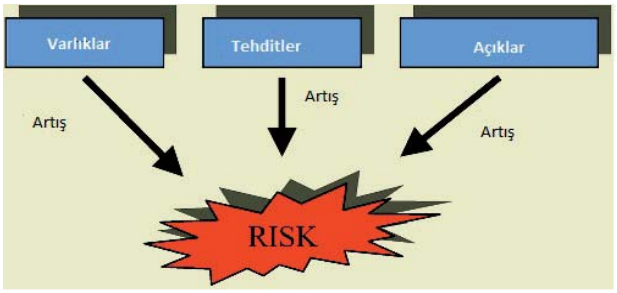
10) Manda Kuralı: Manda yönetimi siber güvenlik konusunda uluslar arası çabaların desteklenmesi ve koordinesini kapsamaktadır. Siber güvenlikle ilgili olarak yasal ve politik araçlar açısından uluslar arası koordinasyonu ve boşlukları ortaya koymayı hedeflemektedir. Bugün bu uyum sağlama çabası hali hazırda hala en az 6 uluslar arası örgütün çalışma planında yer almaktadır. NATO, üye ülkelere gerçekleştirilen siber saldırılara karşı hangi durumlarda silahlı saldırı gerçekleştirilebileceği konusunda net bir karara varamamıştır. Bu bağlamda ülkelerin ortaklaşa ve koordineli olarak çalışmaları ve strateji geliştirmeleri gerekliliği ortadadır [3].

III. RİSK ANALİZİ

Bir varlığın korunabilmesi için öncelikle değerinin bilinmesi ve hangi risklere maruz olduğunun tespiti gereklidir. Yapılan incelemelerde siber saldırıların her geçen yıl artış gösterdiği tespit edilmiştir. Bu nedenle güvenlik risklerinin analiz edilerek gerekli risk modellerinin oluşturulması hayati bir önem taşır noktaya gelmeye başlamıştır [5].

Risk analizinin başlıca faydaları aşağıda sıralanmıştır [5]:

- Güvenli bilgi yönetimini geliştirmek
- Organizasyonun kritik varlıkları izlenmesi ve etkili bir şekilde korunmasını sağlamak
- Karar vermede etkin bilgi güvenliği politikalarının desteklenmesini sağlamak
- Organizasyonlara yönelik pratik güvenlik politikalarının belirlenmesini sağlamak
- Gelecekteki tahminler için değerli analiz verilerinin teminini sağlamak



Şekil 1. Güvenlik Riski ve İlgili Öğeler [5].

Şekil 1'de görüldüğü gibi risk faktörü varlıklar, tehditler ve varolan açıklardan etkilenmektedir. Varlıklar, tehditler ya da açıklar arttıkça karşı karşıya olunan risk de artacaktır.

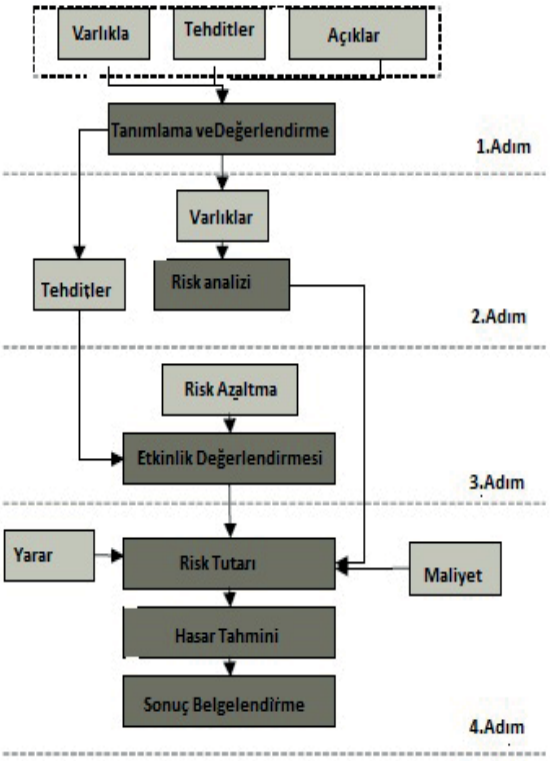
Varlıklar genel olarak bilgi/veri, evraklar, donanım, yazılım, insan kaynakları ve şartlardan oluşur. Tehditler insani/insani olmayan faktörler, ağ/fiziksel, teknik/çevresel, içerden/ dışarıdan ve kasıtlı/kazara kaynaklı tehditler olarak sınıflandırılabilir. Açıklar ise idari belgeler, personel, yönetmelikler, fiziksel koşullar ve imkânlar, teknik donanım, yazılım, iletişim/ağ kaynaklı açıklar şeklinde sınıflandırılabilir [6].

Matematiksel olarak risk, varlıkların herhangi bir açığa maruz kalması sonucunda değerlerinde oluşan azalma ile ilgili güvenlik açığına karşı tehdit oluşma olasılığının çarpımıyla hesaplanır [5].

Risk = Kayıp * Olasılık

Şekil 2'de gösterildiği gibi risk analiz işlemi genel olarak dört adımdan oluşmaktadır. Birinci adımda varlıklar, tehditler ve açıklar üzerinde bir tanımlama ve değerlendirme işlemi yapılmalıdır. İkinci adımda varlıklar, tehditler ve mevcut açıklar göz önüne alınarak sistemin toplam bir risk değerlendirmesi yapılmalıdır [6].

Üçüncü adımda mevcut tehditlerin riskinin azaltılması için gerekli yöntemin belirlenmesi ve etkinlik



Şekil 2. Güvenlik Riski Analiz Modeli [5].

değerlendirmesi yapılır. Organizasyon tarafından riskler belirlenip bu riskleri mümkün olduğunca minimize edecek yöntem seçilmelidir.

Bazı risk azaltma yöntemlerinde hangi uygulamaların kullanılabileceği aşağıda özetlenmeye çalışılmıştır [5]:

1) Erişim Kontrolü: Şifre tanımlamaya dayalı sistemler, fiziksel erişim ekipmanları (akıllı kart), kimlik doğrulama sistemi kullanılabilir.

2) Şifre Kontrolü: Açık anahtar altyapısı (AAA), vb şifreleme algoritmaları kullanılabilir.

3) İnternet Güvenlik Kontrolü: Saldırı tespit sistemi (Ids), güvenlik duvarı, vb önlemler alınabilir.

4) Uygulama Güvenlik Denetimi: Veri tabanı güvenliği, sistem dosyası güvenliği gibi uygulamaları kapsar.

5) Fiziksel/Çevresel Güvenlik Kontrolü: Tesisleri güvenliği, kurum güvenliği, giriş/çıkış kontrolü gibi uygulamaları kapsar.

Dördüncü adımda ikinci ve üçüncü adımda hesaplanan risk tutarına fayda ve maliyetler de eklenerek son risk tutarı elde edilir. Bu risk tutarı üzerinden hasar tespiti yapılarak ileriki çalışmalara zemin hazırlaması ve durumun daha net görülmesinin sağlaması için sonuç belgesi hazırlanır [5].

Toplam Maliyet = Maliyet + Operasyon Maliyeti + İş Fırsat Maliyeti

Maliyet, bir varlığı satın alma veya yükleme maliyetidir. Operasyonlu maliyet, hasarlı varlığı kurtarmak için yapılan maliyettir. İş fırsatı maliyeti ise parasal kazanç kazanmak için iş kaybıdır. Bu hesaplama dikkate alınarak organizasyon risk yönetim politikasına karar verilebilir [5].

A. Güvenlik Açığı Risk Analizi

Risk faktörlerinden birinci öncelikli olan güvenlik açıklarına daha yakından bakıldığında bir yaşam döngüsüne sahip olduğu fark edilebilir. Her sistemde bir açık vardır ve bu açığın saldırıya maruz kalması olasıdır. Eğer şanslı iseniz açıklar beyaz korsanlar tarafından keşfedilir ve kapatılması için bir fırsatınız olur. Açıkların ilk fark edildiği zamana keşif tarihi, açıkla ilgili ayrıntılı bilgi verildiği tarihe bilgilendirme tarihi, kamuoyuna açıklandığı tarihe tanıtım tarihi, açık için oluşturulan yararlanma kodunun web siteleri aracılığıyla yayınlandığı tarihe yararlanma tarihi, açığın kapatılması için ilgili yamanın yayınlandığı tarihi de yama tarihi denir. Yayınlanan her yama yeni bir açık keşfinin yani yeni bir



Şekil 3. Güvenlik Açığı Yaşam Döngüsü Olayları [8].

döngünün başlangıcı olabilir [8].

Şekil 3'de gösterilen döngü, güvenlik açığının yaşam döngüsüdür. Açıklara yönelik saldırılar bu tarihlere göre isimlendirilir [8].

- **Sıfır Gün Saldırısı**: Genellikle kötü niyetli korsanlar tarafından keşfedilen açığın, yama tarihinden önce kullanıldığı saldırılardır.
- **Sözde Sıfır Gün Saldırısı**: Piyasaya sürülen yamanın sisteme eklenmesi kaynaklı saldırılardır.
- **Olası Sözde Sıfır Gün Saldırısı**: Bu saldırı tipinde düzeltme yayınlanmış ama saldırıya uğrama olasılığı hala gündemdedir.
- **Saldırı Olasılığı**: Sistem açığının bulunmuş, ilgili yamanın hazırlanmış fakat dağıtımının yeterli yapılamadığı durumda gerçekleşme ihtimali olan saldırı tipidir.

- **Pasif**: Bu tip saldırılar henüz gerçekleşmemiş ya da kodları bile hazırlanmamış saldırılardır.

İşletim Sistemi / Saldırı Tipi	Linux		Windows	
	Açık	Oran	Açık	Oran
Sıfır Gün Saldırısı	0	0	21	8.79
Sözde Sıfır Gün Saldırısı	5	2.49	20	8.37
Olası Sözde Sıfır Gün Saldırısı	133	66.17	78	23.64
Olası Saldırı	1	0.5	5	2.09
Pasif Saldırı	62	30.84	115	48.12
Toplam	**201**	**100%**	**239**	**100%**

Şekil 4. Saldırıların İşletim Sistemlerine Göre Oranları [8].

Şekil 4'de bir fikir oluşturulması amacıyla her bir saldırı tipinin işletim sistemlerinde görülen açık sayısı ve görülme oranları ifade edilmiştir [8].

Bir açığın hedef olmasını etkileyen faktörler 3 alanda kategorize edilebilir. Bu alanlar aşağıda açıklanmıştır [8]:

1) Her uygulama güvenlik açığı yaşam döngüsü boyunca mutlaka saldırıya hedef olma olasılığına sahiptir. Bir uygulamanın ya da sistemin saldırıya maruz kalması, güvenlik açığı yaşam döngüsünün hangi aşamada sekteye uğradığına veya ne kadarının gerçekleştirildiğine bağlıdır. Döngünün tamamlanma olasılığı arttıkça açık cazip bir hedef olmaktan uzaklaşır [8].

2) Açığın popülerliği ve piyasa payının büyük olması saldırı hedefi olmasını arttıran faktörlerdendir. Pazar payı ve popülerlik oranı %60'dan büyükse yüksek risk grubunda, %30'dan küçükse düşük risk grubunda değerlendirilebilir [8].

3) Açığın yaşı, yamayı aldığı son tarih ve açığın tanıtım tarihleri de etkili faktörler arasındadır. Bir açık keşif tarihinden itibaren bir yıl içinde genç, 1-3 yıl içinde orta yaşlı, 3 yıldan sonra ise yaşlı olarak değerlendirilir. Açık, keşfinin üzerinden zaman geçtikçe değerini kaybeder. Yaralanma ile yama tarihi arasındaki fark 20 günü geçtiyse ya da yama henüz yayınlanmadıysa risk yüksek, 1 günden azsa veya yararlanma kodu yayınlanmadıysa risk düşüktür. Aynı şekilde tanıtım tarihi ile yama tarihi arasındaki fark 80 günden büyükse risk yüksek, küçükse risk düşüktür [8].

B. Güvenlik Risk Değerlendirme Yöntemleri

Güvenlik risk değerlendirmesi yapılırken bazı yöntemlerden faydalanılır. Bunlardan başlıcaları; Bilgi Güvenliği Değerlendirme Metodolojisi (IAM), Güvenlik Açığı Değerlendirme Çerçevesi (VAF) ve Operasyonlu Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi (OCTAVE) dir [5].

1) Bilgi Güvenliği Değerlendirme Metodolojisi (IAM), NSA ve ABD Savunma Bakanlığı tarafından kullanılan, yapısal güvenlik açıklarını analiz ederek güvenlik risklerini değerlendiren bir yöntemdir [5].

2) Güvenlik Açığı Değerlendirme Çerçevesi (VAF), 1998'de ABD Kritik Altyapı Güvencesi Ofisi Komisyonu ile KPMG Marwick LLP tarafından geliştirilen, ilgili kuruluşun asgari temel altyapısı ile seçilen varlıklarının açıklarını analiz ederek değerlendirme sonucunda güvenlik notunu hesaplayan bir yöntemdir [5].

3) Operasyonel Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi (OCTAVE), ABD'de Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü tarafından geliştirilen, varlığa dayalı tehdit senaryolarının oluşturulması, önemli tesisler hakkında açıklarını tanımlanması ve risk değerlendirilmesi ile güvenlik stratejilerinin geliştirilmesi olmak üzere üç aşamadan oluşan bir güvenlik değerlendirme yöntemidir [5].

IV. SİBER TEHDİT VE HAZIRLIK SEVİYELERİ

Siber savunma hazırlık süreci birbirini takip eden dört aşama şeklinde özetlenebilir. Birinci aşamada siber tehditlere karşı kurumun misyonu kategorize edilmeli, ikinci aşamada misyonun başarısının sağlanması için hazırlık düzeyi belirlenmeli, üçüncü aşamada hazırlık hedefleri belirlenerek siber güvenlik için strateji planı geliştirilmeli ve dördüncü aşamada gerekli güvenlik yatırımları planlanmalı ve kararlar alınmalıdır [13]. Bu başlık altında siber savunmanın birinci ve ikinci aşamasını oluşturan tehdit ile hazırlık seviyelerindeki adımlardan bahsedilmiştir.

A. Tehdit Seviyeleri

Siber savunmanın temel adımı tehdit seviyelerinin belirlenmesidir. Tehdit seviyelerinin belirlenmesi süreci beş aşamalı bir süreçtir. Ek A'da verilen Tablo 1'de tehdit seviyeleri, bu seviyelerdeki saldırgan tipleri, hedefler, strateji ve yöntemleri listelenmiştir [13].

B. Hazırlık Seviyeleri

Siber savunmanın ikinci adımı hazırlık seviyelerinin belirlenmesidir. Hazırlık seviyelerinin belirlenmesi süreci beş aşamalı bir süreçtir. Ek B'de verilen Tablo 2'de hazırlık seviyeleri, amaçları, alınacak tedbirler ve çözüm önerileri listelenmiştir [13].

V. SİBER TEHDİT ARAÇLARI

Siber tehditlerin etkilerini kısa ve uzun vadeli olarak ayırmak mümkündür. Kısa vadeli tehditler, hedef aldığı organizasyonun, hükümet, işletme ve son kullanıcıların günlük faaliyetlerini etkileyen tehditlerdir. Dolandırıcılık faaliyetleri, müşteri veri ihlalleri, ATM den usulsüz nakit çekimi gibi günlük faaliyetler örnek verilebilir. Uzun vadeli tehditler ise daha çok etkileri uzun süre devam eden, ülkenin ve toplumun dengelerini değiştirmeyi hedefleyen, endüstriyel ve askeri casusluk, sosyal hoşnutsuzluk ve huzursuzluk yaratma, ulusal güvenlik ihlali gibi tehditlerdir [4].

A. Kötü Amaçlı Yazılımlar

Truva atı, virüs, klavye dinleme, casus yazılımlar, önemsiz e-posta gibi kötücül yazılımlar, açıkları kullanarak verileri elde etme, değiştirme ya da yok etme gibi amaçlarla kullanılırlar. Kötü amaçlı yazılımlar gerek kullanım kolaylıkları gerekse hızlı sonuç verebilmeleri açısından sıkça tercih edilen, hükümet, işletme ve son kullanıcılar için en tehlikeli siber saldırı araçlarından sayılmaktadırlar. Kötü amaçlı uygulamalar yazılımsal olduğu kadar donanımsal da olabilirler. Donanımsal olarak

işlem yapan klavye dinleme cihazları buna bir örnektir. Kimi zaman cihazın içine yerleştirilen küçük bir aygıt ile klavyeden girilen her türlü bilgi (şifreleriniz, dosya isimleriniz, dosya içerikleriniz v.b.) kaydedilebilir [4].

Saldırılar mutlaka ağ üzerinden yapılmak zorunda değildir. Kötü amaçlı yazılımları ağ bağlantısı olmayan cihazlara yüklenerek veri hırsızlığı yapılabilir. ATM ve POS cihazlarına yüklenen casus yazılımlar sayesinde kullanıcının verileri yasadışı olarak ele geçirilebilir ya da maddi kayıplara neden olunabilir [4].

B. Güvensiz Ortamlar

Ağ güvenliği, omurgayı oluşturan ağ elemanların güvenliğine bağlıdır. Ürünün güvenlik açıklarından faydalanı-larak sistemlere saldırı gerçekleştirmek ve bilgilere erişmek mümkündür. Bunun örneği Stuxnet adlı virüs tarafından gerçekleştirilmiştir. Belli bir ürün markasının PLC rootkit indeksindeki açıklardan faydalanılarak geliştirilen bu virüs endüstriyel sistemi tamamen durma noktasına getirmiştir [4].

C. Kimlik Hırsızlığı

Bu tür saldırılarda saldırgan erişim izni olan bir kullanıcının kimliğine bürünerek sisteme sızmayı başarır. Ağ saldırıları, mesaj tekrarları, yazılım ve sömürü saldırıları kimlik saldırılarına örnek olarak verilebilir [7].

D. DOS Saldırıları

DOS(*Denial of Service – Sistem Engelleme*) ve DDOS(*Distributed Denial of Service* - Dağıtık Hizmet Engelleme) saldırıları direk olarak sistemi hedef alan saldırılardır. Bu saldırılar sistemleri durdurarak ya da aksatmaya uğratarak ciddi zararlara yol açarlar [7]. DDOS saldırıları bilginin erişilebilirlik kuralını hedef alan, işletim sistemi, sunucu ya da uygulamanın cevaplayabileceğinden fazla sayıda istek göndererek sistemi durma noktasına getirirmeyi hedefleyen saldırılardır [12].

E. Şifre Ele Geçirme Saldırıları

Gizlilik ihlali kapsamında değerlendirilen bu saldırılarda kullanılan başlıca yöntemler sosyal mühendislik atakları, sözlük saldırıları ve parola tahmin uygulamalarıdır. Daha çok sosyal mühendislik atakları ve sosyal beceriler ile kişilerin bilgileri elde edilerek sisteme nüfus etmeye çalışılır [7].

F. Yan Kanal Saldırıları

Yan kanal saldırıları sistemlerin güç analizine, elektromanyetik uygulamalarına ve zamanlanmış görevlerine yönelik saldırılardır. Bu saldırılarda asıl amaç şifreleme anahtarını ele geçirecek bir casus uygulamayı sisteme sızdırmaktır. Birçok Akıllı Sistem maalesef bu saldırıların sonucunda müşteri bilgilerini, kullanım bilgilerini ve şifrelerini kaybetmiştir [7].

G. HTML Enjeksiyonu

Bu açık, programcıların kodlama sırasında yaptığı hatalı kodlamadan faydalanır. Web yazılımlarımda veri tabanına giren verilerin ya da veri tabanından çekilen verilerin bir kontrol mekanizmasından geçirilmemesi açığa neden olmaktadır. XSS olarak da bilinen açıktan faydalanılarak session ve cookie çalması yapılır [10].

Uygulamalarda sayfaya gönderilen bir isteğe bir cevap döndürülmesi mantığı kullanılır. Sayfaya gönderilen istek sunucuda değerlendirilip bir cevap döndürülür. Ama eğer giriş yaptığınız sayfa kötü amaçlı bir url adresine yönlendirildiyse ya da Truva atı gibi araçlar yerleştirtildiyse aldığınız yanıt beklenenden farklı olacaktır. Bu saldırı tipinde amaç web uygulamasına zarar vermek değil daha çok uygulamayı ziyaret eden kullanıcılara erişmektir [9].

H. SQL Enjeksiyonu

SQL enjeksiyonu veri tabanından yapılan sorgulama işlemini hedef alan bir saldırı şeklidir. Bu saldırı şeklinde sorgulama dili yapısı kullanılarak saldırı gerçekleştirilir [14,15].

Bir web uygulamasının kullanıcı adı ve şifre ikilisi veri tabanına

*"SELECT * FROM TABLE_PERSONEL WHERE username = '" +Kullanıcı + "' AND password= '" +Şifre + "'"*

şeklinde gönderildiğinde ("") işaretleri içindeki veri bir filtrelemeye tabi tutulmazsa kullanıcının buraya yazacağı (OR "1=) şeklinde bir ifade sorguyu

*"SELECT * FROM TABLE_PERSONEL WHERE username = '' OR "1=1" AND Password = '' OR "1=1'"*

haline getirir. Bu durumda sorgudan var olan bütün kayıtlar dönecektir [14,15].

I. Komut Enjeksiyonu

Genellikle komut(shell) enjeksiyon saldırıları SQL enjeksiyon ve XSS saldırılarının aksine doğrudan sunucuları hedefleyen bir saldırı tipidir. Web uygulamasının komut satırını kullanarak uzaktan erişimle işletim sistemi, veri tabanı yönetim sistemi ve sunucudaki bilgilere erişimi hedefler [9].

VI. SONUÇ

Bilgi varlıklarımızın siber dünyadaki bütünlüklerinin ve doğruluklarının korunabilmesi için siber güvenliğin unsurlarının özümsenmesi büyük önem taşımaktadır. Yapılan bu inceleme çalışmasının da gösterdiği gibi siber güvenliğin sağlanabilmesi için bilgi varlıkları üzerinde bir risk analizi yapılmalı, yapılan analizler ve siber süreçlerin gelişimi dikkate alınarak mevcut ve olası tehditlerin tespiti yapılmalı, tehditler karşısında uygulanması gereken hazırlık seviyeleri ve çözümleri belirlenerek popüler siber tehdit araçları konusunda önlem alınmalıdır.

EKLER

Ek A. Siber Tehdit Seviyeleri
Ek B. Siber Hazırlık Seviyeleri

KAYNAKLAR

[1] ALKAN Mustafa," Siber Güvenlik ve Siber Savaşlar" , Siber Güvenlik Siber Savaşlar TBMM İnternet Komisyonu, Mayıs 2012
[2] EMRE Bâkır, "Siber Savaşlar – Başlangıç", http://www.siberguvenlik.org.tr/ makaleler/siber-savaslar-i/, Aralık 2012
[3] TIKK Eneken, "Ten Rules for Cyber Security", Survival: Global Politics and Strategy, Mayıs 2011,(119-132)

[4] CHOO Kim-Kwang Raymond , "The cyber threat landscape: Challenges and future research directions", Computers and Security, Kasım 2011, (719-731)
[5] IN Hoh Peter, KİM Young-Gab, LEE Taek, MOON Chang-Joo, JUNG Yoonjung, KİM Injung, "A Security Risk Analysis Model for Information Systems", http://www.luisolis.com/seminario2011/papers/A Security Risk Analysis Model for Information Systems.pdf, 2011
[6] WİLLS David Barnard, ASHENDEN Debi, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk" ,Space and Culture, Mayıs 2012, (110-123)
[7] YANG Y., LİTTLER Tim, SEZER S., MCLAUGHLİN K. , WANG H. F.,"Impact of Cyber-Security Issues on Smart Grid", Innovative Smart Grid Technologies (ISGT Europe),Aralık 2011,(1 – 7)
[8] JUMRATJAROENVANIT A. , TENG-AMNUAY Y., " Probability of Attack Based on System Vulnerability Life Cycle", Electronic Commerce and Security, 2008 International Symposium on, Ağustos 2008, (531 – 535)
[9] DWEN-REN Tsai; CHANG A.Y., PEİCHİ Liu, HSUAN-CHANG Chen, "Optimum Tuning of Defense Settings for Common Attacks on the Web Applications", Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on ,Ocak 2009, (89 – 94)
[10] ÇİTİL Ferhat, "HTML Injection Tehlikesi", http://www.cyber-security.org.tr/Madde/220/HTML-Injection-Tehlikesi- ,2009
[11] ÜNVER Mustafa, CANBAY Cafer , "Ulusal ve Uluslar Arası Boyutlarıyla Siber Güvenlik",EMO- elektrik mühendisliği, Mart 2010, (94-103)
[12] .ALTUNDAL Ömer Faruk, "DDoS nedir, ne değildir?", http://www.siberguvenlik.org.tr/makaleler/ddos-nedir-ne-degildir/, Ağustos 2012
[13] BODEAU Deborah J., GRAUBART Richard, FABİUS-GREENE Jennifer," Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels", 2010 IEEE Second International Conference on Social Computing (SocialCom), Ağustos 2010 ,(1147 – 1152)
[14] OWASP," SQL Injection" , https://www.owasp.org/index.php/SQL_Injection, 2010
[15] OWASP "Reviewing Code for SQL Injection", https://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection, 2010

Seda YILMAZ Gazi Üniversitesi Bilgisayar Bilimleri Bölümünde yüksek lisans eğitimine devam etmektedir. Araştırma konuları arasında kablosuz sensor ağlarda güvenlik, web yazılım güvenliği, siber güvenlik, bilgi ve bilgisayar güvenliği yer almaktadır.

Şeref SAĞIROĞLU Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesidir. Zeki sistem kimliklendirme, tanıma ve modelleme, ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizi ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları; yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar gibi konularda çalışmaktadır. 50'nin üzerinde SCI tarafından taranan uluslar arası dergilerde yayınlanmış makalesi, 50'nin üzerinde ulusal dergilerde yayınlanmış makalesi, 100'ün üzerinde uluslar arası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş100'e yakın bildirisi bulunmaktadır. 3 adet alınmış patenti vardır. 5 adet yayınlanmış kitabı, 2 adet kitapta bölüm yazarlığı bulunmaktadır. 4 kitabın da editörlüğünü yapmıştır.

Ulusal ve uluslar arası pek çok proje yürütmüş ve konferanslar düzenlemiş olup akademik çalışmalarına devam etmektedir.

EK A

TABLO 1
SİBER TEHDİT SEVİYELERİ [13]

Seviye	Saldırgan Tipleri	Saldırgan Hedef/Amacı	Yöntemleri
1.Seviye (Siber Vandalizm)	-Küçük saldırgan grupları	-Kurum organizasyon yapısını bozmak -İtibarını zedelemek	-Hassas verilere erişmek -Giriş denemeleri gerçekleştirmek -Genel erişime sahip sistemler üzerindeki dosyaları hedef almak -Ağ yapısına yönelik keşif saldırıları yapmak -Kurum çalışanlarına yönelik sosyal mühendislik faaliyetleri uygulamak
2.Seviye (Siber Hırsızlık)	-Bireysel ya da küçük saldırgan grupları	-Siyasi-ideolojik amaçlar -Endüstiriyel casusluk -Kar edinme	-Kurum içi yardım ile fiziksel erişim sağlama -Siber saldırı için kullanılan bilgilere açık kaynaktan erişim -Veri trafiğini izleme -Bilgi sistem cihazlarını çalma -Dış bilgi sistemlerini ve ağları izleme -IIS bağlantılarına erişmek için açıklardan ayarlanma
3.Seviye (Siber Gözetleme)	-Büyük saldırgan gruplar -Sofistik terör örgütleri -Profesyonel organize suç örgütleri	-Siber kaynakları elde etmek -Genel altyapı bilgisine sahip olmak -Büyük çaplı saldırılara temel olacak verileri elde etmek	-Veri transferini kolaylaştırmak için örgütsel yapıya casus kod parçaları yerleştirmek -Dahili ağlara genel amaçlı bilgi toplayıcıları ekleme -Haritalama ve organizasyon ağlarını tarama -Bilgi sistem ortamları ve operasyonlara keşif gerçekleştirme -Yaygın kullanılan yazılımı ele geçirme -Hedefli sıfır gün saldırıları gerçekleştirme -Yetkili kişilerin verilerini ele geçirme
4.Seviye (Siber Casusluk)	-Profesyonel istihbarat örgütleri	-Ülkelerin özel misyon ve programları	-Sahte donanım tedarik zinciri ekleme -Oturum bilgisini ele geçirme -İzleme içeriklerini kurumsal bilgi sistemleri ve ağları üzerine yükleme -Örgüt içine casus yerleştirilmesi -Ana bilgisayarlar ve kritik noktaları hedefleme -Sıfır gün saldırılarıyla kurumsal bilgi sistemlerini hedefleme -Hedef kuruluşun ISSini hedefleyen, kuruluş tarafından kullanılmasını sağlamak üzere kötü amaçlı yazılımlar tasarlama -Kablosuz algılayıcıları hedef yapı içine gizlice eklemek
5.Seviye (Siber Savaş)	-Terörist gruplar	-Hedefin bilgi altyapısını yok etmek	-Kritik bilgi sistem bileşenleri ve işlevlerini hedef alma -Tasarım, üretim ve/veya dağıtım bileşenlerini kullanarak bilinen organizasyonu tehlikeye atmak -İç, dış ve tedarik zinciri saldırını koordineli şekilde kullanarak kuruluşa saldırılar düzenlemek -Kuruluşun tedarik zincirine kötü niyetli yazılımlar enjekte ederek yanlış-açık organizasyonları yaratmak -ISSe yanlış ama inandırıcı veri enjekte etmek -ISS içine sistem yapılandırmalarına dayalı özel, sıradan olmayan, kötü amaçlı yazılım eklemek -Kablosuz iletişim sistemine erişim sağlamak -Kuruluş içindeki ayrıcalıklı pozisyonlara casus yerleştirilmek

EK B

TABLO 2
HAZIRLIK SEVİYELERİ [13]

Seviye	Amaç	Tedbirler	Çözümler
1.Seviye (Çevre Savunması)	-Dış çevreden gelecek saldırılara karşı genel hazırlık	-Ticari güvenlik ürünleri ve masaüstü uygulamaları	-Güvenlik duvarı oluşturmak ve saldırı tespiti yapmak -Kimlik doğrulaması yapmak -E-posta sunucuları ve istemci sistemlerine anti-virüs yazılımları yüklenmesi -Denetim günlüğü ile açıkları ve çevre sistemlerini izlemek
2.Seviye (Kritik Bilgileri Koruma)	-Kritik yada hassas verilere erişimi engellemek	-Gelişmiş kimlik doğrulama -Erişim kontrol sistemleri -Şifreleme -Kritik verilerin bağımsız sistemlerde saklanması	-Dış ve iç sistemler arasında güvenilir şifreli uygulamaların kullanımı (SSL, VPNs) -Kurumsal ağlarda ayrılmış ve arındırılmış bölge oluşturulması -Taşınabilir sistemlerin (dizüstü bilgisayarlar, flaş sürücüler, vb) iç ağa yeniden bağlanmadan önce taranması -Kötü niyetli iç erişimleri önlemek için kritik sistemlere güçlü bir fiziksel güvenlik kontrolünün oluşturulması -Periyodik açık arama ve bilgi savunma ayarlarının yapılması -Riskli kullanıcı davranışlarını daha iyi kontrol edebilmek için masaüstü bilgisayarlarının sanallaştırılması -Tasarım/mimariyi ek güvenlik yazılımları ile geliştirmek
3.Seviye (Farkındalık)	-Bilgi sistem altyapısını korumak	-Penetrasyon testleri	-Saldırıları algılamak için kritik noktalara alıcıları dağıtmak -Anormal koşulları ve sıra dışı akışları izlemek için ağ trafiğini analiz etmek -İçeriden çıkan dağılımı izlemek -Siber ve fiziksel erişim analizi yapmak -Yasadışı veri aktarımı için çevre iletim kanallarını izleme
4.Seviye (Mimari Esneklik)	-Saldırı geçmişini incelemek	-Bilgi sistem altyapısının yedeklenmesi -Erişimlerin sınırlandırılması -Saldırılar karşısında esnek bir mimari oluşturulması	-Kritik bilgi sistemlerine güçlü erişimler kullanmak -İç yapıyı kontrol etmek ve yeniden konfigürasyonları hızlı bir şekilde yapmak için sistemi alt bölümlere bölmek -Sipariş ve tedarik zinciri arasındaki süreyi en aza indirmek -Kuruluşdaki yapılara fiziksel güvenlik uygulamak (Penetrasyon Testi) -Güvenilir aygıtlar kullanmak -Sık sık yazılım yapılandırmalarında küçük değişiklikler yapmak
5.Seviye (Çeviklik)	-Direk organizasyon yapısını hedef alan saldırılara hazırlık	-Sistemlerin mümkün olduğunca bağımsız tasarlanması -Esnek ve uyarlanabilir mimari seçilmesi	-Anahtar bileşenleri için birden çok tedarikçi kullanmak -Kuruluş adına kritik bileşenleri güvenilir aracılar yoluyla elde etmek -Penetrasyon testlerini kullanmak -Hizmetleri sanallaştırmak -Periyodik olarak saldırgan yeteneğini azaltmak için kritik işlevleri yeniden oluştumak -Gelecekteki saldırılara cevap verebilmek için yakın zamanlı saldırıların yapısal incelemesini ve analizini yapmak

Solution of a Conjecture: On 2-PCD RFID Distance Bounding Protocols

Eren KOCAAĞA, Bünyamin TANIL, Muhammed Ali BİNGÖL, Süleyman KARDAŞ

***Abstract*—It is a popular challenge to design distance bounding protocols that are both secure and efficient. Motivated by this, many distance bounding protocols against relay attacks have been advanced in recent times. Another interesting question is whether these protocols provides the best security. In 2010, Kara et al. analysis the optimal security limits of low-cost distance bounding protocols having bit-wise fast phases and no final signature. As for the classification, they have introduced the notion of k-previous challenge dependent (k-PCD) protocols where each response bit depends on the current and the k previous challenges. They have given the theoretical security bounds for two specific classes $k = 0$ and 1, but have left the security bounds for $k \geq 2$ as an open problem. In this paper, we aim to answer the open question concerning the security limits of 2-PCD protocols. We describe two generic attacks for mafia and distance frauds that can be applied on any 2-PCD protocols. Then, we provide the optimal trade-off curve between the security levels of mafia and distance frauds that determines the security limits of 2-PCD protocols. Finally our results also prove the conjecture that 2-PCD protocols enhance the security compared to 0-PCD and 1-PCD cases.**

***Index Terms*—RFID, distance bounding protocol, relay attack, security, trade-off.**

I. Introduction

RADIO Frequency IDentification protocols, as a part of wireless authentication, are commonly used in many applications such as credit cards, toll payment systems, e-passport etc. Since the communication occurs in the air, these protocols are vulnerable to relay attacks in which an attacker defeats the authentication system by only relaying messages verbatim between the legitimate parties (generally a prover and a verifier). The concept of relay attack was originally proposed by Conway using a scenario called "Grand Master Chess Problem" in 1976 [1], and advanced by Desmedt et al. in Crypto'87 [2]. Relay attacks can be simply classified as mafia, terrorist and distance fraud attacks [3].

Based on the authentication protocols that include challenge-response messages, mafia and terrorist fraud scenarios can be defined as follows (Fig. 1). An adversary pretending to be a legitimate prover (or tag) first gets the challenge from the verifier (or reader) and relay it to the legitimate prover which is out of neighbourhood at the beginning of attack. After that she gets the valid response for this challenge and forwards it to the reader as her answer. Some relay attack demonstrations and constructive considerations are given in [4]–[6].

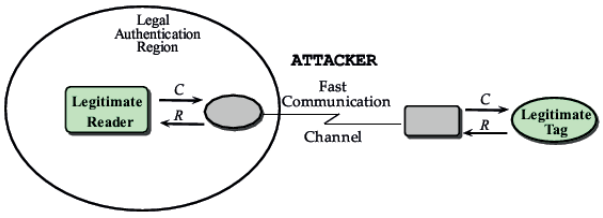


Fig. 1. Mafia and terrorist fraud scenarios

The aforementioned scenario that the prover has no awareness of attack is an example of mafia fraud. In order to give a more realistic illustration, we can think that mafia fraud attack can be completed against the point-of-sale credit card terminal although the credit cards are tamper resistant and certificated. The remaining type of the relay attack is called *distance fraud* attack where adversary has an ability to reach secret key (she is a kind of dishonest legitimate tag) to convince the verifier that she is within the neighbourhood whereas she is not. A typical and easily comprehensible illustration of this attack is home confinement that a person wears a bracelet and electronically monitored. This person would make use of distance fraud attack and leave his home temporarily without being detected. (Fig. 2).

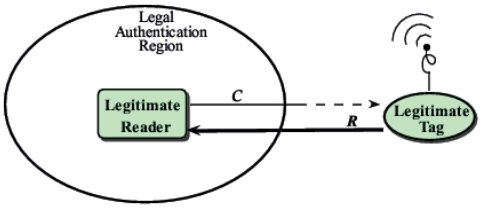


Fig. 2. Distance fraud scenario

Researchers have developed two main approaches to mitigate relay attacks. One of them is related to measuring radio signal strength (RSS) that the verifier measures this value in order to understand whether the prover is close or not. On the other hand, this solution suggestion is not applicable because adversary can have the ability to adjust its signal strength to persuade the verifier that she is in the neighbourhood region. The other approach to prevent these attacks is focused on calculating the round trip time (RTT) of the prover's response after a challenge sent by the verifier. The verifier

E.Kocaağa and B. Tanıl are with Istanbul Technical University Maslak, Istanbul, and M. A. Bingöl, and S. Kardaş are with National Research Institute of Electronics and Cryptology (TUBITAK UEKAE), Gebze 41470 Kocaeli/Turkey and Sabanci University Istanbul/Turkey, e-mail: {muhammedali.bingol, suleyman.kardas}@tubitak.gov.tr

checks the distance of a prover under favour of measuring RTT of a signal. Upper bound for the speed of radio signal, which has importance in this approach, can not be faster than that of light. Brands and Chaum took the first step in their seminal work [7] and they offered the rapid bit exchange conception to design a protocol that includes measurement of RTT in 1993. Afterwards, Hancke and Kuhn proposed the first RFID-related distance bounding protocol [8], which does not involve any final signature. These studies triggered the other researchers and several distance bounding protocols that use round trip time method have been proposed to increase security conditions against relay attacks which are mafia fraud, distance fraud and terrorist fraud [9]–[14]. We refer to [3] for further introduction on distance bounding protocols.

It is still a popular challenge to design distance bounding protocols that are both secure and efficient. In 2010, optimal security limits of low-cost RFID distance-bounding protocols are analyzed by Kara, Kardaş, Bingöl, and Avoine [15]. They focus on the low-cost distance-bounding protocols having bit-wise fast phases and no final signature. As for the classification, they introduce the notion of k-previous challenge dependent (k-PCD) protocols where each response bit depends on the current and the k previous challenges. They provide trade-off curves between the optimal security limits of mafia and distance frauds for $k = 0$ and 1. The authors leave as an open question to find the best the trade-off curves for $k \geq 2$, and they conjecture that the security should be enhanced when k is increased.

In this paper, we aim at to support anticipations about the open questions of k-PCD protocols (general extension). In this respect, we analysis 2-PCD protocols and make attack resistance calculations of this protocol against mafia and distance fraud attacks. Our results show that when we increase the number 'k', the security level of distance bounding protocols enhanced as it is expected. We also demonstrate the results calculated on software program and observe 2-PCD trade-off curve below that of 1-PCD. The most important property of previous challenge dependent distance bounding protocols is that the current response bit in the rapid bit phase depends on previous challenges as well. It is observed that the security of protocols against mafia fraud and distance fraud attacks improved without any supplementary overhead on the computation by virtue of k-PCD protocols can be succeeded. The another expected properties of distance bounding protocols such as resistance of channel errors in noisy environment and preservation of privacy also provided by these protocols. Moreover, mutual authentication is also made between prover and verifier without generating any overhead in these protocols. In conclusion, development of k-PCD protocols has crucial importance on RFID framework and this is what we try to do in general of this study.

The composition of the paper is following: In Section II we briefly explain the current challenge dependent (CCD) protocols. In Section III, conjectures and open questions of k-PCD protocols and some relevant definitions are given. Section IV consists of our results and analysis related to 2-PCD protocols that answers the previous conjectures and simulations that supports theoretical results.

II. Current Challenge Protocols (CCD)

In general, distance bounding protocols consist of three phases; slow phase-I, fast phase and slow phase-II. However slow phase-II usually contains time consuming message namely a final signature. Therefore, we focus on CCD protocols that have no slow phase-II as it is primarily defined in [15]. For instance, Hancke and Kuhn's protocol as an example of current challenge dependent protocols includes only the first two phases. In slow phase-I, parties interchange nonces. After that, responses are generated by parties using the same pseudo random functions. During the fast phase each response r_i only corresponds to a current challenge c_i. This protocol satisfies the following properties:

- During the fast phase, each response bit r_i is computed as $r_i := f(c_i, y_i^0, ..., y_{m-1}^i)$, where c_i is the i-th bit and $(y_i^0, ..., y_{m-1}^i)$ is the i-th string of the session secret shared by both prover and verifier for $i = 1, ..., n$, where n is the number of rapid bit exchanges. The response function f is defined as: $r_i := f(c_i, y_i^0, ..., y_{m-1}^i) = c_i.y_1^i \bigoplus((1 \bigoplus c_i).y_0^i)$
- There is no final slow phase.

Final signature is not a compulsory phase for practical solutions to suitable requirements of RFID tags. On the other hand, these protocols are vulnerable to terrorist attacks without final signature. However, CCD protocols satisfy some sucurity levels against mafia and distance frauds. Success probabilities of mafia and distance frauds have the following property [15]:

$$P_{maf} + P_{dis} \geq \tfrac{3}{2}.$$

III. k-PCD Protocols

k-Previous Challenge Dependent (k-PCD) protocol is a natural extension of CCD protocols. In CCD protocols, the response is only related to current challenge. On the other side, the response depends on both current challenge and k previous challenges in k-PCD protocols. This protocol satisfies the properties below

- During the fast phase, each response bit r_i is computed as $r_i := f(c_i, ..., c_{i-k}, y_i^0, ..., y_{m-1}^i)$, where c_i is the i-th bit and $(y_i^0, ..., y_{m-1}^i)$ is the i-th string of the session secret shared by both prover and verifier for $i = 1, ..., n$, where n is the number of rapid bit exchanges.
- There is no final slow phase.

Remark : From definitions, a CCD protocol can be thought as a k-PCD protocol when k=0.

As a result, protocols that the response of the prover in fast bit exchange phase depends on previous challenges are more secure against relay attacks compared to CCD protocols. Hence, k-PCD protocols are expected to reach the optimum security against mafia fraud and distance fraud when k tends to be infinity. This conjecture is generated from calculations that take part in following sections.

IV. The Security Analysis of 2-PCD Protocols

In this section, we introduce and analyze the security of 2-PCD protocols. First of all, description of security regions

for analysis of distance fraud attack is given in order to easily comprehend the idea of the generic attack. Second, we receive some help from different sets which defined in this section just as used in CCD and 1-PCD protocols [15]. Then, we verify optimum security limits for 2-PCD protocols against mafia and distance fraud, and plot the trade-off curve for k-PCD protocols where $k = 0, 1$ and 2.

A. Security Regions for Distance Fraud

k-PCD protocols are composed of two main parties; reader and prover. When the subject matter is a distance fraud attack against these protocols, another party called adversary emerges in addition to main parties. In distance fraud attack, the adversary has a right to access while staying on legal authentication region. Besides, the adversary may stay on the outside of this region and pretend to be in the authentication region. In brief, distance fraud attacks are based on this scenario in RFID framework.

When an adversary is outside of legal authentication region, receiving and time requirement to receive challenges depend on the distance between the adversary and bounds of this region. Therefore, in order to make the analysis of distance fraud attacks simpler, we describe four spherical regions (Z_1, Z_2, Z_3, Z_4) in which the adversary can communicate with the verifier.

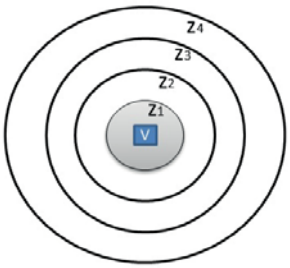


Fig. 3. Security Regions for Distance Fraud

TABLE I
DISTANCE FRAUD SCENARIOS IN DIFFERENT REGIONS

Where is adversary?	What should she do?
Z_1	She always access
Z_2	Send r_i before c_i
Z_3	Send r_i before c_i, c_{i-1}
Z_4	Send r_i before $c_i, c_{i-1}, ..., c_{i-k}$

While designing the distance fraud attack scenario we assume that the adversary is in Z_4 region since the dependency parameter k is equal to 2. In the next subsection, calculations of security limits of 2-PCD protocols against distance fraud attacks are made based on this scenario.

B. Security Trade-off for 2-PCD Protocols

Let g be the response function that have inputs c_i, c_{i-1}, c_{i-2}, y and output response bit r_i. To analyze the distance and mafia fraud attack, we define a variable a_y as the equation below,

$$\begin{aligned} a_y &= \sum g(c_i, c_{i-1}, c_{i-2}, y) - 4 \\ & c_i \in (0,1) \\ & c_{i-1} \in (0,1) \\ & c_{i-2} \in (0,1) \end{aligned}$$

Also we define the following sets:

$$\begin{aligned} A &= y \in F_2^m : |a_y| = 4, \\ B_1 &= y \in F_2^m : |a_y| = 3, \\ B_2 &= y \in F_2^m : |a_y| = 2, \\ B_3 &= y \in F_2^m : |a_y| = 1, \\ C &= y \in F_2^m : |a_y| = 0. \end{aligned}$$

$a + b_1 + b_2 + b_3 + c = 2^m$, where a is the cardinality of the set A, b_1 is the cardinality of the set B_1, b_2 is the cardinality of the set B_2, b_3 is the cardinality of the set B_3 and c is the cardinality of the set C.

The set A includes the session secrets that produce the same response bits r_i. The other three sets B_1, B_2 and B_3 are the majority groups that have same response bits with probability $\frac{7}{8}, \frac{3}{4}$ and $\frac{5}{8}$ respectively. Finally, set C has same response bits in half.

Success probabilities of mafia fraud and distance fraud attacks depend on the cardinality of sets in 2-PCD protocol. Success probability calculations of distance fraud attack for 2-PCD protocols as follows:

$$\begin{aligned} P_{dis} &= \frac{a}{2^m} + \frac{7}{8} \cdot \frac{b_1}{2^m} + \frac{6}{8} \cdot \frac{b_2}{2^m} + \frac{5}{8} \cdot \frac{b_3}{2^m} + \frac{4}{8} \cdot \frac{c}{2^m} \\ &= \frac{1}{2} + \frac{4a + 3b_1 + 2b_2 + b_3}{2^{m+3}} \end{aligned}$$

Success probability calculations of mafia fraud attack for 2-PCD protocols as follows:

$$\begin{aligned} P_{maf}^{no-flip} &= \frac{1}{8} + \frac{7}{8} \cdot [\frac{a}{2^m} + \frac{3}{4} \cdot \frac{b_1}{2^m} + \\ & \quad \frac{4}{7} \cdot \frac{b_2}{2^m} + \frac{13}{28} \cdot \frac{b_3}{2^m} + \frac{3}{7} \cdot \frac{c}{2^m}] \\ &= \frac{1}{2} + \frac{16a + 9b_1 + 4b_2 + b_3}{2^{m+5}} \end{aligned}$$

$$\begin{aligned} P_{maf}^{flip} &= \frac{1}{8} + \frac{7}{8} \cdot [\frac{1}{4} \cdot \frac{b_1}{2^m} + \frac{3}{7} \cdot \frac{b_2}{2^m} + \\ & \quad \frac{15}{28} \cdot \frac{b_3}{2^m} + \frac{4}{7} \cdot \frac{c}{2^m}] \\ &= \frac{1}{8} + \frac{7b_1 + 12b_2 + 15b_3 + 16c}{2^{m+5}} \end{aligned}$$

Success probabilities of distance fraud attack and mafia fraud attack inversely related to each other. Trade-off curve calculations between mafia fraud and distance fraud for 2-PCD protocols as follows:

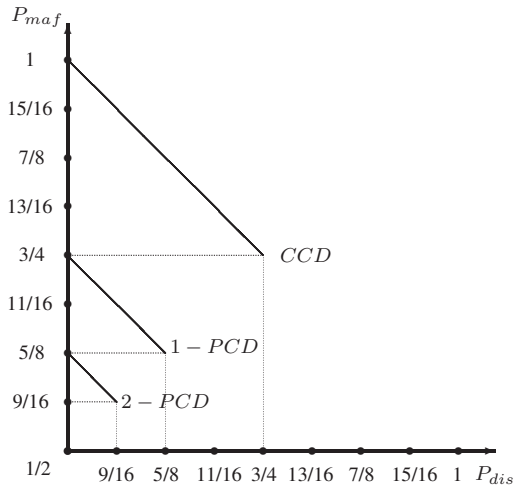
$$P_{maf}^{flip} + P_{dis} = \frac{9}{8} + \frac{3b_1 + 4b_2 + 3b_3}{2^{m+5}}$$
$$P_{maf}^{no-flip} + P_{dis} = \frac{9}{8} + \frac{28a + 17b_1 + 8b_2 + b_3 - 4c}{2^{m+5}}$$

This implies that, $P_{maf} + P_{dis} \geq \frac{9}{8}$. Thus, lower success probability bound for the summation of both mafia fraud attack and distance fraud attack is calculated as $\frac{9}{8}$.

TABLE II
MAXIMUM SECURITY LIMITS

DB Protocols	$P_{dist} + P_{maf} \geq$
CCD	3/2
1-PCD	5/4
2-PCD	9/8

TABLE III
TRADE-OFF CURVE FOR CCD,1-PCD,2-PCD



As it is easily shown in the figure when the parameter k goes the infinity k-PCD protocols will reach the ideal security level.

C. The Optimum Design of Mafia and Distance Fraud Attack Algorithm Against 2-PCD Protocols

Compatibility between calculations and verification of distance fraud attack and mafia fraud attack with algorithms provides huge contributions on the optimum security results.

We compare mafia fraud attacks $max(P_{maf}^{no-flip}, P_{maf}^{flip})$ with an approximation (neglecting b_1, b_2 and b_3). Then, this approximation gives that optimum security limit for mafia fraud is satisfied when $c = 7a$. So, it is clear that flipping the response is more preferable under the condition of $c > 7a$ in order to learn each bit of register for an adversary.

We design a generic mafia fraud attack algorithm for 2-PCD protocols which is given in Algorithm IV.1.

Algorithm IV.1: MAFIA FRAUD ATTACK FOR 2-PCD PROTOCOLS(n, a, c)

n: Number of rounds
flip: Deciding on flipping the response
Send a random challenge $c'_0 \in \{0,1\}$ and $c'_1 \in \{0,1\}$ to the prover
if $c \geq 7a$
  then $flip \leftarrow 1$

  else $flip \leftarrow 0$
for $i \leftarrow 0$ **to** n
  do { Send a random challenge $c'_i \in \{0,1\}$ to the prover
  Record the prover's response r'_i
*/*Then, Mafia continues the protocol with the verifier*/*
Record first challenge c_{i-1} and second challenge c_{i-2} of the verif
for $i \leftarrow 2$ **to** n
  do { record i-th challenge of the verifier in c_i
  if $c'_i = c_i$ **and** $c'_{i-1} = c_{i-1}$ **and** $c'_{i-2} = c_{i-2}$
    then Send r'_i

    else Send $r'_i \oplus flip$
  $c_{i-1} \leftarrow c_i$ **and** $c_{i-2} \leftarrow c_{i-1}$

We also design a generic distance fraud attack algorithm for 2-PCD protocols which is given in Algorithm IV.2.

Algorithm IV.2: DISTANCE FRAUD ATTACK FOR 2-PCD PROTOCOLS(n)

n: Number of rounds
$c'_0 \in \{0,1\}$ and $c'_1 \in \{0,1\}$
for $i \leftarrow 2$ **to** n
  do { **if** $a_y = 3$ **or** $a_y = 2$ **or** $a_y = 1$
    Send 1
    if $g(0, c_{i-1}, c_{i-2}, y) = 1$
      if $c_{i-1} = 0$
      then $c_{i-2} \leftarrow 0$

        else $c_{i-1} \leftarrow 0$ **and** $c_{i-2} \leftarrow 1$
      else
      if $c_{i-1} = 0$
      then $c_{i-1} \leftarrow 1$ **and** $c_{i-2} \leftarrow 0$

        else $c_{i-1} \leftarrow 1$ **and** $c_{i-2} \leftarrow 1$
    else if $a_y = -3$ **or** $a_y = -2$ **or** $a_y = -1$
    Send 0
    if $g(0, c_{i-1}, c_{i-2}, y) = 1$
      if $c_{i-1} = 0$
      then $c_{i-2} \leftarrow 0$

        else $c_{i-1} \leftarrow 0$ **and** $c_{i-2} \leftarrow 1$
      else
      if $c_{i-1} = 0$
      then $c_{i-1} \leftarrow 1$ **and** $c_{i-2} \leftarrow 0$

        else $c_{i-1} \leftarrow 1$ **and** $c_{i-2} \leftarrow 1$
    else
    Send $g(0, c_{i-1}, c_{i-2}, y)$
    then $c_{i-1} \leftarrow 0$ **and** $c_{i-2} \leftarrow c_{i-1}$

D. Simulation Results

We implement four different 2-PCD response generating functions on HK protocol structure. We simulate the attacks given in Algorithms IV.1 and IV.2 for each of them. The simulation for each protocol is repeated 2^{20} times with fresh nonces. We have shown that the experimental results, which are shown in Table IV, are in parallel with the results obtained in Section IV-B.

TABLE IV
THE SIMULATION RESULTS FOR SUCCESS PROBABILITIES OF MAFIA FRAUD AND DISTANCE FRAUD.

a	$\sum_{i=1}^{3} b_i$	c	P_{maf}^{flip}	$P_{maf}^{no-flip}$	P_{dis}
1	0	7	0.5626	0.5656	0.5626
4	2	2	0.3260	0.7942	0.8200
0	0	8	0.6242	0.4992	0.4969
0	8	0	0.4485	0.6818	0.7821

Note that, in all experiments we took $b_1 = b_2 = b_3$ for the sake of simplicity.

V. Conclusion

In this paper, we have explained RFID distance bounding protocols and briefly reviewed at current challenge dependent protocols. We also introduced the notion of k-PCD protocols. Thus, we have shown that when we increase the dependency parameter 'k', security level against mafia fraud attack and distance fraud attack increase as they are expected. We have supported these expectations by calculating success probabilities of distance fraud and mafia fraud attacks for 2-PCD protocols. On the other hand, trade-of curve of 2-PCD protocol is plotted and compared with CCD and 1-PCD protocols.

We also prove the conjecture that the best trade-off curve for k_1-PCD protocols lies above the best trade-off curve for k_2-PCD protocols where $k_1 < k_2$.

We also claim that a general formula for k-PCD protocols can be obtained but we also left this problem as an future work.

VI. Acknowledgements

We would like to thank Oğuz Yildiz for his helpful contributions.

References

[1] J. H. Conway, *On Numbers and Games*, ser. London Mathematical Society Monographs. Academic Press, London-New-San Francisco, 1976, no. 6.

[2] Y. Desmedt, C. Goutier, and S. Bengio, "Special uses and abuses of the fiat-shamir passport protocol," in *Advances in Cryptology – CRYPTO'87*, ser. Lecture Notes in Computer Science, C. Pomerance, Ed., vol. 293. Santa Barbara, California, USA: Springer-Verlag, August 1988, pp. 21–39.

[3] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, "A Framework for Analyzing RFID Distance Bounding Protocols," *Journal of Computer Security – Special Issue on RFID System Security*, vol. 19, no. 2, pp. 289–317, March 2011.

[4] G. Hancke, K. Mayes, and K. Markantonakis, "Confidence in Smart Token Proximity: Relay Attacks Revisited," in *Elsevier Computers & Security*, ser. 7, vol. 28, June 2009, pp. 615–627.

[5] G. P. Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards," Manuscript, University of Cambridge, United Kingdom, February 2005.

[6] L. Sportiello and A. Ciardulli, "Long distance relay attack," in *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.

[7] S. Brands and D. Chaum, "Distance-Bounding Protocols," in *EUROCRYPT'93: Advances in Cryptology*. Secaucus, NJ, USA: Springer-Verlag Newyork Inc, 1994, pp. 344–359.

[8] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," in *SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 67–73.

[9] S. Kardaş, M. S. Kiraz, M. A. Bingöl, and H. Demirci, "A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions," in *Workshop on RFID Security – RFIDSec'11*, ser. Lecture Notes in Computer Science, A. Juels and C. Paar, Eds., vol. 7055. Amherst, Massachusetts, USA: Springer Berlin Heidelberg, June 2012, pp. 78–93.

[10] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "The Swiss-Knife RFID Distance Bounding Protocol," in *International Conference on Information Security and Cryptology – ICISC*, ser. Lecture Notes in Computer Science. Seoul, Korea: Springer-Verlag, 2008, pp. 98–115.

[11] G. Avoine, C. Lauradoux, and B. Martin, "How secret-sharing can defeat terrorist fraud," in *Proceedings of the 4th ACM Conference on Wireless Network Security – WiSec'11*, ACM. Hamburg, Germany: ACM Press, June 2011.

[12] Y.-J. Tu and S. Piramuthu, "RFID Distance Bounding Protocols," in *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.

[13] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting Relay Attacks with Timing-Based Protocols," in *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*. New York, NY, USA: ACM, 2007, pp. 204–213.

[14] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Secure and Lightweight Distance-Bounding," in *Second International Workshop on Lightweight Cryptography for Security and Privacy – LightSec 2013*, Gebze, Turkey, May 2013.

[15] O. Kara, S. Kardaş, M. A. Bingöl, and G. Avoine, "Optimal Security Limits of RFID Distance Bounding Protocols," in *Workshop on RFID Security – RFIDSec'10*, ser. Lecture Notes in Computer Science, S. O. Yalcin, Ed., vol. 6370. Istanbul, Turkey: Springer, June 2010, pp. 220–238.

Some Results On Three-Valued Walsh Transforms from Decimations of Helleseth-Gong Sequences

Hasan Dilek, Ernist Tilenbaev, Zülfükar Saygı and Çetin Ürtiş

***Abstract*—The Walsh transform of two-level autocorrelation sequences has played an important role in construction of the set of sequences. For p-ary sequences, there are only two basic classes of two-level autocorrelation sequences with no subfield structures for an arbitrary odd prime p. One is the class of p-ary m-sequences and the other of p-ary Helleseth-Gong sequences. Gong, Helleseth, and Hu found many decimation numbers which yield three-valued Walsh transforms by computer search. They proved two cases and also found additional values of decimation number which yield three-valued Walsh transform. Gong, Helleseth, Hu and Li proved two more cases with new observations. In this paper, for $p = 5$, $k = 1$, $n = 5$ and $s = 2$ we proved that the decimation value $d = 481$ yields a three-valued Walsh transform, which is not covered in previous studies. Also we present a conjecture for $p = 3$ at the end of the paper.**

***Index Terms*—Autocorrelation, cross-correlation, m-sequences, p-ary sequences, Walsh transform, Helleseth-Gong sequences.**

I. INTRODUCTION

Given two sequences $\{a(t)\}$ and $\{b(t)\}$ of period N with elements from a finite field $\mathbb{F}_p$. The cross-correlation between the sequences at shift τ is defined by

$$C_{a,b}(\tau) = \sum_{t=0}^{N-1} w^{a(t+\tau)-b(t)}$$

where w is a complex p th root of unity. In the particular case when two sequences are the same, we denote it by the autocorrelation $A_{a,a}(\tau)$. A sequence $\{a(t)\}$ is said to have (ideal) two-level autocorrelation if $A_{a,a}(\tau) = -1$ for all $\tau \neq 0 \pmod N$. We say two vectors in a vector space of dimension n over the complex field is orthogonal if their inner product is equal to zero.

Recently, Gong, Helleseth, and Hu studied the Walsh transform of a subclass of Helleseth-Gong sequences as well as the Walsh transform of their certain decimations [1]. They found many decimation numbers which yield three-valued Walsh transforms by computer search. They proved two cases of them. But later on, Gong, Helleseth, Hu, and Li present more decimation numbers for three-valued Walsh transform than in [1] which involves some new obversations [2]. There are some main differences between [1] and [2]. One is that u_i which will be defined later is not limited $(-1)^i$ as in [1], but it is relaxed to that in the definition of Helleseth-Gong sequences.

This paper is organized as follows. Section II contains necessary backgound on Helleseth-Gong sequences and the Walsh transform. Section III contains the known results and Section IV contains experimental results. Finally, the paper is concluded in Section V.

H.Dilek, Department of Mathematics, TOBB University of Economics and Technology

E.Tilanbaev, Department of Mathematics, TOBB University of Economics and Technology

Z.Saygi, Department of Mathematics, TOBB University of Economics and Technology

Ç.Ürtiş, Department of Mathematics, TOBB University of Economics and Technology

II. PRELIMINARIES

For any prime p, and any positive integer n, let $\mathbb{F}_{p^n}$ denote the finite field with p^n elements. Let α be a primitive element in $\mathbb{F}_{p^n}$ and let

$$Tr_k^n(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ik}}$$

be the trace from the finite field $\mathbb{F}_{p^n}$ to the subfield $\mathbb{F}_{p^k}$ for some $k\,|n$. In particular, we denote the (absolute) trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ by $Tr_n(x)$.

Definition 1: For any function $f(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, and $\lambda \in \mathbb{F}_{p^n}$, the Walsh transform of f at λ is defined by

$$\hat{f}(\lambda) = \sum_{x \in F_{p^n}} w^{f(x)+Tr_n(\lambda x)}.$$

The Walsh transform is an important tool in cryptography and in design and analysis of sequences over finite fields. For binary and nonbinary functions, the Walsh transform determines the cross-correlation between a pair of p-ary sequences, the sequence defined by $a(t) = f(\alpha^t)$ and the m-sequence given by $b(t) = Tr_n(\alpha^t)$.

The cross-correlation at shift τ between these two sequences is given by

$$\begin{aligned} C_{a,b}(\tau) &= \sum_{t=0}^{p^n-2} w^{a(t+\tau)-b(t)} \\ &= \sum_{t=0}^{p^n-2} w^{f(\alpha^\tau \alpha^t)-Tr_n(\alpha^t)} \\ &= \sum_{x \in F_{p^n}\setminus\{0\}} w^{f(x)+Tr_n(\lambda x)} \\ &= -w^{f(0)} + \hat{f}(\lambda), \end{aligned}$$

where $\lambda = -\alpha^{-\tau}$.

Helleseth and Gong proved the following fact.

Fact 2: ([3]): Let α be a primitive element of $\mathbb{F}_{p^n}$. Let $n = (2m+1)k$ and let s, $1 \leq s \leq 2m$, be an integer such that $gcd(s, 2m+1) = 1$. Let $b_0 = 1$,$b_i = b_{2m+1-i}$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, where indices of b_{is} are taken $\bmod 2m+1$.

Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, ..., m$. Define

$$f(x) = \sum_{i=0}^{m} u_i x^{(p^{2ki}+1)/2}.$$

Then the sequence over $\mathbb{F}_p$ defined by

$$s(t) = Tr_n(f(\alpha^t))$$

has an ideal two-level autocorrelation.

The fact above in the special case $s = 2$ gives $b_{2i} = u_i = (-1)^i (= b_{2m+1-i})$ for $i = 1, 2, ..., m$ and $b_0 = 2u_0 = 1$ i.e., $u_0 = (p+1)/2$.

Lemma 3: ([1],[2],[3]): Let $Q(y)$ be a quadratic form over $\mathbb{F}_q$, $q = p^k$ in n/k variables of rank ρ. Let r be a nonsquare in $\mathbb{F}_q$ and define

$$S = \frac{1}{2}\left(\sum_{y \in \mathbb{F}_{p^n}} w^{Tr_k(Q(y))} + \sum_{y \in \mathbb{F}_{p^n}} w^{Tr_k(rQ(y))} \right)$$

Then

$$S = \begin{cases} 0, & \text{if } \rho \text{ is odd} \\ \pm\, \rho^{\frac{n}{k}-\frac{\rho}{2}}, & \text{if } \rho \text{ is even} \end{cases}$$

III. KNOWN RESULTS

Helleseth and Gong proved the following theorem.

Theorem 4: ([1]): Let $u_0 = (p+1)/2$ and $u_i = (-1)^i$ for $i = 1, 2, ..., m$, and let $d \in \left\{1, \frac{p^n+1}{p^k+1}\right\}$.The Walsh tarnsform of

$$h(x) = Tr_n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2ki}+1}{2} d} \right)$$

defined by

$$\hat{h}(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} w^{h(x)+Tr_n(\lambda x)}$$

has values in the set $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$. The distribution of $\hat{h}(\lambda)$ when λ runs through $\mathbb{F}_{p^n}$ is

0	occurs	$p^n - p^{n-k}$	times
$-p^{(n+k)/2}$	occurs	$(p^{n-k} - p^{(n-k)/2})/2$	times
$p^{(n+k)/2}$	occurs	$(p^{n-k} + p^{(n-k)/2})/2$	times

Also some experimental results are given in Table 1.

Theorem 5: ([2]): Let p be an odd prime number, and $q = p^k$. Let $n = (2m+1)k$ and s, $1 \le s \le 2m$, be an integer such that $gcd(s, 2m+1) = 1$. Let $b_0 = 1$,$b_i = b_{2m+1-i}$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, where indices of b_{is} are taken $\bmod\ 2m+1$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, ..., m$. Define

$$f(x) = \sum_{i=0}^{m} u_i x^{(q^{2i}+1)/2}.$$

The Walsh transform of $f(x)$ has values in the set $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$. The distribution of $\hat{f}(\lambda)$ when λ runs through $\mathbb{F}_{p^n}$ is

0	occurs	$p^n - p^{n-k}$	times
$-p^{(n+k)/2}$	occurs	$(p^{n-k} - p^{(n-k)/2})/2$	times
$p^{(n+k)/2}$	occurs	$(p^{n-k} + p^{(n-k)/2})/2$	times

TABLE I
EXPERIMENTAL DATA

Finite Field	s	d
$\mathbb{F}_{3^5}$	1	$1, 49, 61$
	2	$7, 23, 35, 49$
$\mathbb{F}_{3^7}$	1	$1, 391$
	2	$61, 169$
	3	$1, 439$
$\mathbb{F}_{3^9}$	1	$1, 3361$
	2	$547, 1667$
	4	$1, 3937$
$\mathbb{F}_{3^{11}}$	1	$1, 29767$
	2	$4921, 14641$
	3	$1, 34571$
	4	$1, 35431$
	5	$1, 31639$
$\mathbb{F}_{3^{13}}$	1	$1, 266449$
	2	$44287, 133103$
	3	$1, 307105$
	4	$1, 318865$
	5	$1, 311105$
	6	$1, 284701$
$\mathbb{F}_{3^{15}}$	1	$1, 2393671$
	2	$398581, 1194649$
	4	$1, 2869783$
	7	$1, 2449831$

Theorem 6: ([2]): Let p be an odd prime number, and $q = p^k$. Let $n = (2m+1)k$ and s, $1 \le s \le 2m$, be an integer such that $gcd(s, 2m+1) = 1$. Let $b_0 = 1$,$b_i = b_{2m+1-i}$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, where indices of b_{is} are taken $\bmod\ 2m+1$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, ..., m$. Define

$$f(x) = \sum_{i=0}^{m} u_i x^{(q^{2i}+1)/2}.$$

Let $1 < d < q^{2m+1} - 1$ be an integer satisfying

$$(q^{(m+1)s}+1)d \equiv 2q^h (\bmod\, q^{2m+1s} - 1) \ \text{ for } 0 \le h < 2m+1.$$

The Walsh transform of $g(x) = f(x^d)$ has values in the set $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$. The distribution of $\hat{g}(\lambda)$ when λ runs through $\mathbb{F}_{p^n}$ is

0	occurs	$p^n - p^{n-k}$	times
$-p^{(n+k)/2}$	occurs	$(p^{n-k} - p^{(n-k)/2})/2$	times
$p^{(n+k)/2}$	occurs	$(p^{n-k} + p^{(n-k)/2})/2$	times

From Theorem 2 and Theorem 3, we see that the following decimation numbers and the corresponding correlation values remain open. For this reason, in the next section, we try to prove some of cases in Table 2.

TABLE II
EXPERIMENTAL DATA (DECIMATIONS NUMBERS WHICH HAVE NOT BEEN PROVED YET)

Finite Field	s	d
$\mathbb{F}_{3^5}$	2	$7, 23, 35, 49$
$\mathbb{F}_{3^7}$	2	$61, 169$
$\mathbb{F}_{3^9}$	2	$547, 1667$
$\mathbb{F}_{3^{11}}$	2	$4921, 14641$
$\mathbb{F}_{3^{13}}$	2	$44287, 133103$
$\mathbb{F}_{3^{15}}$	2	$398581, 1194649$

IV. EXPERIMENTAL RESULTS

We have implemented a SAGE code to find the exact cross-correlation distribution of Helleseth-Gong sequences and its decimated ones. Note that these cross-correlation values can be easily obtained by (Table 2). For this reason we only concantrated on the values of Walsh transform. For $p = 3$ we have confirmed the decimation values given in Table 1. Furthermore, in our search for $p = 5$, $k = 1$, $n = 5$ and $s = 2$ we see that the decimation value $d = 481$ also yields a three-valued Walsh transform.

We observe that this decimation numbers is not covered in the results of [1] and [2]. In the following we state and prove this observation. Also at the end of this section we give a conjecture for $p = 3$ using Table 1 which was also confirmed in our experiments for some values of n.

Theorem 7: Let $p = 5$, $k = 1$, $n = 5$, $s = 2$ and $d = 481$. and let $u_i = (-1)^i$ for $i = 0, 1, 2, ..., m$. The Walsh tarnsform of

$$h(x) = Tr_n\left(\sum_{i=0}^{2} u_i x^{\frac{5^{2i}+1}{2}481}\right)$$

defined by

$$\hat{h}(\lambda) = \sum_{x\in\mathbb{F}_{p^n}} w^{h(x)+Tr_n(\lambda x)}$$

has values in the set $\left\{0, \pm 5^3\right\}$. The distribution of $\hat{h}(\lambda)$ when λ runs through $\mathbb{F}_{5^5}$ is

0	occurs	$5^5 - 5^4$	$= 2500$	times
-5^3	occurs	$(5^4 - 5^2)/2$	$= 300$	times
5^3	occurs	$(5^4 + 5^2)/2$	$= 325$	times

Proof: Define the function $F(x)$ from $\mathbb{F}_{5^5}$ to $\mathbb{F}_5$ by

$$F(x) = Tr_5(f(x^{481}) + \lambda x) = Tr_5\left(\sum_{i=0}^{2} u_i x^{\frac{5^{2i}+1}{2}481} + \lambda x\right)$$

and observe that

$$h(x) + Tr_5(\lambda x) = Tr_5(f(x^{481}) + \lambda x) = F(x).$$

It follows that $F(rx) = rF(x)$ for any $r \in \mathbb{F}_5$, since

$$\frac{5^{2i}+1}{2} \cdot 481 = 1 \cdot 1 = 1 \bmod 4$$

Furthermore,

$$\begin{aligned} F(x) &= Tr_5(u_0x^{481} + u_1x^{13\cdot 481} + u_2x^{313\cdot 481} + \lambda x) \\ &= Tr_5(u_0x^{481} + u_1x^5 + u_2x^{601} + \lambda x). \end{aligned}$$

Now taking the $5^4 + 5 = 630$ th power of x, we obtained that

$$\begin{aligned} F(x^{630}) &= Tr_5(u_0x^2 + u_1x^{26} + u_2x^{626} + \lambda x^{630}) \\ &= Tr_5(u_0x^{5^0+1} + u_1x^{5^2+1} + u_2x^{5^4+1} + \lambda x^{5^4+5}). \end{aligned}$$

Here we see that $F(x^{630})$ is a quadratic form over $\mathbb{F}_5$. Now using the same technique in Lemma 1 and Lemma2 of [1], we complete the proof. Note that this technique uses the results from Trachtenberg [6] and Helleseth and Gong [3]. ■

Moreover, based on numerical results on SAGE, we have the following conjecture for $p = 3$.

Conjecture 8: Let $p = 3$, $n = 2m + 1$, $n \geq 5$, $u_0 = (p + 1)/2$ and $u_i = (-1)^i$ for $i = 1, 2, ..., m$, and let $d = \frac{p^{n-2}+1}{p+1}$.The Walsh transform of

$$h(x) = Tr_n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2i}+1}{2}d}\right)$$

defined by

$$\hat{h}(\lambda) = \sum_{x\in\mathbb{F}_{p^n}} w^{h(x)+Tr_n(\lambda x)}$$

has values in the set $\left\{0, \pm p^{\frac{n+1}{2}}\right\}$. The distribution of $\hat{h}(\lambda)$ when λ runs through $\mathbb{F}_{p^n}$ is

0	occurs	$p^n - p^{n-k}$	times
$-p^{(n+k)/2}$	occurs	$(p^{n-k} - p^{(n-k)/2})/2$	times
$p^{(n+k)/2}$	occurs	$(p^{n-k} + p^{(n-k)/2})/2$	times

We have tried to prove this conjecture using similar technique in [1] and [2]. After some point in the proof we get a form having higher degrees instead of a quadratic form. The crucial part of the proofs in [1] and [2] based on getting a quadratic form in the computation of Walsh transform. For this reason, we can prove the case $p = 5$, $n = 5$ and $d = 481$, but we can not complete our conjecture.

V. CONCLUSION

Gong, Helleseth, and Hu studied the Walsh transform of a subclass of Helleseth-Gong sequences as well as the Walsh transform of their certain decimations. They give many decimations numbers which have not been proved yet. We have made some numerical computations. Based on these results we present a conjecture which requires some more techniques to be proved. Also for $p = 5$, $k = 1$, $n = 5$ and $s = 2$ we proved that the decimation value $d = 481$ yields a three-valued Walsh transform.

APPENDIX
SAGE CODE

```
""Defining variables.""
import fractions;
m=2;
p=5;
k=1;
n=(2*m+1)*k;
q=p^n;

Fq.<a>=GF(q,'a');
def correct(value):
  value = coerce( complex,value );
  value = round( value.real, 4) +
round( value.imag, 4)*I;
  return value;
def u(i):
    if i==0:
        return coerce(int, (p+1)/2);
    return (-1)^i;
d_degerleri = [];
```

```
d_karaliste = [];
d = 481;
"""Defining h(x)..."""
def h(x):
  sum = 0;
  for i in range(m+1):
  sum = sum + u(i)*x^( (p^(2*k*i)+1)*d/2 );
  return sum.trace();

"""defining walsh transform"""
def h_head(lam):
    sum = 0;
    for x in Fq:
        y = h(x)+(lam*x).trace();
        y = coerce( int, coerce(str,y) );
        sum = sum + exp(2*pi*I*( y )/p);
    return sum;

print "\n tum degerler...\n";
h_head_values = [];
Unique_h_values = [];
for x in range(q-1):
    value = h_head(a^x);
    value = numerical_approx( value );
    value = correct( value );
    print value;
    h_head_values.append(value);
    for i in h_head_values:
       if i not in Unique_h_values:
           Unique_h_values.append(i);
    if len(Unique_h_values)>3:
      d_karaliste.append(d);
      z = 1;
      while (d*p^z % (q-1) != d ):
         d_karaliste.append(d*p^z % (q-1));
            z = z + 1;
        break;
else:
   d_degerleri.append(d);
   z = 1;
   while (d*p^z % (q-1) != d ):
      d_degerleri.append(d*p^z % (q-1));
       z = z + 1;
```

ACKNOWLEDGMENT

The authors would like to thank the anonymous referee for their valuable and helpful comments and also the first and the third authors were partially supported by TÜBİTAK under Grant no. TBAG-109T344. The numerical calculations reported in this paper were performed at TÜBİTAK ULAKBİM, High Performance and Grid Computing Center (TRUBA Resources).

REFERENCES

[1] G. Gong, T. Helleseth and H. Hu, "A three-valued Walsh transform from decimations of Helleseth-Gong sequences," IEEE Trans. Inf. Theory, vol. 58, no. 2,pp. 1158-1162, Feb. 2012.
[2] G. Gong, T. Helleseth, H. Hu and C. Li, "New three valued walsh transforms from decimations of Helleseth-Gong sequences," Proceeding of International Conference on Sequences and Their Applications SETA 2012, LNCS 7280, pp. 327-337, Sep. 2012.
[3] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation," IEEE Trans. Inf. Theory, vol. 48, no. 11, pp. 2868-2872, Nov. 2002.
[4] H. M. Trachtenberg, "On the cross-correlation functions of maximal linear sequences, " Ph.D. thesis, Univ. Southern California, Los Angeles, CA, 1970.
[5] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," Discr. Math., vol.48, no. 11, pp. 209-232, Nov. 1976.
[6] R. Lidl and H. Niederreiter, Finite Fields. Cambridge University Press, Cambridge, 2nd edition, 1997.

A Secure Internet Voting Protocol Based on Homomorphic Encryption

Ahmet Sinak*, Mehmet Sabir Kiraz*'**, Secil Ozkan*, and Hakan Yildirim*

***Abstract*—In this paper, we focus on Internet voting protocol. Our protocol is similar to the Norwegian scheme which has been used in local elections in 2011. The primary focus of this paper is to prevent a possible cooperation between Ballot Box and Receipt Generator in the Norwegian scheme. The other purpose of this research is to present the alternative solution of coercion which is one of the most important problem in Internet voting. In our protocol, a voter can verify whether her vote is in the counting process.**

***Index Terms*—Electronic Voting, Internet Voting, Homomorphic Encryption**

I. Introduction

ELECTRONIC voting solutions are used by most of the countries around the world besides the classical solutions for elections. In particular, Internet voting (i-voting) is popular and used lately in some countries. Estonia is the first country which is using i-voting for general elections since 2005. Estonian i-voting system and the analysis of the elections are presented in [8], where more than 140 000 people cast their votes in the new system that makes the almost quarter of the whole population. Internet voting is believed to be useful for the voters in the country and for the expatriates since they spend too much time to go to the polling station. In Estonia, about half of the i-voting system users stated that they were spending about half an our to go the place in order to cast their votes. Therefore, it is obvious that Internet voting system simplified the voting process. Norway is another country who is using i-voting for local governmental elections in September 2011 and preparing a new and enhanced i-voting system for the national elections in 2017. The original cryptographic protocol for Norwegian elections was prepared by a Spanish company (Scytl) and later has been modified in order to suffice certain requirements. In order to create society's trust to the new system, Norwegian government made all parts of the technical details of the solution public [4]. Moreover, Norwegian Internet Voting System is analyzed and some improvements has been accomplished in [6], [7]. While Estonia and Norway are the pioneer countries using the i-voting, it is also used in Switzerland for several years. France also used Internet voting for expatriates in the general elections in 2012. Subsequently, more countries got interest to apply for the local and general elections.

Main drawback in an Internet voting is coercion. It is obvious that coercion can manipulate the election results and harm the voters freewill. Coercion can be done not only by force or threat, but also with personal relationships. Moreover, in some parts of the world, coercion might not only be personal but a group can also be forced or threatened to vote for a given candidate. Therefore, the effect of coercion on the election results cannot be ignored and some precautions should be taken. In order to prevent from coercion, the voters, in the previous works, are allowed to cast their votes more than once and only the final vote is counted. In addition to this, we propose to use secret number while casting a vote. One of the most important findings of our work is to find a solution to avoid coercion. In addition to coercion, there are many other issues to be solved but the most crucial ones are listed below: authentication, vote buying/selling, vote alteration, vote privacy, wrong tallying. Similar to coercion, preventing from vote buying is also another important problem. This can also be done personally or a group's votes can be directed to a specific candidate. Integrity is also need to be ensured while casting a vote, and voter must be sure whether if her vote has been stored, transported and tallied correctly. If there exist some voters who think that their votes are being tallied dishonestly, then their confidence to the ruling authority will diminish. Vote privacy is also related with the voters freewill; without privacy, voters can be divided into groups or maybe some of them can be alienated from the community. Therefore, voting should be thought as not only an election but also a chance for a voter to use her own will and to feel as a member of a community. If no precautions can be taken against those crucial problems, it cannot then be stated to have made an election at the end.

In our i-voting protocol, we tried to take some precautions against those problems. In addition the problems stated above, elections in most of the countries have a concrete date (one day). Most of the time, voters have to cast their vote in a specific place during the elections. Thus, in classical election method, there can be rush in airports, terminals in which people are trying to go to the place where they cast their votes. Some people have to stop their holidays or change their places for a specific time interval (during elections) which lead to a loss of time and money. Moreover, obligation to cast vote in a certain place decreases the percentage of people who casts their vote. This can be seen as a side effect of this problem. Therefore, i-voting scheme not only makes people's lives easier, but also increases voter participation.

One other key subject that has to be discussed here is receipt freeness. Receipt freeness is the case where voter cannot prove some other people that she casts her vote to a certain party or a candidate. If she cannot prove her election preference to the vote buyer then there does not exist other way to convince

**TUBITAK BILGEM UEKAE, Kocaeli, Turkey. * Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey.

E-Mails:ahmet.sinak@metu.edu.tr, mehmet.kiraz@tubitak.gov.tr, {seilzkan, hakyildirim}@gmail.com

vote buyer. Receipt freeness is a crucial problem for i-voting systems since it is hard to construct a system which satisfies this property.

A. Contributions

The main concern of this paper is robustness. Our aim is to present a secure, almost end-2-end Internet voting system. There are four motivations of this paper. The first one is to simplify *receipt code* based paper. In the Norwegian system, receipt codes are constructed by a receipt code generator. This generator enables that if two parties in the system cooperate, they can obtain private key of election. We try to exclude a possible cooperation of them. In our protocol, even if they cooperate, the system ensures the privacy of vote. In order to prevent this problem, we use the hash values of the encrypted vote instead of their receipt code algorithm. Next motivation is to use *voter secret number* to protect any type of coercion. We propose to use secret number of the voter while casting a vote. When the entered secret number is right, the vote is tallied; otherwise, it will be canceled. Namely, if the voter is under coercion, he can enter a wrong secret number. A secret number is generated for each voter and they are sent to voters by SMS before the election. Third one is to use *Bulletin Board* in our protocol. The voter can verify whether his vote reaches to the counting process from Bulletin Board. It increases the credibility of the our protocol. Finally, our protocol is *new and almost End-2-End Secure*. The design approach of our system enables the easy usage with considering all the security and privacy conditions. Moreover, our i-voting solution is almost end-2-end secure, in which the system's security is considered from the initial point of system to the final point. In our i-voting system, the voter can verify that her vote was counted as cast.

B. Organization of the Paper

The rest of this paper is organized as follows. Section II describes the basic algorithms and definitions which are used in our protocol. In Section III, we explain the main infrastructures of our protocol. Key generation is also explained in this section. Section IV presents the vote submission and counting processes in our protocol. Section V evaluates security issue. Section VI gives summary of our work. Finally, our protocol is depicted in Appendix.

II. Preliminaries

In this section, we present fundamental definitions and algorithms used in our protocol. In general, e-voting solutions can be stated as a computer system which uses pure mathematics and algorithms. The following algorithms are required for our protocol. For the completeness of the paper, we summarized the underlying cryptographic primitives.

A. Discrete Log Assumption

Let $G =< g >$ be a cyclic group of prime order p (p is a very large prime). Discrete Log Assumption states that it is hard to calculate x by using the generator g and the random group element $y := g^x$.

$$G = \langle g \rangle = \left\{ g^0, g^1, \cdots, g^{p-1} \right\}$$

B. ElGamal Encryption Scheme

ElGamal encryption is used to encrypt the votes in our protocol. ElGamal signature is also used to sign the votes in our protocol. The ElGamal scheme [12] is a public-key cryptographic system based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol. Security of the ElGamal algorithm depends on the difficulty of computing discrete logs in a large prime number. ElGamal has the disadvantage that the ciphertext is twice as long as the plaintext. It has an advantage such that the same plaintext gives a different ciphertext each time it is encrypted (because of randomized encryption).

1) Homomorphic Encryption: Homomorphic encryption is an encryption scheme with a special property that allows operations applied to ciphertext be preserved and carried over to the plaintext. Let M be the set of plaintexts, C be the set of ciphertexts, and K be the set of keys. An encryption scheme is said to be homomorphic if for any given encryption key $k \in K$ the encryption function E satisfies:

$$E_k(m_1 \odot_M m_2) = E_k(m_1) \odot_C E_k(m_2), \forall m_1; m_2 \in M$$

C. Commitment Schemes

Commitments are the important part of the cryptographic protocols. Damgard explains the commitment schemes clearly in [3]. Informally speaking, a commitment scheme consists of commit and reveal phases between two parties, called the sender and the receiver. In many cases, the protocols commit and reveal can be done in terms of a single algorithm, requiring no interaction between the sender and receiver at all.

Pedersen Commitment Scheme: Pedersen introduced a commitment scheme in 1992 [6]. Receiver chooses large primes p and q such that q divides p^{n-1}, generator g of the order-q subgroup of $Z^*_{p^n}$, he selects a random secret x from Z_q, $h = g^x \ mod \ p$. p, q, g, h are public, x is secret.

- Commit: To commit to some $m \in Z_q$, sender chooses random $r \in_R Z_q$ and sends $c = g^m h^r \ mod \ p^n$ to the receiver.
- Reveal: To open the commitment, sender reveals m and r, receiver verifies that $c = g^m h^r \ mod \ p^n$.

D. Threshold Cryptography

In cryptography, threshold is meant to distribute basic cryptographic schemes between a group of participant [9]. Each distributed part can be an algorithm or a key. Secret sharing is the main basis of threshold cryptography. In a *secret sharing scheme* there exist a dealer D and participants $P_1, \cdots, P_n$.

In a $(t, n)-$threshold cryptosystem there are n participants in total. If in order to decrypt an encrypted message a number of parties exceeding a threshold is required to cooperate in the decryption protocol. The message is encrypted using a public

key and the corresponding private key is shared among the participating parties. Let n be the number of parties. Such a system is called $(t, n)-$threshold, if at least t of these parties can efficiently decrypt the ciphertext, while less than t have no useful information.

E. Zero knowledge Proofs

Zero knowledge proofs are a type of proof systems which is first introduced by Goldwasser, Micali and Rackoff [11]. In the zero knowledge proofs there are two players, a prover (P) and a verifier (V). The aim is that a prover convinces a verifier of the truth of the argument without revealing any information about the statement.

III. Models

In this section, we first give the components used in our protocol. In the next step, how the private key of the election and the other secret values are generated will be explained. Finally, the main infrastructures of our protocol will be described.

A. Components

The parameters used in this paper are presented in the Table I.

TABLE I
COMPONENTS

$V \rightarrow$ The voter	$v \rightarrow$ Ballot
$B \rightarrow$ Classical Ballot Box	$PC \rightarrow$ Voter's computer
$TC \rightarrow$ Thin Client	$TS \rightarrow$ Terminal Server
$AB \rightarrow$ Authentication Box	$CB \rightarrow$ Control Box
$A \rightarrow$ Authority	$DS \rightarrow$ Decryption Service
$BB \rightarrow$ Bulletin Board	$C \rightarrow$ Counter
$TP \rightarrow$ Trusted Parties	$CA \rightarrow$ Certification Authority

B. Key Generation

Distributed key generation is the main component of the threshold cryptosystems. There are many solutions to the distributed generation of private keys. Here in our solution, private key will be created by the shares of parties that may be a governmental institution, university or political party which are independent from each other. In our solution we have t of them and any number of institutions less than t cooperating together cannot calculate the private key. The threshold scheme is perfect if knowledge of $t-1$ or fewer shares give no information regarding the private key. In our protocol, the key x is the private key of election whose shares is only known by the trusted parties. the corresponding key $h = g^x mod\ p$ is the public key of election.

Moreover, in our protocol, the secret parameters a_1 belongs to AB, a_2 belongs to CB and a_3 belongs to C are generated by CA which satisfy $a_1 + a_2 = a_3^{-1}\ mod\ p-1$ (a_3 is invertible in $mod\ p-1$). The aim of using this parameters in our protocol is to increase the privacy and security of the system. Moreover, these parameters make the link among the components AB, CB and C. It should be noted that each voter V has a secret number n. This number will be required by the system while casting a vote. The purpose of using this number is to prevent coercion. In our protocol, all secret values are committed by using *Pedersen commitment scheme*.

C. Main infrastructures of our protocol

Before we describe our protocol we would like to highlight the main infrastructures of our system.

- **Voter's Secret Number:** As mentioned before, coercion is one of the most important problem for Internet voting. To overcome this problem, we consider that a voter who is under coercion should use a secret number which is specific for each voter. When voter wants to cast her vote, the system requires her secret number. If voter enters the correct secret number, the vote will be tallied correctly. However, if the entered secret number is not correct, the system will ignore her vote to be tallied without giving a warning to the voter. In that case, the coercer will not notice whether her vote will be tallied.
  Each voter's secret number will be sent to her mobile phone via SMS. Let's assume that coercer have voter's mobile phone for a short time. In this case, there exist solution to satisfy secrecy of her secret number. This number will be sent to voters at an unpredictable time (e.g., anytime in a month) before the election. Coercer has to keep the mobile phones for a long time which is not realistic. On the other hand, the coercer may want from the voter to show her secret number from the phone. To show a fake secret number to the coercer, the voter can demand a new secret number after she receives the first correct secret number. The system will send a new fake secret number. Without legal recourse, always the first secret number will be valid and used in the tallying process; however, fake ones will ignore votes from tallying.
- **Receipt Code:** In the Norwegian system, if the ballot box B and the receipt generator R cooperate, they can obtain private key of election. We consider that, this assumption is strong and should be excluded from an Internet voting system. In our protocol, even if any of the components in the system cooperate, the privacy of the voters will still be ensured. In order to prevent this problem in the Norwegian system, we use the hash values of the encrypted vote instead of their receipt code. That is, a receipt code is the list of hash values of all possible cast-votes. We also note that since every voter has different random number in ElGamal scheme, their encrypted votes and their hash values will be different. Therefore, nobody can understand the others vote knowing the hash value since any two voter casting the same candidate have different receipt values.
  Before the election, High Election Board (HEB) produces a receipt code paper for each voter. Receipt code paper consists of hash values of all possible encrypted votes for a random number. The random number is generated uniquely for each voter, and is sent to the voters inside the receipt code paper. However, it should be noted that the link between voter and her random number have to be unknown in order to satisfy privacy of the voter. Therefore, these papers will be in a sealed envelope and should be anonymously sent to the voters. Before the election period, these papers are delivered to the election

precincts in uniformly random order. During the election period, voters can get randomly one of them from their election precinct or postal services. Thus, nobody knows the link between voter and her random number. For example, let's assume that HEB sends the predetermined random number in receipt code paper to the specific election precinct. Suppose that there exists about 100 voters at a region and therefore about 100 receipt code papers will exist. A voter can select randomly one of the papers. The probability of identifying the link between specific voter and specific random number will be about $\frac{1}{100}$ which is ignorable probability.
We highlight that the verification of the correctness of the system using the receipt code papers is not compulsory, about 5% of the voters will be sufficient in order to guarantee the correctness of the system. For example, voter who trusts the system can cast her vote without verification using the receipt code paper. On the other hand, one who does not trust the system may want to do this checking operation.

- **Bulletin Board (BB):** BB is online and is part of the verification mechanism. After the vote is arrived to the tallying process, the hash value is sent to the voter with SMS by BB. In order to protect coercion, voters are informed about their votes even if it is not counted. There may be some delay here since this process is done periodically. Moreover, voters can verify whether casted votes are passed all the encryption and masking processes over the system without alteration from the BB. That is, voter can check whether her vote is arrived to the tallying procedure. In the BB, the query is done by the hash value and ID number of the voter. When voter makes a query in the system and if any record is found, the record include hash value of the encrypted vote and a commitment of the voter's secret number. That is, the voter can see her ID number, the commitment of the secret number and hash value of the encrypted vote in the BB. Wrong information in the BB guarantees to the voter that at least one of the system component is compromised.
  Let's assume that there exists a coercer who can see the casted-votes in the BB. Here, there might be a possible attack scenario that any coercer can check the receipt codes of the voter from the BB one by one. To solve this problem, the voter casts all the candidates from the list. Therefore, if coercer wants to check from the BB, he will see all the possible voting cases, but he never learns which is the correct choice of the voter.

IV. The main protocol

A. General Structure

Voting system is based on web which can be in one of the portals of government. It is assumed that this portal is authenticating citizens by their electronic ID cards or by user ID and passwords. To sign the vote, every voter needs her ID card during the i-voting process since the private key is identified to the citizen's ID-Card. The corresponding public key with owner ID are sent to AB module in the system in order to verify the voter. Before the election, private and public key of the election is generated (one can use distributed key generation protocol where each party receives a share of the private key and all parties learn public key of the election [1]). Receipt code paper which consists of receipt codes (hash values of encrypted votes) of the all possible votes and used random number will be sent to the voter or to the election precinct in a independent safe channel at the same time. Voters who wish can do the offline checking operation by using receipt code paper. In order to protect voters from coercion we not only give opportunity to voters to cast their votes multiple times, but also we protect them by giving each voter a secret number n. This secret number and the commitment of it are sent to the voter with SMS. The commitment of the secret number is transported with other values while casting the vote. On the other hand, both commitment of secret number and ID number of each voter are given to C so that secret number is checked in the tallying process by C. If the entered secret number is correct the vote is tallied, if it is wrong, it is canceled.

B. Vote Submission

The voter casts her vote as follows: We are now ready to describe our vote submission and counting processes. The voter casts a vote v over a PC or a TC where she is authenticated with her electronic ID (e-ID) card. During the following procedures, you can derive benefit from diagram of our protocol in Figure 1 in Appendix.

- *Online process:*

1) Voter authenticates herself to the voting system using her ID card. She selects her candidate and inputs her secret number n.
2) First, computer encrypts vote $E(v,r) = (g^r, g^v h^r) = c$ where r is the random number, $h = g^x$ public key of the election and x is the private key of the election. In addition, it calculates hash of encrypted vote, $h := H(c)$, and signs this hash using the private key of voter, $Sign := Sign(h)$. Computer sends the sign, encrypted vote, users ID number, zero knowledge proof (ZK_{PC}) of it's own computation and commitment of secret number $(\alpha = commit(r,n))$ to AB.
   $PC \xrightarrow{Sign,c,ID,ZK_{PC},\alpha} AB.$
3) AB verifies $Sign \rightarrow c$ using the public key of the voter and check the proof ZK_{PC}. AB gives a unique number u to each vote so that the next module A can match vote pairs coming from AB and CB. It also adds a sequence number s to each voter's vote in order to determine the final vote in C. (Actually, this sequence number shows how many times does voter cast a vote).
4) AB sends the zero knowledge of it's own computations (ZK_{AB}), u, s and all the data received from PC except *Sign* to CB.
   $AB \xrightarrow{c,ID,ZK_{PC},ZK_{AB},\alpha,s,u} CB.$
5) CB checks the proofs ZK_{PC}, ZK_{AB}. It computes hash of encrypted vote and sends it to the V by using a safe

channel (like SMS). CB also sends this hash data to PC.
$CB \xrightarrow{h} V$ and PC.

6) The received hash value should be checked by PC. Moreover, voter has opportunity to check the received hash from her receipt code paper. By doing those controls the voter will be sure whether her vote is received by CB without any alteration or not. If the received hash value is true, it will be sure that the vote is transmitted by AB truly and the vote is valid; otherwise, she can see that whether her computer is compromised or any alteration is occurred in the system and the vote will be canceled.
7) If the vote is valid, AB and CB are masking the encrypted vote c with a_1, c^{a_1}, and a_2, c^{a_2}, respectively. These keys check that none of AB, CB and A produces any vote using the voters information. These masking operations also ensure that every vote pass over AB and CB. AB send the masked encrypted vote, bullet's unique number, bullet's sequence number, ZK_{AB} and the received data from PC except *Sign* and c to A.
$AB \xrightarrow{c^{a_1},ID,ZK_{PC},ZK_{AB},\alpha,s,u} A$
CB also sends the masked encrypted vote, zero knowledge proof of it's own computation (ZK_{CB}) and the received data from AB except c to A.
$CB \xrightarrow{c^{a_2},ID,ZK_{PC},ZK_{AB},ZK_{CB},\alpha,s,u} A$.
8) A matches vote pairs by the unique number u and multiplies the pair of masked encrypted votes coming from AB and CB.

$$c^{a_1} \cdot c^{a_2} = E(v^{a_1}; r \cdot a_1) \cdot E(v^{a_2}; r \cdot a_2) = E(v^{a_1+a_2}; r \cdot (a_1 + a_2)) = (g^r, g^v h^r)^{a_1+a_2} = c^{a_1+a_2}$$

9) A verifies the proofs ZK_{PC}, ZK_{AB} and ZK_{CB}. It stores all the received data in a database.

- *Offline process:*

10) The masked data $c^{a_1+a_2}$, ZK_A and received data except c^{a_1}, c^{a_2} and u are periodically offline exported to C.
$A \xrightarrow{c^{a_1+a_2},ID,ZK_{PC},ZK_{AB},ZK_{CB},ZK_A,\alpha,s} C$
11) C verifies the proofs ZK_{PC}, ZK_{AB}, ZK_{CB} and ZK_A and decrypts $c^{a_1+a_2}$ by using a_3.

$$(c^{a_1+a_2})^{a_3} mod\ p \rightarrow (c^{a_3^{-1}})^{a_3} = c\ mod\ p.$$

12) Next, C checks the commitment of the secret number, α; If it is correct, the vote is valid; otherwise, invalid.
13) For each vote, the value h is calculated by C and sent to the BB with voter's ID and α.
$C \xrightarrow{h,ID,\alpha} BB$
The data transfer from C to BB is done by using an external disc.

- *Online process:*

14) BB sends h to the voter by SMS in order to guarantee her vote comes to the counter process. Each voter can also check her vote whether her vote is in the BB. BB is listing all the votes (It is not matter whether if voter inputs right or wrong secret number to the system) cast by the voter with the commitment of the secret number. In BB, the query is done by the hash of the encrypted vote and ID number of the voter. Each voter expects hash of her encrypted vote in BB.

C. Counting Process

15) When the election is over, C permutes the list of valid final votes (votes received which have the greatest sequence number and correct secret number). By using the homomorphic property of ElGamal encryption, it gets l of them randomly (This limit is done because of the discrete logarithm problem) and multiply them:

$$E(v_1; r_1) * E(v_2; r_2) * \cdots * E(v_l; r_l) = E(v_1 + v_2 + \cdots + v_l; r_1 + r_2 + \cdots r_l)$$

16) The bunch votes are sent to DS which is far away from C by using a one way filter which does not let any traffic from DS to C. Thus, private key of the election is kept away from the encrypted votes.
$C \xrightarrow{E(v_1+v_2+\cdots+v_l;r_1+r_2+\cdots r_l)} DS$
17) At least t trusted parties in DS gather and decrypt the encrypted results:
DS has $D_x(E(v_1 + v_2 + \cdots + v_l; r_1 + r_2 + \cdots r_l)) = g^{v_1+v_2+\cdots+v_l}$.
18) Finally, election results will be announced.

V. Security Analysis

We now show that our protocol is secure by considering the correctness our system and privacy of voters in for each corrupted party.

Theorem V.1. *Our protocol is correct in the case that PC is corrupted.*

Proof: If PC is corrupted, it can either change the vote or the secret number. If the vote is changed, hash value of the encrypted vote will also be changed. However, the receipt code sent by CB can help the voter to detect whether her vote has been changed by PC. Furthermore, if secret number is changed, the voter can also detect this case during the search from BB using her ID. Namely, during the BB search, the voter can see her vote in two columns. First column will be the hash of her vote and the second one will be commitment of her secret number. Any alteration in this information shows that her vote has been compromised. ■

Theorem V.2. *Our protocol is correct in the case that AB is corrupted.*

Proof: A compromised AB can generate a vote on behalf of a voter. In that case, this fake vote is sent to CB. CB then sends a notification (e.g., SMS) to the voter. If a voter receives suddenly a SMS although she do not vote, the voter notice that there is an attack to the system and a fake vote is casted. Therefore, the notification sent by CB prevents a possible attack by AB. ■

Theorem V.3. *Our protocol is correct in the case that CB is corrupted.*

Proof: Assume that a corrupted CB generates a fake vote and masks it to send to A. A checks the unique number of generated-vote coming from AB. If there is no match, the generated-vote will be canceled. Masking process is performed to protect the system from a corrupted CB. Furthermore, ZK_{CB} proofs are also verified until the counting process. ■

Theorem V.4. *Our protocol is correct in the case that AB and CB are corrupted and cooperate.*

Proof: If AB and CB are compromised and cooperate, they generate a fake vote. Note that their fake generated-vote will be listed in BB. However, the voter notices the malicious cooperation since BB also sends the hash of encrypted vote via SMS to the voter. If a voter receives an SMS from BB where she do not vote, it shows that AB and CB are compromised. In our system, they can not obtain the private key of election and therefore, the attack will not successful. Furthermore, note that a_1 and a_2 are masking keys in the system. These keys verify that none of AB, CB and A produces any vote using the voters information. These masking operations also ensure that every votes pass over AB and CB. ■

Theorem V.5. *Our protocol is correct in the case that PC and BB are corrupted and cooperate.*

Proof: When PC and BB are compromised and cooperate they can agree on canceling the valid votes by changing secret numbers. Assume that PC changes the correct secret number, in this case the valid-vote will not be tallied, and BB shows the commitment of the correct secret number. Therefore, the voter cannot understand whether her vote is canceled. However, ZK-proofs protect the voter from these types of attack. Receipt freeness and privacy is also satisfied by the underlying additive homomorphic encryption method. In our system the votes are encrypted at the PC or TC and transported in encrypted form. After vote submission, voter can check hash of encrypted vote from the bulletin board. After votes have been tallied, in order to announce the results, only the result votes (homomorphically added version of l votes) are decrypted. Therefore, at each step there is no authority who can read the voter's will(privacy) and voter can not have chance to show his will to anybody(receipt freeness). ■

VI. COMPLEXITY

Our i-voting protocol contains sub-protocols between the components. To analyse the complexity of the system, all the sub-protocol steps should be examined separately. Assume that the order of cyclic group G is p, the number of submitted votes is n and the number of votes in a bunch is l. Also assume that all submitted votes are valid.

The complexity of each component: The computational cost of our protocol can be described as follows. Note that we only count the expensive asymmetric operations since symmetric encryptions and hash functions can be ignored.

- In PC; Vote is encrypted by using ElGamal encryption which costs 3 modular exponentiations and 1 modular multiplication for each submission. Each encrypted vote is hashed by a hash function which is a linear function. Hash value of the encrypted vote is signed with ElGamal which costs 1 modular exponentiation and 2 modular multiplications for each submission.
- In AB; Signature is verified, which costs 3 modular exponentiations. The encrypted vote is masked with a_1, which costs 1 modular exponentiation.
- In CB; Encrypted vote is hashed and masked with a_2, which costs 1 modular exponentiation.
- In A; For all vote pairs, 1 multiplication occurs since they are multiplied.
- In C; The masking process is repeated with a_3, which costs 1 modular exponentiation. Until this point, every multiplication and exponentiation occurs for each vote submission. After this point, l votes are grouped and multiplied which costs $(l-1)$ modular multiplications. This process is repeated $\frac{n}{l}$ times. It costs approximately n modular multiplications.
- In DS; The vote bunches are decrypted. In this part, there exists $\frac{n}{l}$ public key decryption. Each decryption process costs 1 modular exponentiation, 1 modular inversion and 1 modular multiplication.

As a result, for each submitted vote, 10 modular exponentiations and 4 modular multiplications are used in the encryption process. Also in counter process, n modular multiplications occur. Additionally, in decryption process, $\frac{n}{l}$ modular exponentiations, $\frac{n}{l}$ modular inversions and $\frac{n}{l}$ modular multiplications occur. We note that the complexities of the modular multiplication, inversion and exponentiation in Z_p are $O(log^2 p)$, $O(log^3 p)$ and $O(log^3 p)$, respectively. Therefore, time complexity of the system is approximately;

$$O((10n + \frac{2n}{l})log^3 p) + O((5n + \frac{n}{l})log^2 p) \approx O(n \cdot log^3 p)$$

Also in the system, 4 zero-knowledge proofs and 15 zero-knowledge proof verifications are used.

VII. CONCLUSION

Internet voting is a growing trend for the countries which are interested in increased voter participation both in the country and overseas. Estonia, Norway and France are a few practical examples that used Internet voting in real elections. In this paper, we construct a new and efficient end-2-end secure Internet voting system. In our protocol, by using the homomorphic property of ElGamal, we gathered, transported and tallied all votes in encrypted form so that no attacker has a chance to see the wish of people. Voters sign their votes by their private key and that made possible for the system to check whether if vote comes from the real voter or not. We prevent voters from coercion with the help of secret number generated before the elections. It is crucial to construct a voting system in which security, transparency, privacy and receipt freeness is satisfied.

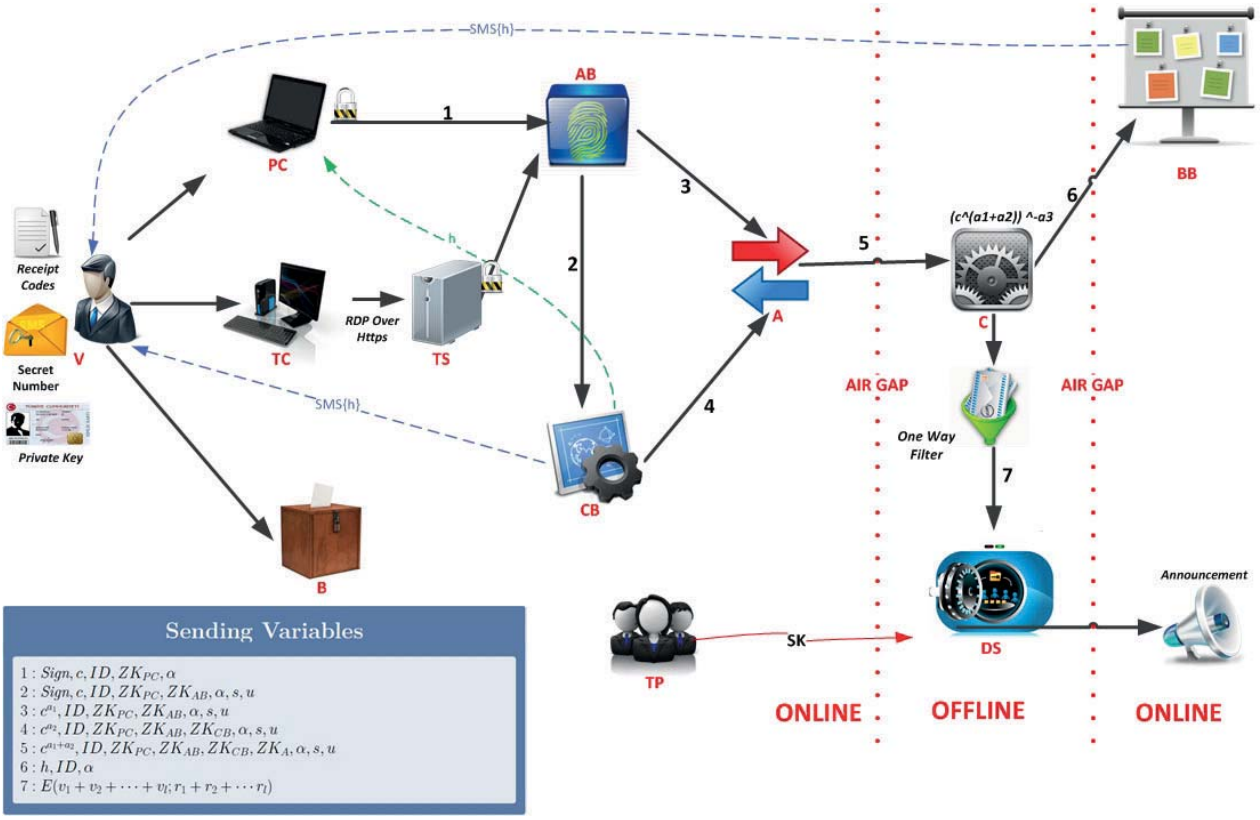


Fig. 1. Our Internet Voting Protocol.

ACKNOWLEDGMENT

Preliminary version of this study is presented as poster at CryptoDays conference, Tubitak, Turkey (June 2013).

APPENDIX

Our protocol is depicted in Figure 1.

REFERENCES

[1] Berry Schoenmakers, *Lecture Notes over Cryptographic Protocols*, Febr. 2013, http://www.win.tue.nl/ berry/2WC13/LectureNotes.pdf

[2] Felix Brandt, *Efficient Cryptographic Protocol Design Based on Distributed ElGamal Encryption*, Springer-Verlag, LNCS, Vol.3935, pp.32-47, 2006.

[3] Ivan Damgard, *Commitment Schemes and Zero-Knowledge Protocols*, Springer-Verlag, LNCS, Vol.1561, pp.63-86, 1999.

[4] Kristian Gjosteen, *Analysis of an Internet Voting Protocol*, March 9, 2010, http://eprint.iacr.org/2010/380.pdf

[5] Martin Hirt and Kazue Sako, *Efficient Receipt-Free Voting Based on Homomorphic Encryption*, Springer-Verlag, LNCS, Vol.1807, pp.539-556, 2000.

[6] Marianne Wiik Oberg, *Improving the Norvegian Internet Voting Protocol*, June 2011, http://daim.idi.ntnu.no/masteroppgaver/005/5823/

[7] Muhammed Ali Bingol and Fatih Birinci and Suleyman Kardas and Mehmet Sabir Kiraz, *Norwegian Internet Voting Protocol Revisited: Security and Privacy Enhancements*, International Conference BulCrypt, Sofia, Bulgaria, September 2012.

[8] P.L.Sven Heiberg and J. Willemson, *On Applying i-voting for Estonian Parliamentary elections*, Springer-Verlag, LNCS, Vol.7187, pp.208-223, 2012.

[9] Ran Canetti , Shafi Goldwasser, *An efficient threshold public key cryptosystem secure against adaptive chosen ciphertext attack*, Springer-Verlag, LNCS, Vol.1592, pp.90-106, 1999.

[10] Shai Halevi,*Efficient Commitment Schemes with Bounded Sender and Unbounded Receiver*, Springer-Verlag, LNCS, Vol.12, No.2, pp.77-89, 1999.

[11] S. Goldwasser, S. Micali and C. Rackoff, *The Knowledge Complexity of Interactive Proof Systems*, SIAM Journal on Computing, Vol.18, No.1, pp.186 - 208, 1989.

[12] T. ElGamal,*A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms*, IEEE Transactions on Information Theory, Vol.31, No.4, pp.469–472, 1985.

Some Observations on Distribution of Cross Correlation of Two Nonbinary Sequences

Ernist Tilenbaev, Hasan Dilek, Zülfükar Saygı and Çetin Ürtiş

***Abstract*—Let p be an odd prime, m an odd integer, $d = \frac{(p^m+1)^2}{2(p+1)}$ and $0 < l < (p^m+1)/2$. In this study we have considered cross correlation distribution of p-ary m-sequence $m(t)$, with period $p^{2m}-1$, and its decimated sequences $m(dt+l)$. In [1] authors had given possible values of cross correlation, as 9 different values for the case $p=3$ and 11 different values for the case $p>3$. For the case $p=3$, $m \leq 5$ and all possible values of l we have given complete distribution table and observed that there are 8 different values in total. Note that it was stated in [1], this distribution has at most 9 values, that is we observe that the candidate $-1+\frac{1+p}{2}p^m$ does not occur. Furthermore, for the case $p=3$, $m=3$ and $l=(p^m+1)/4$ we have observed that there are exactly 6 different values. In this case the distribution is different from the case $l=0$.**

***Index Terms*—nonbinary sequence, cross correlation, exponential sum, quadratic form, cross correlation distribution**

I. INTRODUCTION

Cross correlation and cross correlation distribution of p-ary m-sequence $m(t)$ and its decimated sequences $m(dt)$ or $m(dt+l)$, where $0 \leq l < (p^m+1)/2$ have been studied in [1], [2], [3], [5], [6], [7], [8] and [9]. In [2] cross correlation distribution of m-sequence $m(t)$ and its decimated sequence $m(dt+l)$ have been studied, where $d = \frac{(p^m+1)^2}{2(p^k+1)}$ and $l=0$. In this study we have considered the cross correlation distribution of m-sequence $m(t)$ and its decimated sequences $m(dt+l)$, where $d = \frac{(p^m+1)^2}{2(p+1)}$ and $0 < l < (p^m+1)/2$. Using the same techniques in [3] and [2] we have evaluated some moment identities. Also numerical results indicate that there are 8 distinct values for $p=3$ and 9 distinct values for $p>3$.

The main goal of this study is to derive to complete distribution of correlation values for all odd primes p and all values of $l \neq 0$.

II. PRELIMINARIES

In this section we will give some notations and useful results which was obtained in [1] and [2]. The following notations will be fixed except for specific statements.

- Let p be an odd prime.
- Let m be an odd integer, $n=2m$ and $d = \frac{(p^m+1)^2}{2(p+1)}$.
- Let $\mathbb{F}_{p^n}$ be finite field of order p^n.
- Let α be a primitive element of $\mathbb{F}_{p^n}$.
- Let $\mathrm{Tr}_j^i : \mathbb{F}_{p^i} \to \mathbb{F}_{p^j}$ be the trace mapping for $j \mid i$.
- Let $\omega = \exp\left(2\pi\sqrt{-1}/p\right)$ be the primitive p^{th} root of unity.
- Let $\chi(x) = \omega^{\mathrm{Tr}_p^{p^n}(x)}$ for $x \in \mathbb{F}_{p^n}$ be an additive character.

From [2] we know the following identities,

- $\gcd(p^n-1, d) = \frac{p^m+1}{2}$.
- $d\left(p^{m+1}+1\right) \equiv p^m+1 \pmod{p^n-1}$. (It follows from the fact that $\frac{p(p^m+1)+p+1}{p+1}$ is an even integer and $d\left(p^{m+1}+1\right) = (p^n-1)\frac{p(p^m+1)+p+1}{p+1} + p^m + 1$).

Lemma 1: [10] Assume that $f \mid p^m+1$ and $a \in \mathbb{F}_{p^n}^*$. Then we have

$$\sum_{x \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_1^n(ax^f)} = \begin{cases} (f-1)p^m, & \text{if } a = \alpha^{h+jf} \text{ for some integer } j \\ -p^m, & \text{otherwise.} \end{cases}$$

where $h=0$ if $\frac{p^m+1}{f}$ is even and $h = \frac{f}{2}$ otherwise.

Definition 2: Let (a_t) and (b_t) be two p-ary sequences of period p^n. The cross correlation between the sequences at shift τ, $0 \leq \tau < p^n-1$, is defined by

$$C_{a,b}(\tau) = \sum_{t=0}^{p^n-2} \omega^{a_{t+\tau}-b_t}.$$

p-ary m-sequence $m(t)$ with the period p^n-1 can be expresed as

$$m(t) = \mathrm{Tr}_1^n\left(\alpha^t\right).$$

Since $\gcd(p^n-1, d) = \frac{p^m+1}{2}$, there are $\frac{p^m+1}{2}$ distinct decimated sequences $m(dt+l)$ of period $2(p^m-1)$ for $0 \leq l < \frac{p^m+1}{2}$, which are defined as

$$m(dt+l) = \mathrm{Tr}_1^n\left(\alpha^{dt+l}\right).$$

E.Tilenbaev, Department of Mathematics, TOBB University of Economics and Technology, Ankara
H.Dilek, Department of Mathematics, TOBB University of Economics and Technology, Ankara
Z.Saygı, Department of Mathematics, TOBB University of Economics and Technology, Ankara
Ç.Ürtiş, Department of Mathematics, TOBB University of Economics and Technology, Ankara

The cross-correlation $C_l(\tau)$ between $m(t)$ and $m(dt+l)$ is

$$\begin{aligned} C_l(\tau) &= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau)-m(dt+l)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{Tr}_1^n\left(\alpha^{t+\tau}-\alpha^{dt+l}\right)} \\ &= \sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}_1^n\left(ax-bx^d\right)} \\ &= \sum_{x\in\mathbb{F}_{p^n}^*} \chi\left(ax-bx^d\right) \\ &= C(a,b)-1 \end{aligned} \tag{II.1}$$

where $a=\alpha^\tau$, $b=\alpha^l$ and $C(a,b)=\sum_{x\in\mathbb{F}_{p^n}}\chi\left(ax-bx^d\right)$.

We aim to find the distribution of $C_l(\tau)$ as $0\le\tau<p^n-1$ varies, by II.1 finding distribution of $C(a,b)$ as $a\in\mathbb{F}_{p^n}^*$ varies is the same.

Lemma 3: [1] The possible values of $C_l(\tau)$ are given as follows:

1) For $p=3$ there are 9 possible values in total,

$$\{-1,-1\pm p^m,\ -1\pm\frac{1+i\sqrt{p}}{2}p^m, -1\pm\frac{1-i\sqrt{p}}{2}p^m,-1\pm\frac{1+p}{2}p^m\Big\}.$$

2) For $p\equiv 3\pmod 4\ (\neq 3)$ there are 11 possible values in total,

$$\Big\{-1,-1\pm p^m,-1\pm\frac{1+i\sqrt{p}}{2}p^m,-1\pm\frac{1-i\sqrt{p}}{2}p^m, -1\pm\frac{1+p}{2}p^m,-1\pm\frac{1-p}{2}p^m\Big\}.$$

3) For $p\equiv 1\pmod 4$ there are 11 possible values in total,

$$\Big\{-1,-1\pm p^m,-1\pm\frac{1+\sqrt{p}}{2}p^m,-1\pm\frac{1-\sqrt{p}}{2}p^m, -1\pm\frac{1+p}{2}p^m,-1\pm\frac{1-p}{2}p^m\Big\}.$$

Exactly half of the elements of $\mathbb{F}_{p^n}^*$ are squares and the other half are nonsquares. Using $\gcd\left(p^{m+1}+1,p^m-1\right)=\gcd\left(p^{m+1}+1,p^n-1\right)=2$ and $p^{m+1}+1\equiv 2\pmod 4$, we have $\gcd\left(p^{m+1}+1,p^n-1\right)=2$. Thus square elements in $\mathbb{F}_{p^n}^*$ can be represented as $x=y^{p^{m+1}+1}$ and nonsquares as $x=ry^{p^{m+1}+1}$, where $y\in\mathbb{F}_{p^n}^*$ and r is a nonsquare in $\mathbb{F}_{p^n}^*$. Note that as y runs through $\mathbb{F}_{p^n}^*$, each $x\in\mathbb{F}_{p^n}^*$, either a square or a nonsquare appears twice. Hence $C(a,b)$ can be expressed as

$$\begin{aligned} 2C(a,b) &= \sum_{y\in\mathbb{F}_{p^n}}\chi\left(ay^{p^{m+1}+1}-by^{d\left(p^{m+1}+1\right)}\right) \\ &\quad+\sum_{y\in\mathbb{F}_{p^n}}\chi\left(ary^{p^{m+1}+1}-br^dy^{d\left(p^{m+1}+1\right)}\right) \\ &= \sum_{y\in\mathbb{F}_{p^n}}\chi\left(ay^{p^{m+1}+1}-by^{p^m+1}\right) \\ &\quad+\sum_{y\in\mathbb{F}_{p^n}}\chi\left(ary^{p^{m+1}+1}-br^dy^{p^m+1}\right) \\ &= T(a,b)+T\left(ar,br^d\right) \end{aligned}$$

where $T(a,b)=\sum_{y\in\mathbb{F}_{p^n}}\chi\left(ay^{p^{m+1}+1}-by^{p^m+1}\right)$.

III. RESULTS

Using similar techniques as in [1], [2] and [3] we have derived the following moment identities.

Lemma 4: The following identities hold:

i) $\sum_{a\in\mathbb{F}_{p^n}}C(a,b)=p^n$.

ii) $\sum_{a\in\mathbb{F}_{p^n}}C^2(a,b)=\begin{cases}p^nN, \text{ if } p\equiv 3\pmod 4\\ p^{2n}, \text{ if } p\equiv 1\pmod 4.\end{cases}$
where $N=\begin{cases}\frac{\left(p^n-p^m\right)}{2}, \text{ if } -2b=\alpha^{\frac{p^m+1}{2}j} \text{ for } j\in\mathbb{Z}\\ -p^m, \text{ otherwise.}\end{cases}$

iii) $\sum_{a\in\mathbb{F}_{p^n}}T(a,b)=q$.

iv) $\sum_{a\in\mathbb{F}_{p^n}}T^2(a,b)=\begin{cases}p^{2n}, & \text{if } p\equiv 1\pmod 4\\ p^nN_2 & \text{if } p\equiv 3\pmod 4\end{cases}$
where
$$N_2=\begin{cases}p^n, \text{ if } -2b=\alpha^{\frac{p^m+1}{2}+j\left(p^m+1\right)}, j\in\mathbb{Z}\\ -p^m, \text{ otherwise.}\end{cases}$$

Proof:

i)
$$\begin{aligned}\sum_{a\in\mathbb{F}_{p^n}}C(a,b) &= \sum_{a\in\mathbb{F}_{p^n}}\sum_{x\in\mathbb{F}_{p^n}}\chi\left(ax-bx^d\right)\\ &= \sum_{x\in\mathbb{F}_{p^n}}\chi\left(-bx^d\right)\sum_{a\in\mathbb{F}_{p^n}}\chi(ax)\\ &= p^n\end{aligned}$$
where $\sum_{a\in\mathbb{F}_{p^n}}\chi(ax)=\begin{cases}p^n, \text{ if } x=0\\ 0, \text{ if } x\neq 0.\end{cases}$

ii) Since d is odd when $p\equiv 1\pmod 4$ and even when $p\equiv 3\pmod 4$, we have

$$\begin{aligned}&\sum_{a\in\mathbb{F}_{p^n}}C^2(a,b)\\ &=\sum_{a\in\mathbb{F}_{p^n}}\sum_{x\in\mathbb{F}_{p^n}}\chi\left(ax-bx^d\right)\sum_{y\in\mathbb{F}_{p^n}}\chi\left(ay-by^d\right)\\ &=\sum_{x,y\in\mathbb{F}_{p^n}}\chi\left(-b\left(x^d+y^d\right)\right)\sum_{a\in\mathbb{F}_{p^n}}\chi\left(a\left(x+y\right)\right)\\ &=p^n\sum_{x\in\mathbb{F}_{p^n}}\chi\left(-b\left(x^d+(-x)^d\right)\right)\\ &=\begin{cases}p^{2n}, & \text{if } p\equiv 1\pmod 4\\ p^nN & \text{if } p\equiv 3\pmod 4\end{cases}\end{aligned}$$

where,

$$N = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^d\right)$$
$$= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{\frac{p^m+1}{2}}\right)$$
$$= \frac{1}{2}\sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{p^m+1}\right) + \frac{1}{2}\sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2br^{\frac{p^m+1}{2}}x^{p^m+1}\right)$$
$$= \begin{cases} \frac{1}{2}\left(p^n - p^m\right) & \text{if } -2b = \alpha^{\frac{p^m+1}{2}j} \text{ for } j\in\mathbb{Z} \\ -p^m & \text{otherwise} \end{cases}$$

with r being nonsquare. Also note that $\sum_{a\in\mathbb{F}_{p^n}} \chi\left(a\left(x+y\right)\right) = \begin{cases} p^n, \text{ if } x+y=0 \\ 0, \text{ if } x+y\neq 0. \end{cases}$

iii) $\sum_{a\in\mathbb{F}_{p^n}} T\left(a,b\right)$

$$= \sum_{a,x\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1} - bx^{p^m+1}\right)$$
$$= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-bx^{p^m+1}\right) \sum_{a\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1}\right)$$
$$= p^n.$$

iv) $\sum_{a\in\mathbb{F}_{p^n}} T^2\left(a,b\right)$

$$= \sum_{a,x,y\in\mathbb{F}_{p^n}} \chi\left(a\cdot g\left(x,y\right) - b\left(x^{p^m+1}+y^{p^m+1}\right)\right)$$
$$= \sum_{x,y\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right) \cdot \sum_{a\in\mathbb{F}_{p^n}} \chi\left(a\left(g\left(x,y\right)\right)\right)$$
$$= p^n \cdot \left(\sum_{\left\{\substack{x,y\in\mathbb{F}_{p^n},\\ g(x,y)=0}\right\}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right)\right)$$
$$= p^n \sum_{\left\{\substack{x,y\in\mathbb{F}_{p^n},\\ x^2+y^2=0}\right\}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right)$$
$$= p^n \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+\left(-x^2\right)^{\frac{p^m+1}{2}}\right)\right)$$
$$= p^n \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+(-1)^{\frac{p^m+1}{2}}x^{p^m+1}\right)\right)$$
$$= \begin{cases} p^{2n}, & \text{if } p\equiv 1 \pmod 4 \\ p^n N_2 & \text{if } p\equiv 3 \pmod 4 \end{cases}$$

where $g\left(x,y\right) = x^{p^{m+1}+1} + y^{p^{m+1}+1}$ and

$$N_2 = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{p^m+1}\right)$$
$$= \begin{cases} p^n, \text{ if } -2b = \alpha^{\frac{p^m+1}{2}+j(p^m+1)}, \ j\in\mathbb{Z} \\ -p^m, \text{ otherwise} \end{cases}$$

by Lemma 1.

■

Note that the above identities will be usefull in finding the cross correlation distribution for all values of $l\neq 0$. But they are not sufficient.

IV. EXPERIMENTAL RESULTS

As we stated before, in [1] all possible values of cross correlation between p-ary m-sequence $m\left(t\right)$ and its decimated sequences $m\left(dt+l\right)$ have been given. Where for the case $p=3$ there are 9 and for the case $p>3$ there are 11 possible values in total. But the exact distribution was not given in [1]. In our numerical results for the case $p=3$, $m\leq 5$ and all possible values of l we have observed that there are at most 8 different values. Here we see that the value $C_l\left(\tau\right) = -1+\frac{1+p}{2}p^m$ that was stated in [1] (which we present in Lemma 3) does not occur. For the general case, i.e. $m>5$ it has to be proved. Furthermore, for the case $p=3$, $m=3$ and $l=\left(p^m+1\right)/4$ we have observed that there are exactly 6 different values with distribution being different from the case $l=0$. Note that the case $l=0$ and $p\equiv 3\left(\mathrm{mod}\,4\right)$ was proved in [2] and the case $l=0$ and $p\equiv 1\left(\mathrm{mod}\,4\right)$ was proved in [4].

Computations of this paper were performed in High Performance and Grid Computing Center (TÜBİTAK) by using SAGE program. These codes are partially available online at `www.etilenbaev.etu.edu.tr` . Complexity of a code that computes distribution of $C_l\left(\tau\right)$ for fixed l as τ varies is $O\left(p^{2n}\right)$. Running time for the case $p=3, m=5$ is approximately 2 weeks, while for the case $p=5, m=3$ it took approximately 4 days.

Example 5: When $p=3$, $m=1$ and $0\leq l<\left(p^m+1\right)/2$ complete distribution of cross correlation between m-sequence $m\left(t\right)$ and its decimated sequences $m\left(dt+l\right)$ are given as follows,

	l=0	l=1
$C_l\left(\tau\right)$ values	#$C_l\left(\tau\right)$	#$C_l\left(\tau\right)$
$-1+p^m$	4	4
$-1-\frac{1+i\sqrt{p}}{2}p^m$	2	4
$-1-\frac{1-i\sqrt{p}}{2}p^m$	2	-

Example 6: When $p=3$, $m=3$ and $0\leq l<\left(p^m+1\right)/2$ complete distribution of cross correlation between m-sequence $m\left(t\right)$ and its decimated sequences $m\left(dt+l\right)$ are given as follows. Here we point out the case $l=\left(p^m+1\right)/4=7$,

which is 6 valued.

	$l=0$	l=1,2,3,4, 5,6,8,9,10, 11,12,13	$l=7$
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	252	84	-
$-1+p^m$	196	84	168
$-1-p^m$	-	28	56
$-1+\frac{1-i\sqrt{p}}{2}p^m$	-	140	84
$-1+\frac{1+i\sqrt{p}}{2}p^m$	-	140	84
$-1-\frac{1-i\sqrt{p}}{2}p^m$	126	112	168
$-1-\frac{1+i\sqrt{p}}{2}p^m$	126	112	168
$-1-\frac{1+p}{2}p^m$	28	28	-

Example 7: When $p=3$, $m=5$ and $0 \le l < (p^m+1)/2$ complete distribution of cross correlation between m-sequence $m(t)$ and its decimated sequences $m(dt+l)$ are given as follows,

	$l=0$	l=1,2,3,5,6,9,10,13, 15,18,20,26,27,30, 32,34,39,40,41,44, 45,52,54,58,60,62, 64,68,70,77,78,81, 82,83,88,90,92,95, 96,102,104,107,109, 112,113,116,117, 119,120,121
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	21960	6588
$-1+p^m$	14884	8052
$-1-p^m$	-	2684
$-1+\frac{1-i\sqrt{p}}{2}p^m$	-	9516
$-1+\frac{1+i\sqrt{p}}{2}p^m$	-	9516
$-1-\frac{1-i\sqrt{p}}{2}p^m$	9882	10248
$-1-\frac{1+i\sqrt{p}}{2}p^m$	9882	10248
$-1-\frac{1+p}{2}p^m$	2440	2196

	l=8,11,17,19,23,24, 25,28,29,31,33,35, 37,38,47,49,50,51, 53,57,65,69,71,73, 75,84,85,87,89,91, 93,94,97,98,99, 103,105,111,114	l=4,7,12,14,16, 21,22,36,42,43, 46,48,55,56,59, 61,63,66,67,74, 76,79,80,86,100, 101,106,108, 110,115,118
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	8052	7320
$-1+p^m$	6588	7320
$-1-p^m$	2196	2440
$-1+\frac{1-i\sqrt{p}}{2}p^m$	10492	10004
$-1+\frac{1+i\sqrt{p}}{2}p^m$	10492	10004
$-1-\frac{1-i\sqrt{p}}{2}p^m$	9272	9760
$-1-\frac{1+i\sqrt{p}}{2}p^m$	9272	9760
$-1-\frac{1+p}{2}p^m$	2684	2440

Example 8: When $p=5$, $m=1$ and $0 \le l < (p^m+1)/2$ complete distribution of cross correlation between m-sequence $m(t)$ and its decimated sequences $m(dt+l)$ are given as follows,

	$l=0$	l=1,2
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	6	6
$-1+p^m$	6	–
$-1-p^m$	6	6
$-1+\frac{1-\sqrt{p}}{2}p^m$	3	3
$-1+\frac{1+\sqrt{p}}{2}p^m$	3	3
$-1-\frac{1-\sqrt{p}}{2}p^m$	–	112
$-1-\frac{1+\sqrt{p}}{2}p^m$	–	112
$-1-\frac{1+p}{2}p^m$	–	–

Example 9: When $p=5$, $m=3$ and $0 \le l < (p^m+1)/2$ complete distribution of cross correlation between m-sequence $m(t)$ and its decimated sequences $m(dt+l)$ are given as follows,

	$l=0$	l=1,5,16,17,22, 25,38,41,46,47, 58,62
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	5796	4536
$-1+p^m$	2646	2520
$-1-p^m$	3906	2016
$-1-\frac{1-\sqrt{p}}{2}p^m$	–	1449
$-1-\frac{1+\sqrt{p}}{2}p^m$	–	1449
$-1+\frac{1-\sqrt{p}}{2}p^m$	1575	1701
$-1+\frac{1+\sqrt{p}}{2}p^m$	1575	1701
$-1+\frac{1-p}{2}p^m$	126	126
$-1-\frac{1+p}{2}p^m$	–	126

	l=3,7,12,14,15,28, 35,48,49,51,56,60	l=4,20,26,37, 43,59
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	4536	4536
$-1+p^m$	2772	2898
$-1-p^m$	1764	1638
$-1-\frac{1-\sqrt{p}}{2}p^m$	1701	1827
$-1-\frac{1+\sqrt{p}}{2}p^m$	1701	1827
$-1+\frac{1-\sqrt{p}}{2}p^m$	1449	1323
$-1+\frac{1+\sqrt{p}}{2}p^m$	1449	1323
$-1+\frac{1-p}{2}p^m$	126	126
$-1-\frac{1+p}{2}p^m$	126	126

	l=8,11,23,40,52,55	l=21,42
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	4536	4536
$-1+p^m$	2646	2268
$-1-p^m$	1890	2268
$-1-\frac{1-\sqrt{p}}{2}p^m$	1575	1197
$-1-\frac{1+\sqrt{p}}{2}p^m$	1575	1197
$-1+\frac{1-\sqrt{p}}{2}p^m$	1575	1953
$-1+\frac{1+\sqrt{p}}{2}p^m$	1575	1953
$-1+\frac{1-p}{2}p^m$	126	126
$-1-\frac{1+p}{2}p^m$	126	126

	l=9,18,22,27, 36,45,54	l=19,29,31,32, 34,44
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	5166	5166
$-1+p^m$	2520	2016
$-1-p^m$	1386	1890
$-1-\frac{1-\sqrt{p}}{2}p^m$	1701	1197
$-1-\frac{1+\sqrt{p}}{2}p^m$	1701	1197
$-1+\frac{1-\sqrt{p}}{2}p^m$	1449	1953
$-1+\frac{1+\sqrt{p}}{2}p^m$	1449	1953
$-1+\frac{1-p}{2}p^m$	–	–
$-1-\frac{1+p}{2}p^m$	252	252

	l=6,24,30,33, 39,57	l=2,13,10,50, 53,61
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	5166	5166
$-1+p^m$	2520	2016
$-1-p^m$	1386	1890
$-1-\frac{1-\sqrt{p}}{2}p^m$	1701	1197
$-1-\frac{1+\sqrt{p}}{2}p^m$	1701	1197
$-1+\frac{1-\sqrt{p}}{2}p^m$	1449	1953
$-1+\frac{1+\sqrt{p}}{2}p^m$	1449	1953
$-1+\frac{1-p}{2}p^m$	–	–
$-1-\frac{1+p}{2}p^m$	252	252

V. CONCLUSION

In conclusion, we have observed from the numerical data that for the case $p=3$ there are 8 different possible values when $l \neq 0, (p^m+1)/4$, which has to be proved, and 6 different values of cross correlation occurs when $l=(p^m+1)/4$. Using similar techniques as in [2], [3] we have computed some moment identites. Using additional equations one can compute the distribution of cross correlation for the case $p=3$, $l=(p^m+1)/4$ and a harder problem which is the case $p=3$, $l \neq 0, (p^m+1)/4$, which we leave as a future work.

ACKNOWLEDGMENTS

The authors thank the anonymous referees for their helpful comments. The numerical calculations reported in this paper were performed at TUBITAK ULAKBIM, High Performance and Grid Computing Center (TRUBA Resources). Also the second and the third authors were partially supported by TÜBİTAK under grant no.: TBAG-109T344.

REFERENCES

[1] S.T. Choi, T. Lim, J.S. No and H. Chung, On the cross-correlation of a p-ary m-sequence of period $p^{2m}-1$ and its decimated sequences by $(p^m+1)^2/2(p+1)$, IEEE Trans. Inf. Theory, vol. 58, no. 3, March 2012.

[2] J. Luo, T. Helleseth and A. Kholosha, Two nonbinary sequences with six-valued cross correlation, Proceedings of IWSDA 2011.

[3] E.Y. Seo, Y.S. Kim, J.S. No and D.J. Shin, Cross-correlation distribution of p-ary m-sequences of period p^{4k-1} and its decimated sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$, IEEE Trans. Inf. Theory, vol. 54, no. 7, July 2008.

[4] Y.Sun, H.Li and Z.Wang, The cross-correlation distribution of a p-ary m-sequence of period $p^{2m}-1$ and its decimation by $\frac{(p^m+1)^2}{2(p^e+1)}$ [Online]. Available: http://arxiv.org/abs/1111.3477v1 .

[5] T.Helleseth, L.Hu, A.Kholosha, X.Zeng, N.Li and W.Jiang, Period-different m-sequences with at most four-valued cross correlation, IEEE Trans. Inf. Theory, vol. 55, no. 7, July 2009.

[6] G.J.Ness and T.Helleseth, Cross correlation of m-sequences of different length, IEEE Trans. Inf. Theory, vol. 52, no. 4, April 2006.

[7] T.Helleseth, A.Kholosha and A.Johanssen, m-Sequences of different lengths with four-valued cross correlation, ISIT, July 2008.

[8] A.Johanssen, T.Helleseth and A.Kholosha, Further results on m-sequences with five-valued cross correlation, IEEE Trans. Inf. Theory, vol. 55, no. 12, December 2009.

[9] T.Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math. 16, 209-232, 1976.

[10] R.Lidl and H.Niederreiter, Finite Fields. Cambridge University Press, 1997.

Period Analysis of Pseudorandom Vector Sequences With Dynamical Polynomial Systems

Pınar Balıkçıoğlu, and Melek D. Yücel

***Abstract*—We examine the method of pseudorandom vector sequence generation proposed by Ostafe and Shparlinski, for the three choices of polynomials given by the same authors. We obtain the period distribution of the generated vector sequences for prime fields up to 13 elements and vector sizes of 2 or 3; and observe that the probability of attaining a maximum-period sequence is extremely low.**

***Index Terms*—Nonlinear pseudorandom number generators, pseudorandom vector sequences, triangular polynomial systems, period distribution**

I. Introduction

A CLASSICAL and still very popular method for the generation of uniform pseudorandom number is the linear congruential method introduced by Lehmer [1] in 1951. Unfortunately, in cryptographic settings, such linear generators have been successfully attacked. Ostafe and Shparlinski have been inspired by Lehmer's recursion in their proposal [2], for generating pseudorandom vector sequences. They study a class of dynamical systems generated by iterations of multivariate polynomials and estimate the degree growth of these iterations in [2], [3], [4] and [6]. In [5], they use this construction and design a new class of hash functions. In [7], they study the period of vector sequences generated by triangular polynomial systems and propose a method of generating maximum-period vector sequences. Our aim in this work is to analyse the distribution of the periods of the vector sequences generated by Ostafe and Shparlinski's method, which is described as follows: Let p be a prime and $F_1, ..., F_m \in \mathrm{F}_p[X_1, ..., X_m]$ be m polynomials in m variables over a finite field of p elements. For each $i = 1, ..., m$, the k-th iteration of the polynomial F_i is defined by the recurrence relation,

$$f_i^{(k+1)} = F_i(f_1^{(k)}, ..., f_m^{(k)}), \forall\ k$$

where

$$f_i^{(0)} = X_i. \tag{1}$$

To simplify the notation, one can define a vector $\mathbf{f}^{(k)} = (f_1^{(k)}, ..., f_m^{(k)}) \in \mathrm{F}_p$, $\mathbf{F} = (F_1, ..., F_m) \in \mathrm{F}_p{}^m\ [X_1, ..., X_m]$ and the recurrence relation given by (1) becomes

$$\mathbf{f}^{(k+1)} = \mathbf{F}(\mathbf{f}^{(k)})\ \forall\ k. \tag{2}$$

In particular, for any $k, n \geq 0$ and $i = 0, 1, ..., m$

$$f_i^{(k+n)} = F_i^{(k)}(\mathbf{f}^{(n)}) = F_i^{(k+n)}(\mathbf{f}^{(0)})$$

and

$$f^{(k+n)} = F^{(k)}(\mathbf{f}^{(n)}) = F^{(k+n)}(\mathbf{f}^{(0)}).$$

It is clear that the above vector sequence of vectors $f^{(k)}$ is eventually periodic with some period $\tau \leq p^m$ since we work over a finite field of p elements. On the other hand, one can assume that the vector sequence is purely periodic with period τ, that is,

$$f^{(k+\tau)} = f^{(k)}, \forall\ k.$$

In the series of papers [2]-[7] multivariate polynomial systems $F_1, ..., F_m$ of m polynomials in m variables over a finite field F_p are described in terms of the first iteration of (2), where the initial condition vector $\mathbf{f}^{(0)}$ is chosen as $\mathbf{X} = (X_1, ..., X_m)$ and the first iteration results $\mathbf{f}^{(1)} = (F_1(\mathbf{X}), ..., F_m(\mathbf{X}))$ are found as

$$F_1(\mathbf{X}) = X_1G_1(X_2, ..., X_m) + H_1(X_2, ..., X_m),$$
$$\vdots$$
$$F_{m-1}(\mathbf{X}) = X_{m-1}G_{m-1}(X_m) + H_{m-1}(X_m),$$
$$F_m(\mathbf{X}) = g_mX_m + h_m,$$

with,

$$G_i, H_i \in F_p[X_{i+1}, ..., X_m],\ i = 1, ..., m-1$$

Pınar Balıkçıoğlu is with the Cryptography Department, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey. (pinargurkan82@gmail.com).

Melek D. Yücel is with the Cryptography Department, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey. (melekdy@metu.edu.tr).

and

$$g_i, h_i \in F_p, g_m \neq 0, \quad (3)$$

and the following iteration proceeds by substituting the obtained vector $\mathbf{f}^{(1)} = \mathbf{F}(\mathbf{X})$ instead of $\mathbf{X}$ in (3). The structure of the polynomial description given by (3) is called the 'triangular form', because it defines the first polynomial F_1 as a function of all the elements of $\mathbf{X}$, whereas the last polynomial F_m depends on a single element X_m of $\mathbf{X}$. In order to obtain very fast pseudorandom generators, some choices for the polynomials G_i and H_i are proposed by Ostafe and Shparlinski in [2], [3] and [6], which are summarized in Table I.

TABLE I
POLYNOMIAL CHOICES PROPOSED BY OSTAFE AND SHAPARLINSKI

Choice 1 in [2]: $G_i(X_{i+1},...,X_m) = X_{i+1}$ and $H_i(X_{i+1},...,X_m) = h_i$
Choice 2 in [3]: $G_i(X_{i+1},...,X_m) = X_{i+1}^2 - a_i$ for some quadratic nonresidues a_i and $H_i(X_{i+1},...,X_m) = h_i$
Choice 3 in [6]: $G_i(X_{i+1},...,X_m) = g_i,\ g_i \notin \{0,1\}$ and $H_i(X_{i+1},...,X_m) = h_i$

TABLE II
SIZE OF PARAMETER SETS

Choice	1	2	3
$\mathbf{X_i}$	p^m	p^m	p^m
$\mathbf{g_i}$	–	–	$(p-2)^{m-1}$
$\mathbf{h_i}$	p^{m-1}	–	p^{m-1}
$\mathbf{a_i}$	–	$\bar{Q}_p^{m-1}$	–
$\mathbf{g_m}$	$p-1$	$p-1$	$p-1$
$\mathbf{h_m}$	p	p	p

II. PERIOD ANALYSIS OF GENERATED VECTOR SEQUENCES

A. Exhaustive Search for 8 Cases

Our aim is to investigate the period distribution of the vector sequences generated by (3) for the three choices of the polynomials given in Table I.

TABLE III
NUMBER OF POSSIBLE VECTOR SEQUENCES

Choice	Number of Total Vector Sequences
1	$(p-1)(p^{2m})$
2	$\bar{Q}_p^{m-1}(p-1)(p^{m+1})$
3	$(p-2)^{(m-1)}(p-1)(p^{2m})$

In order to perform an exhaustive search over all possible vector sequences, one needs to know the size of the parameter
sets. Table II shows the size of the paramater sets and Table III depicts the number of possible vector sequences. We consider 8 cases, corresponding to relatively small values of the field size p, and the vector size m (p = 3, 5, 7, 11, 13 with m = 2, and p = 3, 5, 7 with m = 3). Description of these 8 cases is given in Table IV and total numbers of possible vector sequences are shown in Table V.

B. Period Distributions

We generate all vector sequences for the 8 cases given in Table IV by Ostafe and Shparlinski's method [2], using the three polynomial choices shown in Table I. Corresponding period distributions are sketched in Fig. 1 to Fig. 8 for the three choices. In all figures, we indicate the period distribution corresponding to Choice 1 by blue, Choice 2 by red and Choice 3 by green bars. As can be observed from Fig. 1 to Fig.
8, Choice 1 and Choice 3 do not produce any maximum-period ($T = p^m$) sequence for the considered cases (p = 3, 5, 7 with m = 2, 3 and p = 11, 13 with m = 2).

TABLE IV
PARAMETERS OF THE EIGHT CASES USED IN THIS WORK

Case	p	m
1	3	2
2	3	3
3	5	2
4	5	3
5	7	2
6	7	3
7	11	2
8	13	2

TABLE V
NUMBER OF POSSIBLE VECTOR SEQUENCES FOR THE EIGHT CASES

Case	Choice 1	Choice 2	Choice 3
1	162	162	162
2	1458	1458	1458
3	2500	5000	7500
4	62500	25000	562500
5	14406	43218	72030
6	705894	6353046	17647350
7	146410	732050	1317690
8	342732	2056392	377052

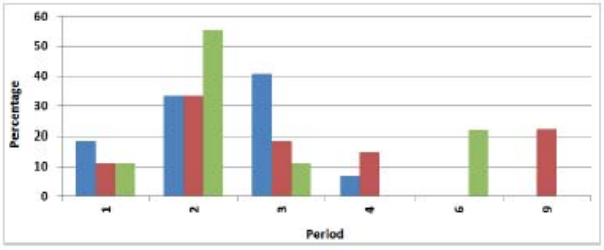


Fig. 1. Period distributions of Choice 1 (blue), Choice 2 (red), Choice 3 (green) (p=3, m=2)

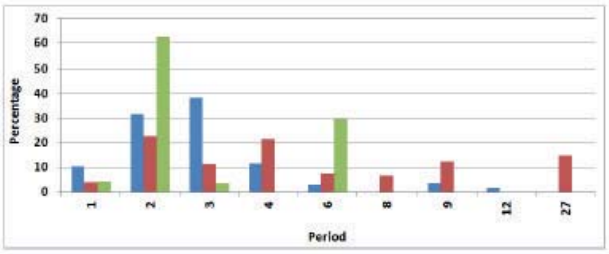


Fig. 2. Period distributions of Choice 1 (blue), Choice 2 (red), Choice 3 (green) (p=3, m=3)

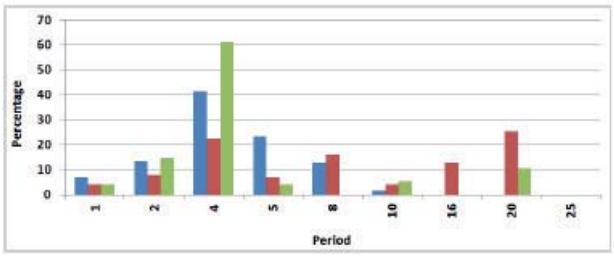


Fig. 3. Period distributions of Choice 1 (blue), Choice 2 (red), Choice 3 (green) (p=5, m=2)

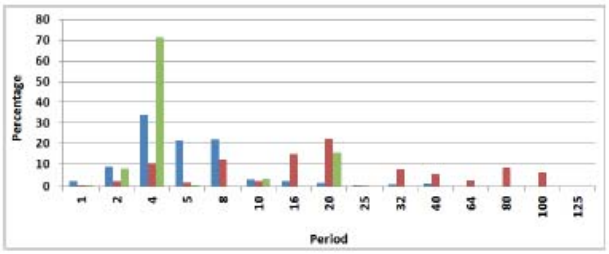


Fig. 4. Period distributions of Choice 1 (blue), Choice 2 (red), Choice 3 (green) (p=5, m=3)

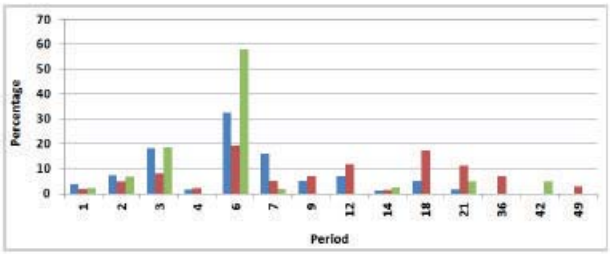


Fig. 5. Period distributions of Choice 1 (blue), Choice 2 (red), Choice 3 (green) (p=7, m=2)

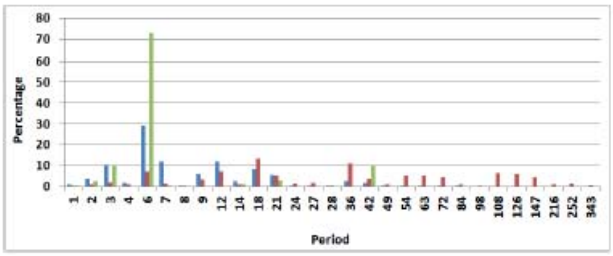


Fig. 6. Period distributions of Choice 1 (blue), Choice 2 (red), Choice 3 (green) (p=7, m=3)

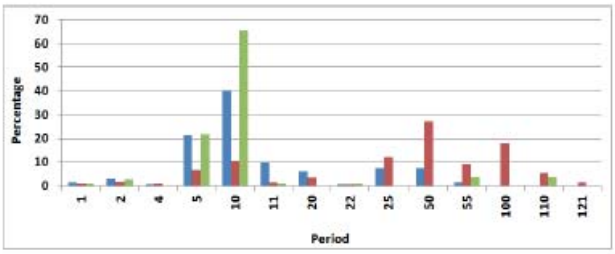


Fig. 7. Period distributions of Choice 1 (blue), Choice 2 (red), Choice 3 (green) (p=11, m=2)

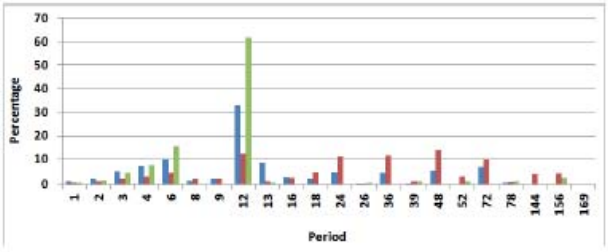


Fig. 8. Period distributions of Choice 1 (blue), Choice 2 (red), Choice 3 (green) (p=13, m=2)

Generation of sequences with maximum periods seems to be possible only with Choice 2; however, they are still not easy to find as shown in Table VI. Another general observation is that 'the sequences with period p or less' seem to be more probable than high-period sequences, especially for Choice 1 and Choice 3. Table VII shows that all three polynomial choices yield sequences with periods less than the field size p, with a high probability.

TABLE VI
PROBABILITY OF GENERATING A SEQUENCE WITH MAXIMUM PERIOD p^m

Case	Choice 1	Choice 2	Choice 3
1	0.00	0.22	0.00
2	0.00	0.15	0.00
3	0.00	0.00	0.00
4	0.00	0.00	0.00
5	0.00	0.03	0.00
6	0.00	0.01	0.00
7	0.00	0.02	0.00
8	0.00	0.00	0.00

TABLE VII
PROBABILITY OF GENERATING A SEQUENCE WITH PERIOD LESS THAN OR EQUAL TO p

Case	Choice 1	Choice 2	Choice 3
1	0.93	0.63	0.78
2	0.80	0.37	0.70
3	0.86	0.42	0.84
4	0.67	0.16	0.81
5	0.80	0.42	0.88
6	0.58	0.13	0.86
7	0.77	0.22	0.92
8	0.71	0.30	0.93

C. *Factors of Periods*

Although the generation of high-period sequences by these three polynomial choices seem to be less probable than low-period sequences, it is still of interest to examine the set of possible periods that can be generated. So, one can start by tabulating all possible periods generated in the 8 considered cases; corresponding to $m = 2$ with $p = 3, 5, 7, 11, 13$ as in Table VIII and $m = 3$ with $p = 3, 5, 7$ as in Table IX. We observe that the possible period values are found by multiplying the factors of $p-1$ with each other, or by p for all three choices of polynomials. More specifically, each period $T = ab$ shown in Table VIII is the product of two integers, where a and b can be equal to p, or to a factor of $p-1$. Choice 2 generates the largest set of period values, which almost always contains Choice 1 sets and some extra values shown as overlined. Choice 1 and Choice 3 sets differ from each other by underlined elements. Choice 3 sets are the smallest of the three; however, the bold underlined values of Choice 3 sets are unique and do not exist in other choices.

It is also of interest to find out the effect of increasing the number of polynomials (i.e., the vector size m) from 2 to 3, which can be done by examining Table IX. Each period shown in Table IX is the product of three integers, $T = abc$, where a, b and c can be equal to p, or to a factor of $p-1$. As understandable from its simple description, Choice 3 gains nothing in terms of the period, if m is raised from 2 to 3; whereas the other two choices do have larger periods as opposed to $m = 2$ case.

TABLE VIII
PERIODS OBTAINED WITH TWO POLYNOMIALS
(m=2)

Case	p	Choice 1	Choice 2	Choice 3
1	3	1, 2, 3, $\underline{4}$	1, 2, 3, 4, $\overline{9}$	1, 2, 3, $\underline{\mathbf{6}}$
3	5	1, 2, 4, 5, $\underline{8}$, 10	1, 2, 4, 5, 8, 10, $\overline{16}$, $\overline{20}$	1, 2, 4, 5, 10, $\underline{20}$
5	7	1, 2, 3, $\underline{4}$, 6, 7, $\underline{9}$, $\underline{12}$, 14, $\underline{18}$, 21	1, 2, 3, 4, 6, 7, 9, 12, 14, 18, 21, $\overline{36}$, $\overline{49}$	1, 2, 3, 6, 7, 14, 21, $\underline{\mathbf{42}}$
7	11	1, 2, $\underline{4}$, 5, 10, 11, $\underline{20}$, 22, $\underline{25}$, $\underline{50}$, 55	1, 2, 4, 5, 10, 11, 20, 22, 25, 50, 55, $\overline{100}$, $\overline{110}$, $\overline{121}$	1, 2, 5, 10, 11, 22, 55, $\underline{110}$
8	13	1, 2, 3, 4, 6, $\underline{8}$, $\underline{9}$, 12, 13, $\underline{16}$, $\underline{18}$, $\underline{24}$, 26, $\underline{36}$, 39, $\underline{48}$, $\underline{72}$, 78	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 24, 26, 36, 39, 48, $\overline{52}$, 72, 78, $\overline{144}$, $\overline{156}$	1, 2, 3, 4, 6, 12, 13, 26, 39, $\underline{52}$, 78, $\underline{156}$
Maximum period		$(p-1)^2$ or $\frac{p(p-1)}{2}$	$p(p-1)$ or p^2	$p(p-1)$

TABLE IX
PERIODS OBTAINED WITH TWO POLYNOMIALS
(m=3)

Case	p	Choice 1	Choice 2	Choice 3
2	3	1, 2, 3, 4, 6, 9, 12	1, 2, 3, 4, 6, 8, 9, 27	1, 2, 3, 6
4	5	1, 2, 4, 5, 8, 10, 16, 20, 25, 32, 40	1, 2, 4, 5, 8, 10, 16, 20, 25, 32, 40, 64, 80, 100	1, 2, 4, 5, 10, 20
6	7	1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 18, 21, 24, 27, 28, 36, 42, 49, 54, 63, 72, 84	1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 18, 21, 24, 27, 28, 36, 42, 49, 54, 63, 72, 84, 98, 108, 126, 147, 216, 252, 343	1, 2, 3, 6, 7, 14, 21, 42
Maximum period		$p(p-1)^2$ or $\frac{p(p-1)^2}{2}$ or $\frac{p(p-1)^2}{3}$	$p^2(p-1)$ or p^3	$p(p-1)$

III. CONCLUSION

Three polynomial choices for the recursive generation method of pseudorandom vector sequences proposed by Ostafe and

Shparlinski were analysed exhaustively in terms of the period distributions and multiplying factors of the generated periods; for the specific choices of the field size p and the vector size m. Our exhaustive search for p = 3, 5, 7 with m = 2, 3 and p = 11, 13 with m = 2 shows that periods are less than p for more than half of the generated vector sequences; and there is no maximum-period sequence for the 1st and the 3rd polynomial choices given in Table I. Choice 2 is more promising since it has smaller percentage of small-period sequences than other choices; and maximum-period sequences with period p^m do exist, although their existence probability is less than 3% if $p > 3$. As an important clue for further theoretical computations**;** our search also shows that the sequence period T is equal to the product of m terms, each of which can be either equal to p or to a factor of $p-1$. Another future work is the investigation of randomness properties of the vector sequences produced by this method.

REFERENCES

[1] D. H. Lehmer, *Mathematical Methods in Large-Scale Computing Units*, in Proc. 2nd Sympos. on Large-Scale Digital Calculating Machinery, Cambridge MA, 1949, Harvard University Press, Cambridge, MA, 1951, pp. 141-146.

[2] A.Ostafe and I. E. Shparlinski, *On The Degree Growth In Some Polynomial Dynamical Systems And Non-linear Pseudorandom Number Generators*, 2010.

[3] A. Ostafe, I. E. Shparlinski E. Pelican, *On Pseudorandom Numbers From Multivariate Polynomial Systems*, 2010.

[4] A.Ostafe, *Multivariate Permutation Polynomial Systems and Non-linear Pseudorandom Number Generators*, 2010.

[5] A. Ostafe and I. E. Shparlinski, *Pseudorandom Numbers and Hash Functions from Iterations of Multivariate Polynomials*, 2010.

[6] A. Ostafe, *Pseudorandom Vector Sequences Derived from Triangular Polynomial Systems with Constant Multipliers*, 2010.

[7] A.Ostafe, *Pseudorandom Vector Sequences of Maximal Period Generated by Triangular Polynomial Dynamical Systems*, 2010.

Off-the-Record Communication with Location Hiding

Halil Kemal Taşkın[1], Murat Demircioğlu

***Abstract*—Cryptography is the main tool on the Internet for protecting private data. Systems such as PGP, SSL make use of long-lived keys for cryptographic purposes. However, a new protocol called Off-the-Record Messaging proposed by Borisov et al. [1] in 2004 changed the way of private communication. OTR is a system which provides end-to-end security with properties such as perfect forward secrecy and repudiability. In this paper, we give a two-party OTR messaging protocol with location hiding property. Besides basic requirements of OTR communication, location hiding enables parties to hide their physical locations namely IP addresses. Also, our design removes the requirement for trusted third parties. As a result, this allows it to be easily deployed on cloud networks.**

***Index Terms*—Private Social Communication, Location Hiding, Repudiability, Perfect Forward Secrecy, Authentication.**

I. Introduction

The invention of the internet has changed the way we communicate. E-mail is one of the newest communication tools coming into our lives. Less then two decades ago, many people had not heard about it, but today many of us use e-mail instead of writing letters. Every day billions of e-mail messages are sent around the world.

But sometimes e-mail is not practical enough. You may want to know if a person you want to send e-mail is online at that moment. Also e-mailing with someone intensively in a short time requires so many clicks. As a result of these kind of requests and difficulties, the instant messaging (IM) became so popular. By using IM, you can keep a list of people you want to communicate with. You can chat with that person as long as they are online.

On the other hand, IM does not provide the security properties available in a physical private conversation, such as repudiation. Online communication systems commonly provide confidentiality, authentication and non-repudiation. In 2004's Workshop on Privacy in Electronic Society (WPES), Borisov et. al. introduced the Off-the-Record (OTR) protocol [1], which allows two-party private conversation, aims to provide repudiation besides authentication, confidentiality and perfect forward secrecy. After OTR protocol was introduced it took attention of many researchers [3], [6], [7], [8]. Multi-party OTR protocol [2], [4] is an extension of OTR but we focus on only two-party communication.

H.K. Taşkın and M. Demircioğlu are with the Department of Cryptography, Institue of Applied Mathematics, Middle East Technical University.

E-Mails: {halil.taskin,demurat}@metu.edu.tr

[1]The author is supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under the project number 112E101 titled "Blok Şifrelerin Olası Olmayan Kriptanalizi".

In this work, we present a new two-party OTR protocol which also provides location hiding. Using our protocol, communicating parties may not know their locations, namely their IP addresses. In our design, we used SHA-3 winner KECCAK [9] as a cryptographic building block for symmetric operations. By this way, having only implementation of KECCAK, it is possible to handle all symmetric operations.

In section II, we state the requirements of OTR protocol. Our new OTR protocol is given in section III. Finally, section IV concludes our work.

II. Cryptographic Requirements

The International Organization for Standardization (ISO) defines five typical security services to support the security in distributed applications. Those are identification/authentication, access control/authorization, confidentiality, integrity, and non-repudiation [12]. The parties using OTR protocol may need these services except non-repudiation. Instead of it, deniability (repudiation) is preferred. By this way, they will be able to deny their past conversations.

A. The OTR Protocol

The OTR protocol consists of four cryptographic primitives [1]; perfect forward secrecy, digital signatures, message authentication codes and malleable encryption.

1) Perfect Forward Secrecy: The past messages should not be recovered retroactively. In order to achieve this property, short-lived encryption/decryption key(s) are used for confidentiality. Used keys should be forgotten by the parties after they are used. It should be computationally infeasible to determine the used keys from the current key or the long-term keys.

2) Digital Signatures: It is used to make parties verify each other. Diffie-Hellman key exchange protocol does not provide the mutual authentication. Digital signatures produced via long term keys may solve this problem. However, attaching signatures to every IM messages leads to non-repudiation which we do not want. The solution is to use Message Authentication Code (MAC) on each message instead of user's digital signature. Authenticating the keys by using digital signature provides the identification service. Therefore, only the person who knows the right key can read the ciphertexts.

3) Message Authentication Codes: The parties shared a MAC key, and each message is sent with the MAC of the message. Deniability is achieved by this way. Since third parties do not know the MAC key, they cannot prove the source of the message. And also the recipient of the message cannot prove the source since it could be a message forged by himself.

4) Malleable Encryption: It will be used to provide forgeability of transcripts, repudiation of contents, and deniability. Forgeability is a little bit stronger than repudiation. Forgeability is achieved through malleable encryption which makes it easy to alter the ciphertext while it is still a proper ciphertext without knowledge of the key. Using stream ciphers can be an example for this.

B. Location (Source) Hiding

The communicating parties may want to hide their physical locations, namely IP addresses. For this purpose, anonymizing models should be used. Also, anonymizing without a trusted third party is an important issue to consider. Therefore, there will not be any direct connection between the messaging parties. So, they cannot obtain their locations.

III. The Protocol

In this chapter, we give the details of our protocol. Our protocol consists of two main parts: Two-party communication protocol and location hiding protocol.

In the constructions, we use Keccak [9] as a building block for hash function, stream cipher and generating message authentication code. Also, 2048-bit RSA is used as public key cryptosystem and 1024-bit Diffie-Hellman (DH) Key Exchange Scheme with generator g is used for public key exchange.

Our notation,

- A and B are the public pseudonyms for the parties.
- $||$ is concatenation.
- e_X and d_X are the public and private keys of part X, respectively.
- $[m]_{d_X}$ is the signature of message m signed by part X.
- $\{m\}_{e_X}$ is the encryption of message m with part X's public key.
- H is the Keccak-512 hash function.
- $ENC_{IV,K}(m)$ and $DEC_{IV,K}(m)$ are Keccak-256 in stream cipher mode encryption and decryption algorithms with message m, key K and initialization vector IV, respectively.
- $MAC_K(m)$ is the message authentication code for message m generated by Keccak-256 in MAC mode with key K.

A. Two-party Communication Protocol

Let A and B be the parties who want to communicate. Two-party off-the-record communication is established as follows:

1) Let n be the re-keying value.
2) A generates ephemeral public/private key pair (e_A, d_A).
   B generates ephemeral public/private key pair (e_B, d_B).
3) A sends its public key to B and B to A.
4) A and B verifies their public keys by an offline method such as voice communication, facebook, whatsapp etc. using the fingerprint of their corresponding public keys.
5) A initiates the counter: $ctr_A \leftarrow 1$
   B initiates the counter: $ctr_B \leftarrow 1$
6) Key exchange process is based on DH key exchange protocol.

$$A \xrightarrow{A, g^{x_1}, [H(g^{x_1})]_{d_A}} B$$

$$\xleftarrow{B, g^{y_1}, [H(g^{y_1})]_{d_B}}$$

   Both sides compute the shared secret $g^{x_1 y_1}$. It is hashed using the hash function H.

$$H(g^{x_1 y_1}) = K$$

   Let $K = (K_L, K_R)$ where K_L is the most significant half and K_R is the least significant half of the K.
   Hash of concatenation of least significant half of K_L and most significant half of K_R is used as session key ID (SKID).
7) If ctr_A mod $n = 0$ or ctr_B mod $n = 0$ then key exchange process is repeated as it is started from step 5. Then, after minimum $n-1$, maximum $2n-2$ messages later, there has to be a key exchange.
8) Part A sends message M_1 to B as follows:
   Let M_1^E be the encapsulated form of M_1. Than, M_1^E is computed as follows:

$$M_1^E = \big(SKID, ctr_A, IV, ENC_{IV,K_L}(M_1), MAC_{K_R}(SKID||ctr_A||IV||M_1)\big)$$

$$ctr_A \leftarrow ctr_A + 1$$

$$A \xrightarrow{M_1^E} B$$

   A random IV is generated for all new messages. Since both parties can check other party's counter value, none of them is able to delay the key exchange phase.
9) Part B decrypts and verifies M_1 as follows:
   It first computes M_1':

$$M_1' = DEC_{IV,K_L}(ENC_{IV,K_L}(M_1))$$

   Then, message authentication code MAC' is computed for M'.

$$MAC' = MAC_{K_R}(SKID||ctr_A||IV||M_1')$$

   If the value of MAC' is same as the one in the M_1^E then message is correctly decrypted and verified.
10) B does the same procedure to send a message to part A.

There is a trade off between perfect forward secrecy and efficiency of the protocol. To get over this issue the re-keying value n is used. The n value can be configured due to the requirements of the communication. For example, taking $n = 2$ forces the system to change keys at most every 2 packets, which is slower but more secure. But, for instant messaging taking higher n values should not be a problem.

B. Location Hiding Protocol

Our protocol which is explained in section III-A can be extended to have location hiding property. Our location hiding protocol makes use of some ideas from the anonymizing network protocols Tor [10] and I2P [11].

Location hiding protocol requires at least three different third party servers which is not required to have secure sockets. Plaintext communication is enough to handle the protocol. Every server should have two capabilities: Connection binding and location redirection.

Connection binding is used as a meeting point for A and B. Location redirection is used to redirect messages from a user to an other user.

Let N_i, N_j and N_k be the three servers.

1) Parties A and B agree on a meeting server N_i and a shared secret passphrase.
2) A selects its meeting server except N_i which is N_j. Similarly, B selects N_k.
3) A opens a connection to N_j. N_j stores the id of A and its corresponding connection session. Than, A is connected to N_i and does a connection binding to N_j with the shared secret passphare as follows:
$$A \xrightarrow{A, ENC_W(A||"Location:"||N_j)} N_i$$
4) Similarly, B does the same process:
$$B \xrightarrow{B, ENC_W(B||"Location:"||N_k)} N_i$$
5) For a party, only the last connection binding session data is stored on a server. So, when a request is sent for a user, only the last binding session data will be responded.
6) A requests B's binding point using the id of B. Encrypted location data is sent to A. Than A decrypts the location using shared secret passphrase to meet with it. If passphrase is validated B's meeting point N_k is recovered.
   If $N_k = N_i$ or $N_k = N_j$ then A rejects the communication. Process is repeated until agreed on different servers.
   Similarly, B gets A's meeting point N_j.
7) A sends message M_a to B using location redirection on server N_k.
$$A \xrightarrow{B, M_a} N_k \xrightarrow{M_a} B$$
8) B sends message M_b to A using location redirection on server N_j.
$$A \xleftarrow{M_b} N_j \xleftarrow{A, M_b} B$$

By design, only 1 hop is used between A and B, but to get higher levels of location hiding it it possible to have more than one hops between two parties. Having more hops decreases speed of communication.

C. Why it is OTR?

In this section, we show that our protocol satisfies the requirements for the OTR communication.

- **Perfect Forward Secrecy:** In our design we do not use any long-lived keys, instead of this we use ephemeral RSA keys for public encryption and signing. Also, rekeying value n is used to force parties to change session keys after at most $2n - 2$ messages.
- **Authentication:** Parties A and B authenticate each other in an offline fashion. This removes the requirement for a long-lived key. This authentication mechanism enables to sign key exchange values without compromising repudiability.
- **Repudiation (Deniability):** Only the hash of key exchange values (i.e. DH key exponents) are signed by parties, it is not computationally possible to show the session key used in encryption is derived from this particular key exchange process.
- **Forgeability (Malleability):** Malleability is stronger form of forgeability. Our design uses a stream cipher for encryption and decryption of messages. So, it is possible to modify ciphertext and it will still be a proper ciphertext due to XOR'ing property of stream ciphers. This property allows us to modify any encapsulated message properly. Anyone who has decryption key can properly decrypt the modified ciphertext. But only recipient will be able to detect this modification because of the MAC value of the encapsulated message.
- **Location Hiding:** We also show that our design enables location hiding when it is used with the protocol given in section III-B. Since authentication is done offline and any message is binded to its source, any server between two parties would not be able to mount a man-in-the-middle attack.

IV. Conclusion

We presented a new off-the-record communication protocol with location hiding property that removes the requirement for a trusted third party. Our main assumption for the security is that it is not feasible for someone to observe both OTR and offline communication channels. Our design is resistant against impersonation attacks for all parties and servers due to authentication is done in an offline fashion. Man-in-the-middle attacks are also not feasible because of two main reasons; first one is that authentication is offline and second one is that every type of packet sent to other party has binding for its source. Using any third party server without considering the security of them allows our design to be easily established on a cloud system. In this way, it is possible to have many servers for location hiding based on plaintext communication.

One of the problems in the OTR is to tell users how to initiate the protocol since the protocol itself is not user-friendly [5], implementations should care about a user friendly interface. Also, location hiding in multi-party OTR is another research area. These are possible future works for our problem.

Acknowledgment

The authors would like to thank Cihangir Tezcan for his comments and guidance.

REFERENCES

[1] N. Borisov, I. Goldberg, E. A. Brewer, *Off-the-record communication, or, why not to use PGP*. WPES 2004: 77-84.

[2] I. Goldberg, B. Ustaoğlu, M. V. Gundy, H. Chen, *Multi-party off-the-record messaging*. ACM Conference on Computer and Communications Security 2009: 358-368.

[3] M. Di Raimondo, R. Gennaro, H. Krawczyk, *Secure off-the-record messaging*. WPES 2005: 81-89.

[4] J. Bian, R. Şeker, Ü. Topaloğlu, *Off-the-Record Instant Messaging for Group Conversation*. IRI 2007: 79-84.

[5] R. Stedman, K. Yoshida, I. Goldberg, *A user study of off-the-record messaging*. SOUPS 2008: 95-104.

[6] I. Goldberg, D. Stebila, B. Ustaoğlu, *Anonymity and one-way authentication in key exchange protocols*. Des. Codes Cryptography 67(2): 245-269 (2013).

[7] M. Di Raimondo, R. Gennaro, H. Krawczyk, *Deniable authentication and key exchange*. ACM Conference on Computer and Communications Security 2006: 400-409.

[8] C. Alexander, I. Goldberg, *Improved user authentication in off-the-record messaging*. WPES 2007: 41-47.

[9] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche. *Keccak sponge function family main document*. Submission to NIST, 2011. Version 3.0.

[10] R. Dingledine, N. Mathewson, P. Syverson. *Tor: The second-generation onion router*. In Proceedings of the 13th USENIX Security Symposium, pages 303-320, August 2004.

[11] Invisible Internet Project (I2P), *http://www.i2p2.de*

[12] I. O. for Standardization. *Information processing systems - Open Systems Interconnection - Basic Reference Model Part 2: Security Architecture*. Number ISO 7498-2. 1988.

RSA Kriptosistemi Parametreleri için Güvenlik Testi Yazılımı

Ersan Akyıldız, Çağdaş Çalık, Mert Özarar, Zaliha Tok, ve Oğuz Yayla

Özet: **RSA kriptosisteminde üretilen açık ve gizli anahtar parametrelerinin güvenilir olması için gereken kriterler çalışılmıştır. Bu kriterler e-imza oluşturma standartlarında ve literatürde bulunmaktadır. Çalışmamızda, bu kriterler test maddeleri halinde sunulmuştur. Ayrıca, söz konusu testleri gerçekleştiren bir yazılım paketi geliştirilmiştir. Yazılım paketi RSA-1024 ve RSA-2048 parametrelerinin testlerini makul sürelerde yapabilmektedir.**

Anahtar Kelimeler: **RSA kriptosistemi, e-imza, güvenlik testi.**

Abstract: **We study the requirements for public key and private key parameters of RSA cryptosystem. The requirements considered are already known in the digital signature standards, directives and literature. We list these requirements in a security testing framework and develop a software package for validating them. The software package is able to test RSA-1024 and RSA-2048 parameters in a reasonable amount of time.**

Keywords: **RSA cryptosystem, digital signatures, security testing.**

I. GİRİŞ

AÇIK anahtarlı kriptosistemler sınıfına ait olan RSA kriptosistemi [7] (kıs. RSA, RSA sistemi), verilerin şifrelenmesi ya da imzalanması amacıyla kullanılır. Dünya'da ve ülkemizde e-imza, SSL/TLS vb. uygulamalarda yaygın olarak kullanılmaktadır. RSA sisteminde kullanılan anahtar ikililerini bilgisayar ortamında üretmek mümkün olmakla birlikte, kişiye/kuruma özel e-sertifikaların kanuni olarak geçerli olması ancak yetkili bir ESHS (Elektronik Sertifika Hizmet Sağlayıcısı) tarafından üretilmeleri koşuluna bağlıdır. Yine yürürlükte olan 5070 Sayılı Elektronik İmza Kanununa [1] göre bu işlem belirli standartlara uygunluk gösteren HSM (Hardware Security Module) cihazlarıyla gerçekleştirilmektedir. Bu tarz cihazların bilgi güvenliği açısından kritik bir konuma sahip olmaları nedeniyle ürettikleri parametrelerin güvenlik testlerinden geçirilmesi gerekir. Bu çalışmada söz konusu testleri gerçekleştiren bir yazılım paketi tanıtılacaktır.

E. Akyıldız: Matematik Bölümü ve Uygulamalı Matematik Enstitüsü, Orta Doğu Teknik Üniversitesi, Ankara, 06800, Türkiye, e-posta: ersan@metu.edu.tr.

Ç. Çalık, M. Özarar, Z. Tok ve O. Yayla: Uygulamalı Matematik Enstitüsü, Orta Doğu Teknik Üniversitesi, Ankara, 06800, Türkiye, e-posta: ccalik@metu.edu.tr, mert.ozarar@gmail.com, zalihayuce@gmail.com, yayla@metu.edu.tr

M. Özarar: TÜRKTRUST Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş., Galyum Blok, Kat:2 No:20, Ankara, 06800 Türkiye e-posta: mert.ozarar@gmail.com

Gönderildi: 15 Temmuz 2013; düzeltildi: 15 Temmuz 2013.

*Bu çalışma TÜRKTRUST Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. tarafından desteklenmiştir.

Tablo I
RSA SİSTEMİ PARAMETRELERİ.

n	açık modülüs parametresi
e	açık üst parametresi
d	gizli üst parametresi
p, q	açık modülüs parametresi n'nin asal çarpanları
$\phi(n)$	n'den küçük ve n ile aralarında asal olan sayıların sayısı

II. TANIMLAR

RSA, her kullanıcının bir gizli bir de açık anahtarının olduğu bir açık anahtarlı kriptosistemdir. Sistemi oluşturan parametreler Tablo I'de gösterilmiştir. Açık anahtar (n, e) ikilisi ile, gizli anahtar ise (n, d) ikilisi ile gösterilir. n sayısı, p ve q olarak gösterilen iki asal sayının çarpımından oluşmaktadır. RSA parametreleri p ve q'yu bilen birisi, $\phi(n) = (p-1)(q-1)$ sayısını hesaplayabilmekte ve $\phi(n)$ modülüsünde birbirinin tersi olan e ve d parametrelerini oluşturabilmektedir. Oluşturulan bu sistemde (n, e) açık anahtarı şifreleme ve imza doğrulama işlemlerinde, (n, d) gizli anahtarı ise deşifreleme ve imza üretme işlemlerinde kullanılır. Birçok uygulamada e sayısı işlemlerin daha hızlı yapılabilmesi için *Fermat asal sayısı* olan $2^{16} + 1 = 65537$ olarak seçilmektedir.

RSA sisteminde (n, e)'nin açık bilgi olduğu göz önüne alındığında, gizli anahtar parametresi d'nin bulunmasının, n sayısından p ve q çarpanlarını bulmanın zorluğuna dayandığına inanılır. Bu nedenle, sistemin güvenliğini sağlamak için çarpanlara ayırma algoritmalarına dayanıklı p ve q, dolayısıyla n sayısı oluşturmak önemlidir. Bunun için de p ve q parametreleri standartlarda belirtilen bir takım kriterlere uygun seçilmelidir [3]–[5]. Uygun şekilde seçilen parametreler de ancak n parametresinin büyüklüğü ile orantılı bir güvenlik seviyesi sunarlar. RSA sisteminin güvenlik seviyesi, bu sistemi kırmak için gereken hesaplama gücünün büyüklüğüne bağlıdır. Güvenliği k-bit olan bir sistemi kırmak için 2^k mertebesinde işlem yapmak gerekmektedir. Simetrik anahtarlı kriptosistemlerde güvenlik doğrudan anahtar boyuna karşılık gelirken, RSA'da ise n parametresine bağlı olarak yapılması gereken işlem miktarının hesaplanmasıyla elde edilir. Tablo II, RSA sistemindeki n parametresinin bit cinsinden uzunluğunun (k) hangi güvenlik seviyesine karşılık geldiğini göstermektedir [6].

Tablo II
RSA GÜVENLİK SEVİYELERİ.

Güvenlik seviyesi (bit)	RSA sayısı n (bit uzunluğu: k)
80	1024
112	2048
128	3072
192	7680
256	15360

III. KAPSAM

RSA sisteminin parametrelerinin güvenlik testleri ile ilgili üç modülden oluşan bir yazılım paketi geliştirilmiştir. Bu modüllerin hangi durumlarda ve ne amaçla kullanıldığı aşağıda açıklanmıştır.

1) **(n,e,d) testi.** RSA parametrelerinden gizli ve açık anahtarların bilinmesi, yani $\{n, e, d\}$'nin bilinmesi. Bu durumda amaç n'nin çarpanları olan p ve q asal sayılarını bulmak ve tüm parametrelerin standartlarda belirtilen şartlara uygunluğunu kontrol etmektir.
2) **(n,e) testi.** RSA parametrelerinden sadece açık anahtarın, yani (n, e) ikilisinin bilinmesi durumu. Bu durumda n sayısı çarpanlarına ayrılmaya çalışılır.
3) **Ortak çarpan testi.** Birden fazla RSA açık anahtarının bilinmesi durumu. Bu durumda anahtarların birbirileri ile ortak çarpanının olup olmadığına bakılır. Bu tarz bir ortak çarpanın bulunması, söz konusu n parametrelerinin çarpanlara ayrılması anlamına gelmektedir. Bu test, p ve q parametrelerinin rastsal bir şekilde seçilmediği ve farklı n parametrelerinin aynı asal sayılar tarafından oluşturulduğunu tespit etmek için kullanılır.

IV. YÖNTEM

Bu bölümde RSA parametrelerinin ETSI TS 102 176-1 (2007), FIPS PUB 186-3 (2009) ve IEEE 1363 (2004) standartlarına ve diğer güvenlik gereksinimlerine uygunluğu için gereken test maddeleri sunulacaktır. Aşağıda temel standartlar sırasıyla ETSI, FIPS ve IEEE şeklinde kısaltılmıştır. Belirtilen güvenlik test maddelerinin hangi standardın gereksinimi olduğu parantez içinde belirtilmiştir.

RSA kriptosistemi parametrelerinin testi üç durumda ele alınmıştır:

A. (n, e, d) parametreleri bilindiği durumda,
B. (n, e) parametreleri bilindiği durumda,
C. $(n_1, n_2, \ldots, n_l)$ parametreleri bilindiği durumda.

A. (n, e, d) testi

Bu teste RSA açık ve gizli anahtarını oluşturan $\{n, e, d\}$ parametrelerinin tamamı girdi olarak verilir. Bu girdilere sırasıyla aşağıdaki işlemler uygulanır:

1) n sayısının bit uzunluğu (k) Tablo II'de verilen güvenlik seviyesini sağlamalıdır. (ETSI, FIPS, IEEE)
2) e sayısı 65537 ve 2^{256} arasında tek tamsayı olmalıdır. (FIPS)
3) d sayısı $2^{k/2}$ den büyük olmalıdır. (ETSI, FIPS, IEEE)
4) Factorn(n, e, d) algoritması (bkz. EK: Algoritma 1) ile n sayısını bölen p sayısı ve sonra da q sayısı bulunur. Aşağıdaki testler yapılır:

Tablo III
P1, P2, Q1 VE Q2 SAYILARININ BİT UZUNLUĞU.

n (bit uzunluğu)	p1, p2, q1 ve q2 (bit uzunluğu)
1024	> 100
2048	> 140
3072	> 170

a) p ve q sayılarının Miller-Rabin (MR) [4] ve Lucas (L) [4] olasılıksal asallık testlerinin birlikte uygulanması ile asal olmama olasılıkları 2^{-100}'den az olmalıdır. Bu amaçla asal sayıların bit uzunluğuna göre aşağıda belirtilen miktarlardaki Miller-Rabin (MR) ve Lucas (L) olasılıksal asallık testleri uygulanmalıdır. (ETSI, FIPS, IEEE)
   i) 512 bit asallar için 7MR + 1L
   ii) 1024 asallar için 4MR + 1L
   iii) 1536 asallar için 3MR + 1L
   iv) 2048 asallar için 3MR + 1L
b) p ve q sayıları $2^{(k-1)/2} \leq p, q \leq (2^{k/2} - 1)$ aralığında olmalıdır. (FIPS)
c) p ve q sayıları arasındaki fark $2^{(k/2)-100}$'den büyük olmalıdır. (FIPS)
d) $(p\pm1)$ ve $(q\pm1)$ sayıları aşağıdaki şartları sağlamalıdır.
   i) $(p-1)$ sayısının en büyük asal böleni $p1$,
   ii) $(p+1)$ sayısının en büyük asal böleni $p2$,
   iii) $(q-1)$ sayısının en büyük asal böleni $q1$,
   iv) $(q+1)$ sayısının en büyük asal böleni $q2$ olsun.
   $p1$, $p2$, $q1$ ve $q2$ asal bölenleri Eliptik Eğri Çarpanlara Ayırma Algoritması [8] ile bulunur. Bu asallar Tablo III'deki minimum bit uzunlukları değerlerini sağlamalıdır. (FIPS)

Bu test basamakları sayesinde RSA kriptosisteminin aşağıda belirtilen güvenlik maddeleri test edilmiş olur:

1) Sistemin gerçek güvenlik derecesi,
2) Kök alma ataklarına karşı sistemin güvenilirliği,
3) Gizli anahtar d'nin güvenliği,
4) p ve q sayılarının asallıkları,
5) Eliptik Eğri temelli (ECM) çarpanlara ayırma yöntemine karşı sistemin dayanıklılığı,
6) Fermat çarpanlarına ayırma yöntemine karşı sistemin dayanıklılığı,
7) $p-1$ ve $p+1$ çarpanlarına ayırma yöntemlerine karşı sistemin dayanıklılığı.

B. (n, e) testi

Bu test girdi olarak RSA parametresi n'yi alarak, bu sayıyı çarpanlarına ayırmaya çalışır. Aşağıdaki çarpanlara ayırma algoritmaları sırayla uygulanır:

1) n sayısının bit uzunluğu Tablo II'de verilen güvenlik seviyesini sağlamalıdır. (ETSI, FIPS, IEEE)
2) e sayısı 65537 ve 2^{256} arasında tek tamsayı olmalıdır. (FIPS)
3) n sayısının küçük böleni olmamalıdır. n sayısının 2^{140}'dan küçük böleni Eliptik Eğri Çarpanlara Ayırma Algoritması [8] ile aranır. (ETSI, FIPS, IEEE)

4) Fermat Çarpanlara Ayırma Algoritması [2] ile n sayısının çarpanı aranır. (ETSI, FIPS, IEEE)

Bu test basamakları sayesinde RSA kriptosisteminin aşağıda belirtilen güvenlik maddeleri test edilmiş olur:

1) Sistemin gerçek güvenlik derecesi,
2) Kök alma ataklarına karşı sistemim güvenilirliği,
3) p ve q sayılarının büyüklüğü,
4) p ve q sayılarının birbirine uzaklığı.

C. Ortak çarpan testi

Bu testin amacı, RSA açık anahtar parametresi n'lerden oluşan $\{n_1, \cdots, n_l\}$ kümesi içinde herhangi farklı iki n_i ve n_j sayısının $(1 \leq i < j \leq l)$ ortak çarpanı olup olmadığına bakmaktır. Böyle bir çarpanın bulunması halinde, yani $d = gcd(n_i, n_j) \neq 1$ ise, bu sayıların bir çarpanı olarak d sayısı bulunmuş olur.

Bu teste girdi olarak verilecek sayılarının $n = p.q$ biçiminde iki tek asal sayının çarpımı olacağı varsayılmakla birlikte, test prosedürüne konulan ek bir kontrol ile bu biçimde olmayan n sayılarını da dikkate alan bir yöntem uygulanabilir.

Verilen $\{n_1, \cdots, n_l\}$ kümesi için P_t sayısı ilk t elemanın çarpımı olsun, yani $P_t = \prod_{i=1}^{t} n_i$. Bu durumda $gcd(P_t, n_{t+1})$ kontrol edilerek n_{t+1} sayısının daha önceki sayılardan herhangi biri ile ortak çarpanı olup olmadığı bulunur. Ortak çarpan var ise n_{t+1}'in hangi eleman ile ortak çarpanı olduğu tek tek karşılaştırma yapılarak bulunur. Eğer ortak çarpan yok ise P_{t+1}'in sonraki değeri $P_{t+1} = P_t.n_{t+1}$ formülüne göre bulunur ve işlem benzer şekilde devam eder.

Diğer bir ifadeyle $p_s = gcd(n_s, n_1 n_2 \ldots n_{s-1})$ hesabı her $s = 1, 2, \ldots, l$ için yapılır. p_s sayısı birden farklı ise n_s sayısının bir asal çarpanı bulunmuştur.

Böylelikle aynı p veya q asal sayılarının sistemde birden fazla n sayısında olup olmadığı test edilmiş olur.

V. Yazılımın Karmaşıklığı

Yazılımın her bir modülünün karmaşıklığı aşağıdaki şekilde özetlenebilir.

1) (n, e, d) testi için $p-1$, $p+1$, $q-1$ ve $q+1$'in çarpanlarının incelendiği testler haricindeki tüm testler ihmal edilebilir düzeyde çalışma süresi gerektirmektedir. $p-1$, $p+1$, $q-1$ ve $q+1$ sayılarının çarpanlarına bakıldığı durumda ise bu sayıların büyüklüğü (512-bit ya da 1024-bit) ve dolayısıyla hangi uzunluğa kadar olan çarpanların arandığına göre ve çarpanlara ayırma yönteminin kesinlik derecesini belirten deneme sayısına göre değişmektedir. 1024-bit RSA anahtarları için p ve q yaklaşık 512-bit olmakta ve standartlara göre de $p-1$, $p+1$, $q-1$ ve $q+1$'in en az 100 bitten büyük bir asal çarpanının olması istenmektedir. Bu dört sayı için de çarpan arama işlemi birbirinden bağımsızdır ve paralel olarak gerçekleştirilebilir, bu sayede testlerin ard arda çalıştırıldığı seri uygulamaya oranla 4 kat avantaj sağlanmış olur. 1024-bit RSA anahtarları için GMP-ECM [8] uygulamasının 30-basamaklı çarpan arama parametreleri kullanılmış ve 3.2 Ghz işlemcili bir masaüstü bilgisayarda ortalama 10 dakikada sayının 100 bitin altındaki çarpanları bulunmuştur. 2048-bit RSA için ise GMP-ECM [8] uygulamasının 40-basamaklı sayıları çarpanlara ayırma parametreleri kullanılmış ve 3.2 Ghz işlemcili bir masaüstü bilgisayarda ortalama 1 günde 140 bitten küçük çarpanlar tesbit edilebilmiştir.
2) (n, e) testinin başarılı olması n sayısının çarpanlarına ayrılması ve dolayısıyla RSA sisteminin kırılması anlamına gelir. Bu yüzden RSA parametrelerinin standartlara uygun seçildiği durumlarda bu testin başarı ile sonuçlanması beklenmemektedir. Bu testin başarılı olacağı iki durum vardır. Birincisi p veya q'un bit uzunluğunun oldukça düşük olması durumudur. Bu durumun testi için ECM methodu [8] ile n sayısının 140 bite kadar olan çarpanları aranmıştır. Bu test ortalama 1 gün sürmektedir. İkinci durumda n sayısının çarpanları p ve q'nun birlerine çok yakın olmasıdır. Bu durumda testin istenen çalışma süresine göre uygun değer verilebilir.
3) Ortak çarpan arama testi modülüs sayısı n'lerin adedi l sayısına doğrusal olarak bağlı bir işlem karmaşıklığı gerektirir, dolayısıyla bu testi gerçekleştirmek modern işlemcili bilgisayarlarda en fazla dakikalar mertebesinde vakit almaktadır. Örneğin 10,000 adet 1024-bitlik RSA modülüsünün ortak çarpan arama işlemi 5 dakikadan kısa bir sürede tamamlanmaktadır.

VI. Sonuç

Bu çalışmada RSA e-imza sistemini oluşturan parametrelerin testi için geliştirilen yazılım paketi sunulmuştur. Testler, açık ve gizli parametrelerin bilinmesine bağlı olarak üç farklı kategoriye ayrılmıştır. Her bir test için yapılacak işlemler özet olarak maddeler halinde belirtilmiştir. Bu maddeleri test eden yazılım paketi oluşturulmuştur. Yazılımın karmaşıklığı $p\pm1$ ve $q\pm1$ sayılarının çarpanlarının bulunması hariç çok düşüktür. $p\pm1$ ve $q\pm1$ sayılarının çarpanlarının bulunması için de en uygun deneme yöntemi yazılımın içine dahil edilmiştir.

Ek

Verilen (n, e, d) üçlüsünden n sayısının p ve q asal çarpanlarının bulunması aşağıda verilen Factorn(n, e, d) algortiması ile bulunur.

Algoritma 1 Factorn: n sayısının p ve q asal çarpanlarının bulunması

Girdi: n, e, d
Çıktı: p, q

$ed - 1 = 2^s t$ şartını sağlayan t tek sayısı bulunur.
for $a = 2$'den n'ye **do**
  $x = a^t - 1 \pmod n$
  $d = gcd(x, n)$
  if $(d! = 1)$ ve $(d! = n)$ **then**
    $p = d$
    $q = n/p$
    DUR.
  end if
end for

KAYNAKÇA

[1] Türkiye Cumhuriyeti 5070 Sayılı Elektronik İmza Kanunu: http://www.tbmm.gov.tr/kanunlar/k5070.html
[2] Cohen H., A course in computational algebraic number theory, Graduate Texts in Mathe-matics 138, Springer, 1993.
[3] ETSI TS 102 176-1 v1.2.1, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms., 2005.
[4] FIPS PUB 186-3, Digital Signature Standard (DSS), 2009.
[5] IEEE 1363-2000, Standard Specifications for Public-Key Cryptography, 2000.
[6] NIST Special Publication 800-57, Recommendation for Key Management - Part 1: General (Revision 3), 2012.
[7] Rivest, R.; Shamir, A.; Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21 (2): (1978). 120–126. doi:10.1145/359340.359342
[8] Zimmermann, P.; Dodson B. "20 years of ECM." Algorithmic number theory. Springer Berlin Heidelberg, 2006. 525-542.

Distribution of Boolean Functions of 6 Variables According to the Frequency of Walsh Coefficients

Erdener Uyan, Ali Doğanaksoy

***Abstract*—This paper further investigates the problem of counting Boolean functions with specified number s of specified Walsh coefficients ω, discussed by Uyan et al. [?]. In that paper, the complete and exact counts for all s and ω values were presented for Boolean functions of up to 5 variables. Here, we extend these results to 6 variables by employing the idea of affine equivalence.**

***Index Terms*—Counting, Boolean functions, Walsh coefficients.**

I. Introduction

COUNTING Boolean functions meeting expected criteria has often taken a considerable amount of attention in cryptography mainly because of its importance in defining and bounding the search space for such functions. There are still open problems in literature that requires counting. Finding the number of bent functions or the number of maximum nonlinear balanced Boolean functions are such two problems. Solving these problems is hard primarily due to their computational complexity cost. When the number of variables increases, the size of the whole Boolean function set expands exponentially. In that case, a useful tool to analyze large function domains is affine equivalence classes.

On the other hand, finding relations among Walsh coefficients can help trivializing many questions concerning the main cryptographic features of Boolean functions such as nonlinearity, correlation immunity, resiliency or even algebraic immunity. Papers by Carlet et. al. [**?**], [**?**], and by Maitra and Pasalic [**?**] are some examples where such relations were studied. This work however tries to find such relations focusing on the frequencies of absolute values of Walsh coefficients.

The study in [**?**] focuses on obtaining general results to help counting n-variable Boolean functions with specified values in their Walsh spectrum. Exact and complete counts are listed only for $n \leq 5$, but for larger values of n, partial counts are given. For instance, the number of functions having $(2^n - 4)$ zeros in their Walsh spectrum is given to be $2\binom{2^n}{3}$. This work is dedicated to grouping the set of Boolean functions of 6 variables with respect to the quantity of their Walsh coefficients and giving exact and complete table of their cardinalities. Furthermore, we provide the number of functions for each level of nonlinearity, which was previously given in Fuller's Ph.D. thesis [**?**] as well.

E. Uyan is with the Institute of Applied Mathematics, METU, Ankara, TURKEY e-mail: uerdener@metu.edu.tr.

A. Doğanaksoy is with the Department of Mathematics, METU, Ankara, TURKEY e-mail: aldoks@metu.edu.tr.

II. Preliminaries

The mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called an n-variable Boolean function. The set of all n-variable Boolean functions $\mathcal{B}_n$ has 2^{2^n} elements. The primary representation of a Boolean function f is its *truth table*, the vector formed by 2^n $f(a)$ values evaluated at each $a \in \mathbb{F}_2^n$. Another representation of a Boolean function is its *Walsh spectrum*, the vector formed by 2^n $W_f(a)$ values evaluated at each $a \in \mathbb{F}_2^n$, where

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}, a \in \mathbb{F}_2^n. \quad (1)$$

Equation (**??**) is called the Walsh-Hadamard transform. Each $W_f(a)$ is named a *Walsh coefficient*, which implies the correlation between f and a linear function $x \in \mathcal{B}_n$ at point $a \in \mathbb{F}_2^n$. Note that a Walsh spectrum represents a Boolean function uniquely just like its truth table.

A prominent cryptographic property of a Boolean function f is its nonlinearity, $nl(f)$, which is its minimum distance to the set of all n-variable linear functions. Nonlinearity is simply computed by means of the Walsh spectrum as follows.

$$nl(f) = 2^{n-1} - \frac{|W_f(a)_{max}|}{2} \quad (2)$$

Equation (2) implies that the absolute values of Walsh coefficients give enough information about nonlinearity. We therefore find the distribution of functions in $\mathcal{B}_6$ with respect to the absolute values of their Walsh coefficients.

III. Distribution of $\mathcal{B}_6$ with respect to Walsh coefficients

In this section, the framework and the algorithms to complete the distribution of 6-variable Boolean functions with respect to their Walsh Coefficients will be explained.

A. Framework and Derived Results

The following two definitions were introduced in [**?**].

- The set of Boolean functions f such that $\#\{\alpha \in \mathbb{F}_2^n | \, |W_f(\alpha)| = \omega\} = s$ is denoted by $\mathcal{S}(n, s, \omega)$, where n,s and ω are nonnegative integers with $n \geq 1$ and ω, $s \leq 2^n$.
- The chart whose (s, ω) entry contains the cardinality of $\mathcal{S}(n, s, \omega)$ is called the *function distribution table* of $\mathcal{B}_n$, denoted by FDT_n (e.g. Table **??** shows FDT_3).

FDT_n for $n \leq 5$ were provided completely in [**?**]. Since there are 2^{64} functions in $\mathcal{B}_6$, it is not feasible to do an exhaustive search to create the complete FDT_6. However,

TABLE I
FDT_3

$s \setminus \lvert\omega\rvert$	0	2	4	6	8
0	128	128	144	128	240
1	0	0	0	128	16
2	0	0	0	0	0
3	0	0	0	0	0
4	112	0	112	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	16	128	0	0	0
8	0	0	0	0	0

using Propositon 4.6 and 4.13 in [**?**], half of FDT_6, where $|\omega| \geq 32$, can easily be formed.

Proposition 1. ***(4.6 in [?])*** *Let $\omega = 2^n - 2k$ such that $k < 2^{n-2}$. Then, $|\mathcal{S}(n,1,\omega)| = 2^{n+1}\binom{2^n}{k}$ and $|\mathcal{S}(n,s,\omega)| = 0$ for all $s > 1$.*

TABLE II
FDT_6, $|\omega| > 32$ †

$\lvert\omega\rvert \setminus s$	**0**	**1**	**2**	**...**	2^n
34	18426325641727123456	20418431982428160	0	0	0
36	18440618544114823168	6125529594728448	0	0	0
38	18445062555781586944	1681517927964672	0	0	0
40	18446323694227560448	420379481991168	0	0	0
42	18446648893449478144	95180260073472	0	0	0
44	18446724685138055168	19388571496448	0	0	0
46	18446740548514734080	3525194817536	0	0	0
48	18446743507160384512	566549167104	0	0	0
50	18446743994193879040	79515672576	0	0	0
52	18446744064112832512	9596719104	0	0	0
54	18446744072733614080	975937536	0	0	0
56	18446744073628223488	81328128	0	0	0
58	18446744073704218624	5332992	0	0	0
60	18446744073709293568	258048	0	0	0
62	18446744073709543424	8192	0	0	0
64	18446744073709551488	128	0	0	0

† For readability, this is a transposed version of the conventional FDT_n seen in [**?**]

Note that the value 128 in the last row of Table **??** corresponds to the number of affine functions in $\mathcal{B}_n$

Proposition 2. ***(4.13 in [?])*** *Let $\omega = 2^{n-1}$. Then,*

1) $|\mathcal{S}(n,s,\omega)| = 0$ *for* $s = 3$ *and* $s \geq 5$
2) $|\mathcal{S}(n,4,\omega)| = 2\binom{2^n}{3}$
3) $|\mathcal{S}(n,2,\omega)| = \beta$
4) $|\mathcal{S}(n,1,\omega)| = \alpha$
5) $|\mathcal{S}(n,0,\omega)| = 2^{2^n} - [\alpha + \beta + 2\binom{2^n}{3}]$, *where*

$\alpha = \mu(\omega) - \left[2\beta + 4 \cdot 2\binom{2^n}{3}\right]$ *and*
$\beta = \left[\binom{2^{n+1}}{2} - 2^n\right]\binom{2^{n-1}}{2^{n-2}} - \binom{4}{3}2\binom{2^n}{3}$ *for* $n \geq 4$.

For the remaining values of FDT_6, we exploit previously known affine classification of $\mathcal{B}_6$. In the next section, a brief introduction on affine equivalence will be given.

B. Affine Equivalence Classes in $\mathcal{B}_6$

Two Boolean functions f and g are called *affine equivalent* if $f(x) = g(Ax+a) \oplus bx \oplus c$, where A is a nonsingular binary $n \times n$ matrix, $a, b \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$.

The set of affine equivalent functions is called an affine *equivalence class*. Many cryptographic features are preserved by affine equivalence such as algebraic degree, nonlinearity or more importantly, the absolute values of Walsh coefficients.

Proposition 3. ***([?]) For every two affine equivalent functions, the distribution of the absolute values of their Walsh spectrum is equal.***

In 1991, Maiorana [**?**] discovered 150.357 equivalence classes in $\mathcal{B}_6$. This classification was later confirmed by the works of Braeken et. al. [**?**], Fuller [**?**], and Langevin [**?**]. We used the data, specifically the representative and the cardinality of each class from [**?**] to create FDT_6 by means of the following algorithm.

Algorithm 1 Complete FDT_6 for $\omega < 32$

Input: $(f_1, c_1), (f_2, c_2), ..., (f_{150357}, c_{150357})$ ▷ Representatives and cardinalities of equivalence classes in $\mathcal{B}_6$
Output: FDT_6

```
ω ← 0
for s ← 0, 2^6 do                                   ▷ Initialize the table
    while ω ≤ 2^6 do
        FDT_6[s][ω] ← 0
        ω ← ω + 2
    end while
end for
for i ← 1, 150357 do                                ▷ Main loop
    WalshSpectrum_i ← abs(WHT(f_i))
    [U, C] ← Count_Unique(WalshSpectrum_i)†
    for j ← 1, length(U) do
        if U[j]<32 then
            FDT_6[C(j)][U(j)] ← FDT_6[C(j)][U(j)] + c_i
        end if
    end for
end for
return FDT_6
```

† ▷ Count_Unique is any procedure that can give unique elements and their respective counts from an input vector.

In order to simplify numbers obtained by this algorithm, we define the normalized versions of $|\mathcal{S}(n,s,\omega)|$ and FDT_n to be as follows.

- $|\overline{\mathcal{S}(n,s,\omega)}| = \frac{|\mathcal{S}(n,s,\omega)|}{2^{n+1}}$
- $\overline{FDT_n}$ is the *normalized function distribution table* of $\mathcal{B}_n$ such that its (s,ω) entry contains $|\overline{\mathcal{S}(n,s,\omega)}|$.

Note that, these definitions are appropriate since $bx \oplus c$ part

TABLE III
FDT_6, $|\omega| = 32$

$s \setminus \lvert\omega\rvert$	**32**
0	143626699006838909
1	488451200955648
2	37868060664
3	0
4	651
5	0
...	0
64	0

in the definition of affine equivalence contributes 2^{n+1} number of times for all functions in an equivalence class as $b \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. In other words, all $|\mathcal{S}(n,s,\omega)|$ values must be divisible by the factor 2^{n+1}.

As an encyclopedic reference, the output of Algorithm **??** is given as $\overline{FDT_6}$ in Appendix **??**. In order to ease its readability and to cut the excess of zeros appearing when $17 \leq s \leq 64$ and $16 \leq \omega \leq 30$, the table is divided into two parts and shortened. One of the important values of this table is the one corresponding to $(s,\omega) = (64,8)$ entry of the table where 42.386.176, the number of 6-variable bent functions divided by 2^{6+1} is seen.

Using the same data and Algorithm **??**, a modified version of the Algorithm **??**, we were able to obtain a survey on the number of functions for each level of nonlinearity, which was also given in [**?**].

Algorithm 2 Number of functions for each nonlinearity in $\mathcal{B}_6$

Input: $(f_1,c_1),(f_2,c_2),...,(f_{150357},c_{150357})$ ▷ Representatives and cardinalities of eq. classes in $\mathcal{B}_6$
Output: Number of Functions per Nonlinearity

1: **for** $nl \leftarrow 0,26$ **do** ▷ Initializing the table
2: $f_{counts}[nl] \leftarrow 0$
3: **end for**
4: **for** $i \leftarrow 1,150357$ **do** ▷ Main loop
5: $WalshSpectrum_i \leftarrow abs(WHT(f_i))$
6: $W_{max} \leftarrow MAX(WalshSpectrum_i)*$
7: $nl = 2^{n-1} - \frac{W_{max}}{2}$
8: $f_{counts}[nl] \leftarrow f_{counts}[nl] + c_i$
9: **end for**
10: **return** f_{counts}

The output of Algorithm **??** is shown as Table **??**, which has been ordered from the highest nonlinearity level of 28 to the lowest 0 value. Note that, the counts below the nonlinearity 16 are equal to the values in $s = 1$ column of Table **??**. This is basically due to the fact that there is a single Walsh value in this part of FDT_n is maximal in the spectrum.

IV. Conclusion and Further Study

In this paper, we have presented the distribution of Boolean functions of 6 variables according to the frequency of Walsh coefficients by means of affine equivalence classes in $\mathcal{B}_6$. Previously, the exact distributions were given in [**?**] for functions with 5 or less variables. The idea of affine equivalence enabled us to lessen the number of functions to check in $\mathcal{B}_6$, from 2^{64} to only $150357 \approx 2^{17.2}$. We have presented two algorithms using the data of representatives and cardinalities of each class; one to complete the function distribution table and one to create the table showing the number of functions per nonlinearity.

FDT_7 can be studied for further analysis. However, according to Hou [**?**], there are about 2^{65} affine equivalence classes in $\mathcal{B}_7$. This makes the algorithms presented here inefficient. In order to find answers for the entries of FDT_7, more efficient algorithms should be found.

TABLE IV
Number of functions for each Nonlinearity

nl(f)	# f
28	5425430528
27	347227553792
26	1617838297055232
25	103868560519987200
24	1305039828998603264
23	3821934098435833856
22	5097726702198767616
21	4011570131804454912
20	2291582136636334080
19	1087405010755682304
18	458313050588725248
17	176395152249028608
16	62526600834171264
15	20418431982428160
14	6125529594728448
13	1681517927964672
12	420379481991168
11	95180260073472
10	19388571496448
9	3525194817536
8	566549167104
7	79515672576
6	9596719104
5	975937536
4	81328128
3	5332992
2	258048
1	8192
0	128

Acknowledgment

The authors would like to thank Zülfükar Saygı and Çağdaş Çalık for their valuable contributions and feedback.

References

[1] A. Braeken, Y. Borissov, S. Nikova, B. Preneel, Classification of boolean functions of 6 variables or less with respect to some cryptographic properties., Automata, Languages and Programming. Springer Berlin Heidelberg, 2005. 324-334.
[2] C. Carlet, D. K. Dalai, K. C. Gupta, S. Maitra, Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction, Information Theory, IEEE Transactions on 52 (7), pp. 3105–3121, 2006.
[3] C. Carlet, P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions, Finite Fields and Their Applications 8 (1) pp.120–130, 2002.
[4] J. Fuller, Analysis of affine equivalent Boolean functions for cryptography, Ph.D. Thesis, QUT, Australia, 2003.
[5] X. D. Hou, AGL (m, 2) acting on R (r, m)/R (s, m), Journal of Algebra 171.3, pp. 921-938, 1995.
[6] P. Langevin, Classification of Boolean functions under the affine group http://langevin.univ-tln.fr/project/agl/agl.html, 2009.
[7] J. Maiorana, A Classification of the Cosets of the Reed-Muller Code R(1,6). Mathematics of Computation 57 (195), pp. 403414, 1991.
[8] S. Maitra, E. Pasalic, Further constructions of resilient Boolean functions with very high nonlinearity., IEEE Transactions on Information Theory 48 (7) pp.1825–1834, 2002.
[9] B. Preneel, Analysis and Design of Cryptographic Hash Functions, Ph.D. Thesis, KU Leuven, Belgium, 1993.
[10] E. Uyan, Ç. Çalık, A. Doğanaksoy, "Counting Boolean functions with specified values in their Walsh spectrum", Journal of Computational and Applied Mathematics, ISSN 0377-0427, http://dx.doi.org/10.1016/j.cam.2013.06.035, 2013.

APPENDIX

TABLE A - $\overline{FDT_6}, |\omega| \leq 30$

$s \setminus \lvert\omega\rvert$	0	2	4	6	8	10	12	14
0	72621222574527744	72057602467610624	72620544008126464	72057622083079424	72622095976660224	72057689154119936	72625034638355584	72142467633545216
1	0	0	0	0	0	662473154560	24023638388736	747614794924032
2	10583322640	0	0	0	0	9130356619776	207318618759168	2995695843194880
3	1722169774080	0	0	279982080	0	44785297890816	719428478963712	7242174646990080
4	18251051857920	0	0	242534476800	2961685440	209499448052160	2188257251009760	11859982725648960
5	87944051220480	0	0	72571355136	91554140160	581080576462848	4396261821235200	13938338817220608
6	266917829165568	0	0	5049693798912	5278134677760	1547109348830976	7844919431271552	12540151435773696
7	769143475666944	0	0	1041773322240	118695723612480	2917542785935680	10411747357832352	9616702651727040
8	2138149299686400	0	0	46160060567040	6868914011366 40	5100761866346496	12066003006382080	6865856427064320
9	4252057890877440	0	0	22294693048320	3207474708480	6941532029071360	11379448548235264	4128919532236800
10	6105590049226752	3563462590464	5375655936	318935587815936	209504767128384	8710898218998528	9359218987896960	1648147202994432
11	8202945889861632	0	0	34485840764928 0	3289041327882240	8950279657439232	5771002952171520	3562930997821 44
12	11169686287323648	17618712330240	173133918720	1147171079476800	13059723162336144	9129127308123648	4124139956982528	31220241776640
13	11950669988167680	13439139840 0	0	1634668654510080	13074183198720	7456265936437248	1301540936048640	1612696780800
14	9472893446016000	10751311872000	11087290368000	3155879210803200	72426209050944 0	6917940343480320	962121643130880	22855680
15	6560061945163776	28670164992	260859303936	3799950102336192	9483549226012848	4811912521887744	312211255867392	10303340544
16	4761952300046592	590073040908288	286056593956224	59661067007324 16	29265523912590336	3886013057246208	113765111566848	0
17	3019781441617920	0	8090362183680	64173068660736 00	4959042600960	2320173419397120	4676820664320	0
18	1421987940696960	2137171158958080	2903602090072320	7885495224337920	302041308119040	1434637361332224	207628438929408	0
19	487272272578560	2167009782497280	120229064847360	6729634715811840	3691807869173760	674302121902080	53756559360	0
20	184216244655744	1362013145579520	12934924056375552	9404376692368896	9531988828669440	296361927622656	107513118720	0
21	117198498816000	6934460358131712	676423606118400	5145082754961408	290808053760	87344169615360	84978881003520	0
22	24292389687552	5486797902458880	24611185665803520	6930253495388160	15474924541440	27830050762752	5375655936	0
23	456630773776000	4270958641152000	1421993706577920	4389266748948480	177256654848000	1451427102720	0	0
24	128100272307840	15327122841354240	19624795765182720	3093122840801280	394568875975680	854505308160	11293655826432	0
25	7570715443200	3923109128945664	1071088413954048	2437301570715648	385255342080	0	0	0
26	99314340475392	8882293960802304	6217932249865728	1516734154801152	8648086487040	0	0	0
27	73120261559296	8271606505078784	250634358374400	724202892492800	50166815784960	0	0	0
28	17335115481600	2729334178099200	753267543104160	618725559029760	72125261493376	2712715264	0	0
29	50189027696640	4319361943142400	7310892072960	145874343444480	684556185600	0	0	0
30	29400528995712	3071917184716800	31322467233792	134730475364352	17263717801344	0	0	0
31	8641366917120	754841031081984	2016	19061180006400	99358640640000	0	0	0
32	16938738915840	1395015149316096	1310636113920	18082642636800	128254086213120	0	0	0
33	1338081024000	117579781079040	0	2153622159360	197107384320	0	0	0
34	2711626444800	218435229250560	0	2814379868160	7552796590080	0	0	0
35	151222321152	11670581035008	0	525278380032	45617816272896	0	0	0
36	46625911584 0	39555770268672	0	302853505024	53903749939200	0	0	0
37	5879623680	1633975418880	0	80634839040	24078458880	0	0	0
38	142153901568	10712646346752	0	0	2019230760960	0	0	0
39	16297290240	1359966289920	0	0	13923508838400	0	0	0
40	16825173120	1207842693120	11293655826432	0	15514367016960	0	0	0
41	1959874560	138871111680	0	0	0	0	0	0
42	840133728	57568315392	84978881003520	5119672320	0	0	0	0
43	209986560	13439139840	0	0	0	0	0	0
44	142178400	9099417600	191545260318720	0	0	0	0	0
45	0	10665984	10695763427328	597295104	0	0	0	0
46	3749760	10543325184	1606894058864 64	0	6089610240	0	0	0
47	0	0	25688915804160	0	1007935488 00	0	0	0
48	241950660	15484842240	51895751792640	0	111866840064	0	0	0
49	0	1142784000	16050995527680	0	0	0	0	0
50	0	0	6288285523968	0	0	0	0	0
51	17498880	1119928320	3226793472000	0	0	0	0	0
52	0	0	376225920000	0	0	0	0	0
53	0	0	179188531200	0	0	0	0	0
54	546840	34997760	34430018560	0	0	0	0	0
55	0	0	5711634432	0	0	0	0	0
56	11160	714240	281981952	0	0	0	0	0
57	0	0	279982080	0	0	0	0	0
58	0	0	104993280	0	0	0	0	0
59	0	0	0	0	0	0	0	0
60	651	41664	4999680	0	0	0	0	0
61	0	0	0	0	0	0	0	0
62	0	0	0	0	0	0	0	0
63	1	64	0	0	0	0	0	0
64	0	0	0	0	42386176	0	0	0

$s \setminus \lvert\omega\rvert$	16	18	20	22	24	26	28	30
0	736401371888883852	78376899729410752	91801043670119456	110117258751722048	125833798480977392	135582604969668032	140532277216848224	142737029667930944
1	5240629419250176	18947976160909824	29921358592984320	27393590186016768	16966291037375232	8345818667585280	3564137512349568	1376946651273984
2	12560023422051840	22835525169348864	17361660563856000	6108505058154240	1292022710254080	186233857770240	18768803969664	1211745943296
3	17917219124686560	15589394844663360	4453518280108128	485968528731840	22914064812240	530580832320	4500024480	10707648
4	16964459254387680	6659042781484800	546544843474560	98370478886 40	161782145280	0	42663936	0
5	10864229316820992	1545493802065920	30350253459456	28222193664	0	0	0	0
6	4861454914971648	155468441216256	699893953920	281148672	291648	0	0	0
7	1513645200518040	5332394704896	11945902080	0	0	0	0	0
8	418173220747800	53756559360	31997952	0	0	0	0	0
9	104723252838400	995491840	0	0	0	0	0	0
10	30139398955008	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	354120459840	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	241284036	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
...	0	0	0	0	0	0	0	0
64	0	0	0	0	0	0	0	0

24 Bit Renkli Dokümanların Farklı Biyometri Teknoloji Kullanılarak Güvenliğinin Sağlanması

Mehmet Kıvılcım Keleş, Ali Güneş

***Özet* — Günümüzde fiziksel dokümanların saklanması, erişimi ve kullanım konularında çeşitli zorluklar vardır. Bilişim ve iletişim teknolojilerindeki gelişmeler fiziksel dokümanların dijital olarak saklanmasını gündeme gelmiştir. Sonuçta birçok kurum ve kuruluş dokümanlarını dijital ortama taşımıştır. Ancak dokümanların dijital ortama taşınması bu alandaki sorunları toptan çözmemiş, aksine yeni sorunların ortaya çıkmasına neden olmuştur. Dijital ortama taşınan dokümanların çalınması, yetkisiz kullanıcılar tarafından açılması ve içindeki bilgilere erişilmesi telafisi çok güç sonuçlar doğurabilmektedir. Bu durum dokuman gizliliğinin ihlali ve bilginin çalınması gibi durumlar doğurabilir. Bu çalışmada, dijital doküman oluşturulma aşamasında veya oluşturulduktan sonra biyometrik yöntemlerle nasıl güvenliğinin sağlanabileceği üzerinde durulmuştur. Çalışmada, avuç damar izi okuyucular kullanılarak oluşturulan biyometrik veriyi, dijital filigran yöntemi ile saklamak ve dokümanı bu şekilde şifreleme konusu ele alınmıştır. Çalışmada 24 renkli dijital bir doküman avuç damar izi teknolojisi kullanarak Steganografi yöntemi ile şifrelenmektedir. Doküman güvenliğinin sağlanması, erişimi ve ilk oluşturanın tespit edilmesi konusunda da, Parmak izi ve avuç damar izi teknolojileri karşılaştırılarak başarı oranları ve süreleri karşılaştırılmaktadır.**

Anahtar Kelimeler — Avuç Damar izi, Doküman güvenliği, Dijital filigran, Şifreleme, , Parmak izi

Abstract — Today, storage, access and usage of the physical documents present various difficulties. The emergences of information and communication technologies have enabled physical documents to be stored as digitally. As a result, many agencies and institutions have moved their physical documents to digital environment. However, transformation of documents to digital media did not solve the problems relating to document, but has led to the emergence of new problems. When these documents are digitized, unauthorized access to the information may present risky consequences. This situation may result in violation of secrecy and theft of information on the document. In this study, we will discuss how security can be achieved by using biometric methods during or after the creation of 24 bit color digital documents. In this study, we will cover the use of palm vein biometric data being used as a digital watermark, in order to secure the document with this encryption method. Also, we will analyze how palm vein data is used as steganography method for encryption and recognition technology in 24 bit color digital documents. These methods are used in providing security of the document for access, and also to identify the creator. Fingerprint and palm vein technologies are compared in regards to their success rates and times.

Keywords— 24 Bit Document security, Biometry, Encryption, Palm Vein, Fingerprint, Watermarking.

I. GİRİŞ

SON yıllarda network altyapısının iyileşmesi ve bulut teknolojilerinin gelişmesi ile dijital ortamdaki dokümanlarda bilgi güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır. Özellikle internetin de yaygınlaşması güvenlik açıklarını beraberinde getirmiş, bunun sonucu olarak da dijital veri güvenliği önemli bir boyut kazanmıştır. Dijital ortama taşınan dokümanların çalınması, yetkisiz kullanıcılar tarafından açılması, içindeki bilgilere erişilmesi ve değiştirilmesi telafisi çok güç sonuçlar doğurabilmektedir. Bu durum dokuman gizliliğinin ihlali ve bilginin çalınması gibi durumlar doğurabilmektedir.

Dijital veri güvenliğini sağlamak amacıyla çeşitli koruma mekanizmaları geliştirilmiş, yeni teknoloji ve uygulamalar ortaya çıkmıştır. Günümüzde en sık kullanılan teknolojilerden biri şifrelemedir. Bu teknoloji de korunması istenen veri, şifreleme algoritmaları ve bir anahtar yardımı ile anlaşılmaz hale dönüştürülmektedir. Ancak şifrelerin zaman içinde kırılabilmesi, unutulması veya çalınması durumları sıklıkla karşımıza çıkmaktadır. Zaman içinde veri güvenliği için şifrelerin tek başına yeterli olmadığını göstermektedir. İşte bu noktada steganografi bilimi gündeme gelmektedir.

Bilgi gizleme yönteminin önemli bir alt disiplini olan Steganografi, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir [1]. Steganografi kökleri binlerce yıl öncesine dayanan bir bilim dalıdır [2]. Görüntü dosyaları üzerinde bilgi gizlemek için geliştirilmiş yöntemleri 3 başlık altında sınıflandırabiliriz. Bunlar En önemsiz bite ekleme, Maskeleme ve filtreleme, Algoritmalar ve dönüşümler [3].

II. DİJİTAL DOKÜMANLARIN YAPISI

Bilgisayar ortamında dijital dokümanlar 24 bit renkli, 8 bit renkli, 4 bit renkli, 8 bit gri tonlamalı, 4 bit gri tonlamalı veya 1bit siyah beyaz olarak saklanırlar. Görüldüğü gibi, 24 bit renkli dokümanlar bilgi saklamak için en fazla alanı sağlamakta ve farklı şifreleme algoritmaları kullanabilme imkânı vermektedir. 24 bit veya 8 bit Renkli dokümanlarda bütün renk değişimleri üç temel rengin birleşmesiyle elde edilir. Bu tip resimler, resimde kullanılan renkleri içeren 256 renkli bir palet taşırlar. Her piksel bu palette bir renge karşılık gelen 3 baytlık değer taşır.

III. BİYOMETRİ TEKNOLOJİSİ

Biyometrik sistemler temelde, kişinin sadece kendisinin sahip olduğu, değiştiremediği ve diğerlerinden ayırt edici olan, fiziksel veya davranışsal bir özelliğinin tanınması ile çalışmaktadırlar [4]. Biyometrik uygulamalar için de en yaygın olarak kullanılmaya başlanan özellik parmak izi tanıma yöntemidir [5]. Parmak izi, elde edilmesinin kolay olması ve kriminal alanda da kullanılabilir olması önemli tercih sebebidir. Biyometrik yaklaşımlar içinde avuç içi, diğer modellere göre yeni bir biyometrik özelliktir [6]. Avuç içi biyometri teknolojisi avuç içindeki damar yapısının sayısallaştırılması sonucu elde edilir. Avuç içi diğer biyometrilere göre en büyük avantajı taklit edilmesinin daha zor olması ve avuç içi özelliklerinin karakteristik, kalıcı ve dış faktörlerden daha az etkilenebilir olmasıdır. Şekil 1 de Avuç içi damar yapısı ile parmak izi görüntüleri gösterilmektedir.



Sekil 1. Avuç damar İzi ve Parmak izi resmi

Farklı biyometri teknolojileri geliştirilmiş olmasına rağmen genel yaklaşım olarak hepsi birbirine teknolojik olarak yakındır. Biyometrik tanıma sistemlerinde, ilk adım görüntüyü kaydetmektir. Bu görüntü sayısal koda çevrilir. Bu kod şifreleme algoritmaları kullanarak şifrelenir ve bilgisayara kaydedilir. Daha sonra kullanıcı herhangi bir biyometrik cihaz kullanarak kendini sisteme tanıtır. Kullanıcının kendini sisteme tanıttığı andaki duruşu ve çevre koşullarından dolayı sistem de kayıtlı olan sayısal kod ile doğrulama aşamasında üretilen kodun birbiriyle tamamıyla aynı olma olasılığı yoktur [7]. Biyometri teknolojilerinde kişi doğrulaması için kayıt olan sayısal kod ile üretilen kodun birbiriyle belirli oranda tutması yeterlidir.

IV. VERİ SAKLAMA YÖNTEMİ – EN ÖNEMSİZ BİTE EKLEME

En önemsiz bite ekleme yöntemi yaygın olarak kullanılan bir yöntemdir. Bu yöntemde; görüntüdeki her pikselin her byte'nın en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri belirlenmiş olan bir fonksiyon ile birer birer yerleştirilmektedir. Bu yöntemde eğer değişiklik olmuşsa da değişiklik yapılan bitin byte'nın en az anlamlı biti olmasından dolayı, değişimler insan tarafından algılanamaz boyutta olmaktadır [8].

Örnek olarak saklamak istediğimiz bir biyometrik verinin 1 byte'nın ikili sistemdeki değeri: 101101101 olsun.

Biyometrik verinin saklanacağı resmin 3 pikselinin değeri:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Resmin içine "101101101" biyometrik veri gizlendiğinde oluşan yeni piksel değerleri aşağıdaki gibi olmaktadır.

10010101 0000110**0** 11001001
1001011**1** 0000111**0** 1100101**1**
10011111 00010000 11001011

Bilginin gömülmesinden sonra bitlerin eklendiği sekiz bayttan sadece dördünde değişiklik meydana geldiği görülmektedir.

V. GÖRÜNTÜ ŞİFRELEME YÖNTEMİ – KARMAŞIK RESİM ŞİFRELEME ALGORİTMASI

Bu çalışmada görüntü şifreleme yöntemi olarak, karmaşık resim şifreleme algoritması kullanılmıştır. Bu algoritma, Chang ve Chen tarafından sunulan karmaşık bir sisteme dayalı yeni bir resim şifreleme yöntemidir [9]. Bu algoritma herhangi bir veri kaybı olmadan, yer değiştirme özelliğini kullanan bir şifreleme algoritmasıdır.

MXN büyüklüğündeki bir görüntüyü f fonksiyonu ile gösterirsek. (x, y) f görüntüsünün koordinatlarını göstermek üzere 0< x < M-1, 0< y < N-1 olacak şekilde f(x, y), görüntüsünün (x, y) noktalarındaki gri görüntü seviyesini göstermektedir,

Algoritma aşağıdaki gibi tanımlanmıştır.

Tanım 1: ROLRJp: f — f eğer /=0 ise f resmindeki i. satırı (0 < i < M-1), p piksel sola, /=1 ise p piksel sağa döndürmek için tanımlanmıştır [10].

Tanım 2: ROUDJ^p: f — f eğer /=0 ise f resmindeki j. sütun (0 < j < N-1), p piksel yukarıya, 1=1 ise p piksel aşağıya döndürmek için tanımlanmıştır [10].

Tanım 3: ROURf ^ p: f — f f resmindeki (x, y) pozisyonundaki pikselleri döndürmek için tanımlanmıştır, öyle ki; x + y = k, 0 < k < M + N - 2, eğer 1=0 ise aşağı-sol yönünde p piksel, 1=1 ise yukarı-sağ yönünde p piksel döndürmek için tanımlanmıştır [10].

Tanım 4: ROULk^p: f — f f resmindeki (x, y) pozisyonundaki pikselleri döndürmek için tanımlanmıştır, öyle ki; x - y = k, -(N - 1) < k < M- 1, eğer 1=0 ise yukarı-sol yönünde p piksel, 1=1 ise aşağı-sağ yönünde p piksel döndürmek için tanımlanmıştır [9].

5x7 boyutunda verilen resmi aşağıda ele alalım.

$$\mathrm{ROLR}^{22}(f),\ \mathrm{ROUR}^{\wedge 2}(f)\ \text{ve}\ \mathrm{ROUL}_0^2 \setminus f)$$

İşlemlerinin sonuçları sırasıyla şekil 2'de gösterilmektedir [11].

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35

a) Orjinal Resim

1	2	3	4	5	6	7
8	9	10	11	12	13	14
20	**21**	**15**	**16**	**17**	**18**	**19**
22	23	24	25	26	27	28
29	30	31	32	33	34	35

b) Sağa – Sola Öteleme

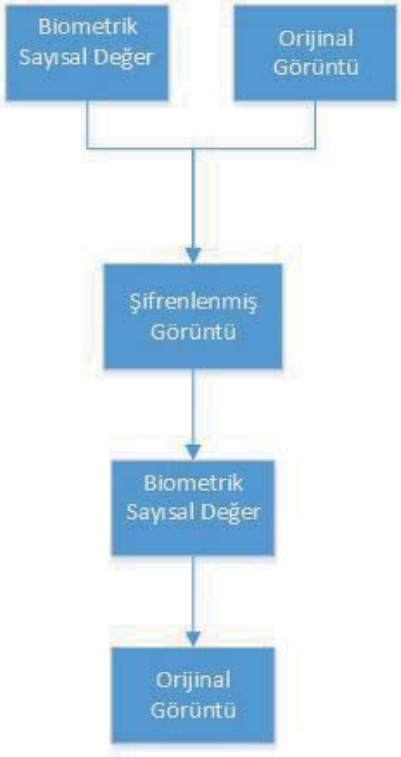
1	2	3	4	5	**18**	7
8	9	10	11	**24**	13	14
15	16	17	**30**	19	20	21
22	23	**6**	25	26	27	28
29	**12**	31	32	33	34	35

c) Sola Aşağı – Yukarı Öteleme

1	2	**19**	4	5	6	7
8	9	10	**27**	12	13	14
15	16	17	18	**35**	20	21
22	23	24	25	26	**3**	28
29	30	31	32	33	34	**11**

d) Sağa Aşağı – Yukarı Öteleme

Şekil 2. Karmaşık resim şifreleme algoritmasının matrislerde gösterilmesi



Şekil 3. Görüntü şifreleme ve çözme yapısı

VI. GERÇEKLEŞTİRİLEN SİSTEM MİMARİSİ

Parmak izi veya Avuç damar izi sayısal verileri ile görüntülerin şifrelenmesi ve görüntünün içine veri gizlenmesi için kullanılan sistem topolojisi şekil 3'de gösterilmektedir.

VII. SONUÇLAR

Bu çalışmada, kullanım oranı hızla artan dijital dokümanların güvenliği Parmak izi biyometrik verisi veya avuç damar izi biyometrik verisi kullanılarak şifrelenmesi anlatılmıştır.

Bu bölümde iki biyometrik verinin şifrelemede kullanılmasıyla elde edilen sonuçları ele alınmaktadır.

Program ile değişik boyutlardaki 24 bit resimler karmaşık şifre algoritması kullanılarak şifrelenmiş, parmak izi veya avuç damar izi veriler resmin içine gizlenmiştir.

Yapılan çalışmada gizlenmek istenen parmak izi verisi için farklı parmak izi sensörleri kullanılmış ve sensör cinsine göre parmak izi biyometrik verisinin 0,5-1 KB arası olduğu gözlemlenmiştir. Gizlenmek istenen Avuç damar izi biyometrik verisinin 2-3 KB arası olduğu tespit edilmiştir.

Biyometrik sayısal veri en önemsiz bite ekleme yöntemi kullanılarak resim içine gizlendiğin de resmin üzerinde gözle görünür bir bozulma olmadığı tespit edilmiştir.

Geliştirilen sistem, .net platformu üzerinde c# yazılım dili ile kodlanmıştır. Test amacıyla Windows 7 64 bit işletim sisteminde Intel i7 2.3 GHz işlemci ve 8GB ana belleğe sahip bilgisayar üzerinde çalıştırılmış ve Parmak izi veya Avuç Damar izi verisinin alınması dâhil şifreleme işleminin ortalama 2 saniye olduğu tespit edilmiştir.

Tablo 1 de, 24 bit renkli üç farklı bitmap resim için önce avuç damar izi sayısal verisi kullanılarak şifreleme işlemi yapılmış ve süreler ölçülmüştür. Aynı üç resim için parmak izi sayısal verisi kullanılarak işlem tekrar edilmiş ve bu süreler karşılaştırılmıştır.

Tablo 1. Avuç damar izi ve Parmak izi ile şifreleme karşılaştırma tablosu

Resim	Resmin Boyutu	Şifrelenen Veri Boyutu [Byte]		Şifreleme Süresi [sn]	Şifre Çözme Süresi [sn]
Örnek 1.bmp	2420X3464	Avuç Damar İzi	2393	2,6	2,5
		Parmak İzi	512	0,9	0,8
Örnek 2.bmp	1976X1147	Avuç Damar İzi	2142	2,1	2,2
		Parmak İzi	480	0,6	0,6
Örnek 3.bmp	1964X1101	Avuç Damar İzi	2215	2,0	1,9
		Parmak İzi	510	0,7	0,6

Oluşturulan yeni resim karmaşık resim şifreleme algoritması ile karıştırılmış olup orijinal görüntünün elde

edilebilmesi için parmak izi veya Avuç damar izi sayısal verisinin uygulama tarafından doğrulanması ile mümkündür.

KAYNAKLAR

[1] Petitcolas F.A.P., Anderson R.J., Kuhn M.G., "Information Hiding–A Survey", Proceedings of the IEEE,Special Issue on Protection of Multimedia Content, 87(7):1062-1078,July 1999..

[2] Caldwell, 2nd Lt. J., "Steganography", CROSSTALK The Journal of Defense Software Engineering, 25-27 (2003).

[3] Sellars D., "An Introduction to Steganography", Student Papers, 1999. http://www.cs.uct.ac.za/courses/CS400 W/NIS04/papers99/dsellars/index.html

[4] Parmak İzi Kullanarak Görüntü Şifreleme Nazlı Akın1, Büşra Takmaz, Erdal Güvenoğlu Maltepe Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul

[5] Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri 6th International Advanced Technologies Symposium (IATS'11), 16-18 May 2011, Elazığ, Turkey

[6] R. Brunelli, D. Falavigna, Person identification using multiple cues, IEEE Trans. Pattern Anal. Mach. Intell. 955–966, 1995.

[7] J. D. Woodward, Jr., N.M. Orlans, P. T. Higgins,―Biometrics‖, McGraw-Hill, 2003

[8] Andaç ŞAHİN, Ercan BULUŞ, M.Tolga SAKALLI - 24-BİT RENKLİ RESİMLER ÜZERİNDE EN ÖNEMSİZ BİTE EKLEME YÖNTEMİNİ KULLANARAK BİLGİ GİZLEME Trakya Univ J Sci, 7(1): 17-22, 2006 ISSN 1305-6468

[9] CHANG C.C., Hwang M.S., Chen T.S.,2001, A new encryption algorithm for image cryptosystems, The Journal of Systems and Software.

[10] Erdal Güvenoğlu , Nurşen Suçsuz - Yer Değiştirme ve Değer Dönüştürme Özelliğine Sahip Görüntü Şifreleme Algoritmalarının Analizi - IX. Akademik Bilişim Konferansı Bildirileri 31 Ocak - 2 Şubat 2007 Dumlupınar Üniversitesi, Kütahya

[11] ÖZTÜRK İ, Soğukpınar İ, 2004. Analysis and Comparison of Image Encryption Algorithms, IJIT Volume 1 Number 2 ISSN:1305 - 239X.

Mehmet Kıvılcım KELEŞ (1986) Zonguldak Karaelmas Üniversitesinden 2011 yılında mezun oldu. Halen İstanbul Aydın Üniversitesinde yüksek lisansına devam etmektedir. Çalıştığı konular biyometrik sistemler ve görüntü işlemedir.

Ali GÜNEŞ (1952) Ortadoğu Teknik Üniversitesinden 1976 yılında mezun oldu. Halen İstanbul Aydın Üniversitesinde Bilgisayar mühendisliği bölümünde görev yapmaktadır.

Kamu Kurumlarında Elektronik İmza Hakkında Karşılaştırmalı Bir Çalışma

Çiğdem Selçukcan Erol, Fatma Önay Koçoğlu, Zeki Özen and Elif Kartal

***Özet*— Yeni teknolojiler her geçen gün organizasyonlara çalışmalarını kolaylaştırmalarına yönelik yeni fırsatlar sunmaktadır. Birçok farklı görevi gerçekleştirmek için elektronik ortamdan faydalanılmaktadır. Bugün, elektronik imza (e-imza), özel sektörde ve kamu kurum ve kuruluşlarında ıslak imzanın yerine kullanılmaya başlanmıştır. Bu çalışmanın amacı, e-imza kullanan kamu kurumlarında çalışan personelin e-imza konusundaki görüşlerini belirleyebilmek; e-imza kullanmayan kamu kurumlarında çalışan personelin ise e-imzaya geçiş sürecinde hazır olup olmadığını tespit edebilmek, çalışma sonuçları ile onlara yol gösterici olabilmektir. Bu kapsamda, sırası ile Sakarya Sosyal Güvelik Kurumu ve İstanbul Üniversitesi personeline e-imza konulu bir anket uygulanmıştır. Ankete toplamda 107 kamu personeli katılmıştır. Bu anket çalışmasının bulgularına göre çalışanlar e-imza kullanımından genel anlamda memnundur, ancak konuya karşı merak oldukça azdır. E-imzaya geçiş sürecinde; personelin e-imza konusunda eğitim gereksinimi, personel tarafından e-imza uygulamasına karşı geliştirilebilecek olası direnç ve mevcut iş süreçlerinin gözden geçirilmesi/yenilenmesi dikkat edilmesi gereken temel unsurlar olarak belirlenmiştir. "Kurum içi kurum dışı yazışma", e-imzanın en çok kullanıldığı/kullanılması planlanan seçenek olarak görülmekte iken e-imzayı kullanan veya kullanmayan araştırmamıza katılan personelin çoğu e-imza kullanımının kurum içinde kâğıt israfını azaltacağını düşünmektedir.**

***Anahtar Kelimeler*—Elektronik imza, E-imza, İstanbul Üniversitesi, Sakarya Sosyal Güvenlik Kurumu.**

***Abstract*— New technologies offer new opportunities for organizations to make their works easier. Electronical environment is used for performing many different tasks. Today, electronic signature (e-signature) has been used instead of the wet signature in private sector and public institutions and organizations. The aim of this study, to determine opinions about e-signature of the staff working in public institutions which use e-signature; to determine whether staff working in public institutions which do not use e-signature is ready for the transition in the use of e-signature, to be a guide for them with the results of the study. In this context, a questionnaire about e-signature is conducted to staff who works respectively in Sakarya Social Security Institution and in Istanbul University. A total of 107 staff participated to our research. According to the findings of this survey, staff is satisfied with the use of e-signature in general; however curiosity toward the subject is quite low. In the process of transition to e-signature; training need of staff about e-signature, possible resistance which can be developed by staff to implementation of e-signature and review of existing business processes / regeneration are identified as the main factors to be considered. On one hand "In-house non-institutional correspondence" could be seen as the most used / planned to be used option for e-signature, on the other hand staff whether uses or does not use e-signature consider that use of e-signature will reduce paper wastage within the organization.**

***Keywords*—Electronic signature, E-signature, İstanbul University, Sakarya Social Security Institution.**

I. Giriş

GÜNÜMÜZDE bilişim teknolojileri, kurum ve kuruluşların çalışmalarına büyük ölçüde yardımcı olmaktadır. İşletmelerdeki iş kalemlerinin önemli bir kısmı, bilişim teknolojileri yardımıyla gerçekleştirilmektedir. 2003 yılında ABD'de işyerlerinde bilgisayar kullanım oranı %55,5 olarak tespit edilmiştir [1]. 2011 verilerine göre dünyada 1,6 milyar ünite bilgisayar kullanılmakta olup [2], 2012 verilerine göre ise dünya nüfusunun %34,3'ü internet kullanmaktadır [3].

Bilgisayarların kullanımının yaygınlaşması ve internet teknolojilerinin gelişmesi, günlük hayattaki alışkanlıklarımızı ve iş görme/iş verme biçimlerimizi de değiştirmektedir. Artık alışveriş, eğitim, eğlence gibi faaliyetler bilgisayarla da gerçekleştirilebilmektedir. Örneğin, yemeğe gitmek yerine internet üzerinden yemek siparişi verilebilmekte, internet üzerinden dersler takip edebilmekte veya iş toplantılarına bir web kamerası aracılığı ile katılabilmek mümkün olmaktadır.. Buna paralel olarak, "Bilgi Çağı" olarak adlandırılan günümüzde, vatandaşların kurumlardan ve devletten hizmet beklentileri de değişmektedir. Bu değişimi karşılamak amacıyla ortaya çıkan e-devlet hizmet anlayışı, kamu yönetiminde her türlü faaliyetin, vatandaşlar, işletmeler, kamu çalışanları ve devletin diğer fonksiyonlarıyla ilgili etkileşimlerinin elektronik ortam üzerine taşınması, birebir ve aracısız olarak kullanılabilir hale gelmesini amaçlamaktadır [4].

Artan internet ve bilgisayar kullanımı beraberinde bilgisayar ile gerçekleştirilen işlemlerde işlemin geçerliliği için işlemi yapan kişinin gerçekten o kişi olup olmadığının tespiti [5] ve işlem verilerine daha sonradan üçüncü taraf kişilerce tahrifat yapılıp yapılmadığının doğrulanması gereksinimlerini; diğer bir deyişle elektronik dünyada ıslak imzanın yerine geçebilecek yeni bir teknolojiyi, e-imzayı gündeme getirmiştir.

Manuscript received July 15, 2013.

Ç. Selçukcan Erol is with the Department of Informatics, İstanbul University, İstanbul, Turkey (e-mail: cigdems@istanbul.edu.tr).

F. Ö. Koçoğlu is with the Department of Informatics, İstanbul University, İstanbul, Turkey (e-mail: fonayk@istanbul.edu.tr).

Z. Özen is with the Department of Informatics, İstanbul University, İstanbul, Turkey (e-mail: zekiozen@istanbul.edu.tr).

E. Kartal is with the Department of Informatics, İstanbul University, İstanbul, Turkey (e-mail: elifk@istanbul.edu.tr).

Elektronik imza (e-imza), imza sahibinin kimliğini imzalanan veriyle ilişkilendirmekte ve imzalanan verinin değiştirilmediğini ispat etmektedir [6]. E-imzanın fonksiyonları, elektronik ortamda gönderilen veya alınan bilgilerin, bunları gönderen kişi veya kuruma ait olduğunun doğrulanması (*kimlik doğrulama*), gönderilen veya alınan bilgilerin içeriğinin değiştirilmemesi, içeriğin başkaları tarafından elde edilse bile anlaşılamaması (*veri bütünlüğü*) ve verileri gönderenlerin gönderdiğini ve alanların aldığını inkâr edememesi (*inkâr edilemezlik*) şeklinde açıklanabilir [7].

Türkiye'de 15.01.2004 tarihli 5070 sayılı Elektronik İmza Kanunu çıkarılmış, elektronik imzanın elle atılan imza ile aynı hukukî sonucu doğurduğu belirtilerek e-imzaya hukukî statü kazandırılmıştır. E-imzanın şifre, parmak izi, retina taraması gibi birçok çeşidi olmakla birlikte [9], bu çalışmada söz konusu olan e-imza, kanunda geçtiği şekliyle "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi" işaret etmektedir [8].

Kanunun hukukî altyapı oluşturmasıyla kamu ve özel kurumlarda e-imza kullanımına yönelik çalışmalar hız kazanmıştır. Türkiye İstatistik Kurumu verilerine göre, 2010 yılı Ocak ayında girişimlerin %10,1'inin e-imza kullandığı tespit edilmiştir [10]. Türkiye Bilişim Derneği "Kamu Bilişim Birimlerinin Analizi ve Öneriler Mayıs 2013" raporunda kamu kurumlarında e-imza bilincinin yerleştiği, kamu kurumlarının %37,7'lik kısmında e-imza kullanıldığı ifade edilmiştir [11]. E-imzanın yaygınlığı arttıkça kullanım sayısı da artış göstermektedir. 2012 senesinde kamu ve özel sektörde ayda yaklaşık 5 milyon e-imza doğrulaması gerçekleştirilmiştir [12].

Kâğıtsız ofis ortamlarının yaratılması hedeflenen günümüzde, özellikle birçok kritik işlemin gerçekleştirildiği kamu kurumlarında çalışan personelin, e-imza konusunda bilgi sahibi olması önem taşımaktadır. Bu çalışmadaki amaç, e-imza kullanan kamu kurumlarında çalışan personelin, e-imza konusundaki görüşlerini belirleyebilmek; e-imza kullanmayan kamu kurumlarında çalışan personelin ise e-imzaya geçiş sürecinde e-imza kullanımına hazır olup olmadığını tespit edebilmek ve çalışma sonuçları ile onlara yol gösterici olabilmektir. İki farklı grubun görüşlerinden yola çıkılarak, kamu kurumlarında e-imzaya geçişte ve e-imza uygulaması sırasında olası sorunlar ve ihtiyaçlar tespit edilerek sürecin iyileştirilmesi hedeflenmiştir. Çalışmanın, ikinci bölümünde kapsam, malzeme ve veri analizi konularını içeren çalışma yöntemi hakkında bilgilere yer verilmiştir. Üçüncü bölümde çalışmanın bulguları ortaya konulmuş, dördüncü bölümde ise sonuçlar ve öneriler paylaşılmıştır.

II. YÖNTEM

A. Kapsam

Çalışmada e-imza kullanan ve kullanmayan iki farklı kamu kurumu ele alınarak personelin e-imza hakkındaki görüşlerinin saptanması ve iki grup arasındaki olası farklılıkların incelenmesi amaçlanmıştır. Bu nedenle çalışma kapsamına Sakarya Sosyal Güvenlik Kurumu (Sakarya ili) ve İstanbul Üniversitesi (İstanbul ili) personeli dâhil edilmiştir. İki farklı ilde bulunan çalışanlar, sırası ile kurumlarında e-imza kullanan ve kullanmayan iki ayrı grubu temsil etmektedir.

Araştırmaya toplam 107 personel katılmıştır. Katılımcı sayılarının kurumlara göre dağılımı aşağıdaki tabloda verilmiştir (Tablo 1).

TABLO I
KATILIMCILAR

Kurum Adı	Katılımcı Sayısı
Sakarya Sosyal Güvenlik Kurumu	53
İstanbul Üniversitesi	54

B. Malzeme

Bu çalışmadaki bulgular, 18 sorudan oluşan e-imza konulu ankete verilen cevapların analizi ile elde edilmiştir. İki kısımdan oluşan anketin birinci kısmında katılımcıların e-imza bilinci ve konu hakkında bilgi sahibi olup olmadıklarını tespit etmeye yönelik sorulara, ikinci kısımda ise katılımcıların yaş, cinsiyet gibi demografik özelliklerine ilişkin sorulara yer verilmiştir.

Anket çalışması önce Sakarya Sosyal Güvenlik Kurumu'nda çalışan personele uygulanmış daha sonra ise anket soruları üzerinde değişikliğe gidilerek henüz e-imzanın kullanılmadığı İstanbul Üniversitesi personeline uygulanmıştır (Örneğin; "Elektronik imzayı hangi işlemleriniz için kullanıyorsunuz?" sorusu "Elektronik imzayı hangi işlemleriniz için kullanmayı düşünürsünüz?" biçiminde değiştirilmiştir).

Sakarya Sosyal Güvenlik Kurumu'nda yapılan anket çalışmasında kurumdan gerekli izinler alınmış olup, anket cevapları üçüncü taraf kişilere açılmayacak, sonuçlar ilk kez konferansta paylaşılacaktır.

C. Veri Analizi

Çalışmada kullanılan veri, anket yardımı ile toplanmış ve Google Drive'da oluşturulan anket formu aracılığı ile elektronik ortama aktarılmıştır. Çalışmanın bulgular kısmında verilen yanıtlar sonucunda Google Drive tarafından sunulan özet bilgilerinden faydalanılmıştır. Elde edilen bulgular sonuçların daha iyi anlaşılmasını sağlayabilmek adına grafikler ile de görselleştirilmiştir.

III. BULGULAR

Bu bölümde iki farklı kamu kurumunda uygulanan e-imza anketinin sonuçlarına yer verilmiştir. İki farklı ilde bulunan anket katılımcıları, e-imza kullanıp kullanmamalarına göre farklılık gösterdiğinden, elde edilen sonuçlar da iki farklı alt bölümde incelenmiştir. Bulgular kısmında verilen oranlar, soruya cevap veren katılımcı sayısına göre hesaplanmıştır.

A. İstanbul Üniversitesi'nden Elde Edilen Bulgular

Anket çalışmamıza İstanbul Üniversitesi'nden yaşları 21 ile 56 arasında değişen 54 personel katılmıştır. Katılımcıların %49'u kadın, %51'i erkek personeldir. Katılımcıların meslekî dağılımı 36 memur, 5 şef, 4 işçi, 2 profesör, 2 lisans öğrencisi, 1 yardımcı doçent ve 1 uzman şeklindedir. Katılımcıların %44'ü (20 kişi) lisans, %36'sı (16 kişi) lise, %9'u (4 kişi) ortaokul, %7'si (3 kişi) yüksek lisans ve %4'ü (2 kişi) doktora mezunudur. Katılımcıların hane içi aylık gelir dağılımı aşağıdaki tabloda verilmiştir (Tablo 2).

TABLO II
KATILIMCILARIN HANE IÇI AYLIK GELIR DAĞILIMI

Hane İçi Aylık Gelir	Kişi Sayısı	Yüzde (%)
1.000 TL altı	1	3
1.000 TL - 2.000 TL	18	49
2.001 TL - 5.000 TL	16	43
5.001 TL ve üzeri	2	5

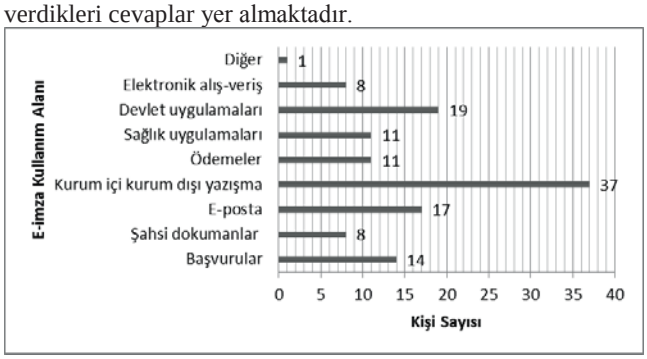
Katılımcıların %85'i (46 kişi) kurumunda elektronik belge yönetim sisteminin kullanılmadığını belirtmiştir. Katılımcıların %22'si (12 kişi) e-imza hakkında yeterli bilgiye sahip olduğunu, %78'i ise (42 kişi) yeterli bilgiye sahip olmadığını söylemiştir.

Katılımcıların tamamı (53 kişi) kurumunda e-imza kullanılmadığını belirtmiştir. Katılımcıların %92'si (47 kişi) kurum haricinde e-imza satın almayı düşünmediğini ifade etmiştir. "Elektronik imza bedelinin nasıl karşılanmasını istersiniz?" sorusuna cevap veren katılımcıların neredeyse tamamı (50 kişi - %98), kurumunun e-imza bedelini karşılamasını talep etmektedir. Katılımcılardan 32 kişi (%67) e-imzayı güvenilir bulmaktadır.

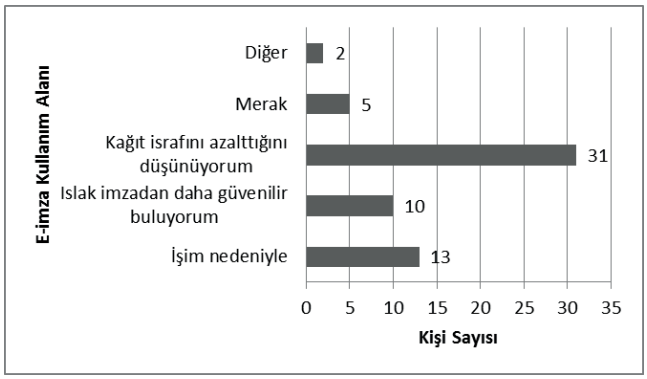
Anket sonucunda, katılımcıların %71'inin (35 kişi) e-imzanın hukukî yaptırımları hakkında bilgi sahibi olmadığı, sadece %8'inin (4 kişi) bilgi sahibi olduğu ortaya çıkmıştır.

Katılımcıların %53'ü (26 kişi) öncelikli olarak ıslak imzayı kullanmayı tercih ederken; %47'si (23 kişi) öncelikli olarak elektronik imzayı kullanmak istediğini söylemiştir.

Aşağıdaki grafiklerde (Şekil 1, Şekil 2) katılımcıların e-imzayı hangi sebepler ile kullanacaklarına ve e-imzayı hangi işlemler için kullanmayı düşündüklerine ilişkin sorulara verdikleri cevaplar yer almaktadır.



Şekil 1: Katılımcıların "Elektronik imzayı hangi işlemleriniz için kullanmayı düşünürsünüz?" sorusuna verdikleri yanıtlar (İstanbul Üniversitesi)



Şekil 2: Katılımcıların "Hangi sebepler ile elektronik imza kullanırsınız?" sorusuna verdikleri yanıtlar (İstanbul Üniversitesi)

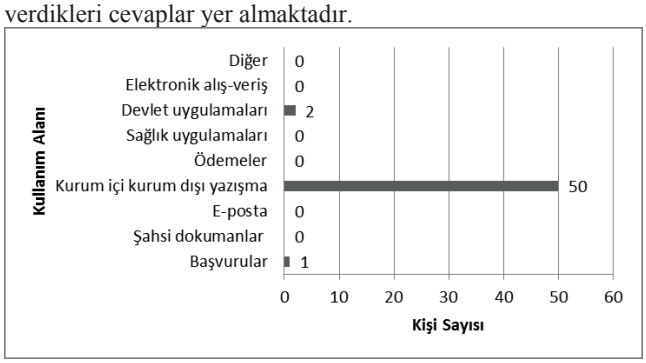
B. Sakarya Sosyal Güvenlik Kurumu'ndan Elde Edilen Bulgular

Anket çalışmasına Sakarya Sosyal Güvenlik Kurumu'ndan yaşları 27 ile 62 arasında değişen %30'u kadın (16 kişi), %70'i erkek (37 kişi) toplam 53 personel katılmıştır. Katılımcıların mesleki dağılımı 49 memur, 1 müdür, 1 şef, 1 veri hazırlama ve kontrol işletmeni şeklindedir. Katılımcıların %38'i (20 kişi) lisans, %62'si (32 kişi) ise lise mezunudur. Katılımcıların %45'inin (24 kişi) hane içi aylık gelirleri 2.001 TL – 5.000 TL arasında iken, %55'inin (29 kişi) 1.000 TL – 2.000 TL aralığındadır.

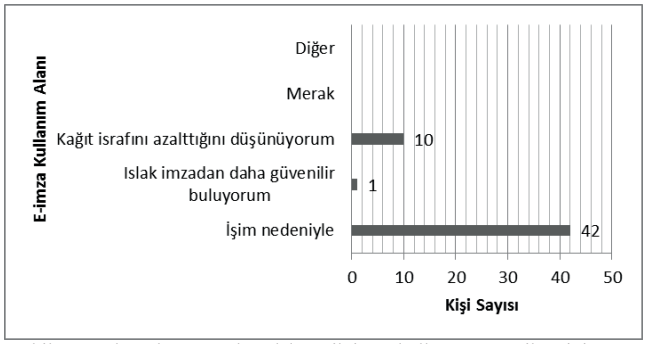
52 kişi kurumunda e-imza ve elektronik belge yönetim sisteminin kullanıldığını ve e-imzayı güvenilir bulduğunu ifade ederken, 53 kişi e-imza bedelinin kurumu tarafından karşılandığını söylemiştir.

Katılımcıların %34'ü (18 kişi) e-imza hakkında yeterli bilgiye sahip olduğunu, %66'sı (35 kişi) ise yeterli bilgiye sahip olmadığını söylemiştir. "E-imza kullanımından memnun musunuz?" sorusuna cevap veren 33 kişiden 30'u e-imza kullanımından memnun olduğunu dile getirmiştir. Katılımcıların %81'i (43 kişi) elektronik imzanın yaptırımları hakkında bilgi sahibi iken, yalnızca 7 kişinin (%13) bilgi sahibi olmadığı gözlemlenmiştir.

Aşağıdaki grafiklerde (Şekil 3, Şekil 4) katılımcıların e-imzayı hangi işlemler için tercih ettikleri ve e-imza kullanmayı tercih etme nedenleri hakkındaki sorulara verdikleri cevaplar yer almaktadır.



Şekil 3: Katılımcıların "Elektronik imzayı hangi işlemleriniz için kullanıyorsunuz?" sorusuna verdikleri yanıtlar (Sakarya Sosyal Güvenlik Kurumu)



Şekil 4: Katılımcıların "Neden elektronik imza kullanmayı tercih ettiniz?" sorusuna verdikleri yanıtlar (Sakarya Sosyal Güvenlik Kurumu)

IV. SONUÇ

Bu çalışmada, e-imza kullanan ve kullanmayan iki farklı kurum personeline e-imza konulu anket uygulanarak elde edilen veriler analiz edilmiştir ve bulgular ortaya konmuştur. Elde edilen bulgular yorumlandığında aşağıdaki sonuçlara

ulaşılmıştır:

Kamuda çalışan personele, e-imza uygulamasına geçmeden önce e-imza konusunda eğitim verilmesi faydalı olacaktır. Çalışanların yaş aralığı, eğitim seviyesi, bilişim teknolojilerini yeteri kadar iyi kullanamayan personelin bulunma olasılığı göz önüne alınarak; e-imzanın hem uygulaması, hem de hukukî yaptırımları hususlarında personelin bilgi sahibi olması gerektiği sonucuna ulaşılmıştır. Bu konuda üniversitelerin ilgili birimlerinden (Enformatik, Bilgisayar Mühendisliği, Hukuk Fakültesi vb.) ya da özel sektörde e-imza temin edilen firmalardan destek istenebilir. E-imza hakkında kurum personeline eğitim verilirken, e-imzanın hukukî boyutunun da eğitim içeriğine dâhil edilmesi oldukça faydalı olacaktır.

Elde edilen bulgulara göre, e-imza kullanan kurum personelinin çoğunun e-imzanın hukukî yaptırımları hakkında da bilgi sahibi olduğu ortaya çıkmıştır. Bu durum e-imza kullanmayan kurumda ise tam tersidir.

E-imzayı kullanan personelin çoğunun e-imzayı güvenilir bulması ve e-imza kullanmayan kurum personelinin çoğunun e-imzayı güvenilir bulmaması da personelin konu hakkındaki bilgi düzeyi veya kullanım tecrübesi ile ilişkilendirilebilir. Belki de bu nedenle, e-imza tecrübesi olan personel e-imzayı ıslak imzadan öncelikli tercih ederken, diğer grupta bu durum tam tersidir. Ancak e-imza kullanan personelin çoğu e-imzayı güvenilir bulurken, elektronik imzayı tercih etme nedenleri arasında "Islak imzadan daha güvenilir buluyorum" seçeneğini işaretleyenlerin sayısının yalnızca 1 olması düşündürücüdür.

Kurum içerisinde yalnızca e-imza hakkında eğitim vermekle sınırlı kalınmayıp, kurum yönetiminin kurum içinde e-imza kullanımına karşı direnç gösteren personeli e-imza kullanımına motive edici toplantı ve seminerleri düzenlemesi önem taşımaktadır.

"Kurum içi kurum dışı yazışma", e-imzanın en çok kullanıldığı/kullanılması planlanan seçenek olarak düşünülmektedir. E-imza kullanmayan kamu kurumunda çalışan personel, e-imzayı başvurular, şahsi dokumanlar, e-posta, kurum içi kurum dışı yazışma, ödemeler, sağlık uygulamaları, devlet uygulamaları, elektronik alış-veriş gibi birçok farklı alanda kullanabileceğini belirtirken; e-imzayı kullanan kurum personeline ait cevaplar, devlet uygulamaları, başvurular ve kurum içi kurum dışı yazışma şıklarında yoğunlaşmıştır. Bu doğrultuda, kurumunda e-imza kullanan ve kurumu tarafından e-imza temin edilen personelde "e-imzayı yalnızca devlet işlerinde kullanabilirim" olgusunun oluştuğu söylenebilir. Henüz uygulamaya geçmeyen kurum personelinin e-imza hakkında yeterli tecrübeye/bilgiye sahip olmamasından dolayı e-imzayı her alanda rahatça kullanabilecekleri fikrine sahip oldukları düşünülebilir.

Çalışmada anketin uygulandığı e-imzayı kullanan veya kullanmayan personelin çoğu, e-imza kullanımının kurum içinde kâğıt israfını azaltacağını düşünmektedir. Burada yalnızca kâğıt israfı bir maliyet kalemi olarak görülmemeli, bir işlemin gerçekleştirilmesi sırasında fiziksel olarak bulunup atılması gereken ıslak imzanın yerini elektronik imza almasından dolayı işlemin gerçekleşme süresinin kısalacağı, personelin/vatandaşın karşılıklı işlerini gerçekleştirirken kolaylık sağlayacağı da göz ardı edilmemelidir.

Kişisel görüşmeler sırasında birkaç personelin, kurumundaki iş süreçlerinden bir kısmının e-imzaya uygun olmadığı görüşünde olduğu gözlemlenmiştir. Bu düşünce personelin e-imza konusundaki bilgi eksikliğinden kaynaklanıyorsa, bu eksikliğin giderilmesi ya da e-imza gibi yeni bir uygulamaya geçerken mevcut iş süreçlerinin de gözden geçirilmesi, iş süreçlerinin e-imza ile sorunsuz çalışacak şekilde uyarlanması/yenilenmesi gündeme gelmektedir. Bu durum kurumların yönetimleri tarafından dikkate alınmalıdır.

E-imza kullanmayan kurum çalışanları e-imza bedelinin kendi kurumları tarafından karşılanmasını talep etmektedir. Bu talep, e-imza uygulamasına geçiş sürecinde yöneticiler tarafından dikkate alınması gereken önemli bir unsurdur. Kurum içinde e-imza uygulaması bir proje olarak düşünülürse, bu unsur projenin maliyet kalemini etkileyecektir. Aksi halde personelin e-imza bedelini kendisinin karşılamasının istenmesi, kurumların e-imzaya geçiş sürecinin uzamasına sebep olacaktır.

Çalışanlar e-imza kullanımından genel anlamda memnundur; ancak e-imzaya karşı merakın oldukça az olduğu gözlemlenmiştir. E-imza uygulamasının kamu kurumlarının özellikle stratejik işlemleri gerçekleştiren birimlerinde kullanılma sürecinin kurum yönetimi tarafından itina ile planlanması, uygulamaya geçmeden personele e-imza hakkında eğitim verilmesi, e-imza kullanımına geliştirilebilecek olası dirençlere karşı önlemlerin alınması tavsiye edilmektedir. Uygulama aşamasında yönetici-personel ilişkilerinde dayanışma ile uygulamanın devamlılığı sağlanmalıdır.

KAYNAKLAR

[1] Bureau of Labor Statistics, U.S. Department of Labor, "The Editor's Desk, Computer use at work in 2003 on the Internet,". [Çevrimiçi]: http://www.bls.gov/opub/ted/2005/aug/wk1/art03.htm. [Erişim Tarihi: 13-Tem-2013].

[2] Computer Industry Almanac Inc., "PCs In-Use Reached over 1.6B in 2011 USA has nearly 311M PCs In-Use," [Çevrimiçi]: http://www.c-i-a.com/pr02012012.htm. [Erişim Tarihi: 12-Tem-2013].

[3] Internet World Stats, "World Internet Users Statistics Usage and World Population Stats," [Çevrimiçi]: http://www.internetworldstats.com/stats.htm. [Erişim Tarihi: 12-Tem-2013].

[4] M. Erdal, *Elektronik devlet: e-Türkiye ve Kurumsal Dönüşüm.* İstanbul: Filiz Kitabevi, 2004.

[5] M. Güler ve U. Ömürgönülşen, "Türkiye'de e-İmza Alanındaki Hukuki Düzenlemeler ve Bazı Kamu Kurumlarındaki e-İmza Uygulamaları," *Sosyoekonomi Dergisi*, c 2011–1, ss 197–230.

[6] E. Gülaçtı, "Elektronik İmza ve Güvenlik," [Çevrimiçi]: http://www.uekae.tubitak.gov.tr/uekae_content_files/EtkinlikWeb/E-imza.pdf. [Erişim Tarihi: 15-Tem-2013].

[7] Ş. Sağıroğlu, D. Kabasakal, ve M. ALKAN, "Elektronik İmzadan Mobil Elektronik İmzaya Geçiş Sürecinde Türkiye," *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, Ankara, 2006, ss 21–27.

[8] "Elektronik İmza Kanunu". [Çevrimiçi]: http://www.tbmm.gov.tr/kanunlar/k5070.html. [Erişim Tarihi: 12-Tem-2013].

[9] Ş. Sağıroğlu ve N. Özkaya, "Açık Anahtar Altyapısı ve Biyometrik Teknikler", *Ulusal Elektronik İmza Sempozyumu*, *ISCTURKEY 2006*, 2006.

[10] DPT, "Bilgi Toplumu İstatistikleri," DPT Yayın No: 2826, Haz 2011.

[11] Türkiye Bilişim Derneği (TBD), "Kamu Bilişim Birimlerinin Analizi ve Öneriler," TBD/Kamu-BIB/2013-ÇG 3E, May 2013.

[12] E-Tuğra, "Türkiye'de E İmza Kullanımı," [Çevrimiçi]: http://www.e-tugra.com.tr/E%C4%B0mza/E%C4%B0mzaNedir/detaysayfas%C4%B1/tabid/135/ArticleId/4/Turkiye-de-E-mza-Kullan-m.aspx. [Erişim Tarihi: 12-Tem-2013].

Ç. Selçukcan Erol, 1980 yılında İstanbul'da doğdu. 2001 yılında İstanbul Üniversitesi Fen Fakültesi Biyoloji Bölümü'nden mezun oldu. Yüksek Lisans derecesini 2005 ve Doktora derecesini 2010 yılında İstanbul Üniversitesi Fen Bilimleri Enstitüsü Biyoloji Anabilim Dalı'nda aldı. Şu anda İstanbul Üniversitesi Enformatik Bölümü'nde Yardımcı Doçent olarak görev yapmaktadır. Yrd. Doç. Dr. Selçukcan Erol matematiksel ve hesaplamalı biyoloji, biyolojik çeşitliliğin korunması ve gelişim biyolojisi konularında çalışmalarını sürdürmektedir**.**

F. Ö. Koçoğlu, 1984'te İstanbul'da doğdu. 2009 yılında İstanbul Üniversitesi Fen Fakültesi Matematik Bölümü'nü bitirdi. 2012 yılında İstanbul Üniversitesi Fen Bilimleri Enstitüsü Enformatik Anabilim Dalı'nda yüksek lisans derecesini aldı. Şu anda İstanbul Üniversitesi Enformatik Bölümü'nde Araştırma görevlisi ve Doktora öğrencisidir. Arş. Gör. Fatma Önay Koçoğlu; veri madenciliği, veri bilimi, veri yapıları ve bilgi yönetimi alanlarında çalışmalarını sürdürmektedir.

Z. Özen, 1983 İstanbul doğumludur. 2008 yılında İstanbul Üniversitesi, Fen Fakültesi Fizik bölümü mezunudur. 2012 yılında İstanbul Üniversitesi Enformatik Bölümünde yüksek lisans eğitimini tamamlamıştır. Şu anda aynı bölümde hem araştırma görevlisi olarak çalışmakta hem de doktorasını yapmaktadır.
Araş. Gör. Özen, bilgi güvenliği, veritabanı sistemleri, sayısal algoritmalar, veri yapıları, kaynak kod intihali ve kaynak kod benzerliği üzerine çalışmaktadır.

E. Kartal, 1986 yılında Sakarya'da doğmuştur. İstanbul Üniversitesi Fen Fakültesi Matematik Bölümü'nden 2008'de mezun olmuştur. İstanbul Üniversitesi Enformatik Bölümü'nde 2011 yılında yüksek lisansını tamamlamıştır. Şu anda İstanbul Üniversitesi Enformatik Bölümü'nde hem araştırma görevlisi olarak çalışmakta hem de doktorasını yapmaktadır.
Araş. Gör. Kartal, sınıflandırmaya dayalı makine öğrenmesi konusu üzerine çalışmaktadır. Diğer ilgi alanları, yapay zeka, makine öğrenmesi, yapay sinir ağları, web tasarımı, programlama dilleri, e-öğrenme, felsefe, müzik, tango, salsa ve karikatür çizmektir.

Donanımsal Truva Atı Tespiti Etkinlik Analizi

M. Şahinoğlu, M. Öztemür ve B. Soysal

***Özet*—Bilgi güvenliğinin sağlanması tüm dünyada üzerinde çalışılan kritik bir konudur. Bu konuda ortaya çıkan en önemli tehditlerden birisi donanım yapıları üzerine truva atı yerleştirilmesidir. Sahip olduğu kritik önem nedeniyle tüm dünyada donanımsal truva atlarının tespitine yönelik çalışmalar yapılmaktadır. Bu kapsamda farklı yöntemler önerilmektedir. Bu yöntemlerin farklı açılardan birbirlerine karşı avantaj ve dezavantajları olabilir. Truva atı tespitinde başarıya ulaşılabilmesi için bu yöntemlerin güvenlik ihtiyacına bağlı olarak etkin bir şekilde kullanılması gerekmektedir. Bu makale kapsamında, literatürdeki truva atı tespit yöntemleri anlatılacak ve bir etkinlik analizi yapılacaktır.**

***Anahtar Kelimeler*—Truva atı, Arka kapı, Yan kanal analizi, Mantıksal davranış testi.**

***Abstract*—Information security is an important subject studied on all over the world. One of the most important threats encountered in this subject is placement of trojan horse on hardware. Studies regarding the detection of trojan horse on hardware have been carried out all over the world because of its critical importance. Different methods are advised on this field. These methods may have advantages and disadvantages to each other in some terms. These methods must be used efficiently for detecting the trojan horse depending on the need of security. In the scope of this article, trojan dedection methods in literature will be explained and an efficency analyze will be presented.**

***Keywords*—Trojan horse, Backdoor, Side channel analysis, Logic test.**

I. GİRİŞ

TRUVA atı, adını Troya kentini ele geçirmekte kullanılan efsanevi tahta truva atından alır. Bir armağan gibi gösterilen bu büyük at, aslında Troya surlarını geçip Troya kentini ele geçirecek Yunan askerlerini taşımıştır. Yaklaşık 10 yıl süren savaş ile ele geçirilemeyen şehir, yüksek güvenlik sağlayan surlarına rağmen bu at sayesinde fethedilmiştir.

Asırlar sonrasında ise teknoloji ilerlemiş; ancak güvenlik önlemlerini bertaraf etmek için insanoğlu yine benzer yöntemlere başvurmuştur. Troya atı durumuna benzer senaryolar teknoloji ürünleri üzerinde de uygulanmaya başlamıştır. IT sektöründe ilk karşılaşılan truva atı 1974 yılında oluşturulan "Pervade-Animal" isimli bir yazılımdır. Aslında güvenlik açıklığı oluşturmayı amaçlamayan bu yazılım, ticari üstünlük sağlamak amacıyla birçok bilgisayara sızmayı başarmıştır. Daha sonra 1980'li yıllarda güvenlik ihlalleri oluşturan truva atları da piyasada yayılmaya başlamıştır [1],[2].

M. Ş. TUBİTAK BİLGEM Siber Güvenlik Enstitüsü , Gebze, KOCAELİ 41470 TÜRKİYE (Telefon Nu: 0262 648 10 00; fax: 0262 648 11 00; e-posta: muhammet.sahinoglu@ tubitak.gov.tr).

M. Ö. TUBİTAK BİLGEM Siber Güvenlik Enstitüsü , Gebze, KOCAELİ 41470 TÜRKİYE (Telefon Nu: 0262 648 10 00; fax: 0262 648 11 00; e-posta: muhammet.oztemur@ tubitak.gov.tr).

B. S. TUBİTAK BİLGEM Siber Güvenlik Enstitüsü , Gebze, KOCAELİ 41470 TÜRKİYE (Telefon Nu: 0262 648 10 00; fax: 0262 648 11 00; e-posta: betul.soysal@ tubitak.gov.tr).

Truva atları ilk aşamada daha çok yazılıma özgü bir uygulama gibi dikkate alınmıştır. Ancak son yıllarda, donanım yapıları içinde truva atlarının ciddi bir tehdit oluşturabileceği bilinci ortaya çıkmıştır. Bu durum "donanımsal truva atı" teriminin ortaya çıkmasına ve bu alanda ciddi çalışmalar yapılmasına zemin oluşturmuştur.

Donanımsal Truva Atı, "*elektronik bir devrenin içerisine, kullanıcının isteği olmaksızın, kasıtlı olarak yerleştirilmiş kötücül devre yapısı"* olarak tanımlanmaktadır [3]. Bu yapı, devrenin normal işleyişi ya da boşta beklemesi esnasında devrenin işlevlerini değiştirebilir, ekstra bir işlem yapmasına sebep olabilir, hatta güvenlik mekanizmalarını devre dışı bırakabilir. Böylece, kritik verilerin işlenmesinde, iletiminde ya da saklanmasında kullanılan ürünün verileri istenmeyen taraflara sızdırması sağlanabilir. Ayrıca, devrelerin içerisine yerleştirilen truva atları ile kritik işlevlerde kullanılmak üzere tasarlanan ürünler planlanmayan ve öngörülemeyen bir şekilde servis dışı kalabilirler [3].

Truva atı kavramı ile bir arada değerlendirilen kavramların biri de arka kapı'dır. Backdoor olarak da yaygın şekilde bilinen arka kapı, *"bir programa, bir online sisteme veya bir bilgisayar sistemine erişmek için standart dokümanlarında belirtilmeyen bir özellik"* demektir [4]. Arka kapılar, yazılımı veya daha genel anlamda sistemi meydana getiren kişiler tarafından oluşturulurlar. Genelde sadece bu kişiler tarafından bilinirler [4]. Arka kapı, bir bakıma truva atı yapısının özel bir hali olarak ta düşünülebilir.

II. GERÇEK HAYATTA TRUVA ATI ÖRNEKLERI

Donanım yapıları içerisine truva atı ve arka kapı yerleştirme uygulamaları ABD-Rusya arası soğuk savaş dönemine dayanmaktadır [5]. Bu dönemde Rusya ve ABD donanımsal truva atı uygulamaları ile birbirlerinin sinyallerini gizlice dinlemeyi başarmışlardır. Daha sonraki yıllarda da Avrupa ülkelerinin Suriye tarafından kullanılan radarlar üzerindeki bir işlemciye, Suriye'nin İsrail'i izlemesini engellemek amaçlı donanımsal truva atı yerleştirdiğinden ve bu şekilde çalışmasını durdurduğundan şüphelenilmiştir [5].

Günümüzde de, donanımsal ürünlerde truva atı ve arka kapı varlıkları konusunda medyada her gün yeni haberler çıkmaktadır. Örneğin, geçtiğimiz günlerde Avusturya Güvenlik Kurumu SEC Consult, Barracuda firmasına ait birçok üründe dokümante edilmeyen arka kapı bulunduğunu bildirmiştir. Firma, bunların üretim aşamasındaki deneysel çalışmalardan sonra unutulan özellikler olduğunu iddia etmiş olmakla beraber dolaylı bir şekilde bu arka kapıların varlığını kabul etmiştir. Cihazlara tasarımı esnasında gömülmüş olduğu iddia edilen bu arka kapılar, cihaz üzerinde kolayca aktif hale getirilebilen ek bir yönetici hesabı şeklinde tanımlanmıştır. Dolayısı ile bu yapılar, saldırganın uzaktan erişim ile yetkilendirilerek ağ üzerindeki hassas veriye erişmesine olanak sağlamaktadır [6],[7].

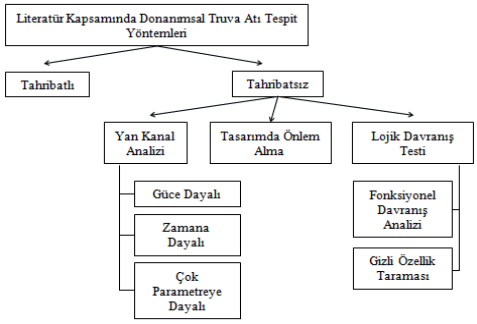
Benzer bir iddia da piyasada yaygın olarak kullanılan ZTE ve Huawei haberleşme cihazları için mevcuttur. Amerika, Çin menşeli ZTE ve Huawei haberleşme cihazlarının truva atı içermesi durumuna yönelik bir araştırma raporu yayınlamış ve bu cihazların kritik projeler içerisinde kullanılmasını engellemiştir [8].

Bu alanda ortaya çıkan en son gelişmelerden bir tanesi de HP firmasının yaygın olarak kullanılan depolama cihazlarında, kullanıcıların oluşturduğu hesaplar dışında, üretimden gelen dokümante edilmemiş erişim haklarının bulunduğunun itiraf etmesidir [9].

Donanım bazında, ilk arka kapı tespit edilmesi ise 2012 senesi yazında olmuştur. Sergei Scorobagatov bir askeri çip olan ACTEL FPGA üzerinde bulduğu arka kapıyı göstermiştir [10].

III. Donanımsal Truva Atı Tespit Yöntemleri

Donanımsal truva atları elektronik sistemlerin güvenliği için büyük bir tehdit oluşturduğundan bu yapıların tespiti için de yoğun bir çalışma yapılmaktadır. Bu çalışmalarda kullanılan yöntemler duruma göre farklılık göstermektedir. Donanımsal truva atlarının tespit edilmesine yönelik çalışmalar incelendiğinde, bu yöntemlerin Şekil 1'de görüldüğü gibi sınıflandırılabileceği değerlendirilmiştir.



Şekil 1. Donanım yapıları içinde truva atı tespiti için literatürde tanımlanmış yöntemlerinin sınıflandırması

A. Tahribatlı Yöntemle Truva Atı Tespiti

Truva atlarının tespit edilmesinde akla ilk gelen yöntemdir. Analiz edilecek olan elektronik devrenin öncelikle üst koruma katmanı açılır. Daha sonra gelişmiş cihazlar ve çeşitli kimyasallar kullanılarak aşama aşama tüm çip katmanları taranarak tersine mühendislik yapılır. Tersine mühendislikle elde edilen görüntüler birleştirerek, çipin en başta tasarlandığı şekilde üretildiğine karar verilir. Tersine mühendislik için en yaygın kullanılan teknik, elektron mikroskobu ile tarama ve light-induce voltage iteration tekniklerdir [14].

Tersine mühendislik yaparak truva atı aramak hem maliyet hemde zaman açısından çok zor bir uygulamadır. Çünkü donanımsal truva atları, bir mantıksal devre üzerinde az sayıda mantıksal kapının eklenmesi, kaldırılması veya modifiye edilmesi suretiyle gerçeklenebilir. Oysa modern bir elektronik devrede milyarlar düzeyinde bu şekilde kapının olması söz konusu olabilir. Bu kadar geniş bir yapı içerisinde truva atını tespit etmek samanlıkta iğne aramakla eşdeğer bir çalışma olabilir [3].

Bununla beraber, diğer bir çok truva atı tespit yöntemi için referans olarak ihtiyaç duyulan güvenilir devre (golden IC) [17] temini için tersine mühendislik yöntemi kullanılabilir.

B. Tahribatsız Yöntemle Truva Atı Tespiti

Tahribatlı devreler ile truva atı tespitinin büyük zorluk içermesi, tahribatsız yöntemlere yönelik çalışmalar yapılması ve bunların kullanılması sonucunu doğurmuştur. Tahribatsız truva atı tespit yöntemleri farklı gruplara ayrılmaktadır.

Mantıksal Davranış Testi

IC'lerin davranışsal yapılarının analiz edilmesi esasına dayanır. Fonksiyonel davranış analizi ve gizli özellik tarama olmak üzere iki grupta incelenir.

Fonksiyonel Davranış Analizi, bir elektronik devre girişine belli test vektörlerinin verilerek çıkışların izlenmesi ve beklenenin dışında bir çıkış elde edildiğinde bir anormalliğin var olduğunun tespit edilmesi esasına dayanır. Aslında bu yöntem, daha çok fonksiyonel hataların tespiti için geçerli bir uygulamadır [15]. Bununla beraber, parametrik truva atlarının (devrenin yapısını değiştirerek truva atı ekleme) tespiti için de kullanılabilir. Bu testlerde kullanılan otomatik test paternleri, normalde devrede olmayan bir fonksiyonu aktif etme yeteneğinde olmadıklarından (devreye ekleme/çıkarma yapılarak konulan) fonksiyonel truva atlarının (devreye ekleme/çıkarma yapılarak konulan) tespitinde kullanılamazlar [16].

Mantıksal test ile truva atı aramanın en büyük problemi büyük elektronik devre yapıları nedeniyle taranması gereken uzayın çok geniş olmasıdır. Uzayın bu kadar geniş olması, test vektörleri ile tüm uzayı taramayı neredeyse imkansız hale getirmektedir. Örneğin; sadece 4 trigger noktası ve 1 payload noktası olan bir truva atı düşünülsün. 451 kapılı c880 tipinde küçük bir ISCAS-85 Benchmark devresinde bu truva atının yerleştirilmesi için 10^{11} muhtemel nokta mevcuttur ve truva atını tetiklemek için yaklaşık 10^{9} deneme yapılması gerekir [17].

Bu kısıtın aşılması için bazı metodlar önerilmiştir. Jha ve Jha bu durum için rastsallığa dayalı bir yöntem önermiştir [18]. Devrenin girişlerine değişik paternler uygulanmıştır. Devrenin bu girişlere verdiği cevaplara bağlı olarak devreye ait olasılıksal (probabilistic) bir imza tespit edilmiştir. Daha sonra aynı paternler, analiz edilen devrelere uygulanmıştır. Devrelerin davranışları daha önce elde edilen olasılıksal imza değeri ile karşılaştırılmıştır. Eğer bir farklılık varsa bu devrelerin truva atlı olduğu sonucuna varılmıştır.

Wolf ve arkadaşları truva atı tespiti için devre üzerinde nadir olarak aktif olan alanlara yoğunlaşmışlardır. Nadir olarak aktif olan bölgeleri tetikleyen test vektörleri üretilerek elektronik devrenin davranışı gözlemlenmiştir [19]. Chackraborty ve arkadaşları da benzer bir yöntemle truva atı tespitinin etkinliğini artırmaya çalışmışlardır [20].

Gizli Özellik Tarama, analiz edilen yapının tanımlı olmayan özelliklerinin tespit edilmesi esasına dayanır. Bu konu ile ilgili bir çalışma Skorobogatov ve Woods tarafından gerçeklenmiştir [10]. Bu çalışmanın literatürdeki diğer donanımsal truva atı tespiti çalışmalarından önemli bir farkı gerçek bir donanım üzerinde gerçekleştirilmiş olmasıdır. Analiz edilen eleman ACTEL firmasına ait ProAsic3 tipi FPGA elemanıdır. Çalışma kapsamında araştırmacılar, analiz edilen FPGA elemanının JTAG arayüzüne yoğunlaşmışlardır. Bu arayüz aracılığı ile FPGA'e ürün dokümanında tanımlı olmayan komutlar

göndererek aynı zamanda elemanın çektiği gücü dinlemişlerdir. Çekilen gücün analizinden, JTAG arayüzünde tanımlı olmayan bazı başka komutların varlığını tespit etmişlerdir. Bu komutların birinin kullanılmak için 128 bit uzunluğunda bir veri talep ettiğini tespit etmişlerdir. Gelişmiş yan kanal analiz teknikleri kullanarak 128 bit uzunluğundaki bu değer elde edilmiştir. Bu anahtar kullanıldığında çipte tanımlı olmadığı belirtilen geri okunma özelliğinin aktif olduğu tespit edilmiştir. Ayrıca çip özelliklerinde "değişmez" olarak belirtilen bazı konfigürasyon bölgelerinin programlanabilir hale geldiği tespit edilmiştir.

Yan Kanal Analizi

Truva atının tespit edilmesinde, devrelerin çalışması esnasında istemsiz olarak yaydıkları yan kanal bilgilerinden faydalanılır. Bu yan kanal bilgisi devrenin güç-akım tüketimi, elektromagnetik yayınımı, çalışma frekansı, çalışma zamanı değerleri olabilir. Yan kanal analizi ile truva atı tespitinde temel yaklaşım olarak, güvenilir devreye ait yukarıda örnekleri verilen yan kanal verileri ölçülerek bir karakteristik çıkarılır. Daha sonra analiz edilecek devrelerin yan kanal bilgilerine bağlı karaktreristikleri orjinal devre ile karşılaştırılarak truva atının olup olmadığına karar verilir.

Yan kanal analizi ile yapılan truva atı tespit çalışmaları, kullanılan yan kanal parametresine göre sınıflandırılabilir.

Güç Tabanlı Analiz, truva atı tespitinde yan kanal parametresi olarak gücü kullanır.

Agrawal ve arkadaşlarının yaptıkları çalışma, truva atı tespitinde gücü ve dolayısıyla yan kanal bilgisini kullanan ilk çalışmadır [11]. Çalışmada öncelikle, rastgele seçilmiş bir grup elektronik devreye rastgele giriş verileri verilmiş ve devrelerin güç ölçümleri alınmıştır. Bu güç tüketimi değerleri bir imza değeri (fingerprint) olarak kabul edilmiştir. Geride kalan devrelere aynı rastgele veriler uygulanarak güç ölçümü almışlardır. Elde edilen değerleri, güvenilir devreye ait imza değeri ile karşılaştırmışlardır.

Yan kanal analizi ile truva atı tespitinde en önemli problemlerden biri, üretim saçılmasından kaynaklanan işlem gürültülerinin (process variation) devredeki yan kanal parametrelerini etkilemesidir. Bu parametrelerde yaşanan değişimler, truva atlarının devreye katacağı yan kanal değerlerinin maskelenmesine neden olmaktadır [26]. Bu da özellikle küçük truva atlarının tespit edilmesine engel oluşturmaktadır. Rad ve arkadaşları tarafından, process değişkenlerinin devreye etkisini azaltmak için devreye bölge tabanlı "transient power signal analizi" yapılması önerilmiştir [22].

Banga ve Hsiao [24]'de truva atının harcadığı gücün devrenin toplam güç tüketiminde fark edilebilir hale gelmesini sağlamak için bölge tabanlı truva atı tespit yöntemini önermiştir. Yine Banga ve Hsiao [25]'da truva atının harcadığı gücün devrenin toplam güç tüketiminde fark edilebilir hale gelmesini sağlamak için geçiş sayısı minimizasyonu (toggle minimization) yöntemini önermiştir. Geçiş sayısı minimizasyon yönteminde truva atının çektiği güç sabit kalırken devrenin çektiği toplam gücü azaltmak hedeflenmiştir.

Alkabani [26]'da truva atının tespitinin hassasiyetini artırmak için tutarlılık tabanlı kapı seviyesi karakterizasyonu yöntemini önermiştir. Alkabani çalışmasında tutarlılık metriği olarak devrenin gerçek güç ölçümleri ile simülasyon yoluyla elde edilmiş güç ölçümlerinin ölçekleme değerinin arasındaki farkı kullanmıştır. Ölçekleme değeri; kapının gerçek güç ölçüm değerini hesaplarken matematiksel işlemlerle elde edilen güç ölçümünün işlem (process) gürültüsünden kaynaklı çarpılması gereken sabit değeridir.

Reece, yan kanal analizi ile Truva atı tespitinde yaygın olarak ihtiyaç duyulan güvenilir devre kullanılmadan Truva atı tespiti yapan bir yapı önermiştir [29],[30]. Elektronik devre tasarımında kullanılan, Process Development Kit ile elektronik devrenin işlem gürültüsü (process variation) ile etkilenmeyecek parametreleri için devreye ait bir imza çıkarılmıştır. Bunun için elektronik devreye farklı voltaj beslemeleri verilirken elektronik devre üzerinde iki nokta arasında oluşan akım değerleri dikkate alınmıştır.

Güç analizi ile Truva atı tespitinde, sonuç alınması için, devreden alınan güç işaretlerinin işlenmesi önem kazanmaktadır. Literatürde bu kapsamda aşağıdaki gibi çalışmalar yapılmıştır.

Baktir ve arkadaşları, simülasyon ortamında gerçekledikleri 16 devreden 8 tanesine Truva atı yerleştirmişlerdir [31]. Daha sonra Truva atı olmayan devreler için elde edilen güç işaretleri ile truva atı içeren devreler için elde edilen güç işaretlerini karşılaştırmışlardır. Güç işaretleri için klasik yöntemle zaman uzayında karşılaştırma yapıldığında sonuç alınamamıştır. Bununla beraber, Discrete Waveleth Transform, Spektogram ve Neural Network kullanılarak işaretler işlendiğinde truva atlarının tespit edildiği gösterilmiştir.

L.Gwon ve arkadaşları DISTROY adını verdikleri bir test ortamıyla etkin sinyal analizi içeren bir yöntem önermişlerdir [33],[34]. Çalışmalarında genel olarak simülasyon ortamından elde ettikleri güç ölçümleri ile gerçek devreden aldıkları güç ölçümlerini karşılaştırarak truva atını tespit etmişlerdir. Ölçümlerin karşılaştırılması öncesinde güç ölçümlerinin işaretin farklı özellikler baz alınarak sıkıştırılması esasına dayanan "compressive sensing" işlemini uygulamışlardır. "Compressive sensing" yöntemi ile yöntemin kullanılmadığı sisteme oranla 10 kat daha hızlı ve 1000 kat daha az ölçüm analiz edilerek truva atı tespit edilmiştir.

ASIC sistemler için yapılan çalışmalar için ASIC modüllerini temin etme zorluğu, araştırmacıları simülasyon üzerinde çalışmaya yöneltmiştir. Oysa bu çalışmaların başarısının değerlendirilmesi için gerçek devreler üzerinde uygulamalar yapılması önemlidir. Bu durum araştırmacıları ASIC yapısının bir benzeri olarak kabul edilen FPGA elemanları üzerinde çalışmalar yapmaya yöneltmiştir.

Wang ve Luo, Spartan3E FPGA üzerinde DES algoritması gerçekleyerek pratik olarak Truva atı yerleştirme ve bulma çalışması yapmışlardır [35].

Zaman Tabanlı Analiz ile truva atı tespiti yapılmasında, yukarıda anlatılan güç tüketimi yerine zaman gecikmeleri kullanılır.

Jin ve Markis, çip üzerinde yer alan kapılar arası gecikmeleri ölçerek truva atı tespiti yöntemi önermişlerdir [36]. Önerdikleri yöntemde, öncelikle güvenilir tasarım üzerinden kapı gecikmeleri ölçülerek bu değerler bir imza (fingerprint) olarak kabul edilmiştir. Aynı yöntemle, değerlendirilen her bir devre için karakteristik çıkarılmıştır. Değerlendirilen devrelerin karakteristikleri, güvenilir devre

ile karşılaştırılarak truva atı olup olmadığına karar verilmiştir.

Wei ve arkadaşları, truva atı tespit etmek için zaman gecikmelerini kullanan yöntemlerin en büyük sıkıntısı olan paralel yollar probleminin çözümünüde içeren bir yöntem önermişlerdir [37]. Zira zaman gecikmesine bakılacak kısmın girişi ile çıkışı arasında birden fazla yol olabilmektedir (reconvergent path). Çalışmada, bu yollara test noktası (D Flip flop) eklenerek ve oradan zaman gecikmesini ölçerek paralel yol problemi ortadan kaldırılmıştır.

Yan kanal analizi ile truva atı tespitinde kullanılan bir yöntem de, birden fazla yan kanal parametresinin birlikte kullanılmasıdır. Çok Parametreli Analiz olarak bilinen bu yöntem kapsamında aşağıdaki çalışmalar yapılmıştır.

Narasinham ve arkadaşları simülasyon ortamında ve sonrasında FPGA kullanarak dinamik akım (I_{DDT}) ve çalışma frekansının maksimum değerini (F_{max}) birlikte kullanarak truva atı tespit etme yöntemini önermişlerdir [12]. I_{DDT} ve F_{max} için bir eğri oluşturulmuş ve eğriden farklılaşan değerler için truva atı tespit edilmiştir. Narasimham ve arkadaşları [13]'te de aynı yöntemle truva atı tespiti üzerinde çalışmışlardır. Ancak bu yöntemde, ek olarak truva atını tespit etme hassasiyetini artırmak için "power gating ve operand isolation" yöntemini kullanmışlardır. Bu yöntem, devrenin analiz edilen kısmı aktif iken geriye kalan kısımlarının pasif hale getirilmesi esasına dayanır.

Potkonjak ve arkadaşları, Kapı seviyesi karekterizasyonu (Gate Level Characterization) ile truva atı tespitini önermişlerdir [27]. Karakterizasyonun çıkarılmasında, statik güç tüketimi ve zaman gecikmesini kullanmışlardır.

Devrenin kontrol edilebilir kapı sayısını artırmak ve karakteristiği çıkarılan kapı sayısını artırmak için Wei [28]'de sıcaklık iyileştirmesini önermiştir. Bir kapının sıcaklığını artırmak için dışarıdan bir sistem ile ısıtmak yerine kapıların 0-1 geçişleri ile doğal yoldan sağlanan sıcaklık artımını kullanmıştır.

Tasarımda Eklenen Yapılar İle Truva Atı Tespiti

Bu yöntemle Truva atı tespitinde, elektronik devrenin üretilmesinden önce devreye truva atı eklenmesi durumunda bunu anlayan bir yapı eklenir. Bu yapı çoğu zaman bir devre veya devre parçasıdır. Literatürde "Design for Hadware Trust" olarak da bilinir. Bu yöntemin tasarıma hakim olunması durumunda uygulanabilen bir yöntem olduğu söylenebilir. Dolayısıyla ASIC devreler üzerinde uygulanabilir. Ancak araştırma çalışmalarında, ASIC üretmenin zorluğu nedeniyle, deneysel olarak FPGA üzerinde de uygulandığı görülmektedir.

Chacraboty ve arkadaşları, mantıksal test kullanarak truva atının eklenmesini tespit eden bir yapı önermişlerdir [38]. Bunun için devreye bir test lojiği ve I/O portları eklenir. Çip normal mod ve saydam mod (transparent mod) olmak üzere 2 modu içerir. Çipin saydam modda olduğu durumlarda devrenin bir imza değeri üreterek çıkışına vermesi sağlanır. Test işlemi, daha önce tanımlanmış anahtar benzeri bir paternin devreye verilmesi ile başlar. Truva atlarının devrelerin en az aktif olan kısımlarına yerleştirileceği varsayımından hareketle, truva atının tespitini sağlayan kontrol devrelerinin de devrelerin en az aktif olan bu kısımlarını gözlemlemesi gerekir. Verilen başlangıç değeri ile kontrol devresinin gözlemlediği değerlerde beklenen değerlerden (imza) farklı bir değer tespit edilmesi halinde truva atının varlığı tespit edilir. Bu yöntemde, devreye kontrol devreleri nedeniyle ek tasarım alanı ve karmaşıklığı oluşması en önemli dezavantajdır.

Bu yapıdan daha karmaşık ancak daha etkin bir önleyici truva atı tespit yöntemi Abromici ve Bradaley tarafından önerilmiştir [39]. Elektronik devre içine, devrenin çalışması esnasında gerçek zamanlı kontrol yaparak truva atını tespit eden bir kontrol lojiği eklenmektedir. DEFENCE (DEsign-For_ENabling-Security) mantıksal olarak da bilinen yapının en önemli özelliği, elektronik devrenin üretilmesinden sonra programlanabilme esnekliğine sahip olmasıdır.

Selmani ve arkadaşları [15] ve [40]'de, fonksiyonel Truva atı devrelerindeki geçiş olaylarının olasılığının artırılmasına dayanan bir yöntem önermişlerdir. Daha sonra bu geçişlerin üretilme zamanları analiz edilmiştir. Yöntemde, öncelikle geometrik dağılım yöntemiyle devre üzerindeki yollarda geçiş olasılıkları hesaplanır [40]. Daha sonra belli bir eşik değeri altında geçiş olasılığı olan yollar üzerine dummy flip floplar yerleştirilir. Bu yöntemle, truva atlarının saklanma ihtimalinin yüksek olduğu devrenin az aktif olan bölgelerinde aktivasyon oranının artırılması hedeflenmiştir.

Bu metodun daha uygulanabilir bir benzeri Li ve Lach tarafından önerilmiştir [41]. Bu metotta çipe yazmaçlar ve kapılar eklenerek, yazmaçtan yazmaca gecikmeler ölçülmüştür.

Reece ve arkadaşları [29] ve [32]'de, FPGA üzerinde belli noktalara ring osilatörler koyarak, ek bir müdahaleyapıldığında bu osilatörlerin frekanslarındaki değişime göre Truva atı tespiti yapan bir yöntem önermişlerdir.

Zhang ve Tehranipoor bu fikri daha ileri düzeyde uygulayan bir çalışma yapmışlardır [42]. Elektronik devre üzerine birbirleri ile bağlı ring osilatör networkü koyup, muhtemel bir trojeni bu osilatörlerdeki değişimden tespit etmeye çalışmışlardır.

Ferraiuolo ve arkadaşları [43]'de aynı yöntemi, 90 nm tenolojisinde gerçeklenmiş ASIC devreler üzerinde analiz etmiştir.

Banga ve Hsiao, elektronik devre üzerinde yer alan mantıksal kapıların başka kapılar ile gerçeklenebilme avantajından faydalanan bir yöntem önermiştir [44]. Bu yöntemde de amaç, truva atlarının daha az aktif olan noktalara konulması varsayımına karşın bu noktalardaki aktivasyon oranını yükseltmektir. Bu amaçla girişlerindeki değişimden daha az etkilenen mantıksal kapılar daha fazla etkilenen mantıksal kapılarla değiştirilmiştir.

Benzer mantıksal temele dayanan bir çalışma Alkabani tarafından gerçekleştirilmiştir [45]. Truva atını tespit etmek için devrenin dual'iyle (aynı devrenin eş değerinin diğer mantıksal kapılarla gerçeklenmiş hali) beraber değerlendirmesinden yola çıkmışlardır. Ayrıca, genellikle truva atı eklenen bir devrede truva atının tetiklenmesi için nadir gerçekleşen bir giriş değerinin seçileceği varsayımıda temel alınmıştır. Bu amaçla, truva atı tespiti için devrenin nadir aktif olan bölgeleri için kapılar seviyesinde duali alınmıştır. Bu şekilde Truva atlarına ait giriş nadir gerçekleşme durumu sık gerçekleşme durumuna dönmüş olmaktadır. Böylelikle truva atı tespit için truva atının çoğu

giriş vektörünün devreye girdiği bir devre elde edilmiş olmaktadır.

Lamech ve arkadaşları, yol gecikmelerinden truva atını tespit etmek için REBEL (Regional Delay Bevavior) isimli gömülü test yapısını önermişlerdir [46]. Truva atı olarak yollara kapasite ya da kapı yerleştirmişlerdir.

IV. SONUÇ

Literatürde donanımsal truva atlarının tespitine yönelik uylanan yöntemler etkinlik açısından farklılık göstermektedir. Uygulanan yöntemler ve bunların etkinliği Tablo-1'de özetlenmiştir. Tabloda yöntemlere ilişkin tüm alt kırılımların gösterilmesi yerine etkinlik açısından birbiriyle farklılık oluşturacak kadar üst seviye olan başlıklar gösterilmiştir. Yöntemlerin etkinlikleri; altyapı ihtiyacı, maliyet, uygulama zamanı, başarı şansı ve uygulanabilecek ürün kapsamları dikkate alınarak incelenmektedir.

TABLO I
TESPIT YÖNTEMLERI ETKINLIK ANALIZI

		Altyapı İhtiyacı	Gerçekleme Kolaylığı	Zaman	Başarı Oranı	Tekrarlama Kolaylığı	Uygulanabilecek Kapsamı	Toplam Etkinlik
Tahribatlı	Tersine Müh.	Çok Gelişmiş	Çok Zor	Çok Uzun	Yüksek	Çok Zor	Dar	Düşük
	Tasarımda Önlem	Gelişmiş	Zor	Uzun	Yüksek	Zor	Dar	Orta
Tahribatsız	Mantıksal Davranış	Orta	Kolay	Orta	Düşük	Orta	Çok Geniş	Orta
	Yan Kanal Analizi	Orta	Orta	Orta	Orta	Orta	Geniş	Yüksek

Tahribatlı yöntemle donanımsal truva atı tespiti her ne kadar başarı şansı yüksek olsa da (tespit sonunda somut bir kanıta ulaşılmış olsa da) bir çok dezavantaj içermektedir. Bu yöntem için ihtiyaç duyulan; altyapı, zaman ve maliyet çok fazladır ve geliştirilen altyapı ve kazanılan yetenek ile çalışmayı tekrarlamak her seferinde yeniden yüksek maliyet ve zaman gerektirecektir. Ayrıca tersine mühendislik çalışması ancak bir referans noktası olarak serim (layout) bilgisi gibi kritik tasarım verilerine sahip olan ASIC uygulamalar için gerçeklenmeye uygundur. Bu nedenlerden dolayı literatürde etkin bir donanımsal truva atı tespit yöntemi olarak önerilmemektedir.

Tahribatsız yöntemlerin etkinliğini farklı alt başlıklar altında incelemek uygun olacaktır. Tasarımda kontrol devresi ekleyerek truva atının tespit edilmesi de tahribatlı tersine mühendislik yöntemi kadar olmasa da altyapı, zaman ve maliyet açısından dezavantaja sahiptir. Her devre için yeniden tasarım yapılması gerekeceği ve yine kontrol devresinin yer kaplaması sorunu tekrar edeceği için bu yöntemin yetenek kazanımı sonrasında yine zorluğu devam etmektedir. Uygulama alanıda, ASIC yapıları ile sınırlıdır. Yöntemin getirdiği yüklerin tahripli yöntem kadar fazla olmaması ve ASIC yapıları için başarı şansının yüksek olması, bu yöntemin literatürde, özellikle ASIC yapıları için etkin sayılabilecek bir yöntem olarak kabul edilmesini sağlamıştır.

Mantıksal davranış testi; alt yapı, zaman ve maliyet açısından avantajlı bir sistemdir. Aslında fonksiyonel bozukluklar için özelleşmiş bu yöntemin başarı şansının da düşük olduğu görülmektedir. Bu durum truva atlarının fonksiyon bozuklukları ile kolayca farkedilemeyeceği varsayımına dayanmaktadır. Ancak bu yöntemin diğer tüm yöntemlere göre çok büyük bir avantajı mevcuttur. Diğer yöntemlerin hiçbirinin çalışmadığı noktalarda bu tespit yöntemine ihtiyaç duyulmaktadır. Örneğin, hakkında hiçbir ön bilgi bulunmayan bir elektronik bileşen veya son ürün üzerinde truva atı aranmasına ilk olarak mantıksal davranış testi ile başlanabilir. Bu geniş kapsamı nedeniyle mantıksal davranış testinin etkin bir yöntem olduğu değerlendirilmektedir.

Yan kanal analizi yöntemi altyapı, zaman ve maliyet açısından avantajlı bir sistemdir. Uygulama kapsamı olarak da bir çok yapı için kapsayıcı durumdadır. Ayrıca mantıksal davranış testi ve tasarımda önlem alma yöntemleri için de yardımcı bir analiz türüdür. Tüm bunlarla beraber başarı şansının da düşük olmaması, bu yöntemi şu an litaratürde tanımlı donanımsal truva atı tespit yöntemleri arasında en etkin yöntem haline getirmiştir.

KAYNAKLAR

[1] K. Jurgen : Selbstreproduktion bei programmen' (VX heavens) Vx.netlux.org. http://vx.netlux.org/lib/mjk00.html. Retrieved 2010-07-10.,

[2] "Fred Cohen 1984 "Computer Viruses – Theory and Experiments". Eecs.umich.edu. 1983-11-03. http://www.eecs.umich.edu/%7Eaprakash/eecs588/handouts/cohen-viruses.html. Retrieved 2012-03-29., Communication of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763.

[3] M. Beaumont, B. Hopkins, Newby T.: Hardware Trojans – Prevention, Detection, Countermeasures (A Literature Review), Defence Science and Technology Organisation (2011)

[4] http://www.webopedia.com/TERM/B/backdoor.html

[5] T. Huffmire, C. Irvine, T. D. Nguyen , T. Levin, R. Kastner: Handbook of FPGA Design Security, Springer (2010).

[6] http://isc.sans.edu/diary/Barracuda+Back+Door+/15004

[7] https://www.seconsult.com/fxdata/seccons/prod/temedia/advisories_txt/20130124-0_Barracuda_Appliances_Backdoor_wo_poc_v10.txt

[8] http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

[9] http://www.theregister.co.uk/2013/07/11/hp_prepping_fix_for_latest_storage_vuln/

[10] S. Skorobogatov, C. Woods : Breakthrough silicon scanning discovers backdoor in military chip. Cryptographic Hardware and Embedded Systems Workshop - CHESS (2012).

[11] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar: Trojan detection using ic fingerprinting. IEEE Symposium on Security and Privacy. (2007).

[12] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. Wolff : Multiple-Parameter Side-Channel Analysis: A Non-Invasive Hardware Trojan Detection Approach. IEEE (2010)

[13] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. Wolff, C. Papachristou, K. Roy, S. Bhunia: Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis. IEEE Transaction on Computers. (2012)

[14] B. Sanno: Detecting Hardware Trojans. Ruhr-University Bochum, Germany. (2009).

[15] H. Salmani, M.Tehranipoor, J. Plusquellic: A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time. IEEE Transaction on very large Scale Integration (VLSI) Systems, VOL. 20, NO. 1. (2012).

[16] X. Wang, M. Tehranipoor, J. Plusquellic: Detect-ing Malicious Inclusions in Secure Hardware, Challenges and Solutions. 1st IEEE International Workshop on Hardware-Oriented Security and Trust - HOST'08. (2008).

[17] R. S. Chakraborty, S. Narasimhan, S. Bhunia: Hardware trojan: Threats and emerging solutions. (2010).

[18] S. Jha, S. K. Jha: Randomization based probabilistic approach to detect trojan circuits. High-Assurance Systems Engineering, IEEE International Symposium on 0, 117–124. (2008).

[19] F. Wolff, C. Papachristou, S. Bhunia, R. S. Chakraborty: Towards Trojan-Free Trustedelektronik devres: Problem Analysis and Detection Scheme. European Design and Automation Association - EDAA. (2008).

[20] R. S. Chakraborty, F. G. Wollf, S. Paul, C. A. Papachristou, S. Bhunia: Mero: A statistical approach for hardware trojan detection. Cryptographic Hardware and Embedded Systems Workshop - CHESS (2009).

[21] M. Tehranipoor, F. Koushanfar: A survey of hardware trojan taxonomy and detection, IEEE Design and Test of Computers 27, 10–25. (2010)
[22] R. Rad, J. Plusquellic, M. Tehranipoor: Sensitivity analysis to hardware trojans using power supply transient signals. IEEE International Symposium on HardwareOriented Security and Trust. (2008)
[23] R. M. Rad, X. Wang, M. Tehranipoor, J. Plusquellic: Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans. IEEE (2008)
[24] M. Banga, M. Hsiao: A Region Based Approach for the Identification of Hardware Trojans. Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust - HOST (2008)
[25] M. Banga, M. Hsiao: A Novel Sustained Vector Technique for the Detection of Hardware Trojans. Proc. 22nd Int'l Conf. VLSI Design, IEEE CS Press, pp. 327-332. (2009)
[26] Y. Alkabani, F. Koushanfar: Consistency-Based Characterization for IC Trojan Detection. Proc. IEEE/ ACM Int'l Conf. Computer-Aided Design - ICCAD (2009)
[27] M. Potkonjak, A. Nahapetian, M. Nelson, T. Massey: 'Hardware Trojan Horse Detection Using Gate-Level Characterization. Proc. 46th Design Automation Conf - DAC (2009)
[28] S. Wei, S. Meguerdichian, M. Potkonjak: Malicious Circuitry Detection Using Thermal Conditioning. IEEE Transaction on very large Scale Integration (VLSI) Systems. VOL. 6, NO. 3. (2011)
[29] T. Reece: Detection of Malicious Hardware Integrated Circuits and Field Programmable Gate Arrays. Submitted to the Faculty of the Graduate School of Vanderbilt University. (2009)
[30] T. Reece, W. H. Robinson, B. L. Bhuva: Signature-based detection of hardware trojans with voltage stepping. Governmental Microcircuit Applications and Critical Technology - GOMACTech (2010)
[31] S. Baktir, T. Güçlüoğlu, A. Özmen: Detection of Trojans in Integrated Circuits. IEEE (2012)
[32] T. Reece, W. H. Robinson: Hardware Trojans: The Defense and Attack of Integrated Circuits. IEEE (2011)
[33] Y. L. Gwon, H. T. Kung, D. Vlah: DISTROY: Detecting Integrated Circuit Trojans with Compressive Measurements. Harvard University. (2011)
[34] Y. Tsaiy, K. Huangy, H. T. Kung, D. Vlah, Y. L. Gwon, L. Cheny: A Chip Architecture for Compressive Sensing Based Detection of IC Trojans. Harvard University. (2012).
[35] L. Wang, H. Luo: A Power Analysis Based Approach to Detect Trojan Circuits. IEEE (2011)
[36] Y. Jin, Y. Makris: Hardware trojan detection using path delay fingerprint. IEEE International Symposium on Hardware-Oriented Security and Trust. (2008)
[37] S. Weiy, K. Liz, F. Koushanfarz, M. Potkonjaky: Provably Complete Hardware Trojan Detection Using Test Point Insertion. IEEE/ACM International Conference on Computer-Aided Design - ICCAD (2012)
[38] R. S. Chakraborty, S. Paul, S. Bhunia: On Demand Transparency for Improving Hardware Trojan Detectability. Proc. IEEE Int'l Workshop Hardware Oriented Security and Trust - HOST (2008).
[39] M. Abramovici, P. Bradley: Integrated Circuit Security: New Threats and Solutions. Proc. 5th Ann. Workshop Cyber Security and Information Intelligence Research: Cyber Security and Information Challenges and Strategies - CSIIRW (2009).
[40] H. Salmani, M. Tehranipoor, J. Plusquellic: New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time. IEEE (2009)
[41] J. Li, J. Lach: At-speed delay characterization for ic authentication and trojan horse detection. Hardware-Oriented Security and Trust - HOST (2008).
[42] X. Zhang, M. Tehranipoor: RON: An On-Chip Ring Oscillator Network for Hardware Trojan Detection. European Design and Automation Association - EDAA. (2011)
[43] A. Ferraiuolo, X. Zhang, M. Tehranipoor: Experimental Analysis of a Ring Oscillator Network for Hardware Trojan Detection in a 90nm ASIC
[44] M. Banga, M. Hsiao: VITAMIN: Voltage InversionTechnique to Ascertain Malicious Insertion in ICs. Proc. 2nd IEEE Int'l Workshop Hardware-Oriented Security and Trust - HOST (2009)
[45] Y. Alkabani: Trojan Immune Circuits Using Duality. 15th Euromicro Conference on Digital System Design. (2012)
[46] C. Lamech, J. Plusquellic: Trojan detection based on delay variations measured using a high-precision, low-overhead embedded test structure. Univercity of New Mexico. (2012)

M. Sahinoglu Isparta'nın Senirkent ilçesinde 1983 yılında dünyaya geldi. 2001'de Isparta Fen Lisesi'nden mezun oldu. 2006 ve 2009'da İstanbul Teknik Üniversitesi Elektronik Mühendisliği bölümünden lisans ve yüksek lisans derecelerini aldı. 2009'dan itibaren Gebze Yüksek Teknoloji Enstitüsünde Elektronik Mühendisliği bölümünde Doktora programına devam etmektedir. Genel çalışma alanı kriptoloji olmakla birlikte özel çalışma alanı kriptografik sistemlere yapılan güvenlik değerlendirmeleridir.
Lisans öğrenimi sırasında sırası ile stajlarını 1 ay sürecek şekilde TRT Radyo (Harbiye - İSTANBUL), NETAŞ (Ümraniye - İSTANBUL) ve ARÇELİK A.Ş'de (Çayırova - KOCAELİ) yapmıştır. Yüksek Lisans tez çalışmaları sırasında İ.T.Ü'de 2006-2008 yılları arasında araştırma personeli olarak çalışmıştır. 2008 yılından itibaren TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsünde (Gebze - KOCAELİ) çalışmaktadır.

M. Öztemür Samsun'un Çarşamba ilçesinde 1985 yılında dünyaya geldi. 2001'de Samsun Bafra Lisesi'nden mezun oldu. 2007 ve 2011'de Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümünden lisans ve yüksek lisans derecelerini aldı. Genel çalışma alanı ürün güvenliği ve gömülü sistemler olmakla birlikte özel çalışma alanı kriptografik sistemlere yapılan güvenlik değerlendirmeleridir.
Lisans öğrenimi sırasında sırası ile stajlarını 1 ay sürecek şekilde Siemens (Kartal - İSTANBUL), AKBİL Otomasyon (Ümraniye - İSTANBUL) yapmıştır. TÜBİTAK bünyesinde çalışmaua başlamadan önce 2009 yılında bir dönem NETAŞ'ta donanım tasarım mühendisi olarak çalışmıştır. 2009 yılından itibaren TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsünde (Gebze - KOCAELİ) çalışmaktadır.

B. Soysal Ankara'da 1983 yılında doğdu. 2001'de Çankırı Fen Lisesi'nden mezun oldu. 2006'da Ortadoğu Teknik Üniversitesi ve 2010'da Boğaziçi Üniversitesi Elektrik Elektronik Mühendisliğinden lisans ve yüksek lisans derecelerini aldı. 2010'dan itibaren Boğaziçi Üniversitesi Elektrik Elektronik Mühendisliği bölümünde Doktora programına devam etmektedir. Genel çalışma alanı kriptoloji olmakla birlikte özel çalışma alanı kriptografik sistemlere yapılan güvenlik değerlendirmeleridir. Lisans öğrenimi sırasında sırası ile stajlarını 1 ay sürecek şekilde TÜBİTAK-BİLTEN (ODTÜ - ANAKRA), ASELSAN (Macunköy - ANAKRA) ve Turkcell A.Ş'de (Söğütözü - ANAKRA) yapmıştır. 2005 yılından itibaren ASELSAN A. Ş.'de önce 1 yıl süre ile aday mühendis olarak daha sonra da 6 ay süre ile mühendis olarak çalışmıştır. 2007'den beri Siber Güvenlik Enstitüsünde (Gebze - KOCAELİ) çalışmaktadır.

Secure Database in Cloud Computing: CryptDB Revisited

Ziynet Nesibe Dayioglu[1,2], Mehmet Sabir Kiraz[1], Fatih Birinci[1], and Ihsan Haluk Akin[2]

***Abstract*—Databases are including valuable and critical data, therefore, they are the most desirable to the malicious adversaries. To preserve the security of database outsourcing scenarios, various techniques have been proposed so far which preserve a certain degree of confidentiality while still allowing to execute some SQL queries effeciently. CryptDB is an approach to outsourcing database while preserving confidentiality and performing a set of SQL queries in an effecient way.**

In this paper, we revisit CryptDB and describe it in more details for ease of understanding. We then highlight the drawbacks of CryptDB from security and efficiency points of view.

***Index Terms*—Secure Database, Encrypted Search, Cryptographic Protocol, Proxy Server**

I. Introduction

CLOUD computing's detailed definition exists at NIST's website [1]. In our work, we simply define cloud computing as the delivery of on-demand computing resources located on the remote servers. Through the evalution of tools and broadband connectivity, cloud computing is getting more feasible from a user's perspective [2], since it reduces cost and increases mobility [5].

With the increasing popularity of cloud computing the security issues also rise [3], [4]. Organizations considering migration to cloud based services must also consider and understand security, privacy, reliability, and regulatory issues. Important research agencies are aware of these risks and have produced reports [6], [7], [8], [9]. According to Gartner, cloud computing security risks can be summarized by seven categories: "Privileged User Access, Regulatory Compliance, Data Location, Data Segregation, Recovery, Investigative Support, Long-term Viability" [6]. Security issues are investigated more deeply under two main subjects namely, "loss of control over data" and "dependence on the Cloud Computing provider" [15].

Outsourcing databases into cloud can increase levels of availability, robustness, elasticity and efficiency as well as minimize administrative reasons. However the data in the cloud can be accessed by the cloud provider. So, the cloud provider, its employees or even subcontractors can deliberately or inadvertently access customers' data. In order to technically ensure data confidentiality, the data can be encrypted before being outsourced. However, executing queries as computationally perfect secrecy on an encrypted data cannot be generated efficiently. Performing non-trivial computations with the data on cloud such as searches, transformations, selections, and access control decisions is useful. Conventional encryption prevents processing this data on the cloud. Genrty solved a thirty year awaited problem in Cyrptography [14]. He propesed a novel encryption scheme which can allow processing on encrypted data. Nevertheless this encryption scheme is far away from being practical. DARPA separate $20 million to search for cryptography's this problem as a practical solution [16]. Popa and friends from MIT bring practical solution to processing encrypted database [10]. This paper focused on their work in more details and concentrated on their work's weeknesses.

(1)TUBITAK BILGEM UEKAE, Kocaeli, Turkey (2)Fatih University, Istanbul, Turkey

E-Mails:{ziynet.dayioglu, mehmet.kiraz, fatih.birinci}@tubitak.gov.tr, ihakin@fatih.edu.tr

A. Related Work

Researchers are trying to find solutions to keep data on the cloud confidential. Processing data securely on the cloud is complicated. In this section, we will give some well-known approaches for solving secure computing on the cloud.

Fully homomorphic encryption. As mentioned in the previous section, the data can be encrypted before uploading to the cloud. However, using conventional encryption schemes, the data cannot be processed on the cloud. In this case, the cloud can only be used for storage purposes. Homomorphic encryption may overcome this limitation upto a certain level, which allows logical operations on ciphertexts without decryption. Homomorphic encryptions like Paillier or ElGamal allow just one operation, namely either addition or multiplication [25], [26]. Fully homomorphic encryptions schemes allow addition and multiplication on ciphertexts, which allows an untrusted server to carry out arbitrary computation on encrypted data on behalf of a client without decryption. Namely, using fully homomorphic encryption schemes the cloud provider can run any program client wishes without obtaining any information about the plaintexts. Fully homomorphic encryption schemes are first invented by Gentry in 2009 [14]. Unfortunately, there is no practical scheme using fully homographic encryption today but a lot of work is being done in this field, some of them may be promising for cloud computing [20].

CryptDB: a weaker attacker model. CryptDB [10] is an implementation that allows query processing over encrypted databases. The database managed by the cloud provider, but database items are encrypted with keys that are only known by the data owner. SQL queries run over the encrypted database using a collection of operations such as equality checks and order comparisons. CryptDB uses encryption schemes that allow such comparisons to be made on ciphertexts. CryptDB represents a weak attacker model because it assumes the existence of a trusted cloud-based application server and proxy.

Nevertheless, CryptDB represents an interesting position on the trade-off between functionality and confidentiality from cloud providers. In this paper, we will go into details of CryptDB.

Private Information Retrieval. To enable search on remote database Secure Multi-party Computation can also be used [19], [21], [24]. These schemes are already used in practice and therefore, may be promising for cloud computing issues in the near future [22], [23]. Private Information Retrieval schemes solves the problem with absolute privacy (e.g., [17]). Curtmola et al. proposed two schemes against non-adaptive and adaptive adversaries with a good performance [18].

B. Contributions

The main contribution of this paper is to provide a detailed thread and performance analysis of CryptDB. For ease of understanding we first describe CryptDB with more detailed explanations. Next, we describe the server structure of CryptDB and we analyse the overhead of Proxy Server. Unfortunately, the original paper does not explain the search algorithm, therefore we have extended the search algorithm of the CryptDB. We show that the current search algorithm is not enough to meet all the search queries. We highlight the security and effeciency points of CryptDB. Finally, we present some remarks and open research areas for CryptDB.

II. CryptDB Architecture

A. Layered Encryption

The encryption of a data in the database is computed in a layered way. There are four different main goals to achieve, and for each goal there exists a different layered particle, which is called as onion [11]: EQ, ORD, SEARCH and ADD onion. EQ onion aims to adjust layers for equality queries, while ORD onion aims to adjust the order leakage for the queries including comparison. SEARCH onion is used to search a text in the database without leaking any information. This onion is not allowed to execute integer values. Finally, ADD onion aims to add encrypted values which only supports integer values. These onions have different layers each encrypted by using different algorithms. Furthermore, these algorithms have different security levels where the outer layer of an onion is more secure than the inner ones. Furthermore, a value has only one current layer in each onion. Once the database has been created, all the onions will be at the most secure layer.

Queries are processed as columns in a database, therefore, CryptDB is also column-oriented. If one value needs to be decrypted to weaker layer, then the whole column is going to be decrypted. However, it causes more information leakage than requested. If we need a value to be the weakest layer, the whole column will be at this layer and leak the information. And also note that the inner layer is the weakest layer, but it also does not reveal any plaintext to DBMS Server. The inner layer of the onions which are Equi-JOIN, OPE-JOIN, SEARCH and HOM layers are never stripped off.

EQ onion.

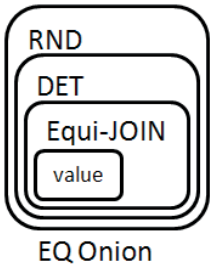


Fig. 1. EQ Onion

At the most secure layer of EQ onion is RND layer. This RND layer encrypts each value with AES (Rjindaels algorithm) in CBC mode. For integer, Blowfish in CBC mode is preferred because of its 64-bit block size instead of 128-bit to decrease the length of the ciphertexts. The initialization value for both encryption type is randomly chosen values. Each value goes to the different ciphertext with high probably even if the plaintexts are the same. For this reason, RND layer is indistinguishable under an adaptive chosen plaintext attack. However, this scheme does not provide an efficient functionality.

When the equality check of the values is needed, the RND layer should be stripped off. The next inner layer of EQ onion is DET layer. This layer is deterministic layer. After encryption is done, if two values are the same, then their corresponding ciphertexts will be the same.

For the values inside the same column, these two layers, RND and DET, are sufficient to process queries. However, some queries need to check either the equality of two different columns or two different columns of different tables. For these situations, the current layer should be updated Equi-JOIN layer. In this layer, JOIN-ADJ is concatenated to the encryption of DET layer.

$$\text{JOIN} = \text{JOIN-ADJ}||\text{DET}$$

JOIN-ADJ allows DBMS server to adjust the key of each column at run time. It is somehow a keyed hash with additional property that hashes can be adjusted to change their key without access to the plaintext. JOIN-ADJ is a deterministic function, also collision resistant (192-bit), non-invertible, and transitive. JOIN-ADJ function is defined below:

$$\text{JOIN-ADJ}_K(\text{value}) = \text{P}^{K.PRF_{k0}(value)}$$

Elliptic Curve Cryptography (ECC) is used as an algorithm. K is initial key for that table, column, onion, and layer. P is a point on an elliptic curve which is a public parameter. PRF is a pseudorandom function mapping values to a pseudorandom number, such as $\text{AES}_{K0}(\text{SHA}(\text{value}))$. K0 is the key which is the same for all columns and derived from Master Key.

The exponentiation is in fact repeated geometric addition of elliptic curve points, and it is faster than RSA exponentiation. Proxy computes $\Delta K = K/K'$ and sends it to DBMS Server. DBMS Server uses a UDF to make them share the same JOIN-ADJ by computing below with the assumptions that column c has K, and column c' has K' as keys at JOIN-ADJ

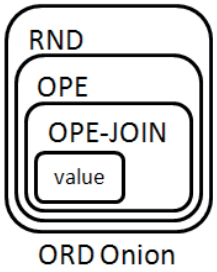


Fig. 2. ORD Onion

layer.

$$[\text{JOIN-ADJ}_{K'}(\text{value})]^{\Delta K} = [\text{P}^{K'.PRF_{k0}(value)}]^{K/K'} = \text{P}^{K.PRF_{k0}(value)} = \text{JOIN-ADJ}_{K}(\text{value})$$

By using the appropriate UDF, the JOIN-ADJ of two different columns are the same anymore. Therefore, it is possible to compare the equality of them by looking at the JOIN-ADJ. Because the DET layer uses different keys for each column for correlations between columns. Security of this scheme is based on the standard Elliptic-Curve Decisional Diffie Hellman hardness assumption.

ORD onion. The most secure layer of the ORD onion is exactly the same as the EQ onion, both is RND layer. The inner layer of the RND for ORD onion is OPE layer. Order preserving encryption algorithms have not enough security and efficiency until now. In the original CryptDB's paper [10], the authors do not consider the order-preserving encryption but they later pointed about this issue in their article "An Ideal-Security Protocol for Order-Preserving Encoding" in [11].

The limited information is given about this onion in CryptDB's article [10]. If the encryption of x is smaller than the encryption of y, then the value x is also smaller than y. If we find any encrypted value which is between these two encryptions, then the plaintext will also lie between x and y. Namely, this scheme leaks the order, therefore, it is a weaker scheme when compared to equality leakage.

For the values at the same column, this layer is enough to process the queries, but if two different columns are compared to check order, then we need to strip off the OPE layer, and reach the OPE-JOIN layer. This layer is lack of functionality than the EQUI-JOIN layer of the EQ onion. To adjust two columns are not possible because of the lack of the Order-Preserving algorithms' efficiency. There are two solutions. First one is, the application will declare the columns which can be joined, and while arranging the keys, the same key will be used for these columns. It is not logical in most situations to declare ahead of time. The second solution is the same key will be used for all columns at this layer. This solution is not a good solution also. Fortunately, range joins are not used too much.

SEARCH & ADD onions. SEARCH onion has just one layer, so there is no decryption process for this onion.

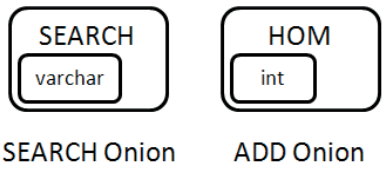


Fig. 3. SEARCH & ADD Onions

SEARCH onion has a value, and the SEARCH layer which covers this value. Search algorithm used in CryptDB is the Song's search algorithm which is described in Section III-D. The aim of the SEARCH onion is searching an encrypted value inside an encrypted table.

ADD onion also has the same situation. The HOM layer is the only one layer of ADD onion. This onion's aim is to provide some functionality with encrypted values without access to the plaintext. This can achieved with homomorphic encrytion. The algorithm used for Homomorphic encryption of CryptDB is the Paillier's algorithm.

B. Adjustable Encryption

If we keep all the layers for each onion, it is not a good way. Because if the weakest layer is given, other layers are not necessary to create. However, if we use a layer for each onion, it is hard to know the most secure layer which meets our need ahead of time. For this reason, it is a requirement to adjust current layer dynamically without leaking the data. This problem is solved with adjustable functionality. There are different onions for different aims. All these onions are put into the table. According to our aim, we choose our onion, and use it as well. And each value is encrypted with all outer layers, beginning from the weakest to the most secure one. With this approach, if no query requests the weaker layers, then these layers are not available to use.

For each column in a table, the same key is used to encrypt the values inside, but for the different tables, columns, onions, and also layers, different keys are used. The key generation is done with a pseudorandom permutation like below:

$$\text{Key} = \text{PRP}_{MK}(\text{table t, column c, onion o, layer l})$$

In the beginning, all onions are the most secure layer which are RND, HOM, or SEARCH layers. If equality or order leakage is requested, the outer layer will be decrypted. This decryption does not give the plaintext because of the layered encryption. The remaining layers still cover our data to keep them secure. Furthermore, the weakest layers which are OPE-JOIN, Equi-JOIN, SEARCH, and ADD layer are never stripped off.

C. UDF: User-Defined Function

A function contains instructions in order to perform a specific task, and provides to repeat this task easily. User-defined function is also a function, and it is created by a user. This user needs to have permissions to perform the processes in the database, or database owner abbreviated as dbo can be

used. dbo is a user which can perform all activities in the database.

If we have a table called Square which has two columns as edge length and order number of the square, then we can create a UDF to calculate the area of the squares inside the database. The sample Square table can be in Table I.

TABLE I
THE SAMPLE SQUARE TABLE

Square	
Number	**EdgeLength**
1	10
2	5
3	7

There is no need to keep the area values causing extra overhead to the database. We can create a UDF, and call it whenever area is needed. Here is an example of creating a UDF.

```
CREATE FUNCTION dbo.area (edge FLOAT) RETURNS FLOAT
RETURN (edge * edge);
```

An example query to use this UDF can be like as follows:

```
SELECT Number, area (EdgeLength) AS Area FROM Square;
```

The returning result will be like Table II.

TABLE II
THE RETURNED RESULT OF THE SQL

Number	Area
1	100
2	25
3	49

Instead of keeping data for each information which can be required, it is better to create a UDF, and call it whenever this task is needed. In CryptDB, UDF is also a requirement. Decryption of the layered architecture to adjust the current layer is done by using user-defined functions. And also updating current state of the onion layers is done by using the UDFs. Changing all existing database mechanism is hard to achieve. Therefore, UDFs are very important to add functionality in the database systems.

D. Server Structure in CryptDB

In the database systems, users request some information or functionality from the applications. The SQL queries are used in order to meet the need of the users. The Application Servers send the queries to DBMS Server. DBMS stands for Database Management System. DBMS Server takes the SQL and responds the result set. This system is open to any eavesdropping and attacks of adversaries. Also DBMS Server may be curious about the queries and track the queries with their results. The other possibility is that the physical access to the disc can cause the data to be stolen. In CryptDB, the mechanism of the queries are the same, but server structure somehow changes, and an extra server called Proxy Server is added to the database system.

It is assumed that all the queries coming from the Application Server is taken by Proxy Server, and sent to DBMS Server after some modifications. The aim is to keep no meaningful information at DBMS Server's side in order to prevent the curious Database Management Administrator to see the contents of the tables in its database [27]. For this reason, we need to make the whole data meaningless.

The first thing is to create a table in order to keep some data inside DBMS Server's database. In CryptDB, the table of DBMS Server is totally different from the real one. Proxy Server changes the table's name. Then, according to type of the column (e.g. int, varchar), there exists some possible onions. Proxy Server keeps all possible onion's data in different columns separately in this table. Table III is a basic example.

New created table from Table III by Proxy Server is shown in Table IV.

The second thing is to add instances to the current tables. The names of the columns are changed, and each value inside the table are encrypted according to algorithm of its onion's layer. For instance, if the current layer of the EQ onion is RND layer, and query deals with the equality, then each value in the corresponding column will be encrypted with AES (Advanced Encryption Standard) in CBC (Cyclic Block Chaining) mode. Or the Paillier's algorithm will be used to encrypt the values which belongs to HOM layer of the ADD onion. All these encryption processes are done by Proxy Server.

When a query comes to Proxy Server, it changes the query. First of all, Proxy Server decides which onion is used for this query. Proxy Server has extra tables, one of them is for keeping the current state of each column's each onion. After deciding the onion of the query, Proxy Server looks at this table, and checks that the current state of the onion is at the needed layer for this query. If not, Proxy Server calls the UDF which is responsible for the stripping off the current layer to the needed layer. After this process, Proxy Server modifies the query, and sends it to DBMS Server. The whole data stored in DBMS Server's database is encrypted, and the queries are not meaningful for the Database Management Administrator.

DBMS Server takes the modified query, and returns an encrypted result to Proxy Server. Proxy Server takes the encrypted values, and decrypts them, and sends to the Application Server. The Application Server is not concerned about any encryption processes, it just sends its original plaintext, and take the results, and gives service to the clients with these results. The basic server structure of the CryptDB is described, and overhead which Proxy Server has to deal with is shown.

III. A BASIC EXAMPLE

In this section we describe an example to explain the basic structure of CryptDB. There is a single principal in our example, no modification or restrictions are done to the principle. Each table has only one Master Key abbreviated as MK throughout the paper. We have an example table called Students. This table has one Master Key which we abbreviate as MK. As mentioned in Section II-B, each table's each column's each onion's each layer has different keys from the following equation:

TABLE III
THE CREATED ORIGINAL TABLE AND ITS COLUMNS

Employees	
ID	**Name**

TABLE IV
THE MODIFIED TABLE FOR DBMS SERVER

Changed Table Name							
ID-IV	ID-EqOn	ID-OrdOn	ID-AddOn	Name-IV	Name-EqOn	Name-OrdOn	Name-SearchOn

$$\text{Key} = \text{PRP}_{MK}(\text{table t, column c, onion o, layer l})$$

A. Queries with security but without functionality

After reading the CryptDB's article [10], even if it easy to understand the structure, it is still hard to combine the CryptDB mechanism with SQL queries. For this reason, we illustrate a basic example in order to clarify the steps in more details.

Students table has two columns ID and Name. ID stands for identification number of the student and Name stands for student's name. ID column takes an integer value while Name column takes a string. Students table is created with the following statement:

```
CREATE TABLE Students (ID int, Name varchar(255));
```

After creating table, we are ready to insert some instances as follows.

```
INSERT INTO Students VALUES (1, "Alice");
INSERT INTO Students VALUES (2, "Bob");
INSERT INTO Students VALUES (3, "Eve");
```

When we run all these queries, the Application Server creates the following table V. This table has pure data, so it is not a good way to store this table inside the database of DBMS Server for the security reasons. Namely, Proxy Server creates a new encrypted table for DBMS Server. The created new encrypted table will be as in Table VI.

TABLE V
THE TABLE AFTER RUNNING THE ABOVE-MENTIONED SQL QUERIES

Students	
ID	**Name**
1	Alice
2	Bob
3	Eve

Since the type of ID column is an integer, SEARCH onion will not be available for this column. Furthermore, since the type of Name column is string, HOM onion will also not available for this column. As described earlier in Section II, all layers will be at the most secure layer at the beginning. There are seven layers. The most secure layers of the onions are the three layers which are RND, SEARCH and HOM. However, they also have less functionality. For example, RND layer does not leak any data, but it has no efficient functionality. If we come back to our example, by using the most secure layer, we can run the queries such as "SELECT * FROM Students;", "SELECT Name FROM Students;".

Note that Proxy must modify the queries in order to protect original table contents. If we continue with the SQL "SELECT Name FROM Students;", the modified SQL will be like below:

```
SELECT C2-IV, C2-Eq FROM DBMS_Table1;
```

DBMS Server will take this query, and return the result in Table VII.

TABLE VII
THE RETURNED RESULT FROM PROXY SERVER TO THE APPLICATION SERVER

C2-IV	C2-Eq
lpw9	dkfm
suc0	d82w
3mnu	snge

The corresponding table which Proxy Server decrypts and sends to the Application Server will be like in Table VIII.

TABLE VIII
THE RETURNED RESULT FROM PROXY SERVER'S SIDE

Name
Alice
Bob
Eve

This query returns the result which has no functionality. However, there is no change at the ciphertext inside DBMS Server's table. You can just read the returned data, but in general the queries which are coming from Application Server require some functionality such as updating current data, selecting and showing some specific rows of the table, calculating average of a column.

B. Queries with equality leakage

Note that equality in the databases is an important feature and is most frequently used one. For example, IDs of the students which got AA grade from a lecture at a university, the names of the clients which buy a specific product in a shopping mall and the phone numbers of the people who send cargo with wrong destination address can be solved by the equality feature in real life. If we come back to our example, we can create such SQL queries:

TABLE VI
THE ENCRYPTED TABLE WHICH IS CREATED ON PROXY SERVER

C1-IV	C1-Eq	C1-Ord	C1-Hom	C2-IV	C2-Eq	C2-Ord	C2-Search
q39f	ge88	hwip	dwna	lpw9	dkfm	fdkw	98wu
c8x3	8n4o	s09s	28bd	suc0	d82w	8mx0	x9ak
sk7x	x7wk	x6sh	s7w9	3mnu	snge	xuwn	u8sb

SELECT name FROM Students WHERE id = 1;

Proxy Server will take this query, and modify it according to desired functionality. Encryption layer of the computed column is checked whether the current layer is at a layer which can respond to the requested query. If not, Proxy Server sends UPDATE query. This UPDATE query provides to adjust the current layer of this column with given keys from Proxy Server. In our example, we need to use a UDF which strips off the RND layer to the DET layer. The reason why is, if we want to know the equality of the two data at the same column, we need to use a deterministic encryption. If we assume STRIP_RND is a UDF which takes the RND layer and decrypts it to the DET layer, then Proxy Server will send below UPDATE query at first. This query will send the decryption key to DBMS Server, and DBMS Server is able to strip off the RND layer.

UPDATE DBMS_Table1 SET C1-Eq = STRIP_RND (Key, C1-IV, C1-Eq);

Recall that the key is coming from the following equation:

$$\text{Key} = \text{PRP}_{MK}(\text{table t, column c, onion o, layer l})$$

After this UDF, the C1-Eq column is at the DET layer anymore. And Proxy Server will update this column's current onion state to the DET layer.

Decrypt_{Key}(C1-IV, C1-Eq) is the structure of the decryption function. Key is RND layer's decryption key for the first column in Students table. Assume that the decryption of this column is given as follows:

$$\text{Decrypt}_{Key}\ (\text{q39f, ge88}) = \text{djes}$$
$$\text{Decrypt}_{Key}\ (\text{c8x3, 8n4o}) = \text{ektd}$$
$$\text{Decrypt}_{Key}\ (\text{sk7x, x7wk}) = \text{3kw7}$$

After modifying DBMS Server's database, the Application Server will change the query for DBMS which will be as follows:

SELECT C1-IV, C1-Eq FROM DBMS_Table1 WHERE C1-Eq = djes;

Key1 is JOIN layer's encryption key for the C1 column of the DBMS_Table1. And also Key2 is DET layer's encryption key for the C1 column of the DBMS_Table1. Then encryption of a value will be generated by encrypting all layers until the current layer. For instance, encryption of the integer 1 will be generated as follows:

$$\text{Enc}_{Key2}\ (\text{Enc}_{Key1}\ (1)) = \text{djes}$$

In this part, we leak the information of the columns which are requested to check equality. If the data in the same column has the same value, the ciphertext of DBMS Server's database will be the same.

C. Queries with order leakage

Order preserving encryption is a difficult issue in private search mechanisms including CryptDB. In the original CryptDB's paper [10], the authors do not consider the order-preserving encryption in details, but later they highlight this issue in another article [11]. This part can be summarized as, if encrypted value of x is less than the encrypted value of y, then we know that the value x is less than y. If we find any encrypted value which is between these encrypted values, then the decrypted form is between x and y. This scheme leaks order, it is the weakest scheme. The queries "bigger than", "smaller than", ORDER BY, SORT, MAX, MIN can be performed with the encryption scheme. The implementation of the order-preserving encryption is not implemented until CryptDB, and also there is even no measure for the scheme's practicality. That is, CryptDB is the first implementation of order preserving encryption which uses Boldyreva's algorithm [12].

D. Queries with search functionality

Implementation of the Song's article is used for CryptDB. The queries with LIKE are done by using this scheme, but the search algorithm allows only to perform the full-word searches. In this section, we will explain the search algorithm of the Song [13]. Let's assume that we have lots of private documents and we have limited storage. Therefore, we can keep them on an untrusted server. This can also be applied to mail server as well, and we need to keep our personal e-mails there. For privacy and security reasons, the data stored on an untrusted party must be encrypted.

Without loss of generality, we will treat the words as N-bit strings. This is just an assumption that all words have the same length, smaller word are padded, and longer word can be divided into the N-bit blocks. While searching among the documents, we are interested in specific documents which contains some special words, a special keyword. If we have a low bandwidth we need to only download the requested files which contain our words instead of downloading all the files. Song's search algorithm is a good candidate for solving this issue.

Note that there two different search algorithms: index-based algorithm and sequential scan algorithm. Song's algorithm is based on the sequential scan algorithm. Using an index for searching big documents is generally faster than sequential scan. While reading data from a source, it is better to use index-based, but here storing and changing words is a hard

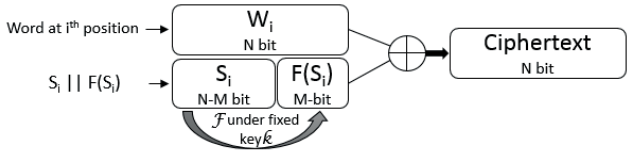


Fig. 4. Basic Scheme

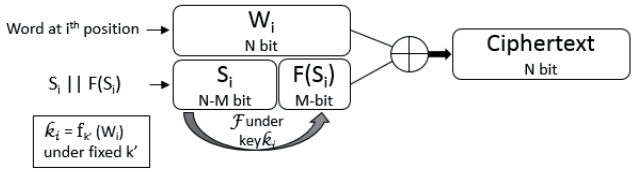


Fig. 5. Second Scheme

issue to consider. Index gives additional information, and this can lead to the statistical attacks. For these reasons, Song's algorithm prefers sequential scan algorithm.

1) Song's Search Algorithm on Encrypted Data: There exist four schemes in the Song's algorithm. First one is the basic scheme which is provably secure. However, there is no controlled searching and the searches are not hidden. To make the system more functional, Song presented three more schemes.

The basic scheme can be roughly described as follows: Let's assume that we search a word on encrypted documents on the untrusted party, but at the same time we do not want to reveal any information about the plaintext. The encryption mechanism of the basic scheme provides the provable secrecy. If you have a document which contains ℓ words of N-bits long, then you create a sequence of ℓ pseudorandom values of $N-M$ bits long. For encrypting an N-bit word at the i-th position, the corresponding sequence value S_i and $F(S_i)$ are concatenated where F is a secure pseudorandom function, i.e., $S_i \| F(S_i)$. This F function is secure pseudorandom function and it uses a key to encrypt. This key can be the same for all words inside the document, or it can be different for each location independently. This scheme is provable secure which means that the untrusted server cannot learn anything about the plaintext.

From the point of basic scheme, if we want to search a word, we give the word itself and keys of the locations which this word may appear. If we do not know anything about locations, we will give all keys. The untrusted party will take them, and XOR the ciphertext with the word. If the result has $S_i \| F(S_i)$ for some S, the matching occurs and the location of the word comes to us. If untrusted party does not know the key of a location, nothing will leak about that plaintext. However, knowing anything about locations causes all keys to be leaked, and this means all document is decrypted to the untrusted party.

Second scheme extends the basic scheme by supporting controlled searching. In this scheme, key generation is tied to another pseudorandom function G which takes the words under a random secret key k'. For each word, it creates the keys for the F function, shown as $k_i = f_{k'}(W_i))$ where W is a word inside the document. After encrypting the document, if we want to search a word, we will give the word and the key which is generated by using the word itself and our secret key k'. This scheme does not reveal any information about the locations which are not including our searching word. This provides controlled searching.

Until now, the word is given to the untrusted server as plaintext, in general this is not an accepted situation. Third scheme extends second scheme, and supports hidden searches. Before we search for a word, we encrypt each word with a deterministic algorithm like ECB (Electronic Code Book) mode encryption. The word we search is encrypted and also our key is generated by using the G function in the second scheme again. However, the key is dependent to the encrypted word, not to the original word anymore. The remaining mechanism is the same as second scheme.

The problem with the second and third scheme is that the decryption is not feasible. After trying concatenation of some S and the $F(S)$, and xoring them with a word, we encrypt the word. However, at the decryption part, to generate $F(S)$ from some S, we need to know the key of this specific word. And this key is dependent to the encrypted word. It is a contradiction that for decryption of an encrypted word requires the decrypted word itself. For this reason, some modification is done to the key generation function. Key is generated with $N-M$ bits of the encrypted word just as the length of S values. While decrypting the word, we use S and first $N-M$ bit of ciphertext to generate the first $N-M$ bit of the plaintext. With this information, we can generate the key, and using this key we find $F(S)$. And finally we find the last M bit of the plaintext by XORing the last M bit of the ciphertext and the $F(S)$ values. This final scheme is also provable secure just like the first scheme. Also we add query isolation feature, that is untrusted party just learns the search result, not additional information about the positions and plaintext forms of the words.

2) CryptDB's Encrypted Search: CryptDB uses the implementation of the Song's search algorithm. This algorithm performs full-word searches with LIKE queries. In CryptDB, repetition of the words are removed, and the words are permuted to provide more security in searching. However by comparing the number of RND ciphertext with SEARCH ciphertext, it is possible to know the number of the duplicated words. After that, the words are padded to the fixed N-bit length to encrypt according to Song's algorithm. The queries can be run as follows:

```
SELECT * FROM Students WHERE Name LIKE "% Alice %";
```

After this query come to Proxy Server, it will modify the query with the encryption of the string "Alice". The encryption is assumed as 98wu in the example.

```
SELECT * FROM DBMS_Table1 WHERE C2-Search;
        LIKE "% 98wu %";
```

One of the UDFs makes DBMS Server to check the matching of the ciphertext in the SEARCH column with the encryption of the string "Alice". The only leakage to DBMS

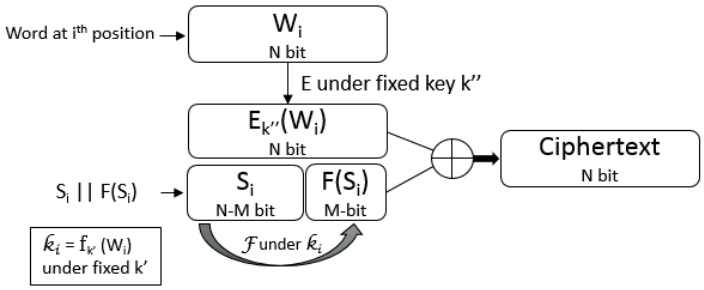


Fig. 6. Third Scheme

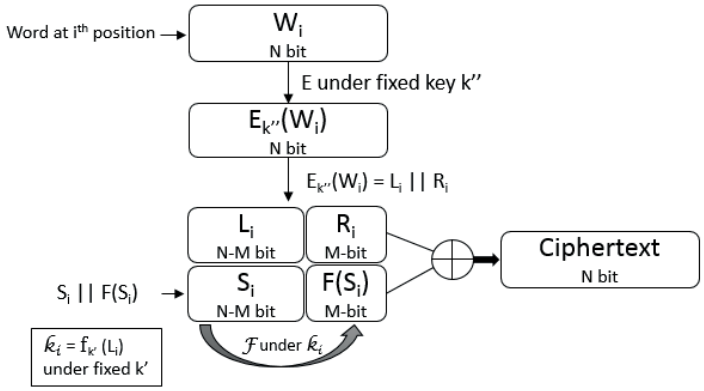


Fig. 7. Final Scheme

Server is that there is any matching with this full-word or not. Regular expressions and multiple words are not supported, just the full-word searches can be done with this algorithm, so this search part of CryptDB is not enough to meet our need for search queries.

TABLE IX
THE UPDATED TABLE WITH GRADE VALUES ADDED

StudentsWithGrades		
ID	**Name**	**Grade**
1	Alice	86
2	Bob	77
3	Eve	95

E. Queries with homomorphic addition functionality

From the point of the SQL queries, summation of the integer is used, not just for SUM queries, but also it is a part of counting average. The way of adding extra functionality to ciphertexts can be achieved by using homomorphic property. If one function is homomorphic, then multiplication of two ciphertexts is the encryption of the multiplication or addition of plaintexts of these two ciphertexts. For CryptDB, multiplication of the plaintext is not used from the point of the SQL queries, so additively homomorphic algorithm is necessary for this structure. Additively homomorphism can be demonstrated as follows:

m_1 and m_2 are the plaintext of the two values.

c_1 is the encryption of the m_1.

c_2 is the encryption of the m_2.

$c_1 \times c_2$ = Enc $(m_1 \times m_2)$ where Enc is an encryption function which has additively homomorphic property.

The homomorphic algorithm used in CryptDB is Paillier's algorithm. There is also Ge & Zdonik's algorithm. This algorithm, in general, aims to prevent the compromise of the database by processing queries on the ciphertext without decrypting them. It combines all the values of a row into one HOM ciphertext for each row. However it requires two times space overhead. For this reason, in CryptDB this algorithm is not implemented.

1) CryptDB's Homomorphic Property: In CryptDB, we keep the values as encrypted in the database. For this reason, homomorphic property is a solution for CryptDB. Queries with SUM and AVG are included in this part. We can create a query according to our example. We will update our table to make a meaningful query, and calculate the summation of the grades of the students. Our updated table is illustrated in Table IX.

Table IX is not kept inside the database as it is. Proxy Server encrypts the values for creating another table for DBMS Server. The created database for DBMS Server will be like in Table X.

Our example query can be like as follows:

```
SELECT SUM (grade) AS average FROM Students;
```

Proxy Server will modify the query, and send to DBMS Server. According to DBMS's Server's table, the modified

TABLE X
THE UPDATED TABLE WHICH IS CREATED ON PROXY SERVER'S SIDE

DBMS_Table2											
C1-IV	**C1-Eq**	**C1-Ord**	**C1-Hom**	**C2-IV**	**C2-Eq**	**C2-Ord**	**C2-Search**	**C3-IV**	**C3-Eq**	**C3-Ord**	**C3-Hom**
smsk	skwl	9dsi	32k0	cos8	qsaw	udb7	6sq8	wj9s	wus8	21do	qmdl
aksi	w8f9	v7sj	3ld0	sk0w	kd8s	lvmh	s99s	kcsk	dfsi	xnsk	ahc0
wipd	msuw	9s9k	389r	kduc	8sjf	k9sk	cnbs	bosm	xl9s	jwmd	h9dj

TABLE XI
AN EXAMPLE TABLE AND ITS ENCRYPTED FORM IN DET LAYER OF EQ ONION

Original_Table				**Encrypted_Table**			
ID	**Track-ID**	**Driver-Name**	**Location**	**col-1**	**col-2**	**col-3**	**col-4**
1005	1	Bob Marley	f.point	29ab74	b3ef12	ed34ef	12ada2
1006	1	Alice	g.point	6d5e5a	b3ef12	132ad3	27aa3b
1007	3	McDonald	g.point	b5aeb3	a214ba	3781e2	27aa3b
1008	3	Bob Marley	g.point	ae22ac	a214ba	ed34ef	27aa3b
1009	3	Bob Marley	a.point	8ebaba	a214ba	ed34ef	34ba9a

query will be as follows:

SELECT SUM (c3-Hom) AS average FROM DBMS_Table2;

After taking this SQL, DBMS Server will call the UDF which is responsible to calculate the summation of the values. This summation will be done by using homomorphic property. That is, the encrypted values of the C3-Hom column will be multiplied, and the result will be the encrypted format of the plaintexts.

Here, the values are $qmdl$, $ahc0$, and $h9dj$. Let's assume that the result of the multiplication is $a83g$.

$$(qmdl \times ahc0 \times h9dj) = a83g$$

Note that DBMS Server will not be able to know the values and the result because of encryption. The ciphertexts are multiplied which will result in a new fresh ciphertext. Proxy Server will take this encrypted result and will decrypt it. This decrypted value will be the the summation of the values inside the Grade column due to the underlying additively homomorphic property.

$$a83g = \mathsf{Enc}\ (86 + 77 + 95)$$

If Dec is the decryption function of the Enc which has additively homomorphic property, then the following equality will also be valid.

$$\mathsf{Dec}\ (a83g) = 86 + 77 + 95$$

Finally, the summation is done accurately on DBMS Server's side without revealing any information on the data itself. Namely, DBMS Server will not be able see the plaintexts, but it can still do the summation by only computing the multiplication over the ciphertexts.

IV. SECURITY & COMPLEXITY OF CRYPTDB AND FURTHER REMARKS

In this section, we are going to analyse the security and complexity of CryptDB and finally conclude our paper by giving further remarks.

CryptDB is open to frequency attack where the adversary knows the frequency of the plaintext. If the RND layer is decrypted to the DET layer in EQ onion, then the frequency attack is possible to apply because deterministic encryption is used in the DET layer. In this attack, the adversary that observes the queries can determine the ciphertext simply by looking at the results' row count. This attack can only be fixed by the RND layer, which has no usable functionality in practice.

For example, assume that we have left part of Table XI, and its encrypted form is the right part in Table XI. By using the knowledge of the frequency, one can learn the corresponding plaintexts from the right encrypted part in Table XI. This issue can be solved easily by using random IV based symmetric encryption, however this will prevent executing queries. The queries are always open in CryptDB which may leak information, too. By using the queries and their results, one can start to group the ciphertexts which is then possible to apply the frequency attack. We note that Private Information Retrieval (PIR) is required to eliminate this threat.

CryptDB is designed to move the database to cloud securely. The cloud is considered cheap for maintenance and administrative reasons. To evaluate the performance of CryptDB, a machine with two 2.4 GHz Intel Xeon E5620 4-core processors and 12 GB of RAM to run the MySQL 5.1.54 server, and a machine with eight 2.4 GHz AMD Opteron 8431 6-core processors and 64 GB of RAM to run the CryptDB proxy and the clients are used. [10] We believe that CryptDB may increase the cost significantly, i.e, one need an additional six core Proxy Server. On the other hand, the security of Proxy Servers must be ensured. This rises another administrative and security cost to the system.

To evaluate the performance, the assumptions are that CryptDB is trained on query set, i.e., onion adjustment is not happened during the test. The TPC-C Throughput is shown in following figure. The hardest hit is at the SUM and incremented UPDATE, the reason is they are using HOM onion. The overall throughput reduction is 26%. As average time, 0.60 ms is added to a query by Proxy Server. [10]

Deployment is another problem in CryptDB. Namely, if

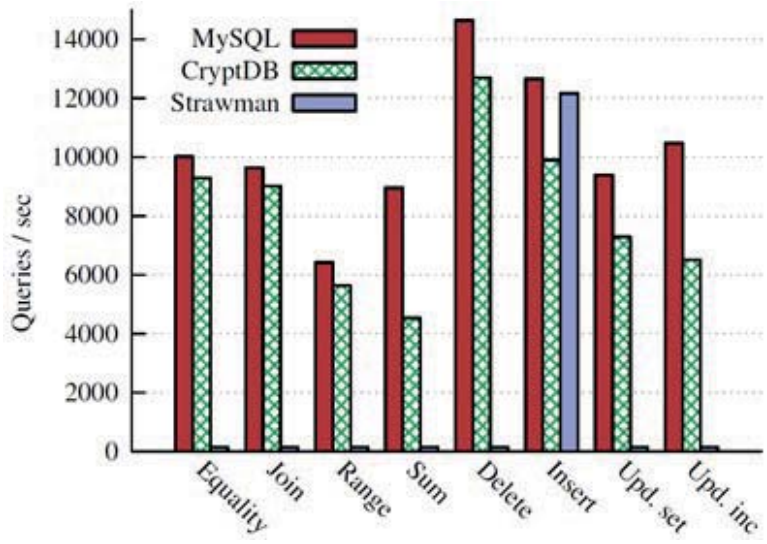


Fig. 8. TPC-C Throughput when CryptDB is trained on query set [10]

there is a bug at the production stage, debugging will be hard because of the encrypted values in the database. Therefore, in the real scenario, the companies will not be interested in using CryptDB.

Reducing the cost of Proxy Server is important in order to use CryptDB. Otherwise, CryptDB will only be useful for government agencies. Eliminating the frequency attack and hiding the queries must be taken into consideration in order to make the CryptDB more secure.

V. Conclusion

In this paper, we first explained CryptDB in a detailed way. CryptDB is the first practical Database Management System for running most standard queries on encrypted data. It does not make any changes to the DBMS. We revisited the server structure of CryptDB and pointed out the large overhead of the Proxy Server. We next explained the search algorithm of CryptDB which is based on Song's algorithm with the inabilities. We showed that the current search algorithm is not enough to meet all the search queries. We give a detailed analysis about the efficiency and security aspects. With some modification to the current form, the system can be more secure and can provide all necessary functionalities in order to execute all possible queries.

References

[1] NIST SP 800-145. The NIST Definition of Cloud Computing, National Institute of Standards and Technology. Retrieved 24 July 2011. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf .

[2] G. Rosen. Amazon usage estimates and updates, October 2009, URL: http://www.jackofallclouds.com/.

[3] Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. 2012. Cross-VM side channels and their use to extract private keys. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, NY, USA, 305-316.

[4] Cloud Security Alliance URL: https://cloudsecurityalliance.org .

[5] Marcos Dias de Assuncao, Alexandre di Costanzo, and Rajkumar Buyya. 2009. Evaluating the cost-benefit of using cloud computing to extend the capacity of clusters. In Proceedings of the 18th ACM international symposium on High performance distributed computing (HPDC '09).

[6] J. Brodkin. Gartner: Seven cloud-computing security risks. Infoworld, 2008.

[7] Cloud Computing Security Considerations, A Microsoft Perspective, Microsoft Whitepaper, 2010, http://www.microsoft.com/malaysia/ea/whitepapers.aspx.

[8] Cloud Computing: Benefits, Risks and Recommendations for Information Security, ENISA Report, 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-riskassessment.

[9] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance (CSA) Report, 2009, http://www.cloudsecurityalliance.org/csaguide.pdf. P. Mell and T. Grance. The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 2009.

[10] CryptDB: Protecting Confidentiality with Encrypted Query Processing. In Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP 2011), Cascais, Portugal, October 2011.

[11] Raluca Ada Popa, Frank H Li, Nickolai Zeldovich. An Ideal-Security Protocol for Order-Preserving Encoding. Symp on Security and Privacy, 2013.

[12] Order-preserving symmetric encryption. A. Boldyreva, N. Chenette, Y. Lee and A. O'Neill. In Eurocrypt '09, pp. 224-241. Springer, 2009.

[13] Practical techniques for searches on encrypted data. D. X. Song, D. Wagner, and A. Perrig. In Proceedings of the 21st IEEE Symposium on Security and Privacy, Oakland, CA, May 2000.

[14] C. Gentry. Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st ACM Symposium on Theory of Computing STOC 2009, pages 16978. ACM, 2009.

[15] Marko Hölbl, Cloud Computing Security and Privacy Issues, The Council of European Professional Informatics Societies (CEPIS), 15.03.2011. URL: http://www.cepis.org/media/CEPIS_Cloud_Computing_Security_v17.11.pdf .

[16] A.Greenberg. DARPA will spend 20 million to search for crypto's Holy Grail. Forbes, April 2011.

[17] Dan Boneh, Eyal Kushilevitz, Rafail Ostrovsky, William Skeith, Public Key Encryption That Allows PIR Queries. Preliminary version appeared in CRYPTO 2007: 50-67.

[18] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions, Journal of Computer Security, 2011.

[19] Andrew C. Yao, Protocols for Secure Computations, IEEE, 1982.

[20] López-Alt, Adriana and Tromer, Eran and Vaikuntanathan, Vinod, On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption, Proceedings of the 44th symposium on Theory of Computing, 2012.

[21] Damgård, Ivan and Zakarias, Sarah, Constant-Overhead Secure Compu-

tation of Boolean Circuits using Preprocessing, Theory of Cryptography, 2013.
[22] Damgård, Ivan and Pastro, Valerio and Smart, Nigel and Zakarias, Sarah, Multiparty Computation from Somewhat Homomorphic Encryption, Advances in Cryptology CRYPTO 2012.
[23] Ivan Damgård, Sebastian Faust, Carmit Hazay, Secure Two-Party Computation with Low Communication, TCC, 2012.
[24] Chen, Hao and Cramer, Ronald, Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields, Advances in Cryptology - CRYPTO 2006.
[25] P. Paillier. Public key cryptosystems based on composite degree residuosity classes. In Proc. of Eurocrypt 99, volume 1592 of LNCS, pages 223238. IACR, Springer-Verlag, 1999.
[26] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, IT-31(4):469472, 1985..
[27] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. Lest we remember: Cold boot attacks on encryption keys. In Proceedings of the 17th Usenix Security Symposium, San Jose, CA, JulyAugust 2008.

Ziynet Nesibe Dayioglu completed her bachelor studies at the department of computer engineering, Fatih University in İstabul, Turkey in 2012. She also completed her double major at the department of mathematics in Fatih University. Following the graduation, she started her masters studies at the department of computer engineering, Fatih University. Since February 2013, she has been working at the cryptology department of TUBITAK BILGEM as a researcher.

Mehmet Sabir Kiraz finished his bachelor studies at the department of mathematics, Middle East Technical University (METU) in Ankara, Turkey in 2000. Following the graduation, he worked at Pamukbank and Yapi Kredi Bank as software analyst and software programmer respectively. In October 2002, he started his masters studies at the International Max-Planck Institute for Computer Science in Saarbrücken, Germany and finished at the end of 2003 with a specialization on security protocols. From March 2004 to March 2008, he was a Ph.D. student at the Coding & Crypto group of the Technische Universiteit Eindhoven, under the supervision of prof. Henk van Tilborg and prof. Berry Schoenmakers. After his Ph.D. studies he worked at Phili, Eindhoven and TomTom, Amsterdam. Since 2010, he has been working as a researcher at the cryptology department of TUBITAK BILGEM.

Fatih Birinci received his Bachelor's degree and Master's degrees from the department of Mathematics, METU in 1995 and 1998 respectively. He also received Master's degree from department of Computer Engineering, Gebze Institute of Technology, in 2002. He has been working in TUBITAK BILGEM since 1997.

Ihsan Haluk Akin finished his bachelor studies at the department of mathematics, METU in Ankara, Turkey in 1999. He finished Master's degree at Sabanci University, Turkey in 2002. He finished his Ph.D. at METU in 2009. He worked at several places including TUBITAK BILGEM between 2000 and 2010. He worked at Fatih University between 2010 and 2013. Currently he is working as postdoc at Worcester Polytechnic Institute.

Yazılım Güvenlik Açıklıklarının Analizi İle Olası Zafiyet Öngörüsü

Oğuz BOZOKLU, Celal Zaim ÇİL, Şeref SAĞIROĞLU

***Özet*–Yazılımlar, güvenliklerinin tam manasıyla sağlanamaması ve güvenilirliklerinde hala şüphelerin bulunmasından dolayı, siber güvenlik ve savunma için önemi artan tehditlerin başında gelmektedir. Yazılım piyasası içerisinde ise; örün (web) tarayıcıları, işlevleri gereği, önemli bir yer işgal etmektedirler. Yaygın olarak kullanılagelen örün tarayıcılara ait güvenlik açıklık verilerinden yararlanılarak gelecekteki olası zafiyete ilişkin yapılabilecek öngörüler; hem yazılıma karşı yaklaşımımızın sınırlarını daha net çizmemize, hem de kaynaklarımızı daha etkin kullanmamıza ve sonuçta karşılaşılabilecek risklerinde minimize edilmesine olanak tanıyacaktır.**

***Anahtar Kelimeler*— açıklık, keşif, tarayıcı, yazılım**

***Abstract*—Software systems are the main threats for cyber defense and security because there is not really secure and reliable software and are a lot of suspects on them. Furthermore, in the software market, web browsers keep their strong positions because of their functions. Predicting and estimating vulnerabilities of widely used web browsers, by utilizing their vulnerability data sets, we can both take realistic decisions about software that we used and allocate and use our resources effectively.**

***Index Terms*— vulnerability, discovery, browser, software,**

I. GİRİŞ

BÜYÜK oranda yazılım güvenliğine dayanan siber güvenliğin artırılmasına ilişkin olarak; özellikle kritik altyapılarda ve savunma alanında kullanılan bilgi sistemlerinde güvenli (secure) ve güvenilir (reliable) yazılım geliştirilmesine ve kullanılmasına yönelik ciddi programlar mevcuttur [1]-[2].

Yazılımlarda tespit edilen güvenlik açıklıkları (software vulnerabilities), konuyla ilgili kamu kurumları ve/veya şirketler tarafından kamuoyuna duyurulmak suretiyle, güvenlik zafiyetinin asgariye indirilmesi hedeflenmektedir.

Bu açıklıkları, oluşturdukları veri tabanları yoluyla ilgililere ileten başlıca organizasyonlar;

ABD Ticaret Bakanlığı'nın bir kuruluşu olan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standarts and Technology - NIST)[3], ABD İç Güvenlik Bakanlığı'na bağlı olarak görev yapan ABD Bilgisayar Olaylarına Müdahale Ekibi (United States Computer Emergency Response Team - US_CERT)[4] ve Bağımsız olarak faaliyetlerini sürdüren Açık Kaynak Açıklık Veri Tabanı (Open Sourced Vulnerability Database - OSVDB) [5], Bilgi Güvenliği alanında faaliyet gösteren ticari şirketler ve organizasyonlar olarak sıralanmaktadır [6]-[8].

Türkiye'de ise, bu konuda görevlendirilmiş [9] TÜBİTAK Bilgisayar Olaylarına Müdahale Ekibi (TR_BOME) tarafından, yazılım güvenlik açıklıkları "Güvenlik Bildirileri" örün (web) sayfası üzerinden ilgililer ile paylaşılmaktadır [10].

Yazılımlarda mevcut güvenlik açıklıkları çoğunlukla, kamuoyu ile paylaşılmadan önce saldırganlar tarafından bilinen, belirli ortamlarda istismar edilmiş (exploit) ve ilgili yazılımın geliştiricisi firma tarafından büyük olasılıkla güvenlik yaması hazırlanarak yayımlanmış hususları içermektedir.

Bu kapsamda; kişi, kurum ve organizasyonları zarara uğratan esas konu, üreticinin, kullanıcının ve dolayısıyla kamuoyunun bilgisi dâhilinde olmayan ve çoğunlukla ancak saldırı sırasında haberdar olunan sıfır(ıncı) gün ('0' Zero Day) güvenlik açıklıklarıdır [11].

Dolayısıyla, olası bir zafiyetin önceden kestirilebilmesi ya da bir yazılım sisteminde belirli bir zaman aralığında hangi miktarda güvenlik açığı olabileceğinin tahmini önem taşımaktadır.

Günümüzde çok fazla sayıda ve çeşitlilikte yazılım hayatımıza girmiş olduğundan, bunların her biri için uygun bir öngörü modeli geliştirilmesi ve hangi yazılım grubuna öncelik verileceği hususu çözüm gerektiren karmaşık bir problemdir.

Konuya ilişkin olarak yapılan bu çalışmada, yukarıda sıralı hususlara ışık tutulması hedeflenmiştir. Bu kapsamda; bu bildirinin ikinci bölümünde temel kavramlar ve açıklık yaşam döngüsü açıklanmakta, üçüncü bölümde literatürde konuya ilişkin yapılan çalışmalar sıralanmakta, dördüncü bölümde öncelik verilmesi gerekli yazılım grubunun ne olması gerektiği irdelenmekte, beşinci bölümde konuya ilişkin Türkiye'deki duruma dair genel bir bakış sunulmakta, çalışma, sonuç ve öneriler ile sonlandırılmaktadır.

II. KAVRAMLAR VE AÇIKLIK YAŞAM DÖNGÜSÜ

Yazılım güvenliği disiplininde kullanılan kavramlar, sayıca çok, sıklıkla birbiri yerine kullanılan, bazen karıştırılan veya gerçek anlamından uzaklaştırılan niteliktedir. Dolayısıyla bu kavramlara açıklık getirilmesi, çalışmaların sağlıklı yürütülmesi açısından önemlidir.

Kavramların açıklanmasında, İngilizce karşılık ve/veya karşılıklarına da yer verilmek suretiyle anlatım kolaylığı hedeflenmiştir.

IEEE tarafından yayımlanan Yazılım Mühendisliği Standart Sözlüğünde [12] yapılan tanıma göre; insan tarafından yapılan bir *yanlışın (mistake)* bir tezahürü olan

Oğuz BOZOKLU, K.H.O. SAVBEN, Doktora Öğrencisi, obozoklu@gmail.com
Prof.Dr.Celal Zaim ÇİL, Çankaya Üniversitesi, czaimcil@cankaya.edu.tr
Prof.Dr.Şeref SAĞIROĞLU, Gazi Üniversitesi, ss@gazi.edu.tr

kusur (fault, defect, bug, flaw*)* sonucunda *başarısızlık (failure)* gelebilir, başarısızlık sonucu hedeften sapma miktarı ise *hatadır (error)*.

Bütün kusurlar *başarısızlığa* yol açmaz, ancak bütün *başarısızlıklar kusurların* sonucudur.

Saldırılara açık olma hali olarak da betimlenebilecek yazılım güvenlik *açıklıkları* (software security vulnerabilities) içinse, yaygın kabul görmüş ve doktrine olmuş bir tanım bulunmamaktadır.

Schneider; tasarım, uygulama ya da işletmede zayıflık veya hata [13] olarak tanımlarken, Veri ve Bilgisayar Güvenliği Sözlüğünde *bilgisayar açıklığı;* bilgi sistem güvenlik süreçlerinde ve idari kontrollerdeki bir zayıflığın, yetkisiz erişim ve saldırılara açık olma hali yaratması olarak açıklanmıştır [14].

Çalışmanın devamında yazılım güvenlik açıklığı yerine anlatım sadeliği maksadıyla çoğunlukla 'açıklık' tabiri kullanılmıştır.

Açıklığın keşfi, duyurulması, önlem alınması gibi işlem adımları, gerçek hayatta tam anlamıyla karşılığını bulamayabilmektedir. Aşağıda sıralı ve Şekil 1'de gösterilen bu adımların doğrusal bir süreç yerine döngüsel nitelikte olduğu, bazen eşzamanlı olarak faaliyetlerin yürütüldüğü, bazen ise basamaklardan bir ya da birkaçının hiç oluşmadığı hatırdan çıkarılmamalıdır.

Teorik olarak tanımlanmış ve Ozment tarafından tasnif edilmiş açıklık yaşam döngüsü kapsamındaki tanımlar aşağıda sıralanmıştır [15]:

--Doğum Tarihi-DT (Injection Date): Açıklığı barındıran kod parçacığının ilk olarak yazılıma eklendiği ve derlendiği tarihtir.

--Piyasaya Sürülme Tarihi-PST (Release Date): Açıklığı ihtiva eden yazılımın piyasaya sürüldüğü tarihtir.

--Keşfedilme Tarihi-KT (Discovery Date): Açıklığın ilk kez fark edildiği tarihtir.

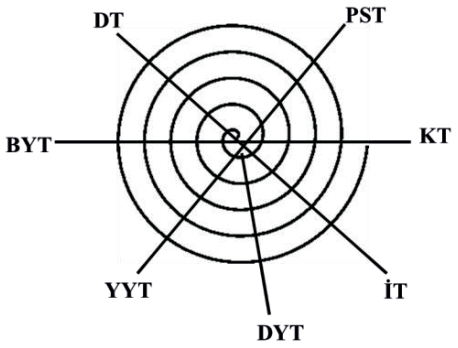
--İfşa Tarihi-İT (Disclosure Date): Açıklığı keşfedenin, yazılım geliştiriciyi ya da ilgili kurumu açıklığa ilişkin haberdar ettiği tarihtir.

--Duyuru Tarihi-DYT (Public Date): Açıklığın kamuoyuna duyurulduğu tarihtir. Genelde açıklık için geliştirilen yamanın yayımlanma tarihi ile aynıdır.

--Yama Yayımlama Tarihi-YYT (Patch Date): Açıklık için ilk düzeltmenin yayımlandığı tarihtir.

--Betik Yayımlama Tarihi-BYT (Scripting Date): Açıklığı istismar etmek üzere hazırlanmış ilk betiğin yayımlandığı tarihtir.

Yukarıda sıralı tarihleri tam ve gerçek bir şekilde tespit edebilmenin zorlukları ortadadır. Özellikle açıklık keşfetme ve ifşa tarihlerindeki belirsizlikler, yapılacak çalışmalarda mutlaka göz önünde bulundurulmalıdır.



Şekil.1. Açıklık Yaşam Döngüsü [15]

Yazılım açıklıklarının yaratılması, keşfi, ortadan kaldırılması vb. işlemlerde aktif olarak yer alan gerçek ve tüzel kişilere daha yakından bakmak gerekirse bunlar aşağıdaki şekilde sıralanabilir [15]:

--Bulucu *(Detector):* Yazılımdaki açıklığın farkına varan, açıklığı bulandır.

--Firma *(Vendor):* Ticari maksadı olsun ya da olmasın yazılımı geliştirendir, onun sahibidir.

--Firma Bulucusu *(Vendor Detector):* Görevi, yazılımdaki açıklıkları arayıp bulmak olan ücretli firma çalışanıdır.

--Bağımsız Bulucu *(External Vendor):* Sistemlerdeki açıklıkları arayarak bulan ancak firmanın maaşlı çalışanı olmayan kişidir.

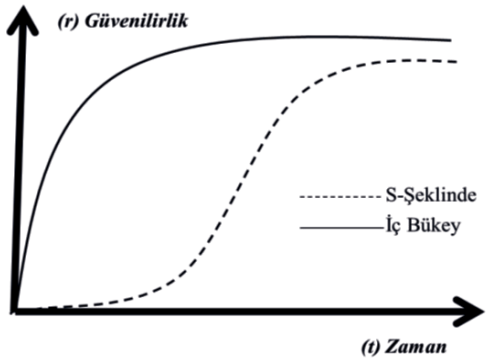
--İfşa Kurumu *(Disclosure Institution):*Bulucunun tespit etmiş olduğu açıklığı rapor ettiği yer, bu açıklığı firmaya ileten organizasyondur.

Açıklığın ifşasında sorumlu davranışta *(responsible disclosure)* bulunulması önemlidir. Yama yayımlanmadan önce açıklığın kamuoyuna duyurulması önemli sakıncalar doğurabilir.

III. LİTERATÜR

Yazılım Açıklıklarının Keşfine dönük modeller (Vulnerability Discovery Models -VDMs) başlangıçta büyük oranda Yazılım Güvenilirliği Geliştirme Modellerine (Software Reliability Growth Models - SRGMs) dayandırılmıştır.

Yaklaşık 30 yıldan fazla bir geçmişi olan Yazılım Güvenilirliğine ilişkin çalışmalar ve ortaya konulan modeller; Şekil 2'de görüleceği üzere iç bükey *(concave)* ve S-şeklinde *(S-shaped)* olmak üzere iki ana grupta toplanmıştır [16].



Şekil.2. Yazılım Güvenilirliği Ana Yaklaşımlar [16].

Yazılım Güvenilirliği Geliştirme yöntem ve modellerinden en önde gelenleri; Goel-Okumoto (G-O) [17], G-O S-Şeklinde [18], Hossain-Dahiya/G-O [19], Gompertz [20], Pareto [21], Weibull [22], Yamada Üssel [23] olarak sıralanmaktadır [16].

Yazılım Açıklık Keşfine dönük önde gelen çalışmalar ise, ABD Colorado Devlet Üniversitesi'nde Malaiya'nın önderliğinde yapılan araştırmalardır [24]. Bu araştırmalar kapsamında ortaya konulan önemli bir yaklaşım S-Şeklinde *(S-Shaped),* Zaman Tabanlı *(Time-Based)* "Alhazmi-Malaiya Lojistik Modeli" (AML)dir. Bu model ve diğer bazı temel yaklaşımlar Şekil 3'de gösterilmiştir.

Sunucu tarafında Windows NT 4.0, istemci tarafında ise Windows 98 işletim sistemleri açıklık verilerinden yararlanılmak suretiyle, takvim zaman aralıklarına dayandırılarak yapılan çalışmada; saldırganların da dâhil olduğu yazılım test grubunun, hedef yazılımı anladıkları ve gerekli bilgileri topladıkları "öğrenme safhası", yazılımın dikkat çekmeye başladığı ve yaygınlaştığı "doğrusal safha", yazılımla ilgili yamaların yayımlanma sıklığının azaldığı ve kullanıcıların yazılımın yeni sürümüne geçişe başladıkları "doygunluk safhası" olarak tanımlanmış ve açıklık/zaman düzleminde S şeklindeki bir eğri üzerine model oturtulmuştur [24].

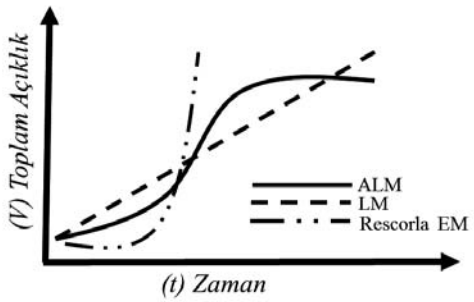
Çalışmada ayrıca, oluşturulacak modellerin, yazılımın yaygınlığı ile yakın ilişkili olduğu vurgulanmıştır. Bu kapsamda; yazılımın yaygın kurulum ve kullanımın, açıklık tespitine yönelik gayretleri de aynı oranda artıracağı varsayımı üzerine bir model inşa edilerek, Gayrete Dayanan (Effort Based) Model olarak literatüre sunulmuştur [24]. Yazılım Güvenilirliği Geliştirme Modelleri (Software Reliability Growth Models [SRGMs]) ile analoji kurularak geliştirilen söz konusu modelde, tanımlanan bir "gayret katsayısı" ile çalışmaya derinlik kazandırılmaktadır.

Çoklu sürüme sahip yazılımlarda açıklık tespitine dönük olarak açık kaynak kodlu Apache HTTP Web Sunucusu ve Mysql Veri Tabanı Yönetim Sistemi (DBMS) açıklık verileri kullanılarak yapılan bir diğer araştırmada da verilerin AML'ye büyük oranda uygunluğu görülmüştür [25].

AML Modelinin Internet Explorer ve Firefox örün (web) tarayıcılarının açıklık veri setlerine uyumluluğunun (goodness-of-fit) denetlendiği başka bir çalışmada, başarılı sonuçlar gözlemlenmiş, gelecekte ortaya çıkarılması beklenen açıklık miktarının tahmin edebilmesi için AML'den yararlanılabileceği belirtilmiştir. Çalışma kapsamında ayrıca, veri setleri, açıklık sebepleri ve açıklığın ciddilik seviyesi ele alınarak tasnif edildiğinde de, modelin öngörülerini destekleyici sonuçlara ulaşılmıştır [26].

Alhazmi ve Malaiya tarafından yapılan bir diğer çalışmada; Apache ve IIS örün (web) sunucularının AML ve Doğrusal (Linear) modele uygunluğu test edilmiş, bunun yanı sıra kısa ve uzun vade açıklık öngörü kabiliyetleri sınanmıştır. AML modelinde tatmin edici sonuçlar alınmakla birlikte, doğrusal modelin öngörüleri ve uyumluluğu dikkat çekici bulunmamıştır [27].

Win2000, WinXP, Red Hat 7.1 için AML ve doğrusal modeller için ile öngörü testi [28], değişik modellerin Win95, WinXP ve RedHat 6.2 için uyumluluk düzeylerinin kıyaslanması [29] araştırmaları, yapılmış olan dikkat çekici diğer bazı araştırmalardır.



Şekil.3. Temel Açıklık Bulma Yaklaşımları [29]

Rescorla [30] tarafından; Doğrusal Model ve Yazılım Güvenilirliği Modeline dayalı üssel yaklaşıma (Rescorla EM) uyumlulukları kapsamında yapılan çalışmada ise; Win NT4, Solaris 2.5.1, Free BSD 4.0 işletim sistemlerinde olumsuz sonuçlar alınmış, Red Hat 6.2 için belirgin neticeler gözlemlenmişse de, modelin öngörü yeteneklerine ilişkin bir analizde bulunulmamıştır.

MIT Lincoln Laboratuvarlarından Ozment [31], açıklık öngörü modellerinin dayandığı varsayımlar ve bu varsayımların karşılanması anlamında eleştiriler getirdiği çalışmasında dört noktaya dikkat çekmiştir. Bunları;

--Açıklıkların tespit edilmesi için geçen ya da harcanan zaman diliminde gösterilen gayretlerin ölçülebilirliğindeki zorluklar,

--Yazılımın kullanıldığı ortamla etkileşimindeki farklılıklar,

--Yazılım kodlarının statik olmadığı ve aslında her bir yamanın yeni açıklıklar yaratma potansiyeli bulunduğu,

--Açıklıkların bazı durumlarda birbirini tekrar eder nitelikte bağımlılıklar içerebildiği şeklinde sıralamıştır.

Ozment ayrıca; yapmış olduğu doktora tezi çalışmasında [15] OpenBSD yazılımının güvenlik açıklık verilerini irdeleyerek, ekonomik boyutunda ele alındığı derinlemesine bir analiz ortaya çıkarmıştır.

McQueen ve diğ. tarafından yapılan bir çalışmada ise; Sıfır Gün Açıklıkları (SGA) üzerine ortaya konulan yöntemdeki öngörüye göre, çalışmanın yapıldığı dönem itibariyle, 2006 yılı için, örnek olarak seçilecek herhangi bir günde ortalama 2500 ila 4500 civarında SGA'nın var olduğu belirtilmiştir [11].

Nguyen ve Sang tarafından, Mozilla Firefox JSE (Java Script Engine) hedef alınarak yapılan çalışmada ise,

karşılıklı bağımlılık grafikleri (Dependency Graphs) yöntemi ile açıklık öngörüsü sınanmış ve olumlu sonuçlar gözlemlenmiştir [32].

Başlangıçta Yazılım Güvenilirliği Geliştirme Modelleri olarak başlayan çalışmaların, son dönemde açıklık keşfetme ve öngörüye dayalı model arayışlarına yöneldiği anlaşılmaktadır. Bu noktada; öngörüde bulunulmak istenen yazılım grubunun seçimine ilişkin alınacak kararın önemi artmaktadır.

IV. AÇIKLIK ÖNGÖRÜSÜNDE BULUNULMASI HEDEFLENEN YAZILIM SEÇİMİ

Yazılım açıklık verilerinin analizi ile geleceğe dönük olarak olası bir kestirimin yapılması araştırmaları, eldeki kısıtlı veriye dayalı, dayandığı varsayımlar itibariyle karmaşık çözümlemeler gerektirebilecek problemli bir alandır. Ancak; güvenilir, öngörü yeteneği yüksek bir modelin geliştirilmesinin sağlayacağı faydalar büyüktür.

Öngörüde bulunulması hedeflenen yazılım grubunun seçilmesi, bu yazılımlara ait açıklık verilerinin tasnifi ve analize hazırlanması, verilerin bilimsel yöntemlerle geçerliliğinin sınanması, sağlıklı bir araştırma için temel adımlardır.

Böylesi bir gayretin merkezine; (a) son dönem bilgi sistem uygulamaların büyük oranda örün tabanlı geliştirilmesi, (b) kullanılacak olan açıklık veri tabanlarında örün tarayıcılarına ait verilerin, oransal olarak görece daha fazla olmasının araştırmanın niteliğine sağlayacağı olumlu katkı, (c) küresel ölçekte %90'lara varan pazar payları olması [33]–[35 nedenleriyle, örün tarayıcılardan Microsoft Internet Explorer, Google Chrome ve Mozilla Firefox yazılımlarının konulması gerektiği değerlendirilmektedir. Bu hususlar aşağıda başlıklar altında sunulmuştur.

A. Örün Tabanlı Uygulamalardaki Artış

Son 15 yıldır bilgi sistem iletişim teknolojilerindeki gelişmeler ve iletişim altyapı bant genişliğinin dikkate değer ölçüde artmış olması sebebiyle, tek başına çalışan sistem ve terminallerin yerini artık ağ tabanlı çalışan ve küresel hizmet veren yapılar almıştır.

Birçok bilgi sistem uygulamasının 'giriş kapısı' karakterine bürünen örün tarayıcılar ise adeta bu dönüşümün öncüleri olarak görev yapmışlardır.

Örün tarayıcılar marifetiyle bilgiyi paylaşan ağ tabanlı sistemlerin yaygınlaşması, saldırganların, hedeflerine tek bir yolla ulaşmaları zorunluluğunu azaltmış, örün tarayıcısına gömülü bir uygulamaya (built-in interpreter; HTML (Hyper Text Markup Language), JavaScript, CSS (Cascading Style Sheets, vb.) zararlı içeriği bir şekilde bulaştırmak suretiyle saldırıların boyutunu değiştirmiştir. Bu yolla uzaktan istismar edilebilir güvenlik açıklarının 2000-2007 yılları arasında %89,4 oranında arttığı rapor edilmiştir [36].

Yaşanan gelişmeler, alınacak güvenlik önlemlerinin en ön sıralarına örün tarayıcıları almamız gerektiğini işaret etmektedir.

B. Açıklık Veri Tabanlarında Bulunan Örün Tarayıcılara Ait Verilerin Oransal Fazlalığı

1997 yılından itibaren açıklık verilerinin tutulduğu ve 2005 yılından itibaren kamuyla paylaşılmaya başlandığı ABD Ulusal Açıklık Veritabanı (NVD) incelendiğinde [40], hâlihazırda **57046** adet açıklığın duyurulmuş olduğu, günde ise ortalama 16 adet duyuru yapıldığı görülmektedir [3].

Bu verilerden;

--Internet Explorer için, ilki 01/03/1997 tarihinde duyurulan "CVE-1999-1128" açıklığından, 10/07/2013 tarihindeki "CVE-2013-3166" açıklığına kadar toplam **1054** adet,

--Google Chrome için, ilki 30/09/2008 tarihinde duyurulan "CVE-2008-4340" açıklığından, 10/07/2013 tarihinde duyurulan "CVE-2013-2880" açıklığına kadar top**lam 877** adet,

--Mozilla Firefox için ise, ilki 27/07/2004 tarihinde duyurulan "CVE-2004-0718" açıklığından, 26/06/2013 tarihindeki "CVE-2013-1700" açıklığına kadar topla**m 1049** adet açıklığın kamuoyu ile paylaşıldığı görülmektedir.

NVD'de onbinlerce yazılıma dair açıklık duyuru verilerinin bulunduğu düşünüldüğünde, bu üç örün tarayıcıya ait **v**erilerin toplam duyuruların yaklaşık %5'ine tekabül etmesi ve görece oransal büyüklüğü dikkat çekicidir.

C. Pazar Payı Olarak Üç Tarayıcının Hâkimiyeti

Bu üç tarayıcının değişik kaynaklardan edinilen bilgilerle derlenen ve ayrıntısı Tablo 1'de sunulan pazar payı oranlarına bakıldığında dünya genelinde yaygın şekilde kullanıldıkları açıkça görülmektedir [33]-[35].

TABLO I
ÖRÜN TARAYICISI PAZAR PAYLARI [33]-[35.]

Tarayıcı	.statcounter [33]	.sitepoint [34]	.w3schools [35]
IE	42,68%	29,82%	12,6%
Chrome	25,44%	37,11%	27,7%
Firefox	20,01%	21,34%	52,9%
TOPLAM	88,12%	89,27%	93,2%

Ülke özelinde bakıldığında da; % 57,97 Chrome, %27,81 IE ve %8,52 Firefox olmak üzere toplamda %94,30'luk oranla Benzer bir sonuç göze çarpmaktadır. Türkiye pazarına yakın zamanda giriş yapan Yandex tarayıcının pazar payı %2,5-3 seviyelerindedir [33].



Şekil.4. Örün Tarayıcı Pazar Payı Değişim Eğilimleri [33].

Zaman ve kullanım yaygınlığı düzleminde oluşturulan Şekil 4'de ise;

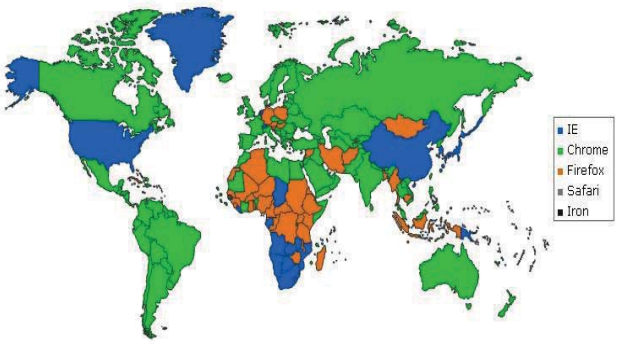
--IE kullanımın genelde ABD ve Çin'de daha çok tercih edildiği (Bknz. Şekil 5.) ve dünya genelinde pazar payının düşüş eğiliminde olduğu,

--Chrome örün tarayıcısının, kullanımının zaman içerisinde yaygınlaştığı,

--Yatay bir eğride seyreden Firefox'un daha tutucu ve sadık bir kullanıcı kitlesine hitap ettiği şeklinde yorumlanabilir.

V. TÜRKİYE'DEKİ DURUMA GENEL BİR BAKIŞ

Türkiye'de, siber güvenlik konusunda artan bir farkındalık ve bilinç söz konusu ise de gerekli örgütlenme ve mekanizmalar arzulanan düzeyde değildir [37]-[39].



Şekil.5. Kullanım Yaygınlığı Haritası [33].

Etkin ve sürdürülebilir bir yapıya kavuşturulması gerekli mekanizmalardan belki de en gerekli olanlardan birisi, yazılım açıklıklarından haberdar olunduğu, ilgililere duyurulduğu, doğru ve güvenilir açıklık öngörülerinin yapılabildiği bir yapının kurulmasıdır.

Mevcut durumda yazılım açıklıklarından görece önemli olduğu değerlendirilenler, TÜBİTAK [10] tarafından, örün sayfası yoluyla, "güvenlik bildirileri" adı altında, ilgililere duyurulmaktadır.

Söz konusu açıklık verileri; yazılım geliştirici firmalara veya ABD kaynaklı diğer ilgili kuruluşlara [3]-[8] dayandırılmaktadır.

Değerli bilgiler içeren ve birçok konuda her seviyeden kullanıcıya bilgi güvenliği konusunda yol gösterici olarak önemli bir işlevi yerine getiren www.bilgiguvenligi.gov.tr [10]'da, güvenlik bildirilerinin kapsamı; "*ülkemizde ve özellikle kamu kurumlarında sıkça kullanıldığı tespit edilen/öngörülen bilgi sistemi varlıklarında yeni bulunan açıklıklar hakkında detaylı bilgileri içerir. Bu açıklıklar TUBİTAK BİLGEM Siber Güvenlik Enstitüsü ağ güvenliği laboratuvarında tespit edilebileceği gibi, farklı açıklık veritabanlarından da alınabilir.*" şeklinde açıklanmaktadır.

TÜBİTAK tarafından yayımlanan güvenlik bildirilerine niceliksel olarak bakıldığında; **12 Mart 2008** ile **18 Haziran 2013** tarihleri arasında **623** adet güvenlik açıklığı ile ilgili duyuru yapıldığı görülmektedir. Aynı zaman aralığında NVD [3]'de **26849**, OSVDB [5]'de **45927,** Securityfocus [6]'da **35684** ve Rapid7 [7]'de ise **6154** adet güvenlik açıklığı ele alınarak duyurulmuştur.

Söz konusu duyuru sayfası [10]; site içi arama seçeneği sunmasına rağmen, açıklığa dair değişik parametrelere göre (açıklığın cinsi, üreticisi, tarihi, risk seviyesi vb.) açıklık veritabanını tarama olanağı sunmamaktadır.

Türkiye'de bilgi güvenliğine katkı kapsamında, yazılım açıklıkları konusu ile doğrudan ya da dolaylı olarak ilgili çeşitli platformlar [41]-[47] bulunmaktadır. Bu ve benzeri diğer platformların içeriğini ve yaygınlığını gün geçtikçe artırdığı görülmektedir.

VI. SONUÇ VE TARTIŞMA

Yazılımlardaki olası bir zafiyete dönük olarak geleceğe dair bir güvenlik açıklık öngörüsünde bulunabilmenin özellikle kritik altyapılar düşünüldüğünde hayati öneme haiz sonuçları olabileceği açıktır.

Bu yazılımların başında örün tarayıcıların her türlü sürümü gelmektedir.

Ülke içerisinde ise, büyük oranda dışa bağımlılık arz eden genel kullanıma dönük yazılımlara dair güvenlik açıklıklarının toplanması, derlenmesi, kendi içerisinde tutarlı bir şekilde sınıflandırılması, analizi ve duyurulması faaliyetlerinin bir takım zorluklar içerdiği anlaşılmaktadır.

Zaman içerisinde kamu başta olmak üzere [48] ülke sathında açık kaynak kodlu yazılımlar ve buna ek olarak özgün milli yazılımların yaygınlaşması öngörüldüğünden, yazılım açıklıklarının saldırganlardan önce tespit edilmesi, önlem alınması ve kullanıcılara duyurulması gün geçtikçe artan bir gereklilik olarak karşımıza çıkacaktır.

Bu çalışma kapsamında elde edilen bulgular ve öneriler aşağıda verilmiştir.

--Kısa sürede NVD, OSVDB, Securityfocus ve Rapid7 gibi güvenlik açıklığı duyurusu yapan yapılar kurulmalı veya bilgiguvenligi.gov.tr de bulunan yapı güncellenmelidir

--Yazılım güvenliği ve güvenilirliğini test eden merkezler açılmalıdır.

--Yazılımları Ortak Kriterlerde farklı seviyelerde test edebilen (EAL seviyeleri) yapılar oluşturulmalıdır.

--Artık günümüzde yazılımların aynı zamanda siber silahlar olduğu, özellikle amaca yönelik olarak geliştirilen yazılımlarla ülkelere büyük boyutta zararlar verilebildiği unutulmadan gerekli önlemler alınmalıdır.

--Ülkemizde yazılım güvenliği ve güvenilirliğine yönelik olarak üniversitelerde ar-ge çalışmalarına önem verilmelidir.

--Ülkemizde bu konuda belirli standartlar geliştirilmeli, kritik görevlerde kullanılan yazılımlar test edilmeden kesinlikle kullanılmamalıdır.

--Bu çalışma kapsamında yer alan örün tarayıcıları konusunda da mutlaka derinlemesine çalışmalar yapılmalı, gerekirse yeni bir örün tarayıcı da geliştirilmelidir.

Açıklıkların analizi ve olası açıklık öngörüsüne ilişkin küresel çerçeveden bir bakışı, yerel oluşum ve yapılanmayı genel olarak inceleyerek destekleyen bu çalışmanın, geleceğe dönük olarak kurulması ve geliştirilmesi hedeflenen özgün yapılar için ışık tutabileceği değerlendirilmektedir.

KAYNAKLAR

[1] Information Security Management System (ISMS), 2005,(ISO 27001)
[2] Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an International Standard (ISO/IEC 15408)
[3] ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Açıklık Veri Tabanı (NVD) Örün (web) Sayfası. http://nvd.nist.gov.

[4] ABD Bilgisayar Olaylarına Müdahale Ekibi Örün (web) Sayfası. http://www.kb.cert.org/vuls

[5] Açık Kaynak Açıklık V eri Tabanı Örün Sayfası, http://osvdb.org.

[6] Security Focus, Symantec. Açıklık Veri Tabanı Örün Sayfası. http://www.securityfocus.com/vulnerabilities,

[7] Rapid7, http://www.rapid7.com/vulndb/index.jsp

[8] The MITRE Corporation, http://cve.mitre.org/,

[9] Bilgi Toplumu Stratejisi Eylem Planı (2006–2010), 88 Numaralı Eylem Maddesi, Devlet Planlama Teşkilatı (DPT).

[10] TÜBİTAK BİLGEM Bşk.lığı Bilgisayar Olaylarına Müdahale Ekibi (TR_BOME) Örün Sayfası, http://www.bilgiguvenligi.gov.tr/guvenlik-bildirileri/index.php

[11] Miles A. McQueen ve diğ., *Empirical Estimates and Observations of 0Day Vulnerabilities*, Hawaii International Conference on System Sciences

[12] IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 610.121990, (Revision and reddgnation of (IEEEstd7921983),1990.

[13] Schneider, Trust in Cyberspace, 1998

[14] Dennis Longley ve Michael Shain, *Data & Computer Security: Dictionary of Standards Concepts and Terms*, 1987, Stockton Pr (December 1987)

[15] Ozment Andy, *Vulnerability Discovery & Software Security*, University of Cambridge Computer Laboratory Computer Security Group & Magdalene College, August 31, 2007, Degree of Doctor of Philosophy

[16] Wood Alan, *Predicting Software Reliability*, 1996, Tandem Computers

[17] A.L.Goel ve Okumoto, "*A Time Dependent Error Detection Model for Software Reliability and Other performance Measures*", IEEE Trans.Reliablity.Ağustos 1979, pp.206-211.

[18] S.Yamada, M.Ohba, ve Osaka, *"S-Shaped reliability Growth Modeling for Software Error Detection"*. IEEE Trans. Reliability. Aralık 1983,pp. 475-484

[19] S.Hossain ve R.Dahiya, "*Estimating the Parameters of Non-Homogeneous Poisson-Process Model of Software Reliability*", Aralık 1993, IEEE Trans. Reliability.pp. 604-612

[20] D.Keçecioğlu, *Reliablity Engineering Handbook*, Vol.2, Prentice-Hall, Englewood Cliffs,NJ,1991.

[21] B.Littlewood,"*Stochastic Reliability Growth:A Model for Fault Removal in Computer Programs and Hardware Design*" IEEETrans reliablity, Aralık 1981, pp.313-320.

[22] J.Musa,A.Iannino ve K.Okumoto, Software Reliability,McGraw-Hill,New York, 1987.

[23] S.Yamada, H.Ohtera, ve H.Narihisa "*Software Reliability Growth Models with Testing Effort*" IEEE Trans Reliablity. Nisan 2986,pp.19-23

[24] Omar H. Alhazmi, Yashwant K. Malaiya, *Quantitative Vulnerability Assessment of Systems Software*, Colorado State University,2005

[25] Jinyoo Kim, Yashwant K. Malaiya, Indrakshi Ray, *Vulnerability Discovery in Multi-Version Software Systems*, Computer Science Department, Colorado State University, Fort Collins,2007.

[26] Sung-Whan Woo, Omar H. Alhazmi and Yashwant K. Malaiya, *An Analysis Of The Vulnerability Discovery Process In Web Browsers*, Computer Science Department, Colorado State University, Fort Collins,

[27] Omar H. Alhazmi and Yashwant K. Malaiya, *Measuring and Enhancing Prediction Capabilities of Vulnerability Discovery Models for Apache and IIS HTTP Servers*, ,2006.

[28] Omar H. Alhazmi,, *Prediction Capabilities of Vulnerability Discovery Models*, Colorado State University Yashwant K. Malaiya, Ph. D., Colorado State University, 2006.

[29] Omar H. Alhazmi and Yashwant K. Malaiya, Senior Member, IEEE *Application of Vulnerability Discovery Models to Major Operating Systems*, 2008.

[30] Eric Rescorla, *Is Finding Security Holes a Good Idea?* RTFM, 2005.

[31] Ozment Andy, *Improving Vulnerability Discovery Models, Problems with Definitions and Assumptions*, MIT Lincoln Laboratory & University of Cambridge.

[32] Nguyen Viet Hung ve Le Minh Sang Tran, *Predicting Vulnerable Software Components with Dependency Graphs*, University of Trento, Italy,2010.

[33] Örün sayfası, http://gs.statcounter.com/

[34] Örün sayfası, http://www.sitepoint.com/browser-trends-march-2013/

[35] Örün sayfası, http://www.w3schools.com/browsers/browsers_stats.asp

[36] Stefan Frei ve diğ., *Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the "insecurity iceberg"*,ETH Zurich Tech Report Nr. 288.

[37] E-Devlet Yuvarlak Masa Toplantısı, 10/03/2009, http://www.bthaber.com.tr/?p=10979&sayi=SAYI:810, , Sheraton Otel.

[38] Sağıroğlu Ş. Prof. Dr. http://ceng.gazi.edu.tr/secure/yazilardetay.aspx?yaziid=10, 06 Mayıs 2012 tarihinde erişim sağlanmıştır.

[39] Acarer Tayfun, BTK Başkanı, "*Siber Saldırılara Hazır Değiliz",* http://www.marmaraweb.com/web-tasarim-blogu/459-siber-saldirilara-hazir-degiliz.html,

[40] Mathias Karlsson, *The Edit History of the National Vulnerability Database and similar Vulnerability Databases*, Master's Thesis.Swiss Federal Institute of Technology, Zurich.

[41] Bilişim Platformu Örün Sayfası, http://www.bilisimplatformu.com/#

[42] E-Siber Örün Sayfasıhttp://www.e-siber.com/, 14 Temmuz 2013 tarihinde erişilmiştir.

[43] Forum Sayfası, http://www.frmtr.com/guvenlik-ve-guvenlik-aciklari/

[44] Örün Sayfası, http://www.olympos.net,

[45] Örün Sayfası, http://www.turk.internet.com/portal/index.php

[46] Örün sayfası, http://www.webguvenligi.org/,

[47] Örün sayfası, http://yazilimportal.com/

[48] M. Raşit ÖZDAŞ, "*Kamuda Açık Kaynak Kodlu Yazılım Kullanımı", Eylül 2012*, Çalışma Raporu – 4, Kalkınma Bakanlığı Bilgi Toplumu Dairesi, Ankara.

DNS Güçlendirme Saldırısı Risk Analizi

Devrim Seral

***Özet*—Son zamanlarda meydana gelen çok büyük Dağıtık Servis Engelleme Saldırılarının ardında DNS güçlendirme saldırılarının tetikçi olduğu bilinmektedir. Bu saldırı türü, dağıtık servis engelleme saldırılarını, farklı ağlardaki özyinelemeye açık DNS sunucuları aracı olarak kullanarak yerine getirmektedir. Bu sistemlerin tespit edilerek tanımlanmaları uzun ve zahmetli bir işlemdir. Bu yüzden bu çalışmada, çalışma kümesi olarak Kuzey Kıbrıs Türk Cumhuriyetinde faaliyet gösteren biri kamu olmak üzere toplamda sekiz adet İnternet Servis Sağlayıcı ağı kullanılmıştır. Geliştirilen bir betikle bu ağlar üzerinde tespit edilen özyinelemeye açık DNS sunucuları ile ilgili toplanan bilgiler sunulmuş ve yaratabilecekleri riskler ortaya konmuştur.**

Anahtar Kelimeler—DDoS, DNS, DNS Güçlendirme Saldırısı

***Abstract*— DNS amplification attacks are known as perpetrator of today's very huge Distributed Denial of Service attacks. This type of attack performs distributed denial of service attack through open recursive DNS servers located in different locations. Discovering and identifying open recursive DNS servers are time consuming and troublesome process. Therefore in this study we use eight Internet Service Provider (One of them government internet provider) networks that operate at Turkish Republic of Northern Cyprus as a working set. A script developed to identifying and collecting information for open recursive DNS servers that available in these networks and risks that sourced by these systems expressed.**

Index Terms—DDoS, DNS, DNS Amplification Attack

I. GİRİŞ

İNTERNET kullanımının sürekli olarak artması ile birlikte servis veren kurum ve şirketlerin erişilebilir olması, gittikçe daha da önemli bir hale gelmiştir. Türkiye'de 2013 yılı ilk üç aylık dönemde geniş bant İnternet abonesi sayısı 20 milyon kişiyi aşmış ve bu abonelerin %78 gibi büyük bir kısmının 8Mbps hıza kadar bağlantı sunan paketleri tercih ettikleri görülmüştür [1]. Ayni zamanda Bankalararası Kart Merkezi verilerine göre 2013 yılı sonuna kadar İnternet üzerinden harcanması beklenen para miktarı 34 milyar TL'ye ve yapılan işlem miktarının da 160 milyonu bulması beklenmektedir [2]. Dünyanın diğer ülkelerinde de ITU (International Telecommunication Union) verilerine göre 2.7 milyar kişinin geniş bant İnternet bağlantısına sahip olduğu bilinmektedir [3]. Diğer yandan 2013 yılı içinde e-ticaretin 1.3 trilyon dolarlık bir büyüklüğe ulaşacağı tahmin edilmektedir [4]. Bu bilgiler ışığında dünyanın birçok ülkesinde gerek kamu gerekse özel şirketlerin çevrimiçi hizmet sayısını sürekli artırdığı kuşku götürmez bir gerçektir. Bu kadar fazla ekonomik büyüklüğe ve kullanıcı sayısına ulaşan çevrimiçi servislere rekabetten, pazar paylaşımından ve hatta siyasi yada politik nedenlerle sorun çıkarmak isteyenlerin bulunması kaçınılmaz olmaktadır. İnternet üzerinden verilen servislere erişimi engellemek için kullanılan en yaygın yöntemlerden biri Hizmet Engelleme Saldırılarıdır (Denial of Service). Bu türdeki saldırılarda, saldırgan hizmeti veren sistemin ağ kaynaklarını yada diğer kaynaklarını (hafıza, işlemci, disk vs.) tüketerek gerçek sistem kullanıcılarının İnternet servislerine erişimini engellemektedir [5]. Hizmet Engelleme Saldırılarının günümüzde en yaygın olanı Dağıtık Hizmet Engelleme Saldırılarıdır (Distributed Denial of Service). Dağıtık Hizmet Engelleme Saldırıları özellikle özel şirketlere saatte 10,000$'dan başlayan miktarlarda mali kayıplara neden olabilmektedir [6]. Bu tür saldırılar kurumlara mali kayıpların yanında ayrıca prestij kaybına da yol açmaktadır. Bu saldırıların ne tür sistemlerden kaynaklandığını bilmek, saldırıları önlemek yada engellenebilmesine yardımcı olmaktadır. Örneğin, Cloudflare şirketinin bir müşterisine, 2012 yılının Eylül ayında 65 Gbps büyüklüğe ulaşan ve Dağıtık Hizmet Engelleme Saldırısının bir türü olan DNS Güçlendirme (Domain Name System Amplification) saldırısı olduğu firma tarafından tespit edilmiştir [7]. DNS Güçlendirme saldırıları ile ilgili önemli bir uyarıda Mart 2013'de Amerika Birleşik Devletleri CERT'den (Computer Emergency Readiness Team) gelmiştir [8]. Bu çalışmanın temel amacı İnternet servislerinde ciddi kesintiye yol açabilecek DNS Güçlendirme saldırısı hakkında bilgi sunarak, bu saldırının tetikçi olarak kullandığı özyinelemeye açık ağ alan çözümleme sistemleri ile ilgili çalışma kümesi olarak kullanılan sekiz adet İnternet Servis Sağlayıcı ağından elde edilen bulgular paylaşılacaktır. Makalenin bundan sonraki bölümleri şu şekildedir; 2. Bölümde DNS Güçlendirme saldırısının çalışma yöntemi ele alınacak, 3. Bölümde bu saldırı türünün aracı olarak kullandığı açık alan adı çözücüleri tespit etmek için geliştirilen betik ve çalışma kümesi anlatılacak, 4. Bölümde elde edilen veriler paylaşılarak ve son olarak Sonuç kısmında bu bulgular değerlendirilecektir.

II. DNS GÜÇLENDİRME SALDIRISI

Bu bölümde önce DNS sisteminin çalışması ile ilgili genel bilgi verilecek daha sonra DNS Güçlendirme saldırısının çalışma yöntemi anlatılacaktır.

A. DNS Nedir?

DNS İnternetin çalışmasını sağlayan gizli kahramanlardan biridir. DNS sisteminin temel görevi istemcilerden gelen alan adı yada sistem isimlerini bilgisayarların anlayacağı adreslere çevirmektir [9]. Ayni zamanda gelen adres bilgilerini isimlere de çevirebilir. Bu sistemler istemci sunucu mimarisinde çalışır ve istek ve cevap bilgisini UDP

Devrim Seral, Uluslararası Kıbrıs Üniversitesi, Mühendislik Fakültesi, Bilişim Sistemleri Mühendisliği, Lefkoşa-Kıbrıs'ta öğretim üyesidir. (e-mail: dseral@ciu.edu.tr)

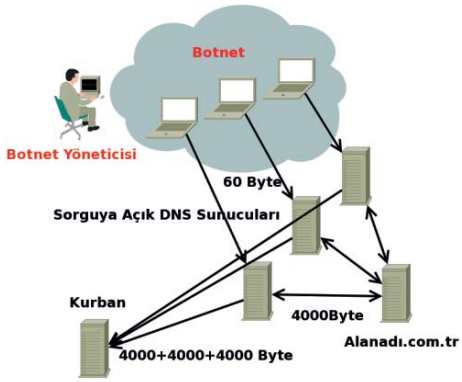
(User Datagram Protocol) protokolü kullanarak taşır.

DNS sistemlerinin 1980'li yıllardan itibaren kullanılmaya başlanmasından sonra sürekli olarak yenilenmiş ve bu alanda ilk uygulama BSD sistemleri üzerinde geliştirilen BIND yazılımı olmuştur [10].

B. *DNS Güçlendirme Saldırısı Nedir?*

İnternet kullanıcı sayısı ve trafiğinin 1990'lı yıllarda artmaya başlaması ile birlikte DNS sistemleri gittikçe önem kazanmıştır. Bundan dolayı DNS sistemlerinin çalışma doğasından gelen açıklar çıkmaya başlamıştır. 2004 yılında Atkins ve Austein RFC 3833 belgesinde DNS sisteminin zayıflıklarının analizini yapmışlardır [11]. Bu belgenin Hizmet Engelleme Saldırıları kısmında DNS Güçlendirme saldırısının yapılabileceğine dair bilgi vermişlerdir. 2006 yılında yapılan diğer bir çalışmada DNS Güçlendirme saldırısının nasıl yapılabileceği ile ilgili ayrıntılı bilgi verilmiştir [12].

DNS Güçlendirme Saldırısı ilke olarak Smurf saldırısının bir benzerini ICMP isteği yerine DNS istek paketleri kullanarak yerine getirmektedir [13]. DNS Güçlendirme Saldırısının nasıl yapıldığını bir senaryo ile anlatmak daha kolay olacaktır. Şekil 1'de DNS Güçlendirme Saldırı senaryosunda gösterildiği gibi, saldırganın Botnet [14] üzerinden binlerce bilgisayarı kontrol ettiğini, Botnet'e dahil olan cihazların kaynak adreslerini kurbanın adresi olarak değiştirerek binlerce DNS sorgusunu, dışarı özyineli sorgulamaya açık DNS sunucularına gönderdiğini varsayalım. Böyle bir saldırıda her bir DNS isteğinin 60 Byte'lık paket boyutunda gönderilebileceğini varsayarsak sorgulama yapılan sunucular eğer EDNS [15] formatında ise cevabın boyutu 4000 Byte'ı aşabilir. Bu sayede 60 Byte'lık bir istek 60 kat güçlenerek kurbanın adresine geri dönebilir. Böylece Botnet üzerindeki saldırıya dahil olan her bir makinenin ürettiği isteğin 60 katı kadar trafik kurbanın üzerine yönlendirilebilmektedir [16].



Şekil 1. DNS Güçlendirme Saldırı senaryosu.

C. *DNS Güçlendirme Saldırısı Nasıl Engellenebilir?*

DNS Güçlendirme Saldırıları aşağıda verilen yöntemlerle engellenebilir [12]:

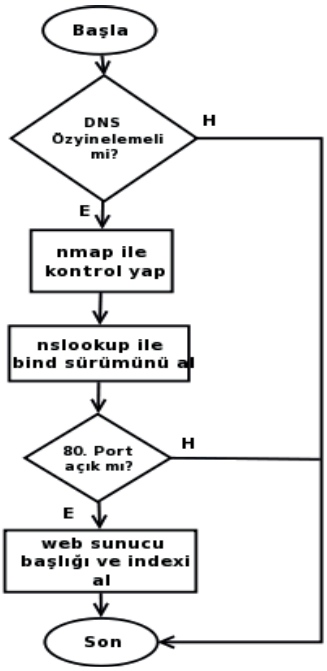
- Özyineleme yapan DNS sunucuların sadece hizmet verilen istemci IP bloklarına cevap verecek şekilde yapılandırılması.
- DNS sunucular eğer özyineleme işlemini tüm istemcilere açık tutmak zorundaysa, bir istemciden gelen istek sayısı belirli oranın üzerinde olması durumda o istemciye cevap vermeyi kesebilir.
- İstemcilere İnternet erişimi veren servis sağlayıcıların IP hilekarlığını (spoofing) önleyici yöntemler uygulaması.

III. ÖZYİNELEMEYE AÇIK DNS SUNUCU TESPİTİ

Bu bölümde özyinelemeye açık DNS sunucuları tespit etmek için geliştirilen betik ve çalışma kümesi ele alınacaktır.

A. *Yöntem*

DNS Güçlendirme Saldırılarına olanak veren en temel neden özyinelemeye açık DNS sunucularıdır. İnternet üzerindeki herhangi Botnet ağından, yanlış yapılandırma yada başka nedenlerle sorgu yapan tüm cihazlara özyinelemeli olarak cevap veren bu türdeki DNS sunucuları doğrudan bu Dağıtık Servis Engelleme Saldırısına yardımcı olmaktadır. Bu yüzden Şekil 2'de akış şeması verilen bir betik yardımı ile bu türde saldırılara olanak veren sunucular bazı özelliklerine göre tespit edilmişlerdir.



Şekil 2. Özyinelemeye açık DNS sunucuları tespit eden betiğin akış şeması..

Özyinelemeye açık DNS sunucuları tespit eden betiğin çalışma adımları aşağıdaki gibidir.

a) Betik, hedef olarak verilen sistemin DNS sorgu portuna (UDP/53) kendi kontrolünde olması mümkün olmayan bir alan adı için (Ör: isc.org) DNS istemcisi ile sorgu gönderir. Eğer hedef sistem DNS sorgularına özyinelemeli olarak cevap veriyorsa bu sistem saldırı için uygun olarak işaretlenir. Cevap vermiyorsa betik diğer sistemleri kontrole devam eder.

b) Özyinelemeli olarak cevap alınan hedef sistemin diğer karakteristiklerini tespit etmek için nmap [17]

port tarama uygulaması ile bazı önemli portları taranarak alınan sonuçlar kaydedilir.

c) DNS sorgulama araçları ile CHAOS sınıfı kullanılarak eğer mümkünse DNS sunucunun sürümü tespit edilir [18].

d) Yine hedef sunucunun HTTP (Hyper Text Transfer Protocol) portu açıksa web sunucunun türü tespit edilir.

B. *Betik Çalışma Kümesi*

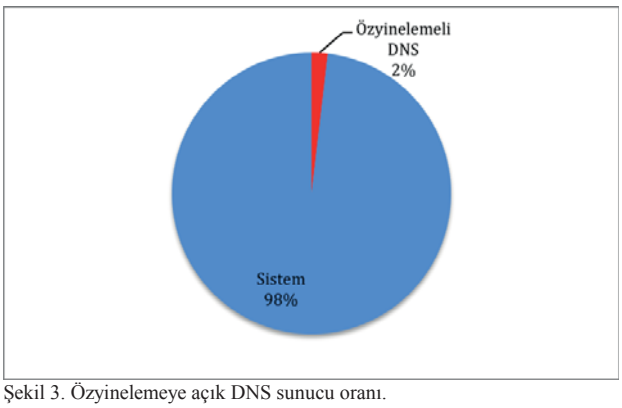
Özyinelemeye açık DNS sunucuları tespit etmek zahmetli ve uzun süren bir işlem olmasından dolayı, betiğin çalışma kümesi olarak Kuzey Kıbrıs Türk Cumhuriyeti sınırları içinde faaliyet gösteren biri kamu olmak üzere sekiz adet İnternet Servis Sağlayıcı (İSS) ağı kullanılmıştır. Çalışmanın yapıldığı bu ağlar mobil İnternet haberleşme dışındaki yaklaşık olarak tüm geniş bant İnternet abonelerini kapsamaktadır. Toplamda test edilen IP adresi sayısı 28416 adet olmuştur. Betik çalışması kontrollü bir şekilde yapılarak test yapılan ağların bu işlemi saldırı yada keşif olarak algılamaması sağlanmaya çalışılmıştır.

IV. ÖZYİNELEMEYE AÇIK DNS SUNUCU BULGULARI

Geliştirilen betik ile toplanan veriler bu bölümde verilecektir.

A. *Özyinelemeye Açık DNS Sunucusu Oranları*

Bölüm III'de ayrıntısı verilen betik ile yapılan analizler sonrası toplamda 28416 IP'den oluşan ve değişik boyutlarda ağlar içeren sekiz ağda bulunan sistemlerden sadece 542'si yada %2'si Özyinelemeye açık DNS sunucu olarak çalışmaktadır. Bu oran Şekil 3'de gösterilmiştir.



Şekil 3. Özyinelemeye açık DNS sunucu oranı.

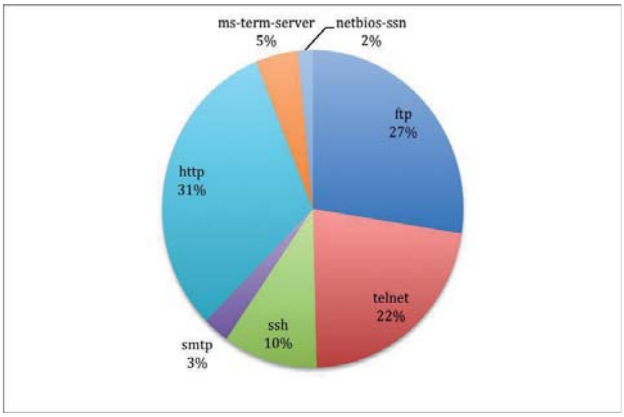
B. *Özyinelemeye Açık Sistemler Üzerindeki Diğer Açık Portlar*

542 adet makine üzerinde DNS dışında çalışan diğer servisleri de tespit edebilmek üzere nmap [17] port tarama uygulaması ile en fazla kullanılan TCP portlarından 21'den 25'e kadar, 80, 139 ve 3389 portları üzerinde tarama yapılmıştır. Ayni zamanda 111 ve 137 UDP portları da taranmasına rağmen UDP protokolünün doğası gereği bu portların durumu hakkında tam anlamıyla doğru bir bilgi alınamamıştır. Tablo I'de nmap ile test edilen ve açık olduğu tespit edilen TCP portların sayıları gösterilmektedir.

TABLO I
AÇIK PORT SAYILARI

Port	ftp	telnet	ssh	smtp	http	Ms-term server	Netbios
Sayı	138	111	51	14	157	23	8

Yine Şekil 4'de açık olan portların diğerlerine göre yüzdelik dağlımı verilmiştir. Bu bilgiler ışığında Özyinelemeye açık DNS sunucu içeren bu sistemlerde UDP 53 dışında ayrıca http ve ftp daha sonra telnet portunun açık olduğu tespit edilmiştir. http,telnet ve ssh portları bu sistemlerin uzaktan yönetilebilir yada yönetilmeye müsait olduklarını göstermektedir. FTP portunun açık olması da bu sistemlerin sadece basit uzaktan yönetilebilir sistemler olmadıklarını bunun yanında kurulum bilgilerinin ya da değiştirilebilir web sayfaları gibi hizmetler de verebildiklerini göstermektedir.



Şekil 4. Sistemler üzerinde açık olan portlar.

C. *HTTP Portu Açık Sistemlerde Çalışan Web Sunucu Türleri*

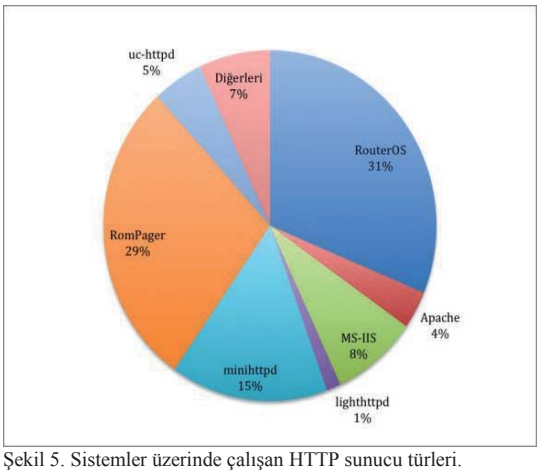
HTTP portu (TCP/80) açık olan sistemler üzerinde HTTP isteğine verilen cevap başlığı üzerinde yapılan analiz sonucu tespit edilen web sunucu türleri Tablo II'de verilmiştir.

TABLO II
WEB SUNUCU TÜRLERİ

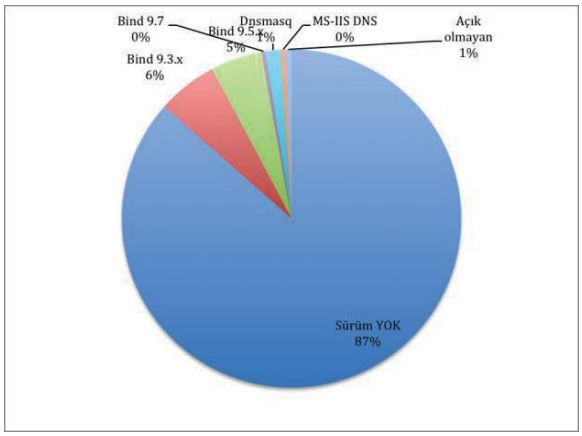
Türü	Rom Pager	Mini httpd	MS-IIS	Uc httpd	Apache	Router OS	Light httpd	Diğer
Sayı	41	22	12	7	5	45	2	10

Şekil 5'de Web sunucu türlerinin yüzdeleri gösterilmektedir.

HTTP geri dönüş başlık bilgisinden sadece 99 sistemin web sunucu türü öğrenilebilmiştir. Ancak istek sonucu cevap olarak gelen sayfa verileri üzerinde yapılan analizle 45 adet sistemin de Mikrotik RouterOS işletim sistemi üzerinde çalıştığı tespit edilmiştir. Burada dikkat çekici olan Web sunucu türleri RomPager, Mini-httpd ve RouterOS şeklinde sıralanmaktadır. Kendini RomPager yada mini-httpd olarak tanıtan sistemler üzerine rastgele web istemci ile bağlantı yapıldığında bu cihazların ADSL modem cihazları yada gömülü sistemler olduğu görülmüştür. RouterOS ise genelde kablosuz sistemlerde kullanılan özel gömülü sistemlerin işletim sistemidir.



Şekil 5. Sistemler üzerinde çalışan HTTP sunucu türleri.



Şekil 6. Sistemler üzerinde çalışan DNS sürümlerinin oranları.

D. DNS sürümü kontrolü

DNS sorgulama araçları ile CHAOS sınıfı kullanarak DNS portu (UDP/53) açık olan cihazların sürüm bilgisi betik ile sorgulanmıştır. Tablo III'de tespit edilebilen sunucu türleri gösterilmektedir. Tespit edilen sunucu türlerine göre bu cihazların %12'si Unix yada türevi cihazlar ve ISC Bind sürümünü çalıştırdığı görülmektedir. İki adet sunucu ise Microsoft firmasının IIS DNS sunucusunu çalıştırmaktadır. Dns-masq sunucular ise DNS sorgularını yönlendirerek yapan genelde güvenlik duvarı sistemleri üzerinde kullanılan sistemlerdir. Geriye kalan %87 DNS sunucuları ise, Bind dışında muhtemelen özel olarak gömülü sistemler için tasarlanmış bir DNS sunucusu çalıştırmaktadır.

TABLO III
DNS SUNUCU TÜRLERİ

Sunucu	Bind 9.3.x	Bind 9.5.x	Bind 9.7	Dns masq	MS-IIS	Sürüm Yok
Sayı	28	24	2	7	2	424

Şekil 6'da Özyinelemeye açık DNS sunucuların tespit edilen DNS sürümlerinin yüzdeleri gösterilmektedir.

V. SONUÇ

Bu çalışmada KKTC'de faaliyet gösteren biri kamu toplamda sekiz adet büyük İnternet Servis Sağlayıcı ağına dahil olan, 28416 IP numarası üzerinde Dağıtık DNS Güçlendirme Saldırısına yardımcı olabilecek Özyinelemeli DNS çağrısına açık DNS sunucuları tespit edilmiştir. Tespit edilen özyinelemeye açık DNS sunucuları her ne kadar da bütün içinde %2'lik bir oranda olsa da, bu cihazların her biri üzerinden belirlenmiş bir kurbana doğru 1 Mbps saldırı yapılabilirse, kurban üzerinde yaklaşık 500 Mbps'lik bir Dağıtık Servis Engelleme Saldırısı gerçekleştirilebilir. Bu büyüklükte gerçekleştirilebilecek bir saldırı coğrafyamızda çoğu şirket ve kurumun baş edemeyeceği bir trafik miktarını ifade etmektedir. Diğer yandan özyinelemeye açık DNS sistemlerinin, ne tür cihazlar oldukları geliştirilen bir betik ile tespit edilmeye çalışılmıştır. Çalışmanın dördüncü bölümünde ayrıntıları da verildiği üzere özyinelemeye açık DNS sunucuların çok büyük bir kısmı ön tanımlı olarak dışarı doğru DNS çağrısına izin veren gömülü sistemlerdir. Bunların dışında kalan DNS sunucuları ise operatörler tarafından yanlış olarak yada gereksinimden dolayı yapılandırılmış sunuculardır. Bu saldırı türünün başarılı olmaması için alınacak birinci önlem, operatörlerin kendi ağ adreslerini taşımayan ancak kendi ağlarından kaynaklanan ağ trafiklerini engellemeleri, ikincisi ise operatörler tarafından son kullanıcılara satılan yada verilen cihazların yapılandırma yapılırken yerel ağ dışında DNS sorgularına cevap vermesinin engellenmesi ile olacaktır.

TEŞEKKÜR

Bu çalışmada sistemlerini ve İnternet bağlantısını kullanmama izin veren sayın Mehmet Alptürk'e teşekkür ederim.

KAYNAKLAR

[1] Sektörel Araştırma ve Strateji Geliştirme Başkanlığı. (2013, Mart). Üç Aylık Pazar Verileri Raporu [Çevrimiçi]. Bağlantı adresi: http://www.tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik13_1.pdf

[2] Bankalararası Kart Merkezi. (2013,Haziran). Haziran 2013 Aylık Bülteni [Çevrimiçi]. Bağlantı adresi: http://www.bkm.com.tr/basin/bultenler/aylik_bulten_052013.pdf

[3] ITU (2013). ICT Fact Figures 2013 [Çevrimiçi]. Bağlantı adresi: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

[4] T. Fredriksson (2013,Nisan). E-commerce and Development Key Trends and Issues [Sunum]. Bağlantı adresi: http://www.wto.org/english/tratop_e/devel_e/wkshop_apr13_e/fredriksson_ecommerce_e.pdf

[5] CMU-CERT (1997,Ekim). Denial Of Service Attacks [Çevrimiçi]. Bağlantı adresi: http://www.cert.org/tech_tips/denial_of_service.html

[6] Neustar (2013,Nisan). 2012 Annual DDOS Attack and Impact Survey: A Year-to-Year Analysis [Çevrimiçi]. Bağlantı adresi: http://www.neustar.biz/enterprise/docs/whitepapers/ddos-protection/2012-ddos-attacks-report.pdf

[7] M. Prince (2012,Eylül). How to lunch a 65Gbps DDoS, and How to Stop One [Çevrimiçi]. Bağlantı adresi: http://blog.cloudflare.com/65gbps-ddos-no-problem

[8] US-CERT (2013,Mart). Alert (TA13-088A) DNS Amplification attacks [Çevrimiçi]. Bağlantı adresi: http://www.us-cert.gov/ncas/alerts/TA13-088A

[9] P. Mockapetris (1983, Kasım). Domain Names – Concepts and Facilities [Çevrimiçi]. Bağlantı adresi: http://tools.ietf.org/html/rfc882

[10] Douglas Brian Terry, Mark Painter, David W. Riggle and Songnian Zhou, The Berkeley Internet Name Domain Server, Proceedings USENIX Summer Conference, Salt Lake City, Utah, Haziran1984, Sayfa 23-31.

[11] D. Atkins, R. Austein (2004, Ağustos). Threat Analysis of the Domain Name System (DNS) [Çevrimiçi]. Bağlantı adresi: http://tools.ietf.org/html/rfc3833

[12] R. Vaughn, G. Evron (2006). "DNS amplification attacks,". [Çevrimiçi]. Bağlantı adresi: http://www.isotf.org/news/DNS-Amplification-Attacks.pdf
[13] CMU-CERT (1998,Ocak). Alert (CA-1998-01) Smurf IP Denial-of-Service Attacks [Çevrimiçi]. Bağlantı adresi: http://www.cert.org/advisories/CA-1998-01.html
[14] B. McCarty, "Botnets: big and bigger", Security & Privacy, IEEE (Volume:1 , Issue: 4), s. 87-90, Haziran-Ağustos 2003.
[15] P. Vixie, (1999,Ağustos). "Extension mechanisms for DNS (EDNS0)," RFC-2671. [Çevrimiçi]. Bağlantı adresi: http://www.ietf.org/rfc/rfc2671.txt
[16] S. Changhua, L. Bin, S. Lei, "Efficient and low-cost hardware defense against DNS amplification attacks," in Proc. IEEE Global Telecommunications Conf. (GLOBECOM'08), Aralık 2008, pp. 1-5.
[17] G. F. Lyon. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning" Insecure, 2009.
[18] S.Woolf, D. Conrad (2007, Haziran). Requirements for Mechanism Identifying a Name Server Instance [Çevrimiçi]. Bağlantı adresi: http://tools.ietf.org/html/rfc4892

Devrim Seral 1977 yılında Kıbrıs'ın Lefkoşa şehrinde doğdu. Lisans eğitimini Ankara'da bulunan Gazi Üniversitesi Teknik Eğitim Fakültesinde 1998 yılında tamamladıktan sonra ayni üniversitenin Fen Bilimleri Enstitüsünden 2000 yılında Master ve 2007 yılında Doktor unvanlarını alarak mezun oldu. Doktora eğitimini sürdürdüğü sırada aynı zamanda özel sektörde bilişim alanında Sistem Mühendisi ve İnternet Mühendisi olarak çalıştı. 2007 Şubat ayında Uluslararası Kıbrıs Üniversitesi Mühendislik Fakültesinde öğretim görevlisi olarak akademisyenlik hayatına geri döndü. Şu anda ayni üniversitenin Bilişim Sistemleri Mühendisliği bölüm başkanlığını sürdürmektedir.

Dr. Seral, İşletim Sistemleri, Yük Dengeleme, Ağ güvenliği gibi konularda çalışmakta ve ayni zamanda Association for Computing Machinery ve IEEE üyesidir.

Güvenli ve Kişisel Aşı Bilgi Sistemi

Okan Bursa, Emine Sezer, Özgü Can, Murat Osman Ünalır

***Özet*— Bilgi güvenliliği ve gizliliğin sağlanması e-sağlık etki alanı içerisindeki uygulamalar için temel bir ihtiyaçtır. Bu amaçla yapılan çalışmaların büyük bir kısmında, genellikle erişim denetim mekanizmaları kullanılmaktadır. Bu çalışmada, politikalar sadece sistemde erişim denetimi sağlamak için değil, aynı zamanda kişiselleştirme için de kullanılmaktadır. Önerilen yaklaşım, e-sağlık uygulamalarının önemli parçalarından biri olan aşı bilgi sistemi temel alınarak açıklanmaktadır. Aşı bilgi sisteminde yer alan her bir paydaş için profil tanımı yapılmaktadır. Aşı etki alanı bilgisi, profiller ve politikalar birlikte kullanılarak sistemin kişiselleştirilmiş kullanımı sağlanmaktadır. Böylelikle, elektronik sağlık kayıtlarına erişim kısıtlandırılarak, hasta gizliliği sağlanmakta ve aşılama işlemi ile ilgili klinik yönergeler etkili bir şekilde gerçekleştirilmektedir.**

***Anahtar Kelimeler*—Erişim Denetimi, Kişiselleştirme, Aşı Bilgi Sistemi, e-Sağlık**

***Abstract*— Ensuring information security and privacy is a fundamental requirement for applications in the e-health domain. In order to achieve this goal, most of the works usually use access control mechanisms. In this work, policies are not only used to control access to the system, but also used for personalization. The proposed approach is explained based on vaccine information system, which is one of the vital part of the e-health applications. A profile definition is made for each stakeholder of the vaccine information system. Vaccine domain information, profiles and policies are both used together in order to provide a personalized usage of the system. Thus, patient privacy is ensured by restricting access to electronic health records and clinical guidance of the vaccination process is achieved in an efficient way.**

***Keywords*—Access Control, Personalization, Vaccine Information System, e-Health**

I. GİRİŞ

E-sağlık sistemleri kişilerin hayat kalitesini arttırmayı amaçlayan uygulamaları içermektedir. Bu sistemde yer alan sağlık alanı çalışanları bir ağ üzerinden hasta sağlık bilgilerine erişebilmekte, izleyebilmekte ve kontrol edebilmektedir.

Okan Bursa, Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 35100, Bornova, İzmir, Türkiye (İlgili yazar, telefon: +90-232-3115335; faks: +90-232-3399405; e-posta: okan.bursa@ ege.edu.tr).

Emine Sezer, Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 35100, Bornova, İzmir, Türkiye (e-posta: emine.sezer@ ege.edu.tr).

Özgü Can, Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 35100, Bornova, İzmir, Türkiye (e-posta: ozgu.can@ ege.edu.tr).

Murat Osman Ünalır, Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 35100, Bornova, İzmir, Türkiye (e-posta: murat.osman.unalir@ ege.edu.tr).

Aşı bilgi sistemi, e-sağlık sisteminin önemli bir parçasını oluşturmaktadır. Sağlıklı bireylerin yetişmesini ve onların ölümcül veya kalıcı sakatlıklara neden olabilecek hastalıklara karşı bağışıklanmasını sağlayan aşı ve aşılama ile ilgili bütün bilgiler aşı bilgi sistemi içerisinde yer almaktadır. Aşı uygulamaları için gerekli hizmetlerin farklı sistemler, kurum, kuruluş ve kişilerce kullanılabilmesi için birlikte çalışabilirliğin desteklenmesi gerekmektedir. Bilgilerin bir kez tanımlandıktan ya da sisteme girildikten sonra sadece bilginin girildiği yerde değil, bilgiye gereksinim duyulan her yerde hem sistemler hem de kişiler tarafından yeniden kullanılabilmesi hizmette başarımı arttırıcı, aynı zamanda maliyeti düşürücü bir sonuç doğuracaktır.

E-sağlık sistemlerinin başarılı ve etkin bir şekilde kullanılabilmesi için güvenlik ve gizlilik ihtiyaçları tanımlanmalı, ve bu ihtiyaçlar doğrultusunda güvenilir bir e-sağlık sistemi geliştirilmelidir. Bu çalışmada, güvenlik ve gizlilik kavramları e-sağlık sistemi içerisinde yer alan aşı etki alanı temel alınarak değerlendirilmektedir.

Aşı bilgi sisteminin etkili ve verimli olabilmesi için sadece aşı ve aşılama ile ilgili bilgileri bulundurması yeterli değildir. Bu nedenle, aşı bilgilerine ek olarak, tüm aşı hizmetlerinin ve bilgilerinin kullanılması ile farklı paydaşlar arasında bilgi paylaşımı ve birlikte çalışabilirlik sağlanmalıdır. Bu nedenle, sistemde yer alan her bir paydaş için profil tanımı yapılarak sistemin kişiselleştirilmiş kullanımı sağlanmalıdır. Yaratılan bu profiller hem aşı bilgi sistemin kişiselleştirilmesine katkıda bulunacak hem de bu profillere özgü yaratılan kurallar sayesinde aşı bilgi sistemine erişim denetim ve aşı işlemi ile ilgili klinik yönergeler etkili bir şekilde gerçekleştirilecektir.

Bu makalenin organizasyonu aşağıdaki şekilde düzenlenmiştir: İkinci bölümde sırası ile e-sağlık ve aşı bilgi sistemleri hakkında bilgi verilmiş, üçüncü bölümde güvenlik ve kişiselleştirme yaklaşımlarından bahsedilmiş, dördüncü bölümde kullanılan teknolojiler ve ilgili çalışmalar özetlenmiş, son bölümde ise sonuç ve gelecek çalışmalar verilmiştir.

II. E-SAĞLIK BİLGİ SİSTEMİ

Bu bölümde, öncelikle, sağlık bilgi sistemi yapısından bahsedilmektedir. Bölümün ikinci kısmında ise sağlık bilgi sisteminin bir parçası olan aşı bilgi sistemi anlatılmaktadır.

A. Sağlık Bilgi Sistemi Yapısı

Günümüzde sağlık hizmeti sunan birimlere bakıldığında, bunların coğrafik olarak dağınık oldukları; devlet hastaneleri, özel hastaneler, kişisel muayenehaneler, laboratuarlar ve sağlık ocakları gibi farklı karmaşıklık düzeylerindeki (farklı hacimlerdeki) sağlık merkezlerinden oluştukları görülmektedir. Bu dağıtık yapının beklenen bütün sosyal gereksinimleri en etkin şekilde karşılayabilmesi için, birbirini tamamlayan bütün bu merkezlerin beraber

çalışması gerekmektedir. Herhangi bir teknolojiyi içeren yeni uygulamaların sağlık alanına uyarlanmasında, her türlü sağlık uygulamasının bireyler üzerinde ölümcül veya kalıcı sakatlık etkileri olabilmesi nedeniyle, uygulamaların doğruluğu ve etkinliği sağlaması gerekliliği göz ardı edilmemesi gereken bir zorunluluktur [1].

Bilgi ve İletişim Teknolojileri (BİT - Information and Communication Technologies) tabanlı çözümler, kurumsal sınırlar içinde hastaların kimlik, adres, sigorta ve sağlık kurumuna giriş tarihi gibi verilerini içermekte, ve bu verileri sadece yönetimsel etkinlikler için kullanmaktadır [2]. Servislerin ve bilgilerin paylaşılmasını ve dağıtılmasını arttırmak için, sağlık alanında yer alan farklı sistemlerin tek bir sistem gibi görülebileceği BİT'e uyarlanması gerekmektedir. Sonuç olarak, kullanılmakta olan tıbbi bilgi sistemlerinin yönetimsel bir uygulama etrafında yapılandırılmış çözümler olduğu görülmektedir.

Standart bir Hastane Bilgi Sistemi (HBS - Hospital Information System), farklı klinik bilgi servisleri, bu servisler ile ilişkili ekonomik/finansal yönetimi ve yönetimsel merkezi verileri içermektedir [2]. Klinik bilgi servisleri, tedavi sürecinin belgelendirilmesi için işlevler sunarak, uzman kadronun en doğru tıbbi deneyimleri izlemesine yardımcı olmakta ve hastanın tıbbi geçmişine ilişkin elektronik bilgiyi getirerek, hastanın klinik tedavisini yönetmektedir. Yönetimsel merkezi veriler ise muhasebenin, insan kaynaklarının, lojistiğin ve denetim düzeneklerinin yönetimine yardımcı olmaktadır. Bu sistemler, sağlık hizmetlerine destek sunmalı ve hem sağlık uzmanları tarafından, hem de yardımcıları tarafından kullanılabilmelidir.

Birbirinden farklı ve oldukça geniş kapsamda uzman bilgi sistemlerinin geliştirilmesi, klinik ortamın merkezi olmayan yapısı nedeniyle, sağlık alanında görülen bir başka eğilimdir. Hastanelerin radyoloji bölümlerinde kullanılan *Görüntü Arşivleme ve İletişim Sistemleri* (Picture Archiving and Communication Systems) [3], hem hastane içinde hem de hastane dışında kullanılan *Laboratuar Bilgi Sistemleri* (Laboratory Information Systems) [4], çoğunluğu aile hekimlerinin ve uzmanların muayenehanelerinde bulunan ve birbirinden farklı bir yapıda tutulan *Elektronik Sağlık Kayıtları* (Electronic Health Records) bu dağıtık ve çok çeşitli yapıya örnek oluşturmaktadır.

Sağlık çalışanları, sürekli olarak bilimsel ve teknolojik bilgiyi yönetmektedirler; fakat yüksek düzeydeki uzmanlıklarına rağmen, uzmanlık alanları ile ilgili gelişmekte olan bilgiyi elde etmek için yeterli zamanları olmayabilmektedir. Bu nedenle, en iyi uygulamalara ve belirtilere ilişkin tüm bilginin erişilebilir duruma gelmesi bir zorunluluktur. Bilgi ve iletişim teknolojileri kullanılarak, sürekli büyüyen e-sağlık uygulamalarının geliştirilmesi, bilginin yönetilmesi kolaylaşmakta ve sağlık hizmetlerinin kalitesini arttırmaktadır [5].

Hastaların sağlık durumlarının izlenmesi gerekliliği, karmaşıklıkları önlemek ve yüksek düzeyde nitelikli bir hayat sağlamak için, doğru bir süreç yönetimini getirmektedir. Özellikle, risk etkenlerinin tanımlanması ve hastanın sağlık geçmişine ilişkin bilgilere erişilebilmesi hastalıktan korunma süreçlerini etkinleştirmeyi sağlayabilmektedir. E-sağlık uygulamaları ile sadece hastalık dönemi değil, hastalık sonrası sağlığı korumak için de bireyin sağlık durumunun izlenebilirliği sağlanabilmektedir.

Yapılmış olan çözümlemeler, tıbbi hataların ve genellikle karşılaşılan yanlış tanı ve tedavi, hasta için ciddi sonuçlar doğurabilmektedir. Bu olayların temel nedenlerinden biri, tedavi sürecini paylaşan kurum içinde veya farklı kurumlarda çalışan farklı sağlık personelleri arasındaki iletişim eksikliğinden kaynaklanmaktadır. E-sağlık uygulamaları ile sağlık açısından risk yaratabilecek etkenlerin yönetiminin gerçekleşmesi beklenmektedir.

Sağlık çalışanlarının günlük görevlerinde yardımcı olacak ve onlara hastanın tıbbi geçmişi ile ilgili tüm bilgileri sunacak etkin bir çözümün gerçekleştirimi günümüzdeki BİT kapsamı dışında olup, yeni nesil BİT çözümleri başlığı altına alınmaktadır. Gelecek BİT çözümlerinin, tüm tıbbi süreçlere destek verecek bir Klinik Bilgi Sistemi olarak hizmet sunması hedeflenmektedir. E-sağlık bilgi sistemi, bir klinik veri deposu olarak hizmet vermeli ve tıbbi bilgiye erişim sağlamalıdır. Bilgi sistemini kullanan yetkili sağlık çalışanları hasta merkezli modeldeki tüm veri, işaret ve görüntülere erişebilmelidir. Ayrıca, yeni nesil e-sağlık çözümlerinin uzman araçların (örneğin LIS, PACS gibi) veritabanlarına ve aile hekimlerinin elektronik sağlık kayıtlarına anında erişimi sağlayacak, güçlü bir bütünleştirme teknolojisine dayanması gerekmektedir.

B. Aşı Bilgi Sistemi

Sağlık alanı çeşitli kurum ve kuruluşlar ile farklı görevlere sahip olan kişilerin hizmet sunduğu, aynı zamanda hizmet aldığı oldukça büyük bir alandır. Sağlıklı bireylerin yetişmesini ve onların ölümcül veya kalıcı sakatlıklara neden olabilecek hastalıklara karşı bağışıklanmasını sağlayan en etkin sağlık yöntemi olan aşı [6], tüm dünyada olduğu gibi ülkemizde de bireylerin doğumu ile başlamaktadır. T.C. Sağlık Bakanlığı tarafından belirlenmiş bir bağışıklama programı olan *Ulusal Aşı Programı*, 0-13 yaş arası çocuklarda yapılması gereken aşıları belirtmektedir [7]. Bu aşılar ücretsiz olarak tüm sağlık ocaklarında ve aile planlama merkezlerinde uygulanmaktadır. Ayrıca, 0-13 yaş grubu için alışıla gelen aşı şemasının yanında, Dünya Sağlık Örgütü (DSÖ) tarafından önerilen bir ek aşı şeması da bulunmaktadır [7]. Bu aşılar, çocukların anne-babaları tarafından özel olarak alınmakta ve özel hastanelerde ya da özel doktorlara yaptırılmaktadır. Aşı ile ilgili uygulamalarda var olan durum, sağlık alanında genellikle görülen problemler ile örtüşmektedir.

Çocuklara yapılan alışıla gelen aşıların ve ek aşıların kayıtları, *Aşı Kartı* olarak adlandırılan ve üzerine sadece aşının yapıldığı tarihin yazıldığı kağıtlar üzerinde tutulmaktadır. Kağıtların kaybolabilme ya da zamanla üzerindeki yazıların silinebilme olasılığına karşı aşı uygulamasına ilişkin bilgilerin kayıt altına alındığı merkezi bir elektronik sistem bulunmamaktadır.

Bağışıklama uygulamalarına hastalığa duyarlı olunan dönemden önce başlanılması gerekmektedir. Bunun için, yapılması gerekli olan aşılar için *Ulusal Aşı Programı*'nda bir aşı takvimi bulunmaktadır. Aşı takvimine göre zamanı gelen aşının hatırlatılması herhangi bir elektronik sistem üzerinden gerçekleşmemekte, sağlık çalışanı veya bireyin kendisi ve/veya anne-babası tarafından izlenebilmesi gerekmektedir. Aşı takvimine göre bazı aşıların okul çağında uygulanması da gerekmektedir. Okullarda aşı uygulamalarından önce çocuğa daha önce uygulanan aşılar ile ilgili bilgiler çocukların anne-babalarından istenmekte, aşı bilgilerinin elektronik bir sistem üzerinde kaydı

tutulmadığı için elektronik bir ortam üzerinden sorgulanması yapılamamaktadır.

Uygulanacak aşının sağlanmasında ise iki farklı durum söz konusudur: aşının uygulanacak sağlık kurumu veya sağlık çalışanı tarafından sağlanması ya da bireyin kendisi veya anne-babası tarafından sağlanmasıdır. Aşıların bozulmadan saklanması, ve uygulanacağı zamanda sağlanmasında, hem ülkemizde hem de dünyada sıkça problemler yaşandığı bilinen bir durumdur [8, 9]. Aşı sağlama zincirini belirleyen, izleyen ya da sağlama süresince aşının saklanma koşulları için ilgili kişileri yönlendiren bir hizmet, yapmış olduğumuz kaynakça araştırmaları doğrultusunda, henüz sunulmamaktadır.

Aşıların sağlıklı bir şekilde sağlanmasından ve uygulanmasından sonra bireyde aşı ile ilgili görülebilecek beklenmeyen yan etkiler olabilmektedir. Dünyada aşı ile ilgili yan etkileri raporlamak için geliştirilen sistemlerden biri *Aşı Yan Etki Raporlama Sistemi* (Vaccine Adverse Event Reporting System - VAERS)'dir [10]. Türkiye'de VAERS ile aynı görevi yerine getiren herhangi bir sistem bulunmamaktadır. Buna karşılık olarak ülkemizde izlenen yöntem, Temel Sağlık Hizmetleri Genel Müdürlüğü tarafından yayınlanan *Aşı Sonrası İstenmeyen Etkiler* (ASİE) durumunda yapılması gerekenlerin belirtildiği genelgede belirtilen adımlardır [11]. Ülkemizde, aşı uygulamasından sonra görülebilecek yan etkileri elektronik olarak izleyen herhangi bir sistem bulunmamaktadır. Aşıların pekiştirme dozlarının var olduğu durumda, aşı uygulamasından önce, kişide daha önce görülen, belki de kişiye bu aşının yeniden uygulanmamasını gerektiren durumlar söz konusu olabileceği bir gerçektir. Ölümcül veya kalıcı sakatlıklara neden olabilecek yan etkilerin veya aşının içindeki bazı maddelere karşı alerjik tepkilerin görülebilme olasılığına rağmen, bu tür durumlar için sağlık çalışanını uyarmak yine kişilerin kendilerine veya anne-babalarına düşmektedir.

Bu sorunlara ek olarak, aşıya ait lot ile ilgili problemler yaşanabilmektedir. Eğer böyle bir durum söz konusu ise aşının bulunduğu lota ait tüm aşıların toplanması ve incelenmesi de gerekebilmektedir. Aşının sağlanma süreci elektronik sistemler tarafından izlenirse, aynı lotta bulunan tüm aşılara ulaşmak kolaylaşacaktır.

Aşılar üzerinde araştırma ve geliştirme yapılan önemli sağlık uygulamalarından biridir [12]. Var olan aşılar ile ilgili geliştirme sürecinde uygulanan aşıların bireyler üzerindeki etkilerine ilişkin bilgilere, bunun yanı sıra henüz aşısı geliştirilmemiş hastalıklar için aşı araştırma çalışmalarında hasta bilgilerine elektronik bir ortam üzerinden erişilebilinmesi aşı araştırma geliştirme çalışmalarına hızlı ve etkin bir yardım sağlayacaktır.

Klinik yönergeler, sağlık alanındaki farklı bölümlerde tanı, yönetim ve tedaviye ilişkin ölçütlere ve kararlara önderlik etmek amacıyla hazırlanan belgelerdir. Günümüzde klinik yönergeler kısaca önleyici, tanı, hastalığın sonucuna ilişkin tahmin (prognoz), ilaç kullanımını içerebilecek tedavi, riskler ve kazançlar ile maliyet etkinliğine ilişkin en iyi bulguları ve en çok rastlanan verileri tanımlamakta, özetlemekte ve değerlendirmektedir. Ayrıca klinik deneyimler ile ilgili en önemli soruları tanımlamakta ve tüm karar seçeneklerini ve bunların getirilerini belirtmektedir. Klinik yönergeler ile sağlık hizmetlerinde standart sağlanması, kalitenin arttırılması, risklerin azaltılması ve maliyetin düşürülmesi sağlanmaktadır [13, 14]. Aşı uygulamaları için de klinik yönergeler bulunmaktadır, bu klinik yönergeler makineler tarafından yorumlanabilir bir içerikte değildir ve kişilerce yorumlanmayı gerekmektedir. Bu durum, karar desteğinde hataya açık olunmasına neden olmaktadır.

Ortaya konan problemler özetlenecek olursa, farklı paydaşlar birlikte çalışabilirliğin nasıl destekleneceği ve bu paydaşlara servislerin uygulamalardan bağımsız nasıl sunulacağı ön plana çıkmaktadır.

III. GÜVENLİK VE KİŞİSELLEŞTİRME

E-sağlık bilgi sisteminde yer alan elektronik sağlık kayıtlarının güvenliğinin ve erişim denetimlerinin sağlanması hasta gizliliğinin korunabilmesi için önemli bir konudur. Bu bölümde, güvenlik kavramı aşı bilgi sistemi için değerlendirilmekte ve kişiselleştirme yaklaşımı anlatılmaktadır.

A. Aşı Bilgi Sisteminde Güvenlik

Aşı bilgi sisteminde güvenlik kavramı, sisteme erişimin denetlenebilmesi ve uygulama güvenliğinin sağlanabilmesi için önemli bir faktördür. Sistemde yer alan kişilerin mahremiyetinin korunabilmesi için hasta kayıtlarının güvenliği sağlanabilmelidir. Bu amaçla, kişisel verilerin gizliliği sağlanmalı ve sadece yetkili kişiler tarafından erişilebilmelidir. Etkin bir aşı bilgi sisteminde, paydaşların ağ üzerinden hasta kayıtlarına erişimi mümkün olacağından, kişisel veriye erişimin yetkilendirilmesi gerekmektedir. Aksi takdirde, çeşitli güvenlik ve gizlilik ihlalleri ile karşılaşılabilmektedir. Bu tehditler aşağıdaki şekilde listelenebilir:

- *Veri gizliliğine yönelik tehditler:* Hastaların kişisel ve sağlık kayıtlarına yönelik istenmeyen erişimler gerçekleşmektedir.
- *Veri bütünlüğüne yönelik tehditler:* Sistemde yer alan kişisel bilgilerin yetkilendirilmemiş kişiler tarafından değiştirilmesidir.
- *Kişisel mahremiyete yönelik tehditler:* Kişisel bilgilerin izlenmesi ve ayrımlandırılmasıdır (profiling). Böyle bir durumda, hasta kişisel ve sağlık bilgilerinin kimler tarafından, ne zaman ve hangi amaçla kullanıldığını ve saklandığını bilmemektedir.

Kişisel kayıtları yukarıda bahsedilen tehditlerden korumak amacı ile sistemde gereksinim duyulan güvenlik ve gizlilik ihtiyaçlarının sağlanması gerekmektedir. Bu nedenle, öncelikle, sisteme, sistemde bulunan kayıtlara ve uygulamalara yönelik erişim denetlenmelidir.

Erişim denetim için politikalar kullanılmaktadır. Politika, sistemin davranış şeklini belirten bir durumdur. Bir servisi, kimin ve hangi koşullar altında kullanabileceğini, bilginin servise nasıl sağlanacağını ve sağlanan bilginin nasıl kullanılacağını belirtir [15]. Bir karar verme süreci olan politika, hem bir karar destek sistemi hem de bildirimsel deyim davranış sistemi olarak davranmaktadır [16].

Politika, politika nesnelerinden oluşan politika kurallarından oluşmaktadır. Politika kuralları dört şekilde ifade edilebilmektedir [17]: izin (permission), yasak (prohibition), zorunluluk (obligation) ve özel izin (dispensation). *İzin*, veriye ya da servise erişenin neleri yapabileceğini; *yasak*, neleri yapamayacağını; *zorunluluk*,

neleri yapması gerektiğini; *özel izin* ise neleri yapmasına gerek kalmadığını belirten durumdur. Aşı bilgi sistemi için bu politika kuralları aşağıdaki dört durum ile örneklendirilmiştir.

- *Durum-1 (İzin)*: Doktor hastasının aşı dosyasına yazma işlemi gerçekleştirebilir.
- *Durum-2 (Yasak)*: Hemşire hastanın aşı dosyasında okuma işlemi gerçekleştiremez.
- *Durum-3 (Zorunluluk)*: Yeni doğan bir bebek annesi Hepatit B hastası ise 12 saat içinde aşı olmalıdır.
- *Durum-4 (Özel İzin)*: Hemşire hastanın sorumlu doktoru ile çalışıyorsa hastanın dosyasını okuyabilir.

Belirtilen bu politika kuralları kullanılarak, aşı bilgi sisteminde hem sisteme erişim hem de hasta aşı kayıtlarına erişim denetim işlemleri gerçekleştirilebilmektedir.

B. Kişiselleştirme

Kişiselleştirme, mevcut bir küme içerisinden uygun seçimlerin yapılmasıdır. Kişiselleştirme işleminde, kullanıcının davranışlarına, ihtiyaçlarına, tercihlerine, ilgi alanlarına ve demografik bilgilerine göre karar verilmektedir [18]. Örneğin, kullanıcılar özelleştirilmiş web sayfalarında kişiselleştirilmiş içeriklere ulaşabilir, profillerine uygun reklamlara erişebilirler.

Sistemde tanımlanmış ve saklanmış olan kullanıcı profil bilgisine göre gerçekleştirilen kişiselleştirme işleminde, kişilerin bilgilerinin tanımlandığı, saklandığı ve kişiler arası bağların belirtildiği arkadaşımın arkadaşı projesi (Friend-Of-A-Friend, FOAF) [19] dokümanları kullanılmaktadır. FOAF dokümanları kullanıcı ya da kişilerin, kişisel bilgilerinin saklandığı, RDF dilinde geliştirilmiş dokümanlardır [20].

Aşı bilgi sisteminde yer alan kullanıcılar için `Doktor`, `Hemşire`, `Hasta`, `Bebek`, `Hamile` gibi örnek profiller tanımlanmaktadır. Profiller kişilerin değişmeyen özelliklerini tanımlayabilecekleri gibi kişilerin günlük hayattaki tercihlerini de saklayabilirler. Ancak, bir kişinin günlük hayatta karşılaşabileceği durumlar ve bu durumlardaki davranışları kişinin o an bulunduğu duruma göre değişebilir. Örneğin, bir kişi aynı duruma karşı hastanede farklı, evde farklı bir şekilde tepki verebilmekte, tercihleri bu durumlara göre oluşabilmektedir. Böyle bir durumda, kişilerin günlük hayatta karşılaşacakları rolleri de içerecek şekilde profillerin genişletilmesi sağlanmalıdır. Böylelikle, aynı kişi hem `Hemşire`, hem `Hamile` hem de `Anne` rollerini farklı durumlarda alabilmekte, bu rollere vereceği tercihleri de değiştirebilmektedir. Sonuç olarak, saklanan profiller özelleştirilmiş ve kişiselleştirilmiş gösterimler sunmaktadır.

Kural tabanlı bir kişiselleştirmede, profillere özgü tanımlanan politika kurallarına göre erişim denetim işlemi gerçekleştirebilir. Aşı bilgi sisteminde yer alan klinik yönergelerin etkin bir şekilde uygulanabilmesi için profil ve politika yaklaşımı birlikte kullanılmaktadır. Profiller kullanılarak daha etkin politikalar tanımlanabilmekte ve kişiselleştirilmiş sağlık hizmeti sağlanabilecektir.

Aşağıda belirtilen durum çalışmasında bir klinik yönergesi örneklendirilmiştir:

Durum Çalışması (Yasak): Hamile profilinde olan bir kişiye canlı aşı yapılamaz.

Bu klinik yönergesinde belirtilen ifade hem aşı bilgi sistemini, hem profil yapısını hem de politika kuralını kullanmaktadır. Canlı aşı olarak ifade edilen durum, `kızamık`, `su çiçeği` gibi aşı bilgi sistemi içerisinde tanımlı olan kavramları kullanmaktadır. Yönergenin uygulanacağı kişi bilgisi, sistemde tanımlanmış profil kavramlarından `Hamile` kavramını, politika kuralı olarak da `Yasak` kavramını içermektedir.

Klinik yönergelerinin bir diğer önemli örneği aşı uygulamalarından sonra karşılaşılabilecek alerji durumlarıdır. Örneğin, kızamık aşısı tavuk yumurta embriyosunda çoğaltılmaktadır. Profil bilgisinde yumurtaya karşı anafilaksi tipinde alerjisi olduğunu belirten bir kişiye kızamık aşısı olamaz şeklinde bir yasak tanımlanmalıdır. Bu durumda, yumurta alerjisi olan kişi için, sistemde kızamık aşısı uygulaması seçildiği anda, *alerji* profili için yaratılmış olan *yasak* politikası aşı bilgi sisteminde belirtilmiş olan *kızamık* aşısının içeriği bilgisini kullandığından, sistem aşıyı yapacak sorumlu kişiye bir uyarı döndürecektir. Aynı zamanda, kızamık, kabakulak ve kızamıkçık aşıları canlı zayıflatılmış aşılar oldukları için doğumsal bağışıklı yetmezliği, AIDS, lösemi, lenfoma, kanser ilaçları, radyasyon ve yüksek doz steroidlerle kanser tedavisi alanlar gibi ciddi bağışıklık sistemi yetersizliği olan kişilere bu aşıların uygulanmaması gerekmektedir [21]. Bu durumların herhangi birini içeren profiller için yine sistemde tanımlanan ilgili politikalar işletilerek, aşı uygulayıcılarına gerekli uyarılar döndürülecektir.

IV. Kullanılan Teknolojiler Ve İlgili Çalışmalar

Bu çalışma, Anlamsal Web teknolojilerini temel almaktadır. Anlamsal Web'de verinin tanımlanmış anlamı ve diğer veriler ile ilişkileri verilerek bir bilgi ağı oluşturulmakta ve bu bilgi ağı kullanılarak, insanların ve bilgisayarların işbirliği içerisinde çalışmasının sağlanması hedeflenmektedir [22]. Anlamsal Web uygulamalarında, bilginin temsilinde ontolojiler kullanılmaktadır. Ontoloji, kavramsallaştırmanın açık ve biçimsel bir belirtimidir [23]. Aşı, profil ve politika ontolojilerinin yaratılması için Protégé [24] ontoloji editörü kullanılmaktadır.

Sağlık alanında Anlamsal Web teknolojilerinin uygulanması, SNOMED-CT [25], MeSH [26] ve GALEN [27] gibi tıbbi bilişim standartlarının veya GO [28] ve OBR-Prox-Femur Uygulama Ontolojisi [29] gibi belirli bir anatomik yapının tanımlanmasını amaçlayan ontoloji geliştirme çalışmaları üzerinde yoğunlaşmıştır. Aşı alanına bakıldığında, He ve arkadaşları tarafından geliştirilen ve hala üzerinde çalışmaların devam ettiği Aşı Ontolojisi (Vaccine Ontology, VO) [30] görülmektedir. VO, hem insanlar hem de hayvanlar üzerinde kullanılan bütün aşıları, aşı ile ilgili öbek, son kullanım tarihi, etken madde gibi öznitelikleri tanımlamak amacıyla geliştirilmekte olan bir ontolojidir. Bu ontolojide aşıya ilişkin her şey bir kavram olarak tanımlanmakta ve bu kavramlara ait örnekler oluşturulmamaktadır. Bu da ontolojinin bir yazılım sisteminde kullanımını zorlaştırmaktadır.

KAoS [31], Rei [32], Ponder [33], Rein [34], XACML [35], Proteus [36], WSPL [37], Protune [38] ve Appel [39] Anlamsal Web politika dillerinden bazılarıdır. [40] çalışmasında yapılan karşılaştırmalar doğrultusunda, bu çalışmada temel alınan politika dili Rei'dir. Rei, OWL-Lite

temelli bir politika tanımlama dilidir ve kullanıcıların yetkiler, yasaklar, zorunluluklar ve özel izinler kavramlarını tanımlamasına izin vermektedir.

V. SONUÇ

Bu çalışmada, e-sağlık sistemine ve bu sistemin en önemli parçalarından biri olan aşı bilgi sistemine ilişkin bilgi ve hizmetleri sunulmuştur. Aşı ve aşılamaya ilişkin tüm bilgilerin kullanılabileceği ve bu alanda hem kişilere hem de kurumlara verilen tüm hizmetlerin aşı bilgi sisteminde kullanılması hedeflenmiştir. Bununla birlikte, e-sağlık sisteminin etkin ve başarılı olabilmesi için, sistem erişim denetiminin ve hasta kayıtlarının gizliliğinin sağlanabilmesi gerektiği ifade edilmiştir. Bu amaçla, aşı bilgi sistemi temel alınarak, erişim denetim politikalarının kullanımı açıklanmıştır. Ayrıca, kişiselleştirme yaklaşımı kullanılarak aşı bilgi sisteminde yer alan klinik yönergelerinin etkin bir şekilde uygulanması hedeflenmiştir.

Geliştirilmekte olan kişiselleştirilmiş aşı bilgi sisteminin temel özellikleri aşağıda maddeler halinde sunulmaktadır:

- Aşılama bilgisinin paylaşımını ve yeniden kullanımını sağlayan bir ontoloji geliştirmek,
- Aşı bilgi sistemi için bir bilgi tabanı oluşturmak,
- Sağlık alanı için kullanıcı profilleri geliştirmek,
- Aşı bilgi sistemine erişim denetimi,
- Aşı öncesi kişileri olası yan etki ve alerjik reaksiyonlar hakkında uyarmak ve böylece kişiselleştirmeyi sağlamak,
- Politikaları kullanarak aşı alanı için klinik yönergeleri tanımlamak.

KAYNAKÇA

[1] E. Della Valle, D. Cerizza, I. Celino, A. Dogac, G. Laleci, Y. Kabak, A. Okcan, O. Gulderen, T. Namli, and V. Bicer, "The need for semantic web service in the eHealth", *W3C workshop on Frameworks for Semantics in Web Services*, 2005.

[2] Intel Information Technology, "Converging technologies in healthcare IT", *Computer Manufacturing Healthcare*, URL: http://www.intel.com/it/pdf/converging-technologies-in-healthcare-it.pdf, Son Erişim: 30 Aralık 2008.

[3] S. Bryan, G. C. Weatherburn, J. R. Watkins, M. J. Buxton, "The benefits of hospital-wide picture archiving and communication systems: a survey of clinical users of radiology services", *Br J Radiol*, 72 (857): 469–78, 1999.

[4] G.A Gibbon, "A brief history of LIMS", *Laboratory Automation and Information Management*,32 (1): 1–5, 1996

[5] G. Eysenbach, "What is e-health?", *Journal of Medical Internet Research (JMIR)*, 3(2):e20, 2001.

[6] World Health Organization, "Vaccine-preventable diseases, vaccines and vaccination", *International Travel and Health*, URL: http://www.who.int/ith/chapters/ith2012en_chap6.pdf, Son Erişim: Temmuz 2013.

[7] T.C. Sağlık Bakanlığı Temel Sağlık Hizmetleri Genel Müdürlüğü, "Genişletilmiş Bağışıklama Programı (GBP) Genelgesi", *Genelge 2009/17*, 2009.

[8] D. Callender, "Vaccine Shortages: Implications for Pediatric Nurse Implications", *J Pediatr Health Care*, Nov-Dec;20(6):426-429, 2006.

[9] TTB Halk Sağlığı Kolu, "Türkiye'de Sağlık Ocaklarında Aşı ile İlgili Sorunların Değerlendirilmesi", *Toplum ve Hekim*, 19 (4): 310-318, 2004.

[10] VAERS-Vaccine Adverse Event Reporting System, URL: http://vaers.hhs.gov/index, Son Erişim: Temmuz 2013.

[11] Temel Sağlık Hizmetleri Genel Müdürlüğü, "Aşı Sonrası İstenmeyen Etkiler Genelgesi", *Genelge 2009/18*, 2009.

[12] National Institute of Allergy and Infectous Diesases, "Understanding Vaccines, What They Are, How They Work", *NIH Publication*, No:08-4219, 2008.

[13] K. M. Hrabak, J. R. Campbell, S.W. Tu, R. McClure, R.T. Weida, "Creating interoperable guidelines requirements of vocabulary standarts in immunization decision support", *Proceedings of the 12th World Congress on Health (Medical) Informatics (MEDINFO 2007)*, 129(Pt 2):930-934, 2007.

[14] R. Shankar, S. Martins, M. O'Connor, D. Parrish, A. K. Das, "Towards Semantic Interoperability in a Clinical Trials Management System", *5th International Semantic Web Conference (ISWC 2006)*, Volume 4273, pp 901-912, 2006.

[15] L. Kagal, T. Finin, M. Paolucci, N. Srinivasen, K. Sycara, G.Denker, "Authorization and Privacy for Semantic Web Services", *IEEE Intelligent Systems*, 19(4), pp. 50-56, July/Aug 2004.

[16] B. Thuraisingham, "Building Trustworthy Semantic Webs", *Auerbach Publications*, 2007

[17] Ö. Can, M. O. Ünalır, "Ontoloji Tabanlı Bilgi Sistemlerinde Politika Yönetimi", *Bilişim Teknolojileri Dergisi*, Cilt:3, Sayı:2, Mayıs 2010.

[18] O. Can, O. Bursa, M. O. Unalir, "A Profile-Policy Integration for A Personalized Lifestyle", *The Seventh International Conference on Advances in Semantic Processing (SEMAPRO 2013)*, 2013.

[19] The Friend of a Friend (FOAF) Project, URL: http://www.foaf-project.org/, Son Erişim: Temmuz 2013.

[20] O. Bursa, M. O. Ünalır, "Anlamsal Web Portal Teknolojileri ve Uygulamaları", *Yazılım Kalitesi ve Yazılım Geliştirme Araçları Sempozyumu 2008 (YKGS 2008)*, İstanbul, 9-10 Ekim, 2008.

[21] T. Pehlivan, S. Altınel, A. G. Doğu, "Aşılar", *Sanofi Pasteur*, İstanbul, 2011.

[22] M. O. Ünalır, Ö. Can, E. Ünalır, "Ontoloji Tabanlı Bilgi Sistemlerinde
Erişim Denetimi: Ulusal Aşı Bilgi Sistemi İçin Durum Çalışması", *TÜBAV Bilim Dergisi*, Cilt:3, Sayı:3, 238-249, 2010.

[23] T. R. Gruber, "Toward principles for the Design of Ontologies Used for Knowledge Sharing", *International Journal of Human-Computer Studies*, 43(5-6), 907-928, 1993.

[24] Protégé ontoloji editörü, URL: http://protege.stanford.edu/, Son Erişim: Temmuz 2013.

[25] NHS, "SNOMED-CT The Language of Electronic Health Records", http://www.connectingforhealth.nhs.uk/systemsandservices/data/uktc/training/snobrochure.pdf, Son Erişim: Temmuz 2013.

[26] D. Newman, S. Karimi, L. Cavedon, "Using Topic Models to Interpret MEDLINE's Medical Subject Headings", *Proceedings of the 22nd Australasian Joint Conference on Advances in Artificial Intelligence*, 270-279, 2009

[27] B. Trombert-Paviot, J. M. Rodrigues, J. E. Rogers, R. Baud, E. Van Der Haring, A. M. Rassinoux, V. Abrial, L. Clavel, and H. Idir, "GALEN: A third generation terminology tool to support a multipurpose national coding system for surgical procedures", *International Journal of Medical Informatics*, 58-59:71-85, 2000.

[28] M. A. Harris, J. Clark, A. Ireland, J. Lomax, M. Ashburner, R. Foulger, et al., "The gene ontology (GO) database and informatics resource", *Nucleic Acids Research*, 32:D258-D261, 2004.

[29] V. Lukovic, D. Milosevic, G. Devedzic, C. Sukic, M. Kudumovic, B. Ristic, "OBR-Prox-femur Application Ontology Development and Modeling", *HealthMED Journal 2010*, 4(2), pp.404-416, 2010.

[30] Y. He, L. Cowell, L., A. D. Diehl, H. L. Mobley, B. Peters, A. Ruttenberg, R. H. Scheuermann, R. R. Brinkman M. Courtot, C. Mungall, "VO: Vaccine Ontology", *In: The 1st International Conference on Biomedical Ontology(ICBO 2009)*, Nature Precedings, Buffalo, NY, USA, 2009.

[31] A. Uszok, J. M. Bradshaw, and R. Jeffers, "KAoS: A Policy and Domain Services Framework for Grid Computing and Semantic Web Services", *In Trust Management (iTrust 2004)*, Volume 2995 of Lecture Notes in Computer Science, pp. 16-26, 2004

[32] L. Kagal, T. Finin, and A. Joshi, "A Policy Language for A Pervasive Computing Environment", *In IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, pp. 63-74, 2003.

[33] N. Dulay, E. Lupu, M. Sloman, and N. Damianou, "A Policy Deployment Model for The Ponder Language", *In Proceedings of IEEE/IFIP International Symposium on Integrated Network Management (IM 2001)*, pp. 14-18, 2001.

[34] L. Kagal, and T. Finin, "Rein : Where Policies Meet Rules in the Semantic Web", Technical report, MIT, 2005.

[35] XACML, URL: http://www.oasis-open.org/committees/xacml/, Son Erişim: Temmuz 2013.

[36] A. Toninelli, R. Montanari, L. Kagal, O. Lassila, "Proteus: A Semantic Context-Aware Adaptive Policy Model", *POLICY '07: Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks*, Bologna, Italy, 129 –140, 2007.

[37] A. H. Anderson, "An Introduction to the Web Services Policy Language (WSPL)", *5th IEEE International Workshop on Policies for Distributed Systems and Networks*, Yorktown Heights, New York, 2004.
[38] Protune, URL: http://rewerse.net/I2/software.html, Son Erişim: Temmuz 2013.
[39] L. Cranor, M. Longheinrich, M. Marchiori, "A P3P Preference Exchange Language-Appel", URL: http://www.w3.org/TR/P3P-preferences, Son Erişim: Temmuz 2013.
[40] Ö. Can, M. O. Ünalır, "Anlamsal Web Politika Dillerinin Karşılaştırması", *Akademik Bilişim 2010*, Muğla, 2010.

Attack Types and Intrusion Detection Systems in Cloud Computing

U. Oktay and O.K. Sahingoz

***Abstract*— In recent years, lots of organizations have adopted their systems for enabling cloud based computing to provide scalable, virtualized on-demand access to a shared pool of computing resources such as networks, servers, storage, applications and services. Mainly cloud computing technology enables users/enterprises to eliminate the requirements for setting up of expensive computing infrastructure and reduces systems' operating costs. As a result, this technology is used by an increasing number of end users. On the other hand, existing security deficiencies and vulnerabilities of underlying technologies can leave an open door for intrusions. Therefore, cloud computing providers need to protect their users' sensitive data from insider or outsider attacks by installing an intrusion detection and prevention system. In this paper, it is aimed to define different attack types, which affect the availability, confidentiality and integrity of resources and services in cloud computing environment. Additionally, the paper also introduces related intrusion detection models to identify and prevent these types of attacks.**

***Index Terms*— cloud computing, intrusion detection, intrusion prevention, security.**

I. Introduction

IN recent years, cloud computing has rapidly emerged as a widely accepted paradigm in computing systems, in which an end-user can request some computing capabilities and services when he need it, and he can reach these resources across networks anytime, anywhere.

Pew Research Institute published a research about "the future of cloud computing", and depicted that about % 71 of technology stakeholders and critics believe that by the year 2020, most people will work in Internet-based applications, which can also be run from smartphones [22]. Therefore, it can be seen that the future of cloud computing technology is bright and will be widely used in the World.

While moving from traditional local computing paradigm to the cloud computing paradigm, new security and privacy challenges emerge because of the distributed nature of cloud computing. Some of these security vulnerabilities leave open doors, which stem from the existing computing models; and some of them, inherent from cloud-based models.

As a result, malicious users force these doors to attack the system, and they attack on end-users' private data; processing power, bandwidth or storage capacity of the cloud network. Cloud computing organizations have to provide a high quality service and protect the users' sensitive data. To prevent these attackers, firewall mechanism and/or Intrusion Detection System (IDS) are effective solutions to resist them. They can provide additional protection mechanisms on the cloud systems' distributed environments. IDS can identify suspicious activities by monitoring network traffic changes, configuration of the system, logs files, and actions of end-users. When such a suspicious event is detected, IDS sends an alert message to a person or monitoring console to trigger some actions for preventing these attacks.

In this paper, it is aimed to provide definitions and properties of different attack types in cloud computing and to introduce intrusion detection and prevention models to resist these types of attacks.

The rest of the paper is organized as follows: In the next section the cloud computing paradigm is introduced; In Section 3, security deficiencies and attack types of cloud computing are described; intrusion detection models and intrusion prevention models in cloud computing are detailed in Section 4 and Section 5 respectively, and finally conclusion and future works are depicted.

II. Cloud Computing

Ubiquitous computing is first defined conceptually as "accessibility of data with technological opportunities has to be realized with a continuous and an invisible way" by Mark Weiser who is a Xerox Palo Alto Research Center (PARC) Incorporated researcher with an inspiration from Philip K. Dick's Ubik novel [2, 3]. In Ubik, all objective entities are communicating each other as a smart entity. This communication occurs dependently with all factors in the environment. Communication networks allow data access perpetually independent from the environment. A real-time and location independent interactive communication environment was started to be used by inclusion of ubiquitous computing in daily life [4].

Cloud computing is an interactive communication model that is constituted in more than one place synchronously, easy to use, can be accessed whenever user needs, consist of configurable computing resources and needs minimal effort to achieve maintainability [5]. Nowadays cloud computing users are using services that they need from providers' computing resources and charged as they profited [6]. Cloud computing has many definitions in different resources, which are similar to each other. As a summary, cloud computing can be defined as today's computing technology that has time and location independent services, shaped with user's

Manuscript received July 15, 2013.

U. Oktay is with Turkish Air Force Academy (TuAFA), Yesilyurt, Istanbul, Turkey (e-mail: uoktay@hho.edu.tr).

O. K. Sahingoz is with Computer Engineering Department of Turkish Air Force Academy (TuAFA), Yesilyurt, Istanbul, Turkey (e-mail: sahingoz@hho.edu.tr).

needs, has a minimum effort to maintain and charged as the service usage.

A. *Specifications of Cloud Computing*

While there are many definitions of cloud computing, Mell and Grance highlight five essential characteristics [5]:

On-demand Service: A user can be provided by oneself with computing abilities such as server time and network storage whenever it is needed without any provider and human interaction.

Wide Network Accessibility: Cloud computing has to be held abilities, which are standardized on the network and can be accessed by different kinds of devices (mobile phones, tablets, laptops, workstations etc.).

Resource Pool: The provider's computing resources such as a storage area, processing power, network bandwidth and memory must be in a physical or virtualized pool, can be allocated dynamically or according to demand of the end-users and can be served multitenant at the same time. Users do not need to have any authority on the resources and do not know where the resources are.

Rapid Elasticity: Opportunities and abilities have to be provided, unserved and scaled interior or exterior in an elastic way. These services are introduced to end-users generally unlimited and provided as much as the requests.

Regular Service: Among to services, which are provided in cloud computing systems; resource usage can be monitored, controlled, reported; resource usage amounts can be determined and providers can serve these to users transparently.

B. *Structure of Cloud Computing Architecture*

Cloud computing architecture contains some types of actors, which can be either an individual or an organizational unit who attend cloud services/tasks. NIST defines five main actors [7]:

Consumer uses the cloud computing service and can be either an individual or an organizational unit. A consumer chooses the most appropriate service or services, which are provided by the cloud provider. Besides, the services are charged against to the agreement that is signed between the consumer and the provider.

Provider is an entity that is responsible for developing resources and services, which are used by individuals, organizations or consumers. Provider manages software, platform or infrastructure that is needed by consumers, and it builds obligatory technical infrastructure and provides specified service levels (mostly trust and security levels).

Auditor inspects whole information technology processes, performance and security issues independently within predefined criteria. Auditor must be a third party and can be either an individual or an organizational unit.

Broker: Manageability of cloud systems is very complicated because of its nature. Consumers can use cloud services not only get in contact with the provider directly but also broker. Broker organizes the connection between provider and consumer, and also manages performance and availability of the system.

Carrier realizes connection, communication and transfers between provider and consumer, and also it enables

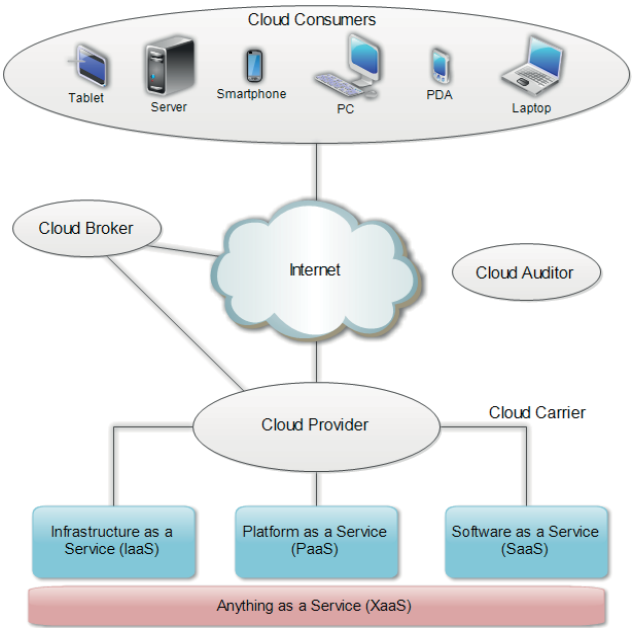


Fig. 1. Service models and actors in cloud computing.

consumers can access to the services over communication infrastructure and other devices such as desktops, laptops or any mobile devices. Distribution of the cloud services can be realized via network and communication infrastructure or communication agents, which have high storage capacity opportunities.

C. *Service Models in Cloud Computing*

About the services, which are served over cloud computing systems there is a definition as *Anything as a Service* (XaaS). The word Anything defines the service, and it can take part as the type of the service like; *Communication as a Service* (CaaS), *Network as a Service* (NaaS) or *Monitoring as a Service* (MaaS). However, there are three fundamental service types to describe and define the service contents. They are *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) and *Software as a Service* (SaaS) [5]. These three main service models/actors of the cloud computing are shown in Figure 1 and detailed as follows.

Infrastructure as a Service (IaaS): With this ability, users can access processing power, storage area, network and other computing resources through opportunity and ability of the provider, also use every kind of software including operating system (OS) and applications. Users are not responsible for controlling and managing the cloud infrastructure, they only have authority on OS, storage, distributed software and network components which are going to be used.

Platform as a Service (PaaS): Users can develop and run software over cloud computing infrastructure via programming languages, libraries, services and with the tools that are supported by provider. Users are not responsible for controlling and managing network, server, OS and storage areas which are founded in cloud computing infrastructure, they can only interfere limited configuration changes.

Software as a Service (SaaS): All the infrastructure,

platform and software utilities are supported and provided by the provider. Users can access to service based applications via different devices and interfaces as thin clients and network browsers. There are only some limited configuration authorities over the service based applications that can be made by users.

III. Security in Cloud Computing

While moving from traditional computing paradigm to cloud computing paradigm new security and privacy challenges has emerged. Security of the cloud computing system can be thought in two dimensions: physical security and cyber security.

Physical security concerns the physical properties of the system. For example, a data center, which is owned by provider infrastructure, has to realize security standards and hold security certifications globally, supervision and manageability on security preventions, incombustibility, uninterrupted power supplies, precautions for natural disasters (earthquake, flood, fire etc.) are indispensable [8]. However twenty four hours and seven days monitoring for heat, humidity and air condition systems and also some biometric entrance systems may help for the business continuity.

On the other hand, *cyber security* defines the prevention of system from cyber world. There is a risk of cyber security attacks on services of cloud computing system. These attack can use huge amounts of computing resources, disables their usage by consumer efficiently. In this section mostly known attack types are detailed.

Insider Attack: Employee, entrepreneur and associates which are still or former attended who can or could access the whole information system with privileged authority are defined as *insider* [9]. Insider attacks are organized and run by these individuals to harm or temper knowledge about consumers or providers and include every kind of attacks which can be executed from inside [10, 11].

Flooding Attack: In this type of attack, attackers can send very large amounts of packets from exploited information resources, and they are called as zombie [11]. Packets can be either one of TCP, UDP, ICMP or a combination of these protocols. These kinds of attacks are mostly realized over unauthorized network connections. Because of cloud computing paradigms' nature, connections to the virtual machines are established over Internet. For this reason, exposition of cloud users with *Denial of Service (DoS)* and *Distributed Denial of Service (DDoS)* attacks are inevitable. Flooding attacks affect the availability of serviced for authorized users. An attack that is realized to a server which serves one kind of service can prevent a vast of scale accessibility to this served service. These kinds of attacks are called DoS attacks. If servers' resources are slogged after flooding attacks and it prevents the execution of other services, which run on the server, this kind of attacks are called indirect DoS attacks.

User to Root Attacks: In this type of attack, an intruder seizes the account and password information of an authorized user, and he can acquire limitless access to the whole system [11]. Buffer overflows are used for establish console connection for authorized processes. This type of intrusion can be realized with writing an excessive amount of data to a statically defined buffers' capacity, and the information is captured by intruders from this overflowed data. An attacker who owned the account and password information of an authorized user can hold the access privilege to servers and also to virtual machines.

Port Scanning: An attack that identifies open, closed and filtered ports on a system [11]. In port scanning, intruders can seize information with the help of open ports like services that run on a system, IP and MAC addresses which belong to a connection, and router, gateway and firewall rules. TCP, UDP, SYN/FIN/ACK and Window scanning are the most common scanning attacks. Port scanning is not used by its own, an intruder realize the actual attack after getting information about open ports and running services.

Attacks on Virtualization: After compromising hypervisor, control of the virtual machines in the virtual environment will be captured [11]. Zero day attacks are one of the methods that attack virtual machines and use hypervisor or other virtual machines to attack other virtual machines. Zero day attacks use known vulnerabilities before system or software developers apply patches or updates.

Multiple virtual machines use the same resource pool, especially hardware and with this kind of access side channel data has a chance to be captured, which flow one virtual machine to other [12].

Backdoor Channel Attacks: A passive attack type in which intruders compromise a node in the cloud and use this compromised node as a zombie resource to execute a DDoS attack. Trojans and similar structures on the system are help to compromise the system. After compromising system become a zombie and also data can be reachable on the system [11].

Storage allocation and multitenancy: There are some issues to be defined about the data that are processed on cloud [13]. Owner and control of the data, maintaining audit records, how and how much of the audit records will be shared with the consumer. To ensure consumers' data privacy, provider has to realize isolation of data and guarantee in service level agreement.

Authorization, Authentication, Encryption, Key and Identity Management: Different from conventional information technologies, in cloud computing deployment of virtual machines, IP addresses and resources are dynamic [13]. Authorization, authentication and identity management have to be configured with affectless from this dynamism in the way of synchronization. While achieving this configuration, data privacy is also indispensable. And the way of achieving data privacy a well-defined, well-configured and well-maintained key management.

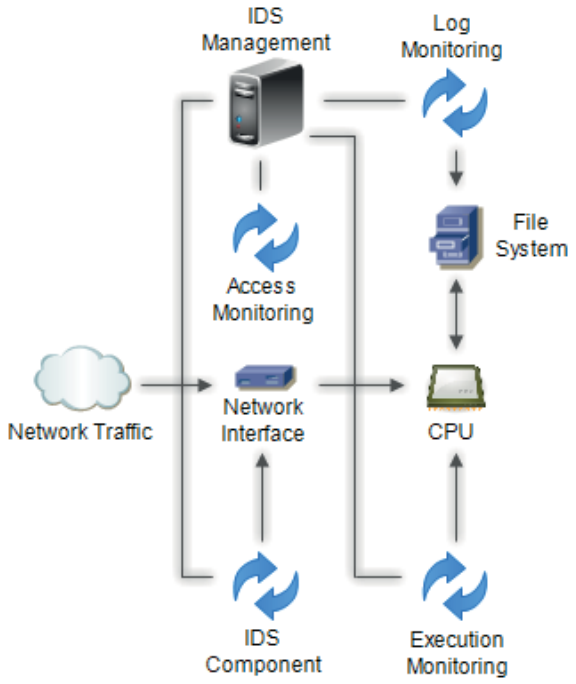


Fig. 2. Host-based Intrusion Detection System architecture.

Data Modification, Forgery and Integrity: Untrusted providers and system administrators can manipulate users' and consumers' data among to their own benefits [14]. Cloud users will be fall into a particularly bad position after such a manipulation or forgery occurs. With a combination of techniques like encryption and hash, this kind of integrity attacks can be prevented. AdjointVM and some improvement on AdjointVM are some solutions to prohibit tampering users' cloud data in the way of virtualization [15, 16].

IV. INTRUSION DETECTION IN CLOUD COMPUTING

As detailed in previous section, there are different types of attacks. *Intrusion Detection Systems (IDSs)* are one of the practical solutions to resist these attacks. IDSs are systems that realize intrusion detection, log detected information, alert or perform predefined procedures [17, 18]. They can be either hardware or software that includes whole observed computing entities. It does not mean every detected suspicious event is an intrusion. Some unexpected events can occur rarely, and it is a crucial point to decide if they are an intrusion or not. Mainly there are three types of IDS in cloud computing systems: *Host based IDS, Network based IDS, and Distributed IDS.*

A. Host-based Intrusion Detection Systems

Host Based IDSs analyze the suspicious activities like system call, processes or thread, asset and configuration access by observing the situation of host. It is especially used to protect valuable and private information on server systems. HIDSs are able to assign as NIDS if they are installed on a single host and configured to detect network activities. HIDS is composed of sensors located on servers or workstations which are made to prevent the attacks to a host. An HIDS is not just monitor network traffic, it can also trace more and settle with local settings of an OS and log records. The basic structure of a HIDS is shown in Figure 2 [18].

B. Network-based Intrusion Detection Systems

Network-based IDSs (NIDS) observe, monitor and analyses the specified and pre-identified network traffic. It can detect different situations based on specified points and generally located between the end point devices like routers, firewalls. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing traffic on the network for signs of malicious activities and events. Network traffic stacks on different layers and every layer delivers the data coming from a layer to another layer. OSI reference model and TCP/IP model define how these layers works and manages the traffic. An example for NIDS architecture and sensor placement is shown in Figure 3 [18].

C. Distributed Intrusion Detection Systems

Distributed Intrusion Detection System (DIDS) is the way of intrusion detection in a distributed environment such as grid and cloud computing [19]. All the components in the distributed area communicate each other with an agent-based approach. There are three fundamental components and assignments are similar to other types of IDSs' components. Main subject in DIDSs deal whole system like a traditional

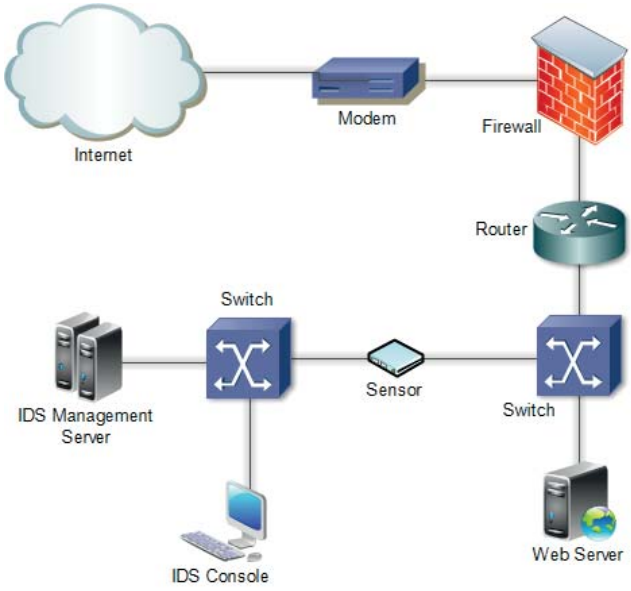


Fig. 3. Network-based Intrusion Detection System architecture.

network or host [20]. DIDS components do not have a worldwide accepted standard, but there are network and host based sensor components, detection engine and management component. A systematic model of a DIDS is shown in Figure 4.

D. Network Behavior Analysis Intrusion Detection

Network Behavior Analysis Intrusion Detection (NBAD) is an intrusion detection methodology which is providing to decide if the network traffic is suspicious or not by the statistical data and formal situation of network traffic. Sensors detect DoS attacks with the help of to be aware of

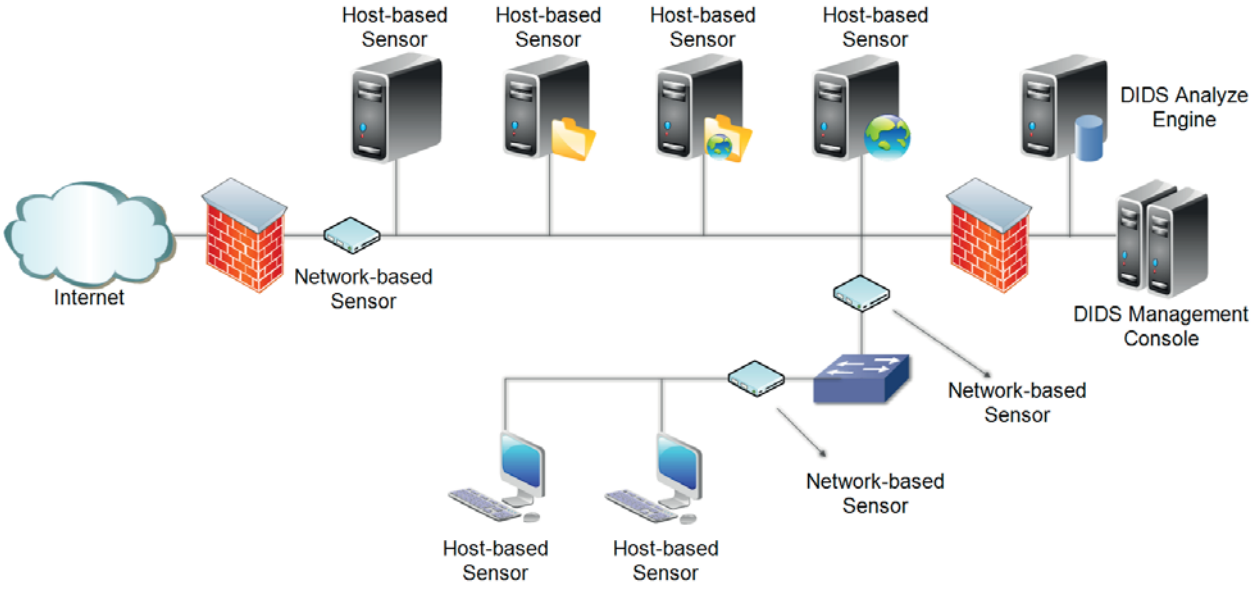


Fig. 4. A systematic view of Distributed Intrusion Detection System.

the network traffic and unexpected application services and rule violations by scanning the network. Traditional NIDSs and NBAD systems share some common components like sensors and management consoles, but NBAD systems generally do not have database servers, unlike the traditional NIDSs. NBAD systems work to decide in the case of unexpected data traffic. It is generally efficient to detect DoS attacks and worms.

V. INTRUSION PREVENTION SYSTEMS

An Intrusion Prevention System (IPS) holds all capabilities of IDSs and plus prevention characteristics [17]. IPSs can interfere most of the component in prevented environment. In a nutshell, security of a system has some traditional steps. There will be a firewall, IDS, IPS and guard system behind modem, router or switches where ever it is needed. IPSs can change configurations of manageable computing entities. If an intrusion detected by the mechanism, a firewall rule can be applied, a routing configuration can be changed, or a virtual machine can be isolated among security procedures.

In cloud computing, intrusion detection and prevention transactions and processes are a challenging issue because of many reasons. Fundamentally, because of the distributed nature of the cloud computing systems, all monitored and prevented resources are taken place in many different locations. Sometimes, they will be in different countries. So that, intrusion detection sensors placement, collecting intrusion data, analyzing by detection engines and interfering for prevention precautions are not easy to implement and apply. At the same time, load balancing, allocation of CPU and memory, deciding for positive and negative rates, bandwidth usage and so the whole price because of pay per usage model is the areas to be overcome.

Proxy Network Intrusion Detection System for Cloud Computing is introduced to minimize expenditures of hardware usage [21, 22]. The study based on locating a NIDS in a virtualization based cloud environment by putting on intrusion detection assignment on a different entity in the network. So the expenditures of hardware usage (CPU and memory) aimed to be reduced. Studies and models must study and concentrate for the most effective and proactive detection and prevention approaches.

VI. CONCLUSION

Cloud computing is a rapidly emerged technology and it is a widely accepted computing paradigm all around the world by its advantages on quick deployment, cost efficiency (on setting up and improvement), large storage space, and easy access to system anytime and anywhere. Apart from these advantages it has some disadvantages on security and privacy concerns, which are seen as the primary obstacles to wide adoption. At the same time, because of the distributed nature of the system, there is a risk of security attacks on services and resources in cloud computing. These attacks can be both outside and inside the cloud provider's network. In this paper, we have introduced the security issues of cloud computing and in terms of attack types and their defense mechanism by means of intrusion detection and prevention systems.

REFERENCES

[1] J.Q.Anderson, L. Rainie, "The Future of Cloud Computing", http://pewinternet.org/~/media//Files/Reports/2010/ PIP_Future_of_the_ Internet_cloud_computing.pdf
[2] M. Weiser, "The Computer for the 21st Century," Scientific American Special Issue on Communications, pp. 94-104, 1991.
[3] P. K. Dick, "Ubik," Doubleday, 1969.
[4] D. Amor, "Internet Future Strategies: How Pervasive Computing Services Will Change the World," New Jersey: Prentice Hall Computer Books, 2000.
[5] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, NIST Special Publication 800-145 (SP800-145)," National Institute of Standards and Technology, Gaithersburg, September 2011.
[6] U. Tupakula, V. Varadharajan and N. Akku, "Intrusion Detection Techniques for Infrastructure as a Service Cloud," *Proc. IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, Sydney, 2011, pp. 744–751.

[7] M. Hogan, F. Liu, A. Sokol and J. Tong, "NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291 (SP500-291)," Gaithersburg, July 2011.
[8] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," *Proc.* MIPRO, 2010 Proceedings of the 33rd International Convention, Opatija, 2010, pp. 344-349.
[9] D. M. Cappelli and R. F. Trzeciak, "Best practices for mitigating insider threat: Lessons learned from 250 cases," [Online]. July 2013, Available: http://www.cert.org/archive/pdf/RSA-CERT-InsiderThreat.pdf.
[10] A. J. Duncan, S. Creese, and M. Goldsmith, "Insider Attacks in Cloud Computing," *Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, 2012, pp. 857–862.
[11] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, January 2013.
[12] J. C. Roberts II and W. Al-Hamdani, "Who Can You Trust in the Cloud? A Review of Security Issues Within Cloud Computing," *Proc. Information Security Curriculum Development Conference,* Kennesaw, 2011, pp. 15-19.
[13] M. K. Srinivasan and P. Rodrigues, "State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud," *Proc. 2nd International Conference on Advances in Computing, Communications and Informatics,"* Mysore, 2012, pp. 470-476.
[14] S. Meena, E. Daniel and N. A. Vasanthi, "Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions," *Proc. International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, Nagercoil, 2013, pp. 1076-1081.
[15] J. Kong, "AdjointVM: a new intrusion detection model for cloud computing," Energy Procedia, vol. 13, pp. 7902-7911, 2011.
[16] U. Oktay, M. A. Aydin and O. K. Sahingoz, "Circular Chain VM Protection in AdjointVM", *Proc. The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE2013)*, Konya, 2013, pp. 94-98.
[17] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94 (SP800-94)," Gaithersburg, February 2007.
[18] G. Tyler, "Information Assurance Tools Report Intrusion Detection Systems," Information Assurance Technology Analysis Center (IATAC), September 2009.
[19] R. Robbins, "Distributed Intrusion Detection Systems: An Introduction and Review," SANS Institute Information Security Reading Room, GSEC Practical Assignment, version 1.4b, Option 1, January 2002.
[20] X. Qing, "The Structure Design of A New Distributed Intrusion Detection System," *Proc. 2nd International Conference on Computer Engineering and Technology (ICCET)*, Chengdu, 2010, pp. 100-103.
[21] U. Oktay, and O. K. Sahingoz, "Proxy Network Intrusion Detection System for Cloud Computing", *Proc. The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE2013)*, Konya, 2013, pp. 99-105.
[22] U. Oktay, "Proxy Network Intrusion Detection System for Cloud Computing," MSc. Thesis, Department of Computer Engineering, Turkish Air Force Academy (TuAFA), Istanbul, 2013.



U. Oktay was born in Istanbul in 1984. He graduated from the Computer Engineering Department of Turkish Air Force Academy (TuAFA) in 2006. He received his M.Sc. degree from Computer Engineering Department of TuAFA Aeronautics and Space Technologies Institute (ASTIN), Istanbul, Turkey in 2013. His research interests include cloud computing, intrusion detection and cyber warfare and security.



O. K. Sahingoz is currently an assistant professor in the Department of Computer Engineering at Turkish Air Force Academy. He graduated from the Computer Engineering Department of Bogazici University in 1993. He received his M.Sc. and Ph.D. degree from Computer Engineering Department of Istanbul Technical University, in 1998 and 2006, respectively. His research interests lie in the areas of Wireless Sensor Networks, Artificial Intelligence, Parallel and Distributed Computing, Soft Computing, Information Systems, Intelligent Agents, Multi Agent Systems.

A Hypergame Model for Information Security

Yadigar Imamverdiyev

***Abstract*—Game theory is one of the most powerful mathematical tools to model information security decision making. However, in game theory it is assumed that all the players have complete knowledge about each player's strategies, preferences, and decision rules used. This assumption is very strong, in reality there is often significant information asymmetry between players. In many real world situations, decision makers do not always have all the information about each player's true intentions, strategies or preferences. Consequently, they have to perceive the situation from their own points of view, and may err in their perceptions. Since the early developments of game theory attempts have been made to incorporate misperceptions in game models of either incomplete or imperfect information. However, most of these attempts are based on quantities (as probabilities, risk factors, etc.) which are too subjective in general. In this paper, we consider a special family of games of incomplete information called hypergames. Hypergame theory extends classical game theory with the ability to deal with differences in players' misperceptions. In the context of hypergames, few works have addressed the study of information security decision making. This paper presents a hypergame approach as an analysis tool in the context of information security. The proposed two level hypergame models defender's and attacker's perception of the information security situation as a series of games. Finally, we conclude and present some future work..**

***Index Terms*— information security; game theory; hypergame;**

I. Introduction

In the modern highly networked world the cost of decisions on information security is very high as it concerns interests of many stakeholders. Therefore, such a decision must be well founded and based on a well-studied theoretical models and best practices. Game theory is a mathematical method of studying the best strategies in games and can provide valuable insights into strategic information security decisions [1].

Game theory is a convenient tool to analyze the interactions of economic agents and it was firstly applied to economy, now it is applied to military strategies, international relations, political science, and evolutionary biology and etc.

In information security area, the interactive process of the attackers and defenders is a game process. Thus, game theory can be used to predict the behavior of attacks and to support decision making.

Manuscript received July 15, 2013.

Yadigar Imamverdiyev is with the Institute of Information Technology of Azerbaijan National Academy of Sciences, AZ1141, B.Bahabzade 9, Baku, Azerbaijan (Phone: 994 12-510-42-53; fax: 994 12-539-61-21; e-mail: yadigar@lan.ab.az).

Information security, when viewed from a game theoretic perspective, can be seen as a game comprising multiple players; the attackers (malicious users) and the defenders (network/system administrators). The benefits of quantifying information security using game-theoretic approach are enormous. Most importantly it may help network administrator to find the optimal defense strategies of a system and to calculate the expected loss associated with different defense strategies [2].

Hypergame theory extends classical game theory with the ability to deal with differences in players' misperceptions [3]. In the context of hypergames, few works have addressed the study of information security decision making. This paper presents a hypergame approach as an analysis tool in the context of information security. The proposed two level hypergame models defender's and attacker's perception of the information security situation as a series of games.

The rest of this paper is organized as follows. In the next section, we shall present an overview of application of game theory in information security. Section 3 presents limitations of game theory. In section 4, we give a brief introduction to hypergames. Finally, Section 5 presents a hypergame model between attacker and defender.

II. Related Work: Game Theory In Information Security

Game theory is a branch of applied mathematics, exploring models of decision making under different interests of the parties (players), where each party seeks to influence the development of the situation in their own interests. Each side has its own purpose and uses some strategy that can lead to gain or losing - depending on the behavior of other players. Game theory helps to choose the best strategy in the light of the views of other participants, their resources and their possible actions.

During the game players can choose and implement a strategy from a set of different behavioral options (strategy space), in order to maximize the payoff they are receiving as an outcome of the game. In game-theoretic analysis the principle of the Nash equilibrium plays a critical role. Game in normal form is characterized by multiple participants or players, each of whom is given a set of possible strategies of behavior and the payoff function. Under the principle of Nash equilibrium rational players have strategies that form equilibrium (Nash), i.e. there is a set of strategies in which the individual player cannot increase his/her gains by changing its strategy when strategies of the other players are fixed.

There are lots of papers on the application of the game theory to information security issues. Game theory has been used to model several areas of information security like network security, intrusion detection, information warfare

and security investment.

Roy et al. provide an excellent review of different approaches to game theory as it can be applied to network security [4]. Also a good overview of applications of game theory in information security can be found in [5, 6, 7].

Qu et.al. [8] presents a game theoretic model as a defense mechanism against a classic bandwidth consuming DoS/DDoS attack. The interaction between the attacker and the defender is modeled as a two-player non-zero-sum game in two attack scenarios: (i) one single attacking node for Denial of Service (DoS) and (ii) multiple attacking nodes for Distributed DoS (DDoS). The defender's challenge is to determine optimal firewall settings to block rogue traffics while allowing legitimate ones.

Modeling of intrusion detection systems (IDS) using game theory attracts more attention. In [9], Alpcan and Başar introduce a a two-person, nonzero-sum, non-cooperative game model with dynamic information where the attacker has two choices, i.e., launching an attack or doing nothing, while the defender's choices are to trigger or not its (costly) detection scheme. Nash equilibrium solutions in closed form are obtained for specific subgames.

Patcha and Park [10] have extended the model proposed by Alpcan and Başar to include mobile ad hock networks, and have analyzed the interaction between an attacker and a host-based IDS as a dynamic two player non-cooperative game.

The same kind of attacker-defender game is studied in [11]. The number of strategies for each player is larger than two: several attack and countermeasure types are considered.

[12] presents some very similar but concrete situations of network security (information warfare) games, with specific numerical values, that also lead to simple strategy sets.

The stochastic game approach is used in [13] to model attacks directed against specific applications, against communication capacities, or against databases. [14, 15] apply stochastic game models as well, to study other specific attack scenarios, and numerically compute mixed Nash strategies. The Bayesian approach is also considered in security games, for example in [12]. The authors consider two types of attackers, namely "normal users" whose behavior is only driven by selfishness, and "malicious nodes" that intend to maximize the damage done. The defender has a priori belief about the probability of its opponent being of each type, and updates that probability as he observes the attacker`s moves. That belief is also used to determine the probability of using the detection mechanisms.

Another important domain where it is believed that game theory could be applied is the case of worm propagation [16]. In [16], the strategy of players is to choose the best quarantining strategy for the detector, while the worm chooses a scanning rate.

Besides the direct game-theoretic modelling of interactions between malicious attacks and protection strategies, game theory can be applied to economic issues of information security [17].

Kunreuther and Heal [18] recently introduced an interesting game-theoretic model for problems of interdependent security, in which a large number of players must make individual investment decisions related to security but the ultimate safety of each participant may depend in a complex way on the actions of the entire population.

III. Limitations of Present Research

Many of the current game-theoretic security approaches are based on static games with perfect information or games with complete information [4]. However, in reality a defender often faces a dynamic game with incomplete and imperfect information against the attacker. Some of the current models involving dynamic game with incomplete and imperfect information are specific to mobile ad hoc networks [10] while others do not consider a realistic attack scenario [4].

In particular, Roy et al. [4] point out that some of the limitations of the present research are: (a) Current stochastic game models only consider perfect information and assume that the defender is always able to detect attacks; (b) Current stochastic game models assume that the state transition probabilities are fixed before the game starts and these probabilities can be computed from the domain knowledge and past statistics; (c) Current game models assume that the players' actions are synchronous, which is not always realistic.

In usual game models it is assumed that each player knows payoff functions and set of strategies of other players. In fact, this condition is often not fulfilled. If a player does not know, payoff functions of other players, then talk about the Nash equilibrium becomes meaningless.

All the complete-knowledge games rely on accurate knowledge of the payoff functions. In real-life any player must observe and make as realistic assumptions about these payoffs (costs) as possible. If the observations about an opponent's costs are unrealistic, a player can end up choosing a non-optimal strategy.

Since the early developments of game theory attempts have been made to incorporate misperceptions in game models of either incomplete or imperfect information. However, most of these attempts are based on quantities (as probabilities, risk factors, etc.) which are too subjective in general. In this paper, we consider a special family of games of incomplete information called hypergames. In the hypergames misperception or misunderstanding by players are explicitly assumed.

Sasaki and Kijima [19] discuss the relationships between two models of games with incomplete information, hypergames [3] and Bayesian games [20]. The authors show that any hypergame can naturally be reformulated in terms of Bayesian games in an unified way and prove that some equilibrium concepts defined for hypergames are in a sense equivalent to those for Bayesian games.

IV. A brief introduction to hypergames

Before introducing the proposed method, we need to explain the hypergame framework.

Definition 1. Simple hypergame

A simple hypergame of players p and q is a pair of (G_p, G_q).

We have $G_p = (S_p, S_{qp}, \geq_p, \geq_{qp})$ and $G_q = (S_{pq}, S_q, \geq_{pq}, \geq_q)$.

In G_p, S_p denotes a set of strategies of p while S_{qp} denotes a set of strategies which the player p recognizes that q possesses. That is, p perceives that S_{qp} is the set of strategies of q. $\geq_p$ denotes a preference ordering on $S_p \times S_{qp}$ of p while $\geq_{qp}$ is a preference ordering on $S_p \times S_{qp}$ that p assumes that q holds. That is, p perceives that q's preference ordering is $\geq_{qp}$. We define $_{Gq}$ in a similar way.

The definition implies that each player independently perceives the problematic situation without mutual understanding. The rationality of a simple hypergame is defined as follows:

Definition 2. Nash equilibrium of simple hypergame
For a simple hypergame (G_p, G_q) of players p and q, $(s^{p*}, s^{qp*}) \in S_p \times S_{qp}$ is a Nash equilibrium of $G_p = (S_p, S_{qp}, \geq_p, \geq_{qp})$ if and only if we have $(\forall s^p \in S_p)(s^{p*}, s^{qp*}) \geq_p (s^p, s^{qp*})$ and $(\forall s^{qp} \in S_{qp})(s^{p*}, s^{qp*}) \geq_{qp} (s^{p*}, s^{qp})$.

This definition shows that if (s^{p*}, s^{qp*}) is a Nash equilibrium of G_p, then p believes that there is no incentive for either of the players to change their strategy as long as the other does not change its strategy.

In the simple hypergame we assume no communication between the players and they make decisions completely independent based on their own subjective (G_p or G_q).

Hypergames are analysed by using Fraser and Hipel's [21] game analysis algorithm. First a new game is constructed to represent the relative aspect of the hypergame that is to be analysed. This is achieved by taking a preference vector for each player from a game that represents their perception of the situation and combining these together to construct the new game.

Many hypergame analyses have been published, showing its use in modelling conflicts and their resolutions. Hypergame analysis methods but can be applied to military conflicts, international disputes [22], economic treaties and agreements [23], social issues [24] and etc. Hypergame approach also was applied to information warfare [25] and cybersecurity [26].

V. A HYPERGAME MODEL

Let us consider two levels of hypergame formally.

Game G can be briefly defined as set of preference vectors of all players. Let V_A be the preference vector of the Attacker, and V_D – the preference vector of the Defender. Then, a game in which the Attacker and the Defender are the only players can be defined as $G = \{V_A, V_D\}$. In games with complete information players evaluate preference vectors of each other fully and adequately, therefore, they all play in the same game.

If in the two-person game, both players are playing the same game G, i.e. correctly estimate preference vectors of each other, then we have zero level hypergame. If at least one of the players mistakenly interprets the preference vector of another player, then there is the first level hypergame. If a player is aware of misperception of the second player, there is the second level hypergame.

Let H^1 denotes the first level hypergame. In this game the players are playing different games. Let V_{ij} be the preference vector of player i from the point of view of player j. Then for two players – the Attacker and the Defender – we have the following types of reflexive preference vectors:

V_{AA} – preference vector of the Attacker from the point of view of the Attacker;

V_{DA} – preference vector of the Defender from the point of view of the Attacker;

V_{AD}– preference vector of the Attacker from the point of view of the Defender;

V_{DD} – preference vector of the Defender from the point of view of the Defender.

The game, played by the Attacker in the first level hypergame H, is denoted as $G_A = \{V_{AA}, V_{DA}\}$, and the game is played by the Defender in the same hypergame – as $G_D = \{V_{AD}, V_{DD}\}$. Accordingly, first level hypergame itself is defined as $H = \{G_A, G_D\}$.

In matrix notation the first level hypergame is shown in Table 1.

TABLE 1
THE FIRST LEVEL HYPERGAME H^1 IN A MATRIX FORM

Players	Game	
	Attacker	Defender
Attacker	V_{AA}	V_{AD}
Defender	V_{DA}	V_{DD}
	G_A	G_D

According to the conditions of the first level hypergame H, the Defender wrongly interprets preference vector of the Attacker, that is, $V_{AA} \neq V_{AD}$ is true, but the Attacker correctly estimates the preference vector of the Defender, $V_{DA} = V_{DD}$.

Even more realistic model of the analyzed situation is represented by the second level hypergame, which, as noted, occurs when one of the players knows about the misinterpretation of his position by another player.

Let H_A^1 denotes the first level hypergame of the Attacker and H_S^1 denotes the first level hypergame of the Defender. Here $H_A^1 = \{G_{AA}, G_{DA}\}$, and $H_D^1 = \{G_{AD}, G_{DD}\}$ where:

G_{AA} = game $G_A = \{V_{AA}, V_{DA}\}$ from the point of view of the Attacker,

G_{DA} = game $G_D = \{V_{AD}, V_{DD}\}$ from the point of view of the Attacker,

G_{AS} = game $G_A = \{V_{AA}, V_{DA}\}$ from the point of view of the Defender,

G_{SS} = game $G_S = \{V_{AD}, V_{DD}\}$ from the point of view of the Defender.

Table 2 shows the second level hypergame H^2 in a matrix form.

TABLE 2
THE SECOND LEVEL HYPERGAME H^2 IN A MATRIX FORM

Players	Game	
	Attacker	Defender
Attacker	G_{AA}	G_{AD}
Defender	G_{DA}	G_{DD}
	H_A^1	H_D^1

Analysing a hypergame involves analysing each of the games for stability and then comparing the results to find stable equilibriums for the hypergame. Algorithm for calculation of stable outcomes and equilibrium points in the second level hypergame H^2 is the following.

1. Sequentially analyze the games G_{AA}, G_{AD}, G_{DA}, and G_{DD}, by comparing corresponding preference vectors for each of them.

2. Analyze the first level hypergame H_A^1, taking into account information about the stability of outcomes only in the preference vectors V_{AA} in the game G_{AA} and V_{DD} in the game G_{DA}. Compute the set of equilibrium points of the hypergame H_A^1: E_H for the attacker $E_H = E_{AA} \cap E_{DA}$ (with respect to games G_{AA} and G_{DA}).

3. Analyze the first level H_S^1, taking into account information about the stability of outcomes only in the preference vectors V_{AA} in the game G_{AD} and V_{DD} in the game G_{DD}. Compute the set of equilibrium points of the hypergame H_D^1: E_H for the defender $= E_{AD} \cap E_{DD}$ (with respect to games G_{AD} and G_{DD}).

4. Analyze the second level hypergame H^2 as a whole, we compute the set of points of equilibrium solutions of the game, ie compute the result of the intersection of the sets of stable outcomes of the preference vector V_{AA} in the game G_{AA} and the preference vector V_{DD} in the game G_{DD}: $E = E_{AA} \cap E_{DD}$ (with respect to games G_{AA} and G_{DD}).

To show how to calculate the stability of the outcomes and the general solution of the game, we introduce some new notations and definitions.

Let a certain outcome q be given. If player A at a constant strategy of his opponent D can make the best choice, i.e. find the outcome of a large preference weight (utility) than q, then A has a unilateral improvement of their position. Let UI_A (UI_D) be the set of outcomes that represent a unilateral improvement of the outcome q for player A [player D].

Let a certain outcome q is given. If player A at a fixed strategy of his opponent D can make the best choice, ie find the outcome of a large preference weight (utility) than q, then A has a unilateral improvement of their position. Let $UI_A(q)$ [$UI_D(q)$] is the set of outcomes that represent a unilateral improvement of the outcome q for player A [player D].

If player A can make equal or worst option at a fixed strategy of the opponent's D, ie find the outcome of the same or smaller weight (utility) than q, then A has the unilateral disimprovement of its position. Let $UD_A(q)$ denotes the set of outcomes representing unilateral disimprovement of the outcome q for player A (player D).

Assume that player A has not a unilateral improvement of the outcome of q, i.e $UI_A = \varnothing$. All outcomes q, which satisfy this condition will be called rationally stable and denoted by the letter r.

Sanction is a reaction of the player in the possible improvement of the position of his opponent, which causes the latter to the outcome whose utility is less than or equal to the value of its original position.

So if the opponent knows about the possible sanctions, it would not make any sense to leave it, because if he does, the result is nothing to gain. Sanctioned position is stable for him, and he can include it in the set of expected rational solutions to the game.

Suppose player A has a non-empty set of $UI_A(q)$ for some outcome q. We also assume that for every $UI_A(q)$ an opponent of player A – player D – has its UI_D or UD_D, whose utility for A less than or equal to the utility of the outcome q. Then A will act rationally if he/she refrains from unilateral improvement of its position in view of the possible sanctions from player D. Outcom q, whose stability for a player based on a possible sanction of his opponent will be called sequentially sanctioned and denoted by the letter s.

Suppose player A has a non-empty set of $UI_A(q)$ for the given outcome q. If at one UI_A of the opponent of player A – player D – there are no sanctions, then the outcome q will be called unstable and denoted by the letter u.

All rational, or sequentially sanctioned outcomes for A represent for him the possible solutions to the game.

It is noted by Wang, Hipel and Fraser [27] that solutions to hypergames may not necessarily be created by outcomes that are stable for all players and that it is possible that an outcome that is unstable individually for players may actually be an equilibrium for the hypergame.

VI. A NUMERICAL EXAMPLE

For a numerical illustration of the above described approach, we use a modified version of the network security model from [9]. In Alpcan and Başar's model the attacker has two choices, i.e. launching an attack or doing nothing, while the defender's choices are to trigger or not its defense mechanism. In this study the action spaces of the players are limited only for illustrative purpose. For this purpose we also assume that actions of each player are mutually exclusive, so that it can initiate only one action at a time.

Let the attacker has two actions that he/she may take:

1 – Attack scenario 1;

#2 – Attack scenario 2.

Let assume that actions for the defender are the following:

3 – Defense Mechanism 1;

4 – Defense Mechanism 2;

5 – Defense Mechanism 3.

As noted above, hypergames are games with imperfect information. This means, at least one player has misperceptions about the game elements. Let`s assume that in this game the players have the following misperceptions:

- Players are misinterpreting the preference vectors of each other;
- The attacker is not aware about the third action available to the Defender.

The second level hypergame consists of the following four games:

- Game G_{AA}: The Attacker's perception of the Attacker's game;
- Game G_{DA}: The Attacker's perception of the Defender's game;

– Game G_{AD}: The Defender's perception of the Attacker's game;
– Game G_{DD}: The Defender's perception of the Defender's game.

From the set of actions the set of players' strategies is formed. (A strategy is any set of actions taken by a player.) The strategies of all the players together is called an outcome. The number of outcomes equals to 2^n, where n - the number of all actions available to the players. However not all of these outcomes may be feasible. Each of these actions can be performed or not performed. Therefore, in this game formally there are $2^4 = 16$ outcomes. But, given that the actions of the attacker and defender are mutually exclusive, all outcomes in which both of these actions are performed at the same time, should be excluded as practically infeasible. Also, assume that players have to take one of the actions. Therefore, in the game G_{AA} (G_{DA}, G_{AD}) there are 16-12 = 4 outcomes.

The next step of the hypergame analysis is to identify the preferences of the players. We assume that both the Attacker and Defender have different utility functions for outcomes and outcomes are ordered by each player according to their individual preferences from the most preferred to least preferred (eg 4 = the most preferred; 3 = the next most preferred; 2 = the next least preferred; 1 = the least preferred).

We solve this numerical example using the HYPANT hypergame theory analysis tool [28]. Note that hypergame models must be written in custom HML (Hypergame Modeling Language) format by a person in order to analyze them by HYPANT.

The results of calculating of individual preference vectors and stability of outcomes for the Attacker (A) and Defender (D) in the game G_{AA} are given in Table 3.

In Table 3, a sign Y indicates that the corresponding action is performed, N - the corresponding action is not performed. Outcomes are numbered from 1 to 4.

The preference vector indicates the players ranking of the possible outcomes. Preference vectors for the respective outcomes are given on the first row of Table 3 (for the Attacker), and on the fourth row (for the Defender).

TABLE 3
THE SECOND LEVEL HYPERGAME G_{AA}

A's preference vector	1	2	3	4
#1	Y	N	N	Y
#2	N	Y	Y	N
D's preference vector	4	2	3	1
#3	Y	N	Y	N
#4	N	Y	N	Y
Outcome	1	2	3	4
Stability for *A*	*r*	*r*	*s*	*u*
Stability for *D*	*u*	*r*	*u*	*r*
Equilibriums		*E*		

Below we show calculation of stability of outcomes for the Attacker:

$q = 1$; $UI_A(1) = \varnothing$. It means that the outcome $q = 1$ is rational for A and it is marked with r.

$q = 2$; $UI_A(2) = \varnothing$. It means that the outcome $q = 2$ is rational for A and it is marked with r.

$q = 3$; $UI_A(3) = \{1\}$. $UI_D(1) = \{4\}$. $w_D(4) = 1 \succ w_A(3) = 3$. It means that the outcome $q = 3$ is sequentially sanctioned for A.

$q = 4$; $UI_A(4) = \{2\}$. $UD_D(2) = \{3\}$. $w_D(3) = 3 \succ w_A(4) = 4$. It means that the outcome $q = 4$ is unstable for A.

The overall stability shows which outcomes are possible solutions to the hypergame. Equilibrium for the game G_{AA} is E_{AA}= {{#2 Attack scenario 2, #4 Defense mechanism 2}}.

The results of games G_{DA}, G_{AD}, and G_{DD} are given in Table 4, 5, 6, respectively. Note that the game G_{DD} has 6 outcomes.

TABLE 4
THE SECOND LEVEL HYPERGAME G_{DA}

A's preference vector	1	2	3	4
#1	Y	N	N	Y
#2	N	Y	Y	N
D's preference vector	4	2	3	1
#3	Y	N	Y	N
#4	N	Y	N	Y
Outcome	1	2	3	4
Stability for *A*	*r*	*r*	*s*	*u*
Stability for *D*	*u*	*r*	*u*	*r*
Equilibriums		*E*		

Equilibrium for the game G_{DA} is E_{DA}= {{#2 Attack scenario 1, #4 Defense mechanism 2}}.

The set of equilibrium points of the hypergame H_A^1 for the attacker is $E_H = E_{AA} \cap E_{DA}$ ={{#2 Attack scenario 2, #4 Defense mechanism 2}}.

TABLE 5
THE SECOND LEVEL HYPERGAME G_{AD}

A's preference vector	1	2	3	4
#1	Y	N	N	Y
#2	N	Y	Y	N
D's preference vector	4	2	3	1
#3	Y	N	Y	N
#4	N	Y	N	Y
Outcome	1	2	3	4
Stability for *A*	*r*	*r*	*s*	*u*
Stability for *D*	*u*	*r*	*u*	*r*
Equilibriums		*E*		

Equilibrium for game G_{AD} is E_{AD} = {{#2 Attack scenario 2, #4 Defense mechanism 2}}.

TABLE 6
THE SECOND LEVEL HYPERGAME G_{DD}

A's preference vector	1	2	3	4	5	6
#1	Y	N	N	Y	N	Y
#2	N	Y	Y	N	Y	N
D's preference vector	6	5	4	3	1	2
#3	Y	Y	N	N	N	N
#4	N	N	Y	N	N	Y
#5	N	N	N	Y	Y	N
Outcome	1	2	3	4	5	6
Stability for *A*	*r*	*s*	*r*	*r*	*s*	*u*
Stability for *D*	*u*	*u*	*u*	*s*	*r*	*r*
Equilibriums				*E*	*E*	

Equilibriums for the game G_{DD} is E_{DD} = {{#1 Attack scenario 1, #5 Defense mechanism 3}, {#2 Attack scenario 2, #5 Defense mechanism 3}}.

The set of equilibrium points of the hypergame H_D^1 for the Defender is E_H ={{#1 Attack scenario 1, #5 Defense mechanism 3}, {#2 Attack scenario 2, #5 Defense

mechanism 3}}.

VII. CONCLUSION

We have investigated possible usage of hypergame theory approach for developing decision making framework in information security. The proposed two level hypergame approach models defender's and attacker's perception of the information security situation as a series of games. We also have given an illustrative numerical example on deciding the best attack and defense mechanisms in the context of network security.

REFERENCES

[1] D. Fudenberg, J. Tirole, Game Theory, Massachussetts, MIT Press, 1995.

[2] K. Sallhammar, S. J. Knapskog, B. E. Helvik "Using stochastic game theory to compute the expected behavior of attackers," *International Symposium on Applications and the Internet (Saint'2005)*. Trento, Italy, 2005, pp. 102-105.

[3] P. G. Bennett, "Toward a theory of hypergames," Omega, vol. 5, no. 6, pp. 749-751, 1977.

[4] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, Q. Wu, "A survey of game theory as applied to network security," *43rd Hawaii International Conference on System Sciences (HICSS)*, Hawaii, 2010, pp.1-10.

[5] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, December 2011

[6] A. Singh, A. Lakhotia, A. Walenstein, "Malware antimalware games," in *Proc. 5th International Conference on Information-Warfare & Security (ICIW)*, 2010, pp. 319-327.

[7] P. Maillé, P. Reichl and B. Tuffin, "Of Threats and Costs: A Game-Theoretic Approach to Security Risk Management," *Springer Optimization and Its Applications*, vol. 46, pp. 33-53, 2011.

[8] Q. Wu, S. Shiva, S. Roy, C. Ellis, V. Datla, "On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks," in *Proc. of the 2010 Spring Simulation Multiconference (SpringSim'10)*, Article No. 159.

[9] T. Alpcan, T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in Proc. of the 42nd Conference on Decision and Control. Maui, HI (2003), vol.3, pp. 2595-2600.

[10] A. Patcha, J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *Intl Journal of Network Security*, vol. 2, no. 2, pp. 131–137, 2006.

[11] S. Bistarelli, M. Dall'Aglio, P. Peretti, "Strategic games on defense trees," in: Proc. of 4th Intl Workshop on Formal Aspects in Security and Trust (FAST'06), LNCS 4691, pp. 1–15, Hamilton, Ontario, Canada, 2006.

[12] J. Jormakka and J. V. E. Mölsä, "Modelling Information Warfare as a Game," *Journal of Information Warfare*, vol. 4, no. 2, pp. 12-25.

[13] K.-W. Lye and J. M. Wing, "Game strategies in network security," in *Proc. Workshop on Foundations of Computer Security*, 2002.

[14] Y. Liang, B. Li, H. Wang, "Dynamic awareness of network security situation based on stochastic game theory," in *Proc. 2nd International Conference on Software Engineering and Data Mining (SEDM)*, 2010, pp. 101-105.

[15] K. Sallhammar, B. E. Helvik, S. J. Knapskog, "A game-theoretic approach to stochastic security and dependability evaluation," in Proc. of 2nd IEEE Intl Symposium on Dependable, Autonomic and Secure Computing (DASC), 2006.

[16] A. Ganesh, D. Gunawardena, P. Jey, L. Massouli´e, J. Scott, "Efficient quarantining of scanning worms: Optimal detection and co-ordination," IEEE INFOCOM 2006. Barcelona, Spain (2006)

[17] H. Cavusoglu, S. Raghunathan, W. Yue, "Decision-theoretic and game theoretic approaches to IT security investment," J Manage Inform Syst, vol. 25, 281, 2008.

[18] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty (Special Issue on Terrorist Risks)*, vol. 26, no. 2, pp. 231-249, 2003.

[19] Y. Sasaki, K. Kijima, "Hypergames and bayesian games: A theoretical comparison of the models of games with incomplete information," *Journal of Systems Science and Complexity*, vol. 25, no. 4, pp. 720-735, 2012.

[20] Harsanyi J.C., "Games with incomplete information played by Bayesian players," *Management Science*, vol. 14, no. 3, pp. 159-182, 1967.

[21] N. M. Fraser, and K. W. Hipel, *Conict Analysis, Models and Resolutions*, Elsevier Science Publishing Co. Inc., New York, 1980.

[22] N. M. Fraser, and K. W. Hipel, "Metagame analysis of the poplar river conflict," *Journal of the Operational Research Society*, vol. 31, pp. 377-385, 1980.

[23] M. Giesen, and P. Bennett, "Aristotle's Fallacy: A Hypergame in the Oil Shipping Business," *Omega*, vol. 7, no. 4, pp. 309-320, 1979.

[24] P. G. Bennett, M. R. Dando, and R. G. Sharp, "Using hypergames to model difficult social issues: an approach to the case of soccer hooliganism," *Journal of the Operational Research Society*, vol. 31, no. 7, pp. 621-635, 1980.

[25] Kopp C., "Shannon, hypergames and information warfare," *Journal of Information Warfare*, vol. 2, no. 2, pp. 108-118, 2002.

[26] J. T. House, and G. Cybenko, "Hypergame Theory applied to Cyber Attack and Defense," *SPIE Defense and Security*, Orlando April 2010. (Proc. SPIE 7666, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IX, 766604 (May 03, 2010); doi:10.1117/12.852338)

[27] M. Wang, K. W. Hipel, and N. M. Fraser, "Modeling misperceptions in games," *Behavioral Science*, vol. 33, pp. 207–223, 1988.

[28] L. Brumley, "HYPANT: A Hypergame Analysis Tool" http://www.csse.monash.edu.au/hons/se-projects/2003/Brumley/

Yadigar Imamverdiyev received the MSc degree in applied mathematics from Azerbaijan State Oil Academy, Baku, Azerbaijan, in 1989, and the PhD degree in technical sciences from the Institute of Information Technology of Azerbaijan National Academy of Sciences (ANAS), Azerbaijan, in 2007. From 25.08.2011 to 25.08.2012 he was a post-doctoral researcher at Biometrics Engineering Research Center (BERC) of Yonsei University, Seoul, South Korea. Dr. Yadigar Imamverdiyev is now head of research department at the Institute of Information Technology of ANAS. His research interests include information security management, e-government security, web security, risk management, public and secret key cryptography, biometrics, speaker recognition, social networks analysis.

Virmon: A Virtualization-Based Automated Dynamic Malware Analysis System

Huseyin Tirli, Abdurrahman Pektas, Yliès Falcone, and Nadia Erdogan

***Abstract*— Nowadays, security companies are faced tens of thousands new malware samples every single day. Analysis of these malicious threats in an automated fashion and in a controlled environment are still the valid choice. Even though there are highly skilled dynamic analysis systems, they are weak against malwares targeting new operating systems.**

In this work, we present Virmon (Virus Monitor), a powerful system for dynamic analysis of Windows malwares. It is designed as an automated and virtualization based system. Virmon collects the behavior activities of analyzed samples in low kernel level. It can also use all Windows operating systems as an analysis environment and successfully analyze malwares targeting latest versions. We implement the system to be adaptable to the new operating systems. To demonstrate our effectiveness, we test the system with a real malware sample observed in June, 2013 and obtained results encourage us.

***Index Terms*— behavior analysis, dynamic analysis, malware detection, virtualization**

I. Introduction

MALICIOUS software (malware), an executable used or created by an attacker to attain access to or steal sensitive information from a computer system, has become a major threat against computer systems and even for smart phones. According to [1], Kaspersky claims that they faced with nearly 200,000 new malware samples during the first half of 2013.

The malwares and 0-day exploits (exploits for unpatched vulnerabilities) are becoming a commercial industry. Previously, one could write malware for fun and prominence, now for money, espionage and ideological purposes. Furthermore, some states develop malwares in order to achieve their objectives. For example, *Stuxnet*, one of the most known sophisticated malware (used for advanced persistent treat – APT attacks) is developed to attack Iran's nuclear facilities and cost an estimated *US$1 million* to create [2]. These information help us to understand how big and vast the malware development research is.

Manuscript received July 15, 2013.

H. T. is with TÜBİTAK BİLGEM Cyber Security Institute, 41470 Gebze/Kocaeli TURKEY (e-mail: huseyin.tirli@ tubitak.gov.tr).

A. P. is with TÜBİTAK BİLGEM Cyber Security Institute, 41470 Gebze/Kocaeli TURKEY (e-mail: abdurrahman.pektas@ tubitak.gov.tr).

Y. F. is with University of Grenoble I LIG, 38400 Saint Martin d'Hères FRANCE (e-mail: ylies.falcone@ujf-grenoble.fr).

N. E. is with Istanbul Technical University Faculty of Computer and Informatics 34469 Maslak/İstanbul TURKEY (e-mail: nerdogan@itu.edu.tr).

Due to the ineffectiveness of anti-viruses on previously unknown malwares (whose signature have not been created yet), many researchers have introduced several techniques to overcome limitation of anti-virus solutions [3-7]. These techniques can be divided into two categories:

- *Static analysis* means examining a file without running on the system. Because of the obfuscation techniques such as polymorphism, metamorphism, compression and encryption, it can be difficult and time consuming to statically analyze malwares.
- *Dynamic analysis* means observing activities of a suspicious file by executing it in a controlled environment so as to understand its purpose.

To successfully detect and take appropriate measures, one must be able to analyze them in a reproducible and controlled environment. There are highly skilled dynamic analysis systems revealed by malware researchers. For instance, *Anubis* formerly TTAnalyze [8], is an emulation based dynamic malware analysis system. It performs analysis operations on Windows XP OS running on Qemu emulator. During analysis, it monitors *Win32* and *native API* functions with their parameters through Qemu. Since the system runs on an emulator, analysis time may be longer and this situation can be realized by malwares.

Another tool, *Capture-BAT* [9] can monitor system changes at kernel level. It can be considered that Capture-BAT has a big disadvantage, since it is not an automated malware analysis system. *Cuckoo* [10], an open source analysis system, uses virtualization technology like Virmon. The user space API hooking technique stands behind its methodology. It can track some Win32 API functions with their parameters. Owing to the fact that Cuckoo runs at user level, it can easily be detected by malwares.

To the best of our knowledge, today's dynamic analysis systems generally employ old versions of windows OS as their analysis environment. Nevertheless, the majority of the computer end users prefer to use the latest ones. It seems that they cannot analyze malwares targeting latest windows OS appropriately. Therefore, it is a necessity that next generation malware analysis solutions should cover latest 64-bit OSs and be adapted easily to future OS versions.

With the increase of dynamic malware analysis popularities, malware authors try to collect private information about analysis systems in order to prevent them detect their malwares. One of the most important private information is *public IP addresses* of malware analysis systems. If the public IP address of the environment in which malware executed is a known address by malware authors, malwares change their behaviors or refuse to run on these systems. For instance, *AV Tracker* [11] is a web

platform publishing public IP addresses of well-known analysis systems. By using these technique, analysis systems can be evaded easily by malwares.

In this work, we propose Virmon, a scalable automated anti-malware system designed to address the above challenges. Our contributions can be described as follows:

- *Portability*: Our system can use all versions of windows OS including windows 8 64-bit. When a new windows version is released, it can be simply adjusted to use new versions.
- *Scalable & distributed analysis environment*: The system capacity can be easily increased by adding new hardware. By using sensor – analysis machine matching mechanism, the network traffic of analysis machines is distributed to different network locations. Thus, it gives an opportunity that, our analysis system is not easily detectable.

The rest of the paper is organized as follows: We start by discussing our proposed dynamic malware analysis system. Then, we follow that with implementation details of the system components. In section 4, we evaluate our system with a real-world malware sample thereby showing the effectiveness of the system. Finally, we conclude the paper with a discussion of the limitations and future works in section 5.

II. System overview

One of the most preferred methods for behavior based dynamic malware analysis is *API hooking*. With API hooking, the call made by an application to a function can be redirected to a custom defined function. When the parameters of this function are analyzed, the intention of call (behavior) can be understood.

There are two types of API hooking: *user* and *kernel* space API hooking. Generally in user space API hooking, the Win32 API and Windows native API functions are targeted. However, malware authors try to find new methods to evade API hooking. Since the applied processes are not transparent to malware, the obtained results can be misleading.

Kernel space API hooking, can be implemented with injection of codes to the kernel. As it is known, malware authors misuse the modifiable property of Windows kernel. Additionally, kernel changes can cause fatal errors and prevent proper working of some applications. Therefore, Microsoft created a kernel protection mechanism (*patchguard*) with Vista 64 bit OS to prevent this type of misusage [12]. This mechanism provides code integrity of kernel and causes a blue screen of death (*BSOD*) when a change attempt occurs. Microsoft encourages the user of Windows to use callback mechanism supplied by OS.

Windows callback mechanism provides the delivery of necessary information needed by drivers when the certain conditions are met [13]. In order to be notified of events (*process, registry* and *file*), kernel space component registers itself to OS. When the desired events occur, OS calls the function of the driver determined at registration time. Owing to the fact that patching the kernel of new OS's is too hard, it is unreasonable to try to patch kernel code for behavior monitoring. Thus, we prefer to use callback mechanism presented by the OS.

Our approach to construct a dynamic analysis environment consists of two main components:

i. *Analysis machine components*: It is responsible of reporting host-based activities such as process, registry and file system activities created by analyzed file.
ii. *Network components*: Network components of Virmon is responsible of reporting network activities of an analyzed file and consists of the following modules:

• The sensors at different locations that forward network traffic of analysis machines to the command and control (C&C) servers.

• Virtualization environment which contains the analysis machines.

• An application server managing whole analysis processes.

• IDS that generates alarms, extracts files and HTTP requests from network traffic.

• A DNS server replying and logging DNS requests.

• An NTP server that used to synchronize all machines in the system.

• A database storing all events captured during analysis.

III. System architecture

In this section, we provide the details of Virmon dynamic analysis system. Firstly, we give information about how we collect behavior activities of analyzed suspicious files from operating system (OS). Next, we discuss the network topology of the system where we automatically analyze files to gather their network activities.

A. Analysis Machine Components

On each machine that analyzes malicious software, there are two main components are activated: application working in user space and managing analysis process, and drivers working in kernel space. The application running in user space can be considered as a bridge between OS and application server. The file taken from application server is executed by user space component. The process id information that is obtained by executing the file is sent to the kernel space component. Kernel space component watches three main activities:

1. Process activity
2. Registry activity
3. File system activity

Activities of the process owned by that executable and (if any) processes created by this process are monitored by kernel space component. In the following part, we describe what and how to monitor each type of activities listed above.

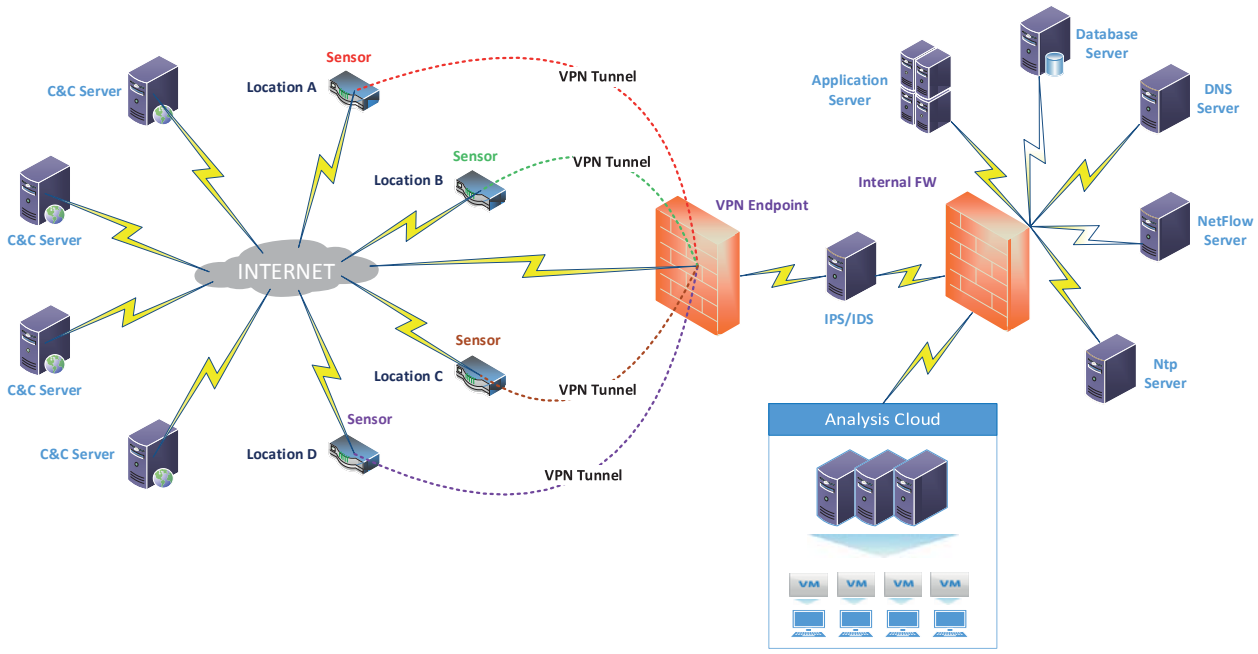


Fig. 1. The topology of Virmon including all the local and remote components of malware analysis system.

1) Process Monitoring

One of the activities needed by malware researchers is process activity of analyzed malware samples. Process monitoring part of the kernel space component observes *process creation/deletion* and *remote thread creation* events. When an application tries to create a new process, OS delivers the information about the process starting the create operation (parent process) and the process to be created to the process monitor. In a similar manner, before a new thread created, OS notifies thread information to the process monitor. If currently working process is one of the processes that is tracked by process monitor and created thread does not belong to current process, this event also recorded as a remote thread creation. In these event types, notification operation happens in the context of the thread creating the new process or thread [14] [15]. On the other hand, in delete process event, notification routine runs in the context of the last thread to exit from the process [14]. Therefore, it is too hard to understand who killed the process. Due to this reason, we only record the deletion events of processes tracked by the process monitor.

2) Registry Monitoring

Windows Registry is a hierarchical database used to store configuration information of applications, hardwares and users [16]. In order to understand what changes are made by the analyzed file on the system, monitoring the registry can be a useful method. Majority of the malwares use windows registry so as to be persistent. They register themselves to the registry to be executed automatically at startup. Also some of them uses the registry to prevent users from calling the task manager, defender etc.

Windows callback mechanism can notify the drivers when events such as read, write and delete on the registry occurs. There are two types of registry notifications: *preoperation* and *postoperation*. By monitoring each types of events, it can be determined whether the operation is successfull or not. *OpenKey*, *CreateKey*, *DeleteKey*, *SetValueKey*, *DeleteValueKey*, *QueryValueKey* and *EnumerateKey* registry operations are watched by registry monitor.

3) File System Monitoring

File system monitor is used to track all file system events (*read/write/delete*) on the system. Monitoring the file system is extremely crucial, since lots of malwares copy themselves to a known location in the OS. Also some of them downloads new payloads or updates itself periodically. Like registry monitor, pre and post IO operation notifications delivered by file system filter manager. The read, write and delete events caused by all tracked processes are recorded by the file monitor.

B. Network Components

Malwares often need to connect C&C servers to send confidential information collected from compromised machines or to take commands from them. That is why analysis of the network activities of malwares is an inevitable requirement for malware analysts. In the proposed system we use different network solutions, such as VLAN, VPN, IPS, and firewall to monitor network activities of suspicious files. We are inspired by our previous work [17] and performed to collect malware samples via high interaction honeypots [18].

The *sensor*, a kind of mini-PC, is placed at any location on the internet in a plug-and-play fashion and is used to match its public IP address to private IP address of an analysis machine. Its main objective is to forward traffic of analysis machines to the Internet. To do this end, each sensor creates a secure channel (*VPN*) to our data center (as depicted in *Figure-1*).

With the use of VPN connection, each analysis machine seems to be directly connected to the Internet. Therefore, IP layer information (e.g. source, destination IP and TTL) of all network packets originating from analysis machine are updated on the sensors to make them appear as if those

packets were sent by sensors. *Figure-2* illustrates logical network topology of analysis machines.

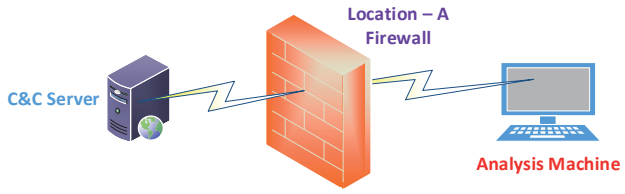


Fig. 2. The logical topology of the system. Each analysis machine is seen by C&C servers as if it is working behind the firewall of network that includes our corresponding sensors.

We assign statically separate *C class* networks to each analysis machines on the *VPN Endpoint*. When a suspicious file analyzed in our system tries to make a connection to remote host, VPN endpoint identifies the related sensor and forwards its network traffic to that sensor.

In addition, to improve transparency of the system, we define separate VLANs for each analysis machines on the internal firewall and virtualization server. So, we reduce the size of broadcast domain, as well as prevent analysis machines from seeing each other.

1) DNS-Server

The Domain Name System is a dynamic database service that translates internet domains and host names to IP addresses. It is a critical service for internet access since internet relies on IP addresses and without the DNS service it would be an obligation for users to know all IP addresses of servers accessed. Similarly, malwares often use domain names to access C&C servers which are changed frequently by attackers to be undetected (fast flux) [19].

To monitor DNS requests made by analysis machines we manually set the DNS server of each machine to our DNS server located in the data center. Meanwhile, in order to prevent malwares to resolve domain name by using public DNS server, (e.g. 8.8.8.8 is Google's well-known public DNS server) we redirect all DNS queries to internal DNS server by using our internal firewall. In this way, all DNS requests made by malwares can be answered and logged by our DNS server. DNS server logs requested domain, time and IP of analysis machine. DNS log file is parsed and the extracted information is sent to database at runtime.

2) IPS/IDS (IPDS):

Intrusion prevention system (*IPS*) is a network security solution monitoring network traffic and system activities. We need an IPS to prevent likely networks attacks caused by suspicious files analyzed in the system.

Due to the following reasons, analysis of web pages requested and files downloaded by malware has become a necessity for the malware analyzer:

1. Nowadays great deal of companies allow their personnel to make only HTTP/HTTPS, FTP etc. connections because of security reasons. Malwares have adapted themselves to use HTTP/HTTPS protocols to communicate with their C&C servers.

2. As it is known, a special type of malware named dropper downloads another malware. Thus, if an analyzed file downloads extra contents via internet, these contents also should be examined.

Suricata [20], an open source IPS solution, can prevent malicious attacks such as distributed denial of service (DDoS), port scanning and shellcodes; it can also extracts files and HTTP requests from live network traffic. Therefore, we have decided to use Suricata as the IPS component of our dynamic analysis system.

Suricata writes HTTP requests to a log file. HTTP log file is parsed at predefined regular intervals and the extracted information is stored to a database. Meanwhile, if the files extracted by Suricata have not already been dissected beforehand, they are enqueued into application server's priority queue.

3) Netflow Server

Netflow server operates to obtain summary information about network traffic of the analysis machines. It records source and destination hosts, the protocol used, ports, flow duration and number of the bytes transferred. To extract these information, all network traffic made by analysis machines is duplicated by internal Firewall and sent to the netflow server. When the server obtains brief information about the flow, it stores them to a database at regular time intervals similar to other servers.

4) NTP-Server

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems. During analysis, we collect information from different analysis servers. The time information of each type of data must be the same on all servers. To do this end, we deploy NTP server so as to synchronize the time of each server in the system.

5) Application Server

It is responsible of the management of the total malware analysis processes. Application server determines the analysis machine on which a submitted file will be analyzed. It collects the activities from all analysis system components. Then, it reformats the collected data and stores them in a database. Furthermore, application server returns the analysis machines to the clean state after the analysis operations are completed.

IV. EVALUATION

In this section, we demonstrate how our dynamic malware analysis system works. Firstly, we explain the communication mechanism between the application server and analysis machines. Then, we show results of a recently observed malware's analysis.

Figure-3 visualizes the communication process between application server and an analysis machine. The process can be described as follows:

1. Analysis application sends a request that specifies the start of new analysis process to the application server.
2. Application server pops a file from its priority queue and sends it to the analysis machine which initiates a new analysis request.
3. Analysis application injects codes to the running *explorer.exe* process. This process executes the file coming from application server in *suspend mode*. If the file is executable, explorer.exe writes id (PID) of newly created process to a shared memory. Analysis application reads PID info from shared memory. Then it sends a message that includes this info to the driver and asks it to record events

initiated by this process.

4. Analysis application waits until the analyzed process exits or a timeout (3 minutes). Then it sends a message to the driver to stop the recording events.
5. Driver stops the recording and writes events to the event file.
6. Analysis application sends the event file to the application server for parse operation.
7. Application server parses the event file and stores them in the database. Than it returns the analysis machine to the clean state.

In order to show the capabilities of our dynamic malware analysis system, we analyze a dropper which was detected on July, 2013 [21]. Dropper is a type of malware created by malware authors to download and install new malwares (e.g. virus, backdoor) on the compromised systems. It can also include the malwares in itself.

The analysis operation is done automatically on a Windows 8 Ultimate 64-bit OS. The steps described above is completed and the activities of malware sample are examined. The important events that have happened on the system is displayed in Table-1.

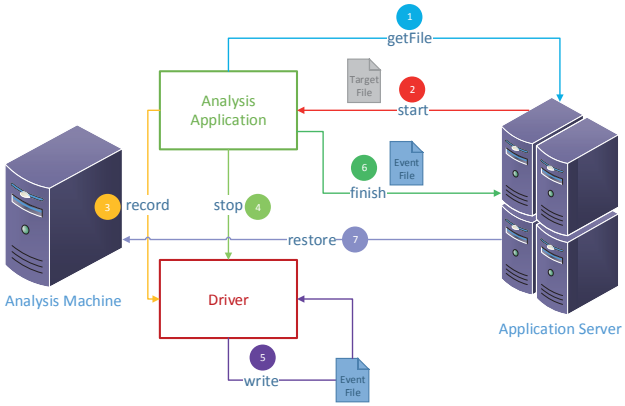


Fig. 3. The communication mechanism between application server and an analysis machine. It demonstrates the main information flow of analysis.

Since the number of events gathered from analysis system for this malware is too high (10000+), only the important events selected manually are included in the table. The majority of the activities are system dll files and registry accesses. If the table is examined, the intention of malware sample can be understood easily.

TABLE I
IMPORTANT ACTIVITIES OF ANALYZED SAMPLE

Time	Event	Process	Detail
2013-07-09 09:50:42.048	Process Create	C:\Windows\explorer.exe	C:\Users\virmon\Desktop\file.exe (Analyzed File)
2013-07-09 09:50:45.018	Process Create	C:\Users\virmon\Desktop\file.exe (Analyzed File)	C:\Users\virmon\Desktop\file.exe
2013-07-09 09:50:45.172	Process Terminate	C:\Users\virmon\Desktop\file.exe (Analyzed File)	-
2013-07-09 09:50:47.906	DNS Query	C:\Users\virmon\Desktop\file.exe	sunelec-kk.com
2013-07-09 09:50:50.393	HTTP Request	C:\Users\virmon\Desktop\file.exe	/tmp/r1.php on sunelec-kk.com (5 times in 24 seconds)
2013-07-09 09:51:15.324	DNS Query	C:\Users\virmon\Desktop\file.exe	japmotors.net
2013-07-09 09:51.15.686	HTTP Request	C:\Users\virmon\Desktop\file.exe	/tmp/r1.php on japmotors.net
2013-07-09 09:51:16.664	DNS Query	C:\Users\virmon\Desktop\file.exe	www.piazzabrothers.com
2013-07-09 09:51:16.876	HTTP Request	C:\Users\virmon\Desktop\file.exe	/tmp/file1.exe on www.piazzabrothers.com
2013-07-09 09:51:17.246	HTTP Request	C:\Users\virmon\Desktop\file.exe	/tmp/file2.exe on www.piazzabrothers.com
2013-07-09 09:51:17.936	DNS Query	C:\Users\virmon\Desktop\file.exe	fondear.es
2013-07-09 09:51:18.776	HTTP Request	C:\Users\virmon\Desktop\file.exe	/tmp/file1.exe on fondear.es
2013-07-09 09:51:18.991	HTTP Request	C:\Users\virmon\Desktop\file.exe	/tmp/file2.exe on fondear.es
2013-07-09 09:51:19.677	File Write	C:\Users\virmon\Desktop\file.exe	C:\Users\virmon\AppData\Local\Temp\990203.bat
2013-07-09 09:51:20.443	Process Create	C:\Users\virmon\Desktop\file.exe	C:\Windows\SysWOW64\cmd.exe
2013-07-09 09:51:20.490	Process Create	C:\Windows\SysWOW64\cmd.exe (cmd /c C:\Users\virmon\AppData\Local \Temp\990203.bat C:\Users\virmon\Desktop\file.exe)	C:\Windows\System32\conhost.exe
2013-07-09 09:51:20.490	Process Terminate	C:\Users\virmon\Desktop\file.exe	-
2013-07-09 09:51:22.115	File Delete	C:\Windows\SysWOW64\cmd.exe	C:\Users\virmon\Desktop\file.exe
2013-07-09 09:51:22.568	File Delete	C:\Windows\SysWOW64\cmd.exe	C:\Users\virmon\AppData\Local\Temp\990203.bat
2013-07-09 09:51:22.662	Process Terminate	C:\Windows\SysWOW64\cmd.exe	-
2013-07-09 09:51:22.678	Process Terminate	C:\Windows\System32\conhost.exe	-

When the sample is executed, firstly the process created by explorer.exe creates a new process having the same name in its directory. This technique, named as *process hollowing* [22], is often used by malwares recently to hide themselves. Then, the process created by explorer.exe terminates itself. The file.exe process created by using hollowing technique sends HTTP requests to predefined four distinct compromised servers respectively to download new malwares. Since the malwares targeted by file.exe are deleted from servers before the analysis operation, it cannot access to malwares and changes its behavior. The dropper creates a script named as *990203.bat* and executes this script. By this execution, malware terminates itself and the script removes malware's footprints. As it is seen on Table-1, our dynamic malware analysis system successfully collects the behavior activities of the analyzed sample.

V. Conclusion

In this paper, we present a virtualization-based automated dynamic malware analysis system. We have developed a kernel driver which can monitor state changes during the malware analysis. Virmon currently supports all Windows OSs and we can easily adapt the system to use new OSs. The distributed architecture of the system can be extended easily. Sensor – analysis machine matching mechanism can help us to hide the analysis system against the malwares using IP based detection techniques.

Currently, we are not fully capable to analyze malwares which are sensitive to virtualized environments because of the fact that our system based on virtualization technology. Also the system can only analyze executable files. Additionally, the network activities of the analysis machines are gathered system-wide. Therefore, we are planning to improve our system to be capable of analyzing virtualized environment sensitive malwares, collect network events on low kernel level and also increase the number of file types that can be analyzed on Virmon. Meanwhile we are working on automated classification of malwares and encouraging ourselves to integrate the classification system into Virmon.

References

[1] "Kaspersky Lab Press Release 2012", Internet: http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Downloads/PDFs/101212_Press_Release_2012_by_numbers.pdf, [Jul 10, 2013].

[2] "Estimated Cost of Stuxnet", Internet: http://www.thenational.ae/business/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack, [Jul 14, 2013].

[3] A. Moser, C. Kruegel, and E. Kırda, "Exploring multiple execution paths for malware analysis," in Proceedings of the IEEE Symposium on Security and Privacy, 2007, pp. 231-245.

[4] H. Agrawal, L. Bahler, J. Micallef, S. Snyder, and A. Virodov, "Detection of global, metamorphic malware variants using control and data flow analysis," in Military Communications Conference (MILCOM), 2012, pp. 1-6.

[5] H. Huang, G. Acampora, V. Loia, C. Lee, and H. Kao, "Applying FML and Fuzzy Ontologies to Malware Behavioral Analysis," in Proceedings of the IEEE Symposium on Fuzzy Systems (FUZZ), 2011, pp. 2018-2025.

[6] G. Tahan, L. Rokach, and Y. Shahar, "Mal-ID: Automatic Malware Detection Using Common Segment Analysis and Meta-Features," in The Journal of Machine Learning Research, vol. 13, 2012, pp. 949-979.

[7] R. Rolles, "Unpacking Virtualization Obfuscators," in Proceedings of the 3rd USENIX conference on Offensive technologies, 2009, pp.1-10.

[8] U. Bayer, C. Kruegel, E. Kirda, "TTAnalyze: A tool for analyzing malware," Internet: http://www.iseclab.org/papers/ttanalyze.pdf, [Jun. 21, 2013].

[9] C. Seiferta, R. Steensona, I. Welcha, and P. Komisarczuka, B. Endicott-Popovskyb, "Capture – A behavioral analysis tool for applications and documents," Digital Investigation: The International Journal of Digital Forensics & Incident Response, vol. 4, 2007, pp. 23-30.

[10] "Cuckoo Sandbox", Internet: http://www.cuckoosandbox.org/, [Jun. 20, 2013].

[11] "AV Tracker", Internet: http://www.avtracker.info/, [Jul. 5, 2013].

[12] "Kernel Patch Protection: Frequently Asked Questions." Internet: http://msdn.microsoft.com/en-us/library/windows/hardware/gg487353.aspx, Jan. 22, 2007 [Jun. 18, 2013].

[13] "Callback Objects." Internet: http://msdn.microsoft.com/en-us/library/windows/hardware/ff540718(v=vs.85).aspx, [Jun. 18, 2013].

[14] "PsSetCreateProcessNotifyRoutineEx routine." Internet: http://msdn.microsoft.com/en-us/library/windows/hardware/ff559953(v=vs.85).aspx, [Jun. 20, 2013].

[15] "PsSetCreateThreadNotifyRoutine routine." Internet: http://msdn.microsoft.com/en-us/library/windows/hardware/ff559954(v=vs.85).aspx, [Jun. 20, 2013].

[16] "What is the registry?" Internet: http://windows.microsoft.com/en-id/windows-vista/what-is-the-registry, [Jun. 21, 2013].

[17] N. E. Siseci, B. Emre, and H. Tirli, "Case Study: Malicious Activity in the Turkish Network," Internet: http://www.syssec-project.eu/media/page-media/3/syssec-d5.3-TurkishNetworkCaseStudy.pdf [Jun. 23, 2013]

[18] A. Caglayan, M. Toothaker, D. Drapaeau, D. Burke, and G. Eaton, "Behavioral Patterns of Fast Flux Service Networks," in in Proceedings of 43rd Hawaii International Conference on System Sciences (HICSS), 2010, pp. 1-9.

[19] J. Nazario, and T. Holz, "As the Net Churns: Fast-Flux Botnet Observations," in Proceedings of 3rd International Conference on Malicious and Unwanted Software, 2008, pp. 24-31.

[20] "Suricata", Internet: http://suricata-ids.org/, [Jul. 1, 2013].

[21] "Antivirus scan for b0d36b9d9a6866a70b13b71772a0de84 at 2013-06-26 16:01:34 UTC - VirusTotal" Internet: https://www.virustotal.com/tr/file/c3833351f751eedcd13e23cff488d66dc9e45aab0b86a4c4b6e3481389bf5e29/analysis/, [Jul. 10, 2013].

[22] M. H. Ligh, S. Adair, B. Hartstein, and M. Richard. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Indianapolis, USA: Wiley Publishing, Inc, 2011, pp. 596-599.

ICT Usage Characteristics and Web Security

Atila Bostan, İbrahim Akman

***Abstract*— In assuring the security in information and communication technologies, user awareness and acquired-user habits are inevitable components, yet they may be qualified as the feeblest ones. As the information technology tries to put its best in providing maximum security, user awareness plays the key-role. The relation in between the demographic factors, usage frequency and issues related web security not to be known yet. Therefore, this study investigates demographic factors, information and communication technology usage characteristics of users on providing secure web usage. For this purpose, a survey was conducted among 466 citizens from different layers of the society. The results indicated existence of significant relations between various socio-demographic factors, reason and frequency of ICT usage factors and web-security issues.**

***Index Terms*— computer security, demographic factors, ICT usage frequency**

I. INTRODUCTION

THE world has witnessed the rapid development in information and communication technologies in the last two decades. Today almost all of the communication and business transactions have been moved onto digital networks. An abundant amount of communication and e-commerce services are running on the Internet with about 2.5 billion of current user count [1]. Among all other digital techniques on the Internet, web is the most common one as a user interface for a variety of services. With user satisfaction and service performance in mind the initial design of web technology did not include any mechanism to stipulate security in transactions. But great demand from baking and e-commerce domains, forced web service to incorporate security mechanisms in time. Unfortunately, whereas the technology tries its best to improve security mechanisms, web based security breaches are proven to be on a constant rise in recent years [2,3]. As it is in other security mechanisms, the key component is almost always pointed as end users in web based security services either. Users, while taking part as administrators, technicians or users in web services are inevitable and weakest rings in security-chain. Uncertainty in human behaviors is generally deemed as the grounds for the weakness of user component. Thus, it is usually hard to predict the expected response of a user when (s)he is exposed to a security related experimental setting. Yet security-responses of two users would most likely be different than each other when they face similar settings although they were subject to the same education and directions. The factors effective in human decision-making process are fuzzy.

Atila Bostan is with Computer Engineering Department, Atılım University, Gölbaşı, Ankara, TURKEY (tel:+90 312 5868792 e-mail: abostan@atilim.edu.tr).

İbrahim Akman is also with Computer Engineering Department, Atilim University, Gölbaşı, Ankara, Turkey (emal: akman@atilim.edu.tr)

Most preferred behavioral practices, habits, of any web user play an important role in predicting user responses towards a security challenge. In one of their scientific studies D'archy and Hovay pointed out; the success in information security greatly depends on user security habits and awareness [4]. In another one, Adams and Sase indicate "Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design" [5]. Appropriate and constructive behavior by end users, system administrators, and others can enhance the effectiveness of information security while inappropriate and destructive behaviors can substantially inhibit its effectiveness [6]. In his interpretation on information security behaviors of human, Secrets and Lies, Schneier asserts ''Mathematics is logical; people are erratic, capricious, and barely comprehensible.''[7]. Security mechanism need to be user friendly otherwise they are most likely laid off. Witten and Tygar highlighted the user discontent in PGP e-mail encryption [8]. Freidman et al. investigated user's perception of security in web-based interactions and noted that problems arise how people assess the security of settings they encounter [9]. Furthermore in one of our previous studies we examined user behavior characteristics in SSL/TLS web applications [10] and found that users do not always pay attention to web security indicators. End user security related behaviors would suggest several instruments to improve observed practices. Most of the academic publications refer to user training on security as a possible cure to develop user behaviors. But, there are scientific studies which prove that user practices are not always in parallel with their beliefs [11,12]. Secure ways of web usage must be practiced and internalized [12]. In addition, age and experience are shown to be correlated with attitudes towards security [13].

An improvement in web usage behavior calls for a change in every day practices of users. Training, user intentions and experiences are factors known to induce behavioral changes. Researchers go along with the need to focus on user motivations and usage habits in designing web security mechanisms [14,15,16].

In this research study we examined the effect of user ICT experience on secure web usage. In order to scrutinize the problem in focus an 14-question survey was carried out in shopping malls on 433 randomly selected participants. Interpretations and conclusions in this study are derived from the results of the survey.

The rest of this paper is organized as follows: In the next chapter research methodology used in the study is presented along with the hypotheses scrutinized. Following the research design and test method, we state the results found in the study. In the final chapter, conclusion is submitted.

II. RESEARCH METHODOLOGY AND HYPOTHESES

The literature reported existence of digital divide within countries [17]. Some studies investigated the attitude of individuals toward using ICT and the relationships between ICT issues and socio-demographic factors (see for example [18-22]).

For the citizens, ICT technologies can offer a huge range of services and the internet is probably the most important one of these services. The literature provides evidences stating that there are many people who do not or can not access to computers and/or internet due to the gap between citizens' attributes including gender, education, income, age, households, business and geographic areas at different socio-economic levels with re1"gard to their use of the internet for a wide variety of activities. Of these attributes, gender, age, education and experience have attracted special interest. Additionally, organizational characteristics play an important role in shaping individuals' attitudes towards the use of IT [23]. Some studies reported significant differences between the types of IT applications among organizations from public and private sectors [24,25]. Lau and Gupta et al. reported significant differences between the types of IT applications among organizations from different sectors. On the other hand, in their study Tan et al. [26] considered security to be a major barrier in using ICT and reported it to be a significant factor influencing internet-based ICT adoption. This research focuses only on small and medium sized enterprises. Maslin and Zuraini [27] examined the influence of demographic factors on awareness for computer-use and security. They reported that age and education level influence awareness for computer use and security.

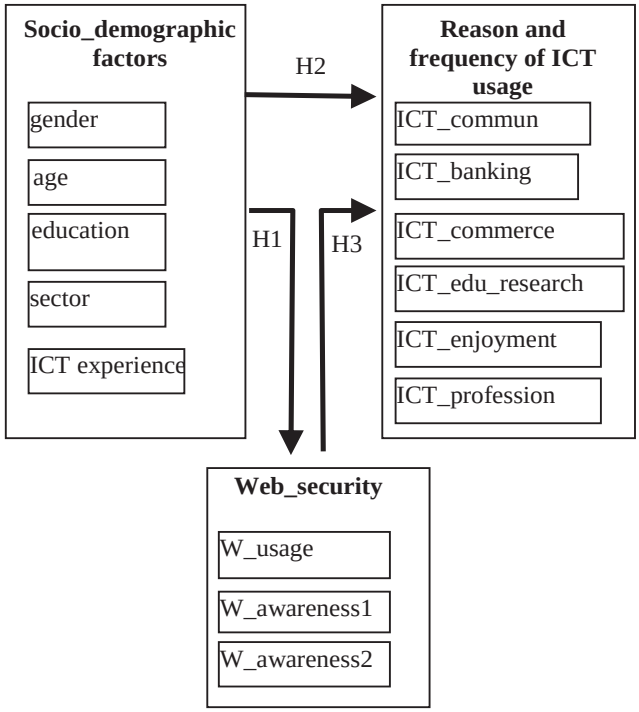


Fig. 1. Research model

This research used data collected from computer science students. Finally, Choi [28] examined how demographic variables are statistically associated with the level of equipping the computer security and reported that demographic factors differentially contribute to computer security issues. All these studies point the need for further research since findings may offer valuable insights to policy makers in general.

The concerns on the internet security have grown in parallel to the increase in the reliance on the Internet [29]. Symantec [30] reported that there are over one million viruses, worms, Trojan horses and other malicious code on the Internet. Therefore, the research on inadequate Internet security has increased gradually during the last decade.

With this backdrop, present study performs a systematic analysis to investigate the impact of independent (decision) variable socio-demographic factors on web security and reason and frequency of ICT usage. Whereas the impact of web security on reason and frequency of ICT usage is also scrutinized. The research model was developed to find an answer to the following main questions:

- Do socio-demographic factors have impact on web security?
- Do socio-demographic factors have impact on reason and frequency of ICT usage?
- Do web security factors have impact on reason and frequency of ICT usage?

For this purpose, three empirical factors are used as follows: (i) Socio-Demographic, (ii) web security and (iii) ICT usage. The justification for empirical factors and their corresponding hypotheses are provided below.

Hyp.	Definition
$H1_{ij}$	web_security $factor_i$ (i=1,2,3) is related to socio-demographic $factor_j$ (j=1,2...,5)
$H2_{ij}$	reason and frequency of ICT_usage $factor_i$ (i=1,2,..,6) is related to socio-demographic $factor_j$ (j=1,2...,5).
$H3_{ij}$	web_security $factor_i$ (i=1,2,3) is related to reason and frequency of ICT_usage $factor_j$ (j=1,2,..,6).

III. RESEARCH DESIGN

The respondents were ordinary citizens belonging to different groups in the society, since the survey was conducted in big shopping malls in different cities in different days of the week by the young members of Turkish Chamber of Electrical Engineers. The sampling method was selected to be "judgment sampling" and the respondents participated in the study voluntarily. A total of 466 completed survey questionnaires were received. Thirty three responses were discarded due to the existence of unqualified data, which means 433 responses included in the analysis. Thus, the approximate response rate was approximately 93 percent which can be considered acceptable for the purpose of this study [31,32]. The research questions and variables are given in Table 1 below.

TABLE 1
RESEARCH QUESTIONS AND VARIABLES

Q	Variable	Definition	Range of values
1	gender	What is your gender?	male, female
2	age	What is your age?	<21, 21-30, 31-40, 41-50, 51-
3	education	What is your education level?	graduate/under graduate/others
4	sector	What is the sector of your organization?	private, public, not working
5	experience	What is the level of your ICT experience (years)	0, 1-5, 6-10, 11-15, 16-20, >20
6	W_usage	Do you visit/use web pages on Internet?	yes/no
7	W_ awareness1	What is the level of your awareness on web security?	very high, high, average, little, very little
8	W_awareness2	Do you have awareness on web	Yes/no
9	ICT_commun	How much do you use ICT for communication?	very high, high, average, little, very little
10	ICT_banking	How much do you use ICT for electronic banking?	very high, high, average, little, very little
11	ICT_commerce	How much do you use ICT for electronic commerce?	very high, high, average, little, very little
12	ICT_edu_resrch	How much do you use ICT for education and research?	very high, high, average, little, very little
13	ICT_enjoyment	How much do you use ICT for enjoyment?	very high, high, average, little, very little
14	ICT_profession	How much do you use ICT for your professional activities?	very high, high, average, little, very little

IV. TEST METHOD

Testing of hypotheses concerning the impact of socio-demographic factors on web security ($H1_{ij}$), the impact of socio-demographic factors on reason and frequency of ICT usage ($H2_{ij}$) and the impact of web security factors on reason and frequency of ICT usage ($H3_{ij}$) were conducted using multivariate regression. Regression Analysis is a powerful statistical tool and is used in a wide variety of applications. It has the advantage that no assumption is made about the nature of the relationship between dependent and independent variables. Additionally, it can handle categorical data better. Therefore, is normally preferred when the independent variables are categorical [33]. The chi-square test method [33] is used whenever there is a need to examine the relationship between the dependent and independent variables.

V. RESULTS

The results of the present survey are presented in the following sequence. Initially, the results of the survey are presented using descriptive analysis. As it was mentioned earlier, Chi-square test method was also used whenever there was a need to have a better insight to the respondents' profile in this part. This is followed by the results of regression analysis for each demographic factor.

A. DESCRIPTIVE RESULTS

The background profile of respondents is provided in Table 2.

TABLE 2
PROFILE OF RESPONDENTS

Variable	Turkish graduate students	
	Number	%
Gender	433	100
Male	239	55
Female	188	44
Unknown	6	1
Age	433	100
<21	91	21
21-30	204	47
31-40	89	21
41-50	40	9
>50	9	2
Sector	433	100
Private	93	21
Public	76	18
Not working	238	55
Unknown	26	6

The respondents were observed to be almost equal in terms of gender (male: 55%; female: 44%) in this survey. This is expected since it was conducted in shopping malls where there is no reason for dominancy of any gender. Of the males in the sample, 14% reported their awareness on web security is above average and this percentage for females is 5%. Chi-square test results indicate that there is significant relation between gender and awareness on web security (Chi-Square = 14.622; DF = 5; P-Value = 0.012).

The age distribution showed a high percentage for the group of less than 30 years of age (68%) whereas this percentage for elder people, who are greater than 40 years is only 11%. This should be considered normal because the percentage of young people visiting shopping malls every day is observed to be high and young people show more interest in responding surveys. Of the young respondents (<30 years of age), 14% reported their awareness on web security to be above average and this percentage for elder people (>40 years of age) is 0%. Chi-square test results indicates significant relationship between age and web security (Chi-Square = 97.110; DF = 12; P-Value = 0.000).

Regarding respondents from private sector organizations 10% reported their security awareness is above average for web services. This percentage for public sector employees is observed to be 5%. Public sector employees seem to be less security-aware on web services and Chi-square test result shows significant relationship between sector and web security awareness (Chi-Square = 33.557; DF = 12; P-Value = 0.001).

B. TEST RESULTS

Regression test results of socio-demographics against web security are shown in Table 3. P-values in last column of Table 3 indicate that except for the hypotheses $H1_{12}$ and $H1_{15}$, the remaining ones are not supported by the survey results at 5% significance level for W_usage. This means $H1_{11}$, $H1_{13}$ and $H1_{14}$ are rejected at 5 percent significance level since their p-values are 0.469, 0.158 and 0.263 respectively. This can also be interpreted as the socio-demographic factors age and experience have impact on the web usage for different purposes. Interestingly, the work sector does not have any impact. Regarding the dependent variable w_awareness1, it is observed from inspection of p-values that $H1_{21}$ (p_value=0.020), $H1_{22}$(p_value=0.000), $H1_{23}$ (p_value=0.000) and $H1_{25}$ (p_value=0.000) are all accepted. This can also be interpreted as gender, age, education and experience are related to w_awareness1. In other words, they have impact on the level of web security awareness. The work sector is the only factor in this category that does not have any effect and $H1_{24}$ is rejected (p_value=0.253). Inspection of the last column of Table 3 states that, except for the hypothesis $H1_{31}$ (p_value=0.986), all the others are accepted at 5 percent significance level for the dependent variable w_awareness2. This means the independent variables age, education, sector and experience have impact on the awareness level for web certificate error. Surprisingly, gender does not have this effect.

TABLE 3
REGRESSION TEST RESULTS OF SOCIO-DEMOGRAPHICS AGAINST WEB SECURITY

Dep.var.	Indep. var.	Hyp.	alpha	p*
W_usage	gender	$H1_{11}$	0.02606	0.469
	age	$H1_{12}$	-0.06764	0.000*
	education	$H1_{13}$	-0.02111	0.158
	sector	$H1_{14}$	0.02673	0.263
	experience	$H1_{15}$	0.15509	0.000*
W_awareness1	gender	$H1_{21}$	-0.36032	0.020*
	age	$H1_{22}$	-0.36032	0.000*
	education	$H1_{23}$	0.16711	0.000*
	sector	$H1_{24}$	-0.06998	0.253
	experience	$H1_{25}$	0.44513	0.000*
W_awareness2	gender	$H1_{31}$	-0.00116	0.986
	age	$H1_{32}$	-0.24484	0.000*
	education	$H1_{33}$	0.07600	0.006*
	sector	$H1_{34}$	0.07600	0.011*
	experience	$H1_{35}$	0.07600	0.000*

*indicates statistically significant at 5 per cent significance level.

Regression test results of socio-demographics against reason and frequency of ICT usage are shown in Table 4. Interestingly, inspection of p-values in the last column of Table 4 indicate acceptance of $H2_{15}$, $H2_{25}$, $H2_{35}$, $H2_{45}$, $H2_{55}$ and $H2_{65}$. This means, that the socio-demographic factor experience has significant impact on all of the dependent factors, ICT_commun, ICT_banking, ICT_commerce, ICT_edu_research, ICT_enjoyment and ICT_profession since p-values are all 0.000. It can also be interpreted as with the increasing level of experience the usage of ICT is increasing in different fields such as communication, banking, commerce, education and research, enjoyment and professional usage.

TABLE 4
REGRESSION TEST RESULTS OF SOCIO-DEMOGRAPHICS AGAINST REASON AND FREQUENCY OF ICT USAGE

Dep. var.	Indep. var.	Hyp.	alpha	p*
ICT_commun	gender	$H2_{11}$	- 0.003	0.975
	age	$H2_{12}$	- 0.548	0.000*
	education	$H2_{13}$	0.085	0.024*
	sector	$H2_{14}$	0.037	0.536
	experience	$H2_{15}$	0.696	0.000*
ICT_banking	gender	$H2_{21}$	- 0.247	0.026*
	age	$H2_{22}$	- 0.045	0.425
	education	$H2_{23}$	0.193	0.000*
	sector	$H2_{24}$	0.067	0.361
	experience	$H2_{25}$	0.593	0.000*
ICT_commerce	gender	$H2_{31}$	- 0.218	0.052*
	age	$H2_{32}$	- 0.130	0023*
	education	$H2_{33}$	0.125	0.008*
	sector	$H2_{34}$	- 0.194	0.009*
	experience	$H2_{35}$	0.436	0.000*
ICT_edu_research	gender	$H2_{41}$	- 0.011	0.924
	age	$H2_{42}$	- 0.447	0.000*
	education	$H2_{43}$	0.196	0.000*
	sector	$H2_{44}$	- 0.364	0.000*
	experience	$H2_{45}$	0.683	0.000*
ICT_enjoyment	gender	$H2_{51}$	- 0.213	0.040*
	age	$H2_{52}$	- 0.602	0.000*
	education	$H2_{53}$	0.066	0.125
	sector	$H2_{54}$	- 0.238	0.001*
	experience	$H2_{55}$	0.649	0.000*
ICT_profession	gender	$H2_{61}$	- 0.259	0.039
	age	$H2_{62}$	- 0.048	0.449
	education	$H2_{63}$	0.242	0.000*
	sector	$H2_{64}$	0.236	0.005*
	experience	$H2_{65}$	0.627	0.000*

*indicates statistically significant at 5 per cent significance level.

On the other hand, p-values indicate acceptance of $H2_{21}$, $H2_{31}$, $H2_{51}$ and $H2_{61}$. In other words, gender is found to have impact on ICT_banking, ICT_commerce, ICT_enjoyment and ICT_profession. This means, there is a significant relationship between gender and usage of ICT for banking, commerce, enjoyment and professional purposes. But the relationship between gender and ICT usage for education and research is strongly rejected with a p-value of 0,924. Regarding the socio-demographic variable age, $H2_{12}$, $H2_{32}$, $H2_{42}$ and $H2_{52}$ are supported by the survey results and, therefore, we accept them. This implies that age has significant impact on usage of ICT for communication, commerce, education and enjoyment purposes. Whereas, the

findings indicate that the relationships between age and ICT usage for banking or profession are insignificant. For the hypotheses $H2_{13}$, $H2_{23}$, $H2_{33}$, $H2_{43}$, and $H2_{63}$, p-values were found to be 0.024, 0.000, 0.008, 0.000, and 0.000 respectively. Therefore, we again accept $H2_{13}$, $H2_{23}$, $H2_{33}$, $H2_{43}$ and $H2_{63}$ at 5% significance level in this empirical category. This also means that for the variables ICT_banking, ICT_commerce, ICT_edu_research and ICT_profession the variable "level of education" has significant influence on ICT usage. In other words, level of education category does not show identical behavior in their populations for ICT usage frequency in communication and enjoyment. Finally, inspection of p-values indicate that the variable sector is in favor of $H2_{34}$, $H2_{44}$, $H2_{54}$ and H264, which leads to their acceptance. A plausible explanation for this finding is that sector of the respondent's work sector has significant impact on the frequency of ICT usage for commerce, education and research, enjoyment and professional usage.

TABLE 5
REGRESSION TEST RESULTS OF WEB SECURITY AGAINST REASON AND FREQUENCY OF ICT USAGE

Dep. var.	Indep.var.	Hyp.	alpha	p*
ICT_commun	w_usage	$H3_{11}$	1.3472	0.000*
	w_awareness1	$H3_{12}$	0.53630	0.000*
	w_awareness2	$H3_{13}$	0.18729	0.014*
ICT_banking	w_usage	$H3_{21}$	0.7415	0.000*
	w_awareness1	$H3_{22}$	0.60200	0.000*
	w_awareness2	$H3_{23}$	-0.25227	0.008*
ICT_commerce	w_usage	$H3_{31}$	0.61780	0.000*
	w_awareness1	$H3_{32}$	0.6178	0.000*
	w_awareness2	$H3_{33}$	-0.29296	0.001*
ICT_edu_research	w_usage	$H3_{41}$	0.5397	0.000*
	w_awareness1	$H3_{42}$	0.78040	0.000*
	w_awareness2	$H3_{43}$	-0.2466	0.014*
ICT_enjoyment	w_usage	$H3_{51}$	1.0013	0.000*
	w_awareness1	$H3_{52}$	0.55697	0.000*
	w_awareness2	$H3_{53}$	0.00563	0.952
ICT_profession	w_usage	$H3_{61}$	0.2445	0.138
	w_awareness1	$H3_{62}$	0.58922	0.000*
	w_awareness2	$H3_{63}$	-0.0006	0.996

*indicates statistically significant at 5 per cent significance level.

The regression test results for the relationship between web security and, reason and frequency of ICT usage are given in Table 5. Interestingly, the inspection of p-values in the last column of Table 5 indicate similar trend for the dependent variables ICT_commun, ICT_banking, ICT_commerce and ICT_edu_research. In other words, $H3_{11}$, $H3_{12}$ and $H3_{13}$ for ICT_commun; $H3_{21}$, $H3_{22}$ and $H3_{23}$ for C_banking; $H3_{31}$, $H3_{32}$ and $H3_{33}$ for C_commerce and $H3_{41}$, $H1_{42}$ and $H1_{43}$ for ICT_edu_research are all accepted at 5 percent significance level. This means the independent variables w_usage, w_awareness1 and w_awareness2 have impact on the dependent variables ICT_commun, ICT_banking, ICT_commerce and ICT_edu_research. In other words, behavior towards usage of web, web security awareness level and certificate error awareness level influence the usage and frequency of ICT usage for communication, banking, commerce and education/research purposes. On the other hand, inspection of p-values on the last column of Table 5 leads to the acceptance of $H3_{51}$ (p_value=0.000) and $H3_{52}$ (p_value=0.000) and rejection of $H3_{53}$ (p_value=0.952). This means there is significant relationship between the behavior towards using ICT for enjoyment and web usage and also between using ICT for enjoyment and level of web security awareness. Level of awareness about certificate error does not have any impact in this category. Finally, depending on p-values for the usage of ICT for professional purposes, the only factor having significant impact appears to be the level of web security awareness (p_value=0.000). Therefore, we accept $H3_{62}$ and reject $H3_{61}$ (p_value=0.138) and $H3_{63}$ (p_value=0.996).

VI. CONCLUSIONS

The paper presents the findings of a survey conducted among the citizens in Ankara. The results show in general that socio-demographic factors are significantly important in reason and frequency of ICT usage and awareness on web security. Our results may provide important insight for companies that are developing web security products and solutions. The findings in this study may also direct academic researchers in conducting and designing of new studies in the field. Furthermore, web security educators and trainers may benefit from the results as well.

The multivariate regression analysis method is used for tests in this study. The results observed in this study supports the existence of significant relationships between socio-demographic factors, factors related to reason/frequency of ICT usage and web security issues at different levels.

There are some limitations to the present study. The sample is composed basically of ordinary citizens, which may not be representative of different layers in the society. Therefore, an extension to consider different groups in the society such as professionals may provide interesting results. Other socio-economic factors such as income should also be investigated. Another important limitation may be based on the studies of Calhoun et al. [34], Chirkov et al. [35] and other researchers which concluded that culture affects the use of ICT in significant way. Furthermore the effect of culture on ICT usage among organizations may be studied from an organizational perspective among different countries in the future.

ACKNOWLEDGMENT

We would like to extend our sincere appreciation to The Chamber of Electrical Engineer-Ankara office for their support in conducting the survey.

REFERENCES

[1] The World in 211 ICT Facts and Figures, International Telecommunication Union, available at http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf, last accessed on March 16, 2013

[2] Computer Security Institute, CSI 2009 14th Annual CSI Computer Crime & Security Survey, Comprehensive Addition, Computer Security Institute, available at http://gocsi.com/sites/default/files/pdf_survey/CSI%20Survey%202009%20Comprehensive%20Edition.pdf, last accessed on March 16, 2013

[3] Computer Security Institute, CSI Computer Crime and Security Survey 2010/2011, Computer Security Institute, available at http://gocsi.com/survey, last accessed on March 16, 2013.

[4] D'Arcy J., Hovay A., Deterring Internal Information Misuse, Communications of the ACM, October 2007, Vol. 50 No.10

[5] Adams A., Sase M. A., Users Are Not The Enemy, Communications of the ACM, December 1999, Vol. 42 No.12

[6] Stanton Jeffrey M., Stam K.R., Mastrangelo P., Jolton J., Analysis of end user security behaviors, Computers & Security, Volume 24, Issue 2, March 2005, Pages 124–133

[7] Schneier B., Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, 2011.

[8] Whitten, A. and Tygar, J.D., Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Proc. 9th USENIX Security Symposium 1999.

[9] Friedman, B., Hurley, D., Howe, D., Felten, E., and Nissenbaum, H. 2002. Users' Conceptions of Web Security: A Comparitive Study. Short paper presented at ACM Conf. Human Factors in Computing Systems CHI 2002 (Minneapolis, MN.)

[10] Bostan A., Web Uygulamalarında SSl/TSL Kullanımı ve Kullnıcı Davranışları, 4th International Information Security & Cryptology Confrence (ISC) Turkey 6-8 May 2010, available at http://www.iscturkey.org/iscold/2010.html, last accessed on March 17,2013

[11] Palfreyman K. and Rodden T. A Protocol For User Awareness And World Wide Web, Computer Supported Cooperative Work'96, Cambridge MA, USA, 1996 ACM 0-89791-765-0/96/11

[12] Gross J. B. and Rosson M. B. Looking for Trouble: Understanding End-User Security Management, CHIMIT'07, March 30-31, 2007, Cambridge MA, USA. 2007 ACM 1-59593-635-6/97/0003

[13] Dourish P., Grinter R.E., de la Flor J.d. and Joseph M., Security in the wild: user strategies for managing security as an everyday, practical problem, Personal and Ubiquitous Computing, November 2004, Volume 8, Issue 6, pp 391-401

[14] Stanton J. M. and Stam K. R. Mastrangelo Paul, Jolton Jeffrey, Analysis of End User Security Behaviors, Computers & Security, March 2005, sayfa 124-133

[15] Herzberg A., Jbara A., Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks, ACM Transactions on Internet Technology, September 2008, Vol. 8, No. 4, Article 16.

[16] West R. The Psychology of Security, Commu-nications of the ACM, April 2008, Vol. 51 No.4

[17] UNPAN 2008, From e-Government to Connected Governance. United Nations e-Government Survey 2008, United Nations New York. Retrieved on April 15, 2013 from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf

[18] Shore B., Venkatachalam A.R., Solorzano E., et al.: 2001, "Softlifting and piracy: behavior across cultures", Technology in Society, 23 (2001), 563-581.

[19] Thomson E.S. and Laing, A.W., The Net Generation: children and young people, the Internet and online shopping, Journal of Marketing Management, 2003, 19, 491–512

[20] Teo T.S.H. and Lim V.K.G., Gender differences in internet usage and task preferences, Behaviour and Information Technology, 2004, 19(4), 283-295.

[21] Fisher Y. and Jacob, O.B., Measuring Internet usage: the Israeli case. International Journal of Human-Computer Studies, 2006, 64, 984-997.

[22] Fang X. And Yen, D. C., Demographics and behavior of Internet users in China. Technology in Society, 2006, 28, 363-387.

[23] Jin, K. G., Drozdenko, R., & Bassett, R. (2007). Information technology professionals' perceived organizational values and managerial ethics: an empirical study".Journal of Business Ethics, 71(2), 149-159.

[24] Lau, E.K.W. "An empirical study of software piracy", Business Ethics: An European Review,2003-12 (3), 233-245.

[25] Gupta, P. B., Gould, S. J. & Pola, B. (2004). To pirate or not to pirate: a comparative study of the ethical versus other influences on the consumer's software acquisition mode decision. Journal of Business Ethics, 55(3), 255-274.

[26] Tan, K. S., Chong, S. C., Lin, B. and Eze, U. C. , Internet-based ICT adoption: evidence from Malaysian SMEs, Industrial Management & Data Systems, 2009, 109 (2), 224 – 244..

[27] Maslin, M. and Zuraini, I., **Examining *the influence of demographic factors on ethical awareness : computer use and security*.** In: ETHICOMP 2008, 24-26 September 2008, University of Pavia, Mantua, Italy.

[28] Choi, K. An Empirical Assessment of the Relationships between Demographic Variables and Risk Factors for Computer Crime", *Paper presented at the annual meeting of the ASC Annual Meeting, St. Louis Adam's Mark, St. Louis, Missouri,* Nov 12, 2008, Retrieved from < ttp://citation.allacademic.com/meta/p_mla_apa_research_citation/2/6/1/6/3/p261632_index.html> on 2013-05-06.

[29] Downs, M. D., Ademaj, I. and Schuck, A. M. , Internet security: Who is leaving the 'virtual door' open and why?, First Monday, Volume 14, Number 1 - 5 January 2009.

[30] Symantec, Symantec global Internet security threat report: Trends for July–December 07, Cupertino, Calif.: Symantec, at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf, accessed 14 July 2013.

[31] Feleming N.C., Nellis J.G., Principles of Applied Statistics 2nd Edition, Thomson Business Press, 2000, ISBN: 1-86152-586-9

[32] Seyal A.H, Md. Mohd M.R.,. Rahman N.A., An Empirical Investigation of Use of Information Technology among Small and Medium Business Organizations: A Bruneian Scenario, The Electronic Journal of Information Systems in Developing Countries, Vol 2,2000.

[33] Milton J. S. and Arnold L.C., Introduction to probability and statistics: principles and applications for engineering and the computing Sciences. 2003, McGraw Hill, Boston, MA.

[34] Calhoun K.J., Teng J.T.C. and Cheon M.J., Impact of national culture on information technology usage behaviour: an exploratory study of decision making in Korea and the US. Behaviour and Information Technology, 2002, 21, 293 – 302.

[35] Chirkov V., Ryan R. M. and Kim, Y., Differentiating autonomy from individualism and independence: a self-determination theory perspective on internalization of cultural orientations and well-being. Journal of Personality and Social Psychology, 2003, 84: 97–110.

Siber Güvenliğin Taarruzi Boyutu ve Uluslararası Hukuk Kurallarının Uygulanabilirliği

Hakan Şentürk, C.Zaim Çil, Şeref Sağıroğlu

***Özet*— Son on yılda, kaynağında bizzat devletlerin ya da devlet-destekli aktörlerin bulunduğu geniş çaplı siber saldırılar yaşandığı ve çok sayıda ülkenin alenen veya gizli olarak taarruzi siber yetenekler geliştirdiği açık olarak görülmektedir. Bu çalışmada; özellikle Ülke olarak siber güvenlik stratejimizin ve ilgili eylem planlarının belirlenmesi sürecinde; taarruzi siber güvenlik yetenekleri geliştirmenin öneminin vurgulanması maksadıyla; uluslararası hukuk kurallarının siber güvenliğe uygulanma durumu incelenmiş, ABD'nin bu alanda izlediği politika ve faaliyetleri ele alınmış, Türkiye'deki mevcut durum değerlendirilerek yapılması gerekenler sunulmuştur.**

***Anahtar Kelimeler*—Siber güvenlik, siber hukuk, siber savaş, taarruzi siber güvenlik**

***Abstract*— In the last decade, it has become evident that states or state-sponsored actors are involved in large scale cyber attacks and that many States have been developing offensive cyber security capabilities. In this study; in order to emphasize the criticality of developing offensive cyber capabilities, especially when the National Cyber Security Strategy and relevant action plans are being determined, the applicability of international law on to the cyber warfare has been researched, the United States's policy and activities are reviewed, current situation in Turkey is analyzed and some proposals are made.**

***Index Terms*—Cyber security, cyber law, cyber warfare, offensive cyber security**

I. GİRİŞ

Devletlerarası düzeyde ilk kez 2007 yılında gerçekleşen Estonya Siber Savaşından günümüze kadar olan dönemde, Rusya-Gürcistan (Güney Osetya Anlaşmazlığı), K.Kore-ABD, Çin-Hindistan, İsrail-Lübnan, Mısır gibi pek çok siber saldırı olayı gerçekleşmiştir. Özellikle son 3-4 yıl içerisinde yaşanan, İran nükleer tesislerinin hedef alındığı Stuxnet saldırısı ile başlayan ve onun türevleri olduğu iddia edilen, daha gelişmiş DuQu solucanı, Ortadoğu sistemleri hedef alınan Flame virüsü ve henüz ne olduğu öğrenilemeyen bir savaş başlığı taşıyan Gauss zararlı yazılımı, Suudi Arabistan'da bulunan AramCo şirketinde 30,000 iş istasyonuna zarar veren Shamoon virüsü gibi saldırılar, siber savaşların şiddetinin zamanla daha da artacağını, kullanılan saldırı teknolojilerinin daha da gelişmekte olduğunu göstermekte ve saldırıların kaynağında bizzat devletlerin ya da devlet-destekli aktörlerin bulunduğuna işaret etmektedir.

Özellikle Stuxnet, DuQu, Flame ve Gauss saldırılarının ABD açıklık veri tabanında kayıtlı bulunan ".lnk" isimli aynı açıklığı (CVE2010-2568) kullandığı, USB bulaşma, metin kodlama/çözme algoritması gibi pek çok ortak modülü paylaştığı, sonuç olarak aynı tesislerde, diğer deyişle aynı siber silah fabrikasında ve bir ya da birden fazla devlet desteğiyle üretildiği anlaşılmaktadır [1-6].

Son 10 yılda siber saldırıların gelişimi ele alındığında ilk yıllarda, basit tekniklerle organize olmayan test saldırıları, 2003 yılından itibaren ekonomik güdülerin öne çıktığı saldırılar, 2007 yılından itibaren ise botnet ve bunları kontrol eden komuta kontrol merkezleri aracılığıyla gerek saldırı sayıları ve bant genişlikleri, gerekse de gelişmiş saldırı teknikleriyle gerçekleştirilen siber saldırıların, siber savaşa doğru bir gelişim gösterdiği değerlendirilmiştir [7].

Buna paralel olarak başta ABD olmak üzere, Çin, K.Kore, İsrail, Fransa vb. çok sayıda ülkenin taarruzi siber yetenekler geliştirdiği bilinmektedir [8]. Siber güvenliğin sadece savunma stratejisi ile mümkün olamayacağı [9] bilinmekte olup ülke güvenliği adına, kara, deniz ve hava harekât alanlarında olduğu gibi siber uzayda da taarruzi yetenek geliştirmenin gerekli olduğu değerlendirilmektedir. Bu tür yeteneklerin kullanımı konusunda ise uluslararası hukuk kurallarının siber güvenliğe uygulanabilirliği konusu da üzerinde tartışılması ve çözüm bulunması gereken konuların başında gelmektedir.

Bu çalışmanın amacı; ulusal siber güvenlik stratejisinin ve ilgili eylem planlarının belirlendiği günümüzde, siber güvenliğin taarruzi boyutuna dikkat çekmek, konuya ilişkin literatürdeki uluslararası hukuk nezdinde yapılan yasal zemin tartışmalarını değerlendirmek ve barış zamanı taarruzi amaçlı yetenek geliştirmenin gerekliliği tartışmaktır.

Belirtilen amaçlarla hazırlanan bu çalışmada; uluslararası hukuk kurallarının siber güvenliğe uygulanıp uygulanamayacağı hususu incelenmiş, ABD'nin konuya ilişkin yaklaşımı ve faaliyetleri ele alınmış, Türkiye'deki mevcut durum değerlendirilerek yapılması gerekenler belirlenmiştir.

Manuscript received July 14, 2013.

Hakan ŞENTÜRK, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara. (Tlf: 312-414-2631; e-mail: hsenturk@hvkk.tsk.tr).

Celal Zaim ÇİL, Çankaya Üniversitesi Elektronik ve Haberleşme Mühendisliği, Ankara (e-mail: czaimcil@cankaya.edu.tr).

Şeref SAĞIROĞLU, Gazi Üniversitesi Bilgisayar Mühendisliği, Ankara (e-mail: ss@gazi.edu.tr)

II. ULUSLARARASI HUKUKUN SİBER GÜVENLİĞE UYGULANABİLİRLİĞİ

Uluslararası Hukuk'un iki ana kaynağı, örf ve adet hukuku ile yazılı kaynaklardır. Yazılı kaynaklar açısından, siber güvenlik alanında uluslararası tek sözleşme Avrupa Konseyi tarafından 2001 yılında hazırlanarak 2004 yılında yürürlüğe giren Avrupa Siber Suç Sözleşmesidir [10]. ABD'nin 2006 yılında imzaladığı, Rusya'nın ise imzaya yanaşmadığı Avrupa Siber Suç Sözleşmesinde 5 asli Siber Suç tanımlanmıştır:

- Yetkisiz erişim (illegal access)
- Yetkisiz müdahale (Illegal interception)
- Veri engelleme/karıştırması (Data interference)
- Sistem engelleme/karıştırması (System interference)
- Cihazların amacı dışında kullandırılması (Misuse of devices)

Asya Pasifik Ekonomik İşbirliği (APEC) 2002 tarihli Siber Güvenlik Stratejisi"nde, Avrupa Siber Suç Sözleşmesi, siber güvenlik alanındaki ilk çok taraflı yasal belge olarak tanınmaktadır [11].

Siber güvenliğin taarruzi boyutu ve bunun devletlerarasında kullanımı söz konusu olduğunda başvurulması gereken temel kaynak, Birleşmiş Milletler (BM) Sözleşmesidir. BM Sözleşmesi'ne göre ülkelerin kendi sınırları dışında kuvvet kullanımına dört istisna halinde izin verilmiştir. Bu istisnalardan ikisi BM'nin kuruluş yıllarına ait olduğundan günümüzde sadece iki istisnadan bahsetmek mümkündür:

a. Meşru müdafaa halinde kuvvet kullanımı (Madde 51)
b. Güvenlik Konseyi kararıyla kuvvet kullanımı (VII. Bölüm)

BM Şartı'nın 51. Maddesi meşru müdafaa hakkını şu şekilde tanımlamaktadır: "Bu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez" [12].

Görüldüğü üzere; meşru müdafaa halinde kuvvet kullanımı ancak bir ülkeye karşı "Silahlı Saldırı (Armed Attack)" söz konusu olması durumunda ortaya çıkmaktadır. Siber güvenlik alanındaki yasal zemin tartışmaları da bu alanda yapılmaktadır [13]. Geçmişte yaşanan, devlet destekli olduğu kuvvetle muhtemel siber saldırıların silahlı saldırı kapsamına girip girmeyeceği, bir saldırının silahlı saldırı sayılabilmesi için hangi şartta ve özellikte olması gerektiği üzerinde uzlaşılmış bir genel yargı bulunmamaktadır.

Stratejik ve Uluslararası Çalışmalar Merkezi uzmanı J. Lewis, bir siber saldırının silahlı saldırı kabul edilebilmesi için sonuçlarına bakılması gerektiği, eğer siber saldırı sonucu oluşturulan etki, geleneksel saldırı sonucu oluşturulan etki ile aynı ise, siber saldırının da diğeriyle aynı kurallara tabi olması gerektiğini belirtmiştir. Örneğin, deniz ablukası ile oluşturulabilecek ticaret kaybı, bir siber saldırı sonucunda da oluşturuluyorsa, bu durumda siber saldırının, silahlı saldırı olarak kabul edilmesi gerektiği ve misilleme hakkı doğurması gerektiğini belirtmektedir [14]. Bu görüşe paralel olarak ABD Dışişleri Bakanlığı Hukuk Danışmanı Harold Koh, 18 Eylül 2012 tarihinde ABD Siber Komutanlığı tarafından düzenlenen bir konferansta ilk kez konu hakkındaki ABD pozisyonuna yönelik önemli açıklamalar yapmış, siber saldırının, silahlı saldırı olarak kabul edilebilmesi için siber harekatın sonuçlandıracağı fiziksel etkinin önemli olduğu, ölüm, yaralanma yada önemli derecede etki yaratacak tahriple sonuçlanan siber operasyonların kuvvet kullanımı olarak kabul edilebileceğini ifade etmiştir [15].

Alandaki yasal boşluğu doldurmaya hizmet amacıyla Tallinn/Estonya'da bulunan NATO İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi öncülüğünde oluşturulan uluslararası uzmanlar grubu tarafından "Uluslararası Hukukun Siber Savaşa Uygulanması Üzerine Tallinn El Kitabı" (Tallinn Manual on the International Law Applicable to Cyber Warfare) isimli doküman hazırlanarak 2013 yılında yayımlanmıştır [16]. Doküman, geçmişte uluslararası hukuk kurallarının deniz, hava ve füze savunmasına uygulanması üzerine hazırlanan San Remo El Kitabı ve Harvard dokümanlarının oluşturulmasında izlenen yöntem takip edilerek hazırlanmış olup kuvvet kullanımı ve silahlı çatışma hukukuna ilişkin uluslararası kuralların siber savaşa uygulanma durumunu incelemek suretiyle hükümetler için siber savaş hukuku alanında bağlayıcı olmayan, çalışmaya katılan uzmanların görüşlerini yansıtan bir referans kaynak niteliğindedir.

Tallinn El Kitabı [16], siber savaşı, uluslararası hukukun iki temel prensibi olan kuvvete başvurma hakkı (jus ad bellum) ile kuvvete başvurulduğunda uyulması gereken çatışma kuralları (jus in bello) normları [17] açısından değerlendirmekte, kuvvet kullanımı seviyesinin altında kalan siber suçlar vb. kavramları kapsam dışı tutmaktadır. Ayrıca El Kitabı, siber harekatlara karşı yapılan siber harekatları temel almış; örneğin bir devletin kritik altyapılarına ya da komuta kontrol merkezine karşı başlatılan siber harekatı uluslararası hukuk açısından incelemiş, ancak benzer bir hedefe yapılan hava taarruzunu kapsam dışında tutmuştur. Bu çerçevede, El Kitabı'nda, aşağıda listelenen 7 bölüm altında, çalışmaya katılan tüm uzmanların üzerinde uzlaştığı 95 adet kural belirlenmiştir. Ana bölümlerin başlığı aşağıda verilmiştir. Bunlar:

1. Devletler ve Siber Uzay
2. Kuvvet Kullanımı
3. Genel Silahlı Çatışma Hukuku
4. Düşmanca Davranma
5. Belirli Kişi, Nesne yada Faaliyetler
6. İşgal
7. Tarafsız Kalma

El Kitabının hazırlanmasında ABD; Kanada, İngiltere ve Almanya'nın askeri dokümanlarından faydalanıldığı belirtilmiştir. Dokümanın hazırlanması üç yıl sürmüş olup,

üzerinde uzlaşıya varılamayan hususlar da not edilmiştir. Örneğin, silahlı çatışma hukuku kapsamında orantılılık prensibinin uygulanmasına yönelik; askeri ve sivil amaçların ve hedeflerin ayrılması gerektiği ve örneğin askeri veri işleyen sivil bir sunucunun askeri hedef olabileceği üzerinde uzlaşılabilmişken, savaşı destekleyen unsurların askeri hedef olması hususundaki ABD yaklaşımı benimsenmemiş, uzmanlarca askeri avantaj kazandıracak hedefler savaşan ve savaşı destekleyen unsurlarla sınırlandırılmıştır. Bu kapsamda örneğin, savaşa mali kaynak için petrol tesislerine ihtiyacı olan bir ülkenin petrol tesisleri, ABD ve az sayıda uzmanın pozisyonuna göre askeri amaç olup silahlı çatışma hukukuna uygunken, çoğunluğun görüşü aksi yönde olmuştur [18]. Dolayısıyla görülmektedir ki, el kitabı temel hukuk prensipleri üzerinde yol gösterici olsa da belirlenen kuralların yorumlanması ve uygulanması ülkeden ülkeye farklılık gösterebilmektedir.

İncelenen yayınların, literatürde uzun soluklu devam edecek çalışmaların ilk ürünleri olduğu görülmüştür. En genel anlamda; her ne kadar Greenberg "Uluslararası hukukta yasaklanmayan herhangi bir hususa, aynı hukuk kurallarına göre izin verildiğini söylemek yanlış olmaz" [19] şeklinde genel geçer bir kural olduğunu belirtse de özellikle ABD politikalarını yansıtan Koh konuşması ve Tallinn El Kitabı bu alandaki pek çok belirsizliği tartışmak suretiyle açıklığa kavuşturabilmiştir. Bundan sonra, yapılması gereken BM sözleşmesindeki "Kuvvet Kullanımı" ve "Silahlı Saldırı" normları temel alınarak uluslararası bir yasal rejim zemini oluşturabilmektir. Uluslararası bir anlaşma hazırlanarak [20], tanımlanacak kuralların uygulanmasını temin ve kontrol edecek politik organizasyonların oluşturulması da söz konusu olabilecektir [21]. Rusya'nın önderliğini yaptığı bir diğer düşünce akımı ise siber savaş silahlarının kısıtlanması hususu olup [21,22] siber silahların etkilerinin artarak hissedilmesi durumunda yakın gelecekte uluslararası anlaşmalarda gündem maddesi olabilecektir.

İncelenen çalışmalar göstermiştir ki, siber güvenlik alanında taarruzi yeteneklerin geliştirilmesine engel bir yasa, kanun ya da anlaşma bulunmamaktadır. Bu yeteneklerin uluslararası hukuk kuralları çerçevesinde nasıl kullanılacağına ilişkin kurallar da bağlayıcı olmamakla beraber üç yıllık süren bir çalışma sonucunda oluşturulan Tallinn El Kitabı'nda tanımlanmıştır. Bu doğrultuda da başta ABD olmak üzere pek çok ülkenin hem savunma hem de taarruzi amaçlarla insan gücü yetiştirdiği ve yetenek kazandığı görülmektedir. Siber silah üretimi konusunda henüz erken olduğunu düşünmenin yanlış olduğunu belirtmekte fayda vardır [23].

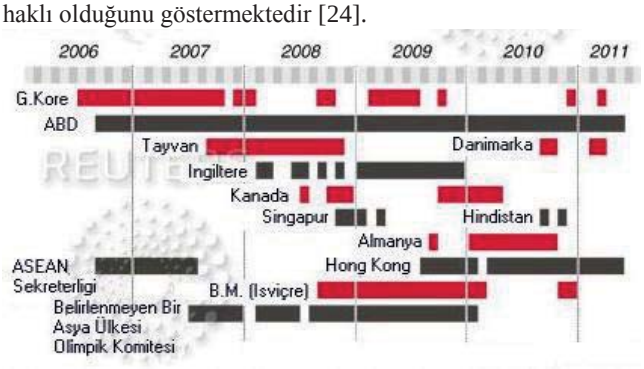
Sonraki bölümde açık kaynaklarda faaliyetlerine ilişkin diğer ülkelere nazaran daha fazla bilgi bulunabilen ABD'nin siber güvenliğin taarruzi boyutuna yaklaşımı ve bu alandaki gelişmeleri incelenecektir.

III. ABD'NIN YAKLAŞIMI ve ÖNEMLİ GELİŞMELER

ABD'de 11 Eylül 2001 saldırılarından sonra Bush yönetimi tarafından oluşturulan yeni ulusal güvenlik stratejisinin önemli ögesi önleyici saldırıdır. Uluslararası hukuka uygunluğu tartışmalı halde olan ve son yıllarda Obama yönetimi tarafından bırakılması tartışılan doktrine göre, ABD, kendisine tehdit teşkil ettiğini değerlendirdiği her unsura karşı kuvvet kullanımını "meşru müdafaa halinde kuvvet kullanımı" ile benzeştirmekte ve bu suretle yasallaştırmaktadır.

Özellikle son iki-üç yıl içerisinde ABD NSA Direktörü ve Savunma Sekreteri tarafından yapılan basın açıklamalarında, "siber 9/11", "siber pearl harbor", gibi ifadeler kullanılarak, siber uzayın kara, deniz, hava ve uzaydan sonra beşinci harekât alanı olduğu ve bu sebeple 2011 strateji belgesinde de ifade edildiği üzere diğer dört harekât alanındaki gibi, siber uzay üstünlüğünün sağlanması için gerekli yetenek geliştirme faaliyetlerinin icra edilmekte olduğu, açıkça dile getirilmektedir.

Şekil 1.de 2006-2011 yılları arasında ülkelerin maruz kaldığı önemli saldırılara ilişkin tarih çizelgesinde ABD'nin tüm zamanlarda saldırı altında olduğu görülmektedir. Bu durum, ABD üst yönetimi tarafından yapılan açıklamaların haklı olduğunu göstermektedir [24].



Şekil 1. 2006-2011 Yılları Arasında Ülkelerin Maruz Kaldığı Siber Saldırılar [24].

Ulusal Savunma Yetkilendirme Yasası'nın 2012 yılı için onaylanmış metninde ABD'nin taarruzi siber harekâtlarının dayandırıldığı yasal zemin şu şekilde belirtilmiştir [25]:

"Kongre, Ülkemizi, Müttefiklerimizi ve milli çıkarlarımızı korumak amacıyla Savunma Bakanlığı'nın siber uzayda taarruzi harekât icra etmek için gerekli yeteneklere sahip olduğunu ve ABD Başkanı'nın aşağıda belirtilen iki hususa bağlı olarak vereceği direktif üzerine gerekli taarruzi harekâtları icra edebileceğini teyit etmektedir:

(1) Savunma Bakanlığı'nın kinetik yetenekler için silahlı çatışma hukuku da dahil olmak üzere izlediği politika prensipleri ve yasal rejimler,

(2) Savaş Üst Kararı (War Powers Resolution) (ABD Başkanı'nın Kongre onayı olmadan savaş ilan edememe yetkisi).

Birinci maddede bahse geçen politika prensipleri ve yasal rejimler ABD Dışişleri Bakanlığı Hukuk Danışmanı Harold Koh'un, 18 Eylül 2012 tarihinde ABD Siber K.lığı tarafından düzenlenen bir konferansta yaptığı yazılı konuşma metninde açıklanmıştır [15]. Ulusal Savunma Yetkilendirme Yasası'nın 2013 yılı için onaylanmış metninde ise her üç aylık dönemde icra edilen taarruzi siber harekatlar için Senato'ya brifing verilmesi hususu belirtilmiştir [26].

ABD Başkanı tarafından açıklanan 2010 tarihli Ulusal Güvenlik Stratejisinde, siber güvenlik tehditlerinin ülke

olarak karşı karşıya olunan en ciddi milli güvenlik, kamu güvenliği ve ekonomik zorluk olduğu belirtilmiştir [27].

Mayıs 2011 tarihli "Siber Uzay için Uluslararası Strateji" isimli strateji belgesinde askeri açıdan 21.yüzyılın tehditlerine hazırlanma, internetin yönetimi ve yetenek geliştirme belirlenen politika öncelikleri arasındadır. Ayrıca, dokümanda Birleşmiş Milletler Sözleşmesi'ne uygun olarak siber uzayda saldırgan davranışlara karşı ABD'nin meşru müdafaa hakkı bulunduğu belirtilmiştir [28].

ABD Savunma Bakanlığı (Department of Defense- DoD) tarafından hazırlanan, "Siber Uzayın İşletilmesi için Savunma Bakanlığı Stratejisi" isimli 2011 Temmuz tarihli belgede ise beş stratejik inisiyatif tanımlanmış olup ilkinin, siber uzayın harekât alanı kabul edilmesi, bu kapsamda DoD tarafından siber uzayın tüm avantajlarından faydalanabilmek maksadıyla kara, hava, deniz ve uzay harekat alanlarında yapılan faaliyetlere paralel olarak siber uzayda da gerekli düzenlemelerin, eğitimlerin ve teçhizatlanmanın yapılması gerektiği belirtilmiştir [29].

Bir diğer strateji dokümanı olan "Kapsamlı Ulusal Siber Güvenlik İnisiyatifi" (Comprehensive National Cybersecurity Initiative-CNCI) dokümanı, 2008 yılında Bush yönetimince "GİZLİ" gizlilik derecesinde hazırlanmış ancak; 2010 Mart ayında bir bölümünün gizlilik derecesi indirgenerek kamuya açılmıştır. Dokümanda; askeri, sivil ve hükümet bilgisayar ağları ve sistemlerinin ve kritik altyapıların korunması ile siber savaşa karşı izlenilecek saldırgan stratejilere ilişkin hükümetin kapsamlı stratejisini kapsayan 12 adet direktif yer almaktadır. Planın kamuya açılan kısmında hükümete bağlı bilgisayar ağlarının korunmasına ilişkin kullanılan Einstein 2 ve Einstein 3 programları altında kurulması planlanan saldırı tespit sistemleri sensörleri ve çoğunluğu özel sektör tarafından işletilen ve kontrol edilen ülke kritik altyapılarının korunmasına ilişkin hükümetin rolü yer almaktadır. Einstein 2 programı, federal ağlara giren ve çıkan tüm ağ paketlerinde tehdit içeren imzaların tespiti amacıyla araştırma yapılmasını; tespit edilen tehdit emarelerinin ABD Bilgisayar Olaylarına Müdahale Ekibi (BOME) merkezine (US-CERT) gerçek zamanlı olarak iletilmesi suretiyle bir siber savaş erken uyarı sisteminin kurulmasını; Einstein 3 ise USCERT'e ilave olarak Ulusal Güvenlik Ajansı (NSA) gibi çeşitli federal başkanlık ve ilgili birimlerle gerçek zamanlı olarak veri paylaşımını da kapsayan bir sistemin kurulmasını öngörmektedir [30].

Çift şapkalı olarak Ulusal Güvenlik Ajansı (National Security Agency-NSA) ve ABD Siber Komutanlığı (USCYBERCOM) direktörü olan General Keith Alexander tarafından ABD'nin siber taarruz gücüne ihtiyacı olduğu basına da açıklanmıştır [31]. Nitekim, Savunma Sekreteri Mr. Leon Panetta tarafından basına yapılan açıklamada da, sadece gelişmiş korunma yöntemleri ile ülkeye yapılması muhtemel saldırıların önlenemeyeceği, ülke topraklarına veya vatandaşlarına zarar verecek saldırıların gerçekleşmesi durumunda, ABD'nin de ülkesini korumaya yönelik farklı seçeneklerinin bulunması gerektiği açıklanmıştır [32].

Aralık 2011'de ABD'de imzalanan Ulusal Savunma Yetki Kanunu ile siber saldırı amaçlı operasyonlara yetki tanınmış, bu kapsamda ABD'nin taarruz amaçlı siber yetenek geliştirmesinin onaylandığı açıklanmıştır [33]. Basına ayrıntıları açıklanmayan Pentagon tarafından başlatılan ve DARPA tarafından icra edilecek olan Plan X projesi kapsamında, ABD tarafından taarruzi amaçlı siber yetenek geliştirildiği medyada yer alan haberler arasındadır [32]. Plan X projesinin amacı, siber uzayın anlaşılması, yönetilmesi ve planlanması için yeni, devrimsel teknolojiler geliştirmek olarak tanımlanmıştır. Ağustos 2012 tarihinde yapılan bir basın açıklamasında da ABD Hava Kuvvetleri Siber K.lığı tarafından hasmın siber uzayı kendi avantajına kullanamaması için, siber uzay yeteneklerinin imhası, azaltılması, caydırılması, aldatılması, bozulması ya da el konulması amacıyla yeni fikirler arandığı açıklanmıştır. Nitekim, ABD Hava K.K.lığı, siber uzayda üstünlüğün kazanılması amacıyla 2013 yılı bütçesi için 4 milyar ABD doları talep etmiştir [34].

ABD Kara K.K.lığının İstihbarat ve Bilgi Harbi Direktörlüğü tarafından hazırlanan bir proje kapsamında elektronik harp ve siber savaş teknolojilerinin entegrasyonu sayesinde kapalı şebekelere sızma amacıyla bir demo programı yürütüldüğü açıklanmıştır. İki yıl sürmesi planlanan projenin ayrıntıları açıklanmamakla beraber adının Taktik Elektromanyetik Siber Savaş Demo Programı olduğu açıklanmıştır [35].

Ekim 2012 ayı içerisinde Pentagon tarafından, ABD'ye yapılan siber saldırılara ABD tarafından aynı şekilde siber saldırılarla cevap verileceği açıklanmıştır. Bu açıklama daha önce yapılan siber saldırıların savaş sebebi kabul edileceği ve karşılığında ABD'nin siber uzayda ya da diğer şekilde askeri operasyonlarla cevap verme hakkının bulunduğuna [36] yönelik açıklamalarla örtüşmektedir. 2013 yılı için hazırlanan ve Başkan Obama tarafından 02 Ocak 2013 tarihinde imzalanarak yasalaşan Ulusal Savunma Yetkilendirme Yasası metninde, Savunma Sekreterliği tarafından, üç ayda bir, siber uzayda icra edilen tüm taarruzi ve önemli savunma harekâtları hakkında bilgilendirme yapılması gerektiği ifadesi bulunmaktadır [37].

Sonuç olarak, ABD'de gerek insan gücü yetiştirme gerekse diğer taarruzi yetenek geliştirme faaliyetlerinin [3] artık kamuoyunda da açıkça dile getirildiği, dolayısıyla siber taarruzların askeri plan, program ve doktrinlerde yer almaya başladığı değerlendirilmektedir.

Sonraki bölümde Türkiye'de son dönemde siber güvenlik ve özellikle siber güvenliğin taarruzi boyutuna ilişkin gelişmeler ele alınmıştır.

IV. TÜRKİYE'DEKİ DURUM

Ülkemizde siber güvenlik yapılanma faaliyetleri kapsamında;

- Temmuz 2012'de TÜBİTAK BİLGEM'e bağlı Siber Güvenlik Enstitüsü kurulmuş,
- Eylül 2012'de TSK Siber Savunma Merkezi Başkanlığı,
- 20 Ekim 2012 tarihinde Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin 2012/3842 sayılı Bakanlar Kurulu kararı Resmi Gazete'de yayımlanmış,

- Ekim 2012'de ise Siber Güvenlik Kurulu kurulmuş ve ilk toplantısını 20 Aralık 2012'de icra etmiş,
- Mayıs 2013 tarihinde Siber Güvenlik Kurulu ikinci toplantısını yapmış, Telekomünikasyon İletişim Başkanlığı (TİB)'na bağlı Ulusal Siber Olaylara Müdahale Merkezi (USOM) faaliyete başlamış,
- 20 Haziran 2013 tarihinde Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı resmi gazetede yayımlanmıştır [38-41].

2012/3842 sayılı Bakanlar Kurulu kararı ile; Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak başta olmak üzere ana koordinasyon ve sorumluluk Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na (UDHB) verilmiştir. Ayrıca, bahse konu karar ile, siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Gnkur.Bşk.lığı MEBS Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile sorumlu bakanlıkça belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur [40].

Ülkemizi etkileyebilecek tehditlere karşı, 7 gün 24 saat müdahale esasına göre çalışan Ulusal Siber Olaylara Müdahale Merkezi (USOM), kendisine bağlı Sektörel Siber Olaylara Müdahale Ekiplerini (SOME) eğitmekte ve UDHB ve ilgili kuruluşlara ait 34 web sitesini siber saldırılara karşı izlemektedir [39].

Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda 29 eylem maddesi belirlenmiş [41], belirlenen 29 eylem maddesinde taarruzi yeteneklerin geliştirilmesine yönelik açık bir ifade bulunmamaktadır.

Siber savunmaya yönelik balküpü kurulması, çeşitli eğitim ve Ar-Ge projeleri bulunmakta olup SSM Müsteşarlığı ile STM A.Ş. arasında 23 Temmuz 2012 tarihinde Bilgi Güvencesi ve Siber Savunma yeteneklerinin kazanılması amacıyla "Bütünleşik Siber Güvenlik Sistemi" Fizibilite Çalışması Sözleşmesi imzalanmıştır. Fizibilite çalışması kapsamında konsept doğrulama amacı ile, sınama ortamı üzerinde çalışan prototip bir ürün geliştirilecek ve Ağ Destekli Yetenek kapsamında kullanılabilecek siber savunma sistemleri, yazılımları ve süreçlerini kapsayan bir fizibilite raporu hazırlanacaktır [42].

Meclis İnternet Komisyonu'nun Aralık 2012 ayında açıklanan bin on bir sayfalık raporunda, TSK bünyesinde siber ordu kurulması önerilmiştir. Komisyonun Meclis Başkanlığı'na sunduğu raporda, acilen ulusal siber güvenlik, ulusal bilgi güvenliği stratejileri ve eylem planları oluşturulmasının yanı sıra, "savaş halinde düşman ülke bilgi sistemlerini hedef alacak siber saldırıların Silahlı Kuvvetler bünyesinde teşkil edilecek siber komutanlık birimlerince yapılması ve bu amaçla gereken altyapının kurulması" da önerilmiştir [43].

25 Aralık 2012-11 Ocak 2013 tarihleri arasında gerçekleştirilen 2'nci Siber Güvenlik Tatbikatı sonrasında Ulaştırma, Denizcilik ve Haberleşme Bakanı, savaşların artık topla tüfekle değil, bilişim teknolojileriyle yapıldığını bildirerek, Türkiye'de, hem askeri anlamda hem sivil anlamda bu tehditle ilgili gerekli adımlar atılmaya başlandığını, siber tehlikenin gelecekte daha da önemli hale geleceğini ve siber saldırı konusunda devletlerin farkındalık bakımından aralarında uçurum olduğunu ifade etmiştir [44].

V. SONUÇ

Siber savaş her geçen gün önemini daha da artırmaktadır. Haziran 2013'de icra edilen NATO Savunma Bakanları toplantısı kapsamında İttifak, tarihinde ilk kez siber savunmayı, ayrı bir oturumda ele almıştır. Önemini her geçen gün artıran siber savaşta kullanılan teknolojiler, nükleer teknoloji gibi birkaç ülkenin tekelinde bulunmamaktadır. Bütün ülkeler veya belli gruplar tarafından bu teknoloji kullanılarak siber saldırılar icra edilebilmektedir.

Türkiye'nin siber savaşlara hazırlanması kapsamında, yazarların 5'nci Bilgi Güvenliği ve Kriptoloji Konferansı'nda sunduğu önerilere [8] ilave olarak aşağıdaki somut önerilerin dikkate alınmasının uygun olacağı değerlendirilmektedir:

- Siber uzayın bir harekât alanı olduğunun kabul edilmesi ve bunun Milli Güvenlik Siyaset Belgesi'ne dahil edilmesi (bu sayede TSK'ya hem savunma hem de taarruzi yetenek geliştirme direktifi verilmesi),
- Bu doğrultuda başta TSK olmak üzere gerek savunma gerek taarruzi siber yetenekler konusunda uzmanlaşmış insan gücü yetiştirmesi,
- Harekât ihtiyacı analizi yapılarak gerekli yetenek boşluklarının çıkarılması ve ilgili projelerin başlatılması,
- Ulusal çapta gerçekleştirilebilecek bir teknoloji yol haritası uygulaması sonucunda savunma ve saldırı amaçlı kullanılabilecek kritik siber teknolojilerin belirlenerek milli olarak geliştirilmesinin sağlanması
- Ulusal Kritik Altyapıların korunması amacıyla müşterek (kamu-özel sektör) SOME'lerin kurulması, başta bünyesinde kritik altyapı barındıran Bakanlıklar olmak üzere tüm Bakanlıkların Siber Güvenlik Stratejik Planlarını oluşturmaları,
- Ulusal ve uluslararası siber güvenlik tatbikatlarına aktif olarak katılınması,
- Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'ndaki 29 numaralı "Siber Güvenliğin Milli Güvenliğe Entegrasyonu" eylem maddesinin revize edilerek milli güvenliği sağlayan kara, deniz ve hava gücüne yönelik izlenen milli güvenlik stratejisinin siber uzay ve siber güvenlik alanında da aynı şekilde izlenmesinin sağlanması,
- Bu konuda yetişmiş insan gücüne duyulan ihtiyacın karşılanması için gerek akademilerde ve gerekse üniversitelerde çalışmalar yapılması.

Sonuç olarak, siber güvenlik alanında taarruzi yeteneklerin geliştirilmesine engel bir yasa, kanun ya da anlaşma bulunmadığı açıktır. Siber uzayın, ABD'de olduğu gibi, harbin beşinci boyutu olarak tanımlanması durumunda, diğer dört boyutun kurallarının siber uzaya da uygulanması gerektiği, bu durumda barış zamanında taarruzi yetenek geliştirmenin siber uzayda üstünlüğün elde edilmesi için kritik öneme sahip olduğu değerlendirilmektedir.

Ulusal Siber Güvenlik Stratejisi kapsamında, siber güvenliğin sağlanması için savunma stratejisinin uygulanmasının, saldırı tekniklerinin her geçen gün gelişmekte olduğu, gerek işletim sistemi gerekse kullanılan uygulama yazılımları ve donanımlarda ortaya çıkarılan sıfır gün açıklıklarının hedefli saldırılarda kullanıldığı düşünüldüğünde, hiçbir zaman yüzde yüz başarı getirmeyeceği bilinmelidir.

Meydansız muharebe olarak tanımlanan siber savaşların kazanılmasının yolunun bu ortamlarda bilgi birikimi, deneyim, yetişmiş insan gücü ve yeteneklerin geliştirilmesi, uzmanlaşma ve önceden hazırlanma ile kazanılacağının farkında olunmalıdır.

Bu bildirinin ihtiva ettiği hususlar, yazarların şahsi görüşleri olup, kurumlarının resmi görüşlerini yansıtmamaktadır.

KAYNAKLAR

[1] Zetter, K., "State-Sponsored Malware 'Flame' Has Smaller, More Devious Cousin", 15 Ekim 2012, erişilme tarihi 12 Temmuz 2013, <http://www.wired.com/threatlevel/2012/10/miniflame-espionage-tool/>

[2] Raiu, Costin., Emm, David., "Kaspersky Security Bulletin 2012. Malware Evolution", 5 Aralık 2012, erişilme tarihi 12 Temmuz 2013, <http://www.securelist.com/en/analysis/204792254/>

[3] Mulrine, A., "Pentagon's Plan X: How it could change cyberwarfare" , 12 Ekim 2012, erişilme tarihi 6 Temmuz 2013, <http://www.csmonitor.com/USA/Military/2012/1012/Pentagon-s-Plan-X-how-it-could-change-cyberwarfare/>

[4] Zetter, K., "Researchers Connect Flame to US-Israel Stuxnet Attack", 06 Kasım 2012, erişilme tarihi 12 Temmuz 2013, <http://www.wired.com/threatlevel/2012/06/flame-tied-to-stuxnet/>

[5] Zetter, K., "Report: US and Israel Behind Flame Espionage Tool", 06 Aralık 2012, erişilme tarihi 12 Temmuz 2013, <http://www.wired.com/threatlevel/2012/06/us-and-israel-behind-flame/>

[6] Gostev, Alexander., "Kaspersky Security Bulletin 2012: Cyber Weapons" 18 Aralık 2012, erişilme tarihi 12 Temmuz 2013, <http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons/>

[7] Chiesa, Raoul. "About Information Warfare: new rules for a new world", Ocak 2011, erişilme tarihi 10 Temmuz 2013, <http://www.chmag.in/article/jan2011/about-information-warfare-new-rules-new-world/>

[8] Şentürk, H., Çil, C. Z., Sağıroğlu, Ş., "Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi", 5'inci Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 15-17 Mayıs 2012, Ankara, Turkey.

[9] Lewis, James A., "Conflict and Negotiation in Cyberspace : A Report of the Public Policy Program", Center for Strategic and International Studies (CSIS), Şubat 2013, <http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf/>

[10] Avrupa Siber Suç Sözleşmesi, <http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm/>

[11] APEC Cyber Security Strategy, Syf.2, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf/>

[12] Birleşmiş Milletler Sözleşmesi Madde 51.

[13] Wallace, David., Reeves, R.Shane, "The Law of Armed Conlict's Wicked Problem: Levée en Masse in Cyber Warfare", International Law Studies, US Naval War College, Vol. 89, 2013

[14] Lewis, James A., "Thresholds for Cyberwarfare", IEE Security & Privacy, Eylül 2011, <http://csis.org/files/publication/101001_ieee_insert.pdf/>

[15] Koh, Harold Hongju, USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, 18 Eylül 2012, <http://www.state.gov/s/l/releases/remarks/197924.htm/>

[16] Tallinn Manual on the International Law Applicable to Cyber Warfare) , Cambridge University Press, ISBN 978-1-107-02443-4, 2013

[17] Aslan, M.Yasin, "Savaş Hukukunun Temel Prensipleri", TBB Dergisi, Sayı 79, 2008

[18] Schmitt, Michael N., "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," 54Harvard International Law Journal. Online13 (2012), <http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/>

[19] Greenberg,L., Goodman, S., Hoo,K., "Information Warfare and International Law", National Defence University Press, 1998

[20] Schjolberg, Stein., "Peace and Justice in Cyberspace : Potential new international legal mechanisms against global cyberattacks and other global cybercrime", Norveç, 2012,

[21] Owens, William A., Dam, Kenneth W. and Lin, Herbert S., "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabıılities", The National Academies Press, Washington, D.C., 2009

[22] Malawer, Stuart, "Cyberwarfare: Law & Policy Proposals for U.S. & Global Governance", (November 18, 2010). Virginia Lawyer, Vol. 58, p. 28, February 2010; GMU School of Public Policy Research Paper No. 2009-11. Available at SSRN: http://ssrn.com/abstract=1437002

[23] Gündoğan, Mete, Prof.Dr., "Siber Silah Endüstrisi ve Türkiye", Siber Güvenlik Konferansı, 22 Aralık 2011, Ankara.

[24] Friedman, Rebecca., "Cyber Attacks Update", 26 Ocak 2012, erişilme tarihi 11 Temmuz 2013, <http://blog.thomsonreuters.com/index.php/tag/cyber-attacks/%EF%BB%BF/>

[25] US National Defense Authorization Act 2012, erişilme tarihi 14 Temmuz 2013, <http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf/>

[26] US National Defense Authorization Act 2013, syf. 257, erişilme tarihi 14 Temmuz 2013, <http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf/>

[27] US White House "National Security Strategy", May 2010, syf 27, erişilme tarihi 14 Temmuz 2013, <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf/>

[28] US White House "International Strategy for Cyber Space", May 2011, syf 10, erişilme tarihi 14 Temmuz 2013, <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf/>

[29] US Department of Defense, "Strategy for Operating in Cyber Space", July 2011, syf. 5, erişilme tarihi 14 Temmuz 2013, <http://www.defense.gov/news/d20110714cyber.pdf/>

[30] US White House, "The Comprehensive National Cybersecurity Initiative", <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative/>

[31] Fransa Basın Ajansı, "NSA director: U.S. needs offensive weapons in cyberwar", 04 Ekim 2012, erişilme tarihi 02 Temmuz 2013, <http://www.rawstory.com/rs/2012/10/04/nsa-director-u-s-needs-offensive-weapons-in-cyberwar/>

[32] Glaser, J., "Pentagon Lays Out 'Offensive Cyber' Attack Policy", 15 Kasım 2011, erişilme tarihi 02 Temmuz 2013, <http://news.antiwar.com/2011/11/15/pentagon-lays-out-offensive-cyber-attack-policy/>

[33] Hoover, Nicholas J., "DARPA Boosts Cybersecurity Research Spending 50%", Information Week, 07 Kasım 2011

[34] Gjelten,T., "First Strike: US Cyber Warriors Seize the Offensive", World Affairs Dergisi, Ocak/Şubat sayısı, erişilme tarihi 04 Temmuz 2013, <http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive/>

[35] FryerBiggs, Z., "Cyber's Next Chapter: Penetrating Sealed Networks", 16 Aralık 2012, erişilme tarihi 03 Temmuz 2013, <http://www.defensenews.com/article/20121216/DEFREG02/312160

002/Cyber-8217-s-Next-Chapter-Penetrating-Sealed-Networks?odyssey=tab%7Ctopnews%7Ctext%7CFRONTPAGE/>
[36] Gorman, Barnes., Barnes, J. "Cyber Combat :Act of War", 30 Mayıs 2011, erişilme tarihi 06 Temmuz 2013, <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html#ixzz1NwkCMvXU/>
[37] Corrin, A., "Defense Bill Emphasize Cyber Operations", 03 Ocak 2013, erişilme tarihi 06 Temmuz 2013, <http://fcw.com/articles/2013/01/03/ndaa-provisions.aspx/>
[38] Türköz, Tahsin, "Ulusal Siber Güvenlik Stratejisi ve Yürütülen Çalışmalar, Siber Güvenlik Konferansı, İstanbul, 17 Mayıs 2013.
[39] Vidinli, İ.B., "Ulusal Siber Güvenlik Çalışmaları ve USOM", Siber Güvenlik Konferansı, İstanbul, 17 Mayıs 2013.
[40] Resmi Gazete, 20 Ekim 2012, <http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm/>
[41] Resmi Gazete, 20 Haziran 2013, <http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf/>
[42] SSM Web Sitesi, erişilme tarihi 06 Ocak 2013, <http://www.ssm.gov.tr/anasayfa/hizli/duyurular/etkinlikler/torenler/Sayfalar/20122507ButSbrGuvSist.aspx/>
[43] Sarıdoğan,Neşe.,Star Gazetesi, 21 Aralık 2012, erişilme tarihi 10 Temmuz 2013, <http://haber.stargazete.com/politika/meclisten-siber-komutanlik-onerisi-geldi/haber-713682/>
[44] TÜBİTAK Web Sitesi, "2.Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı", erişilme tarihi 14 Temmuz 2013, <http://www.tk.gov.tr/sayfa.php?ID=153/>

BOME'lerin Kritik Altyapıların Siber Güvenliğinin Sağlanmasında Kullanımının Etkinleştirilmesi

Melih Durak, İnan Semiz, Selçuk Sönmez

***Özet*—Bilişim teknolojilerinin hızla gelişmesi bu teknolojilerin kritik altyapıların yönetiminde kullanılmasını arttırmıştır. Ancak bu gelişen teknoloji ile yüz yüze kaldığımız siber saldırılar kritik altyapıların korunması sürecinde ülkeleri farklı tedbirler almaya itmiştir. Bu çerçevede Bilgisayar Olaylarına Müdahale Ekipleri (BOME) ulusal seviyede tesis edilmiştir. BOME'lerin güvenlik sürecinde etkin kullanımı saldırıların önlenmesinde büyük önem taşıyacaktır.**

***Anahtar Kelimeler*—Supervisor Control and Data Acqusition Systems (SCADA), Kritik Altyapı, Bilgisayar Olaylarına Müdahale Ekibi (BOME).**

***Abstract*—Fast development of information technologies increase the usage of these technologies in the management of critical infrastructure. However, with the developing technologies we are facing cyber attacks which make countries take differrent precautions for the protection of critical infrastructures. In this regard 'Computer Emergency Response Teams' (CERT) are established in national level. Efficently acting of CERT in cyber security process will play important role in preventing attacks.**

***Index Terms*—Supervisor Control and Data Acqusition Systems (SCADA), Critical Infrastructure, Computer Emergency Response Team (CERT).**

I. GİRİŞ

BİLGİ teknolojilerinin yoğun bir şekilde kullanıldığı kritik altyapılarla ilgili birçok tanımlama yapılmaktadır. Ancak genel olarak bir tanım yapmak gerekirse; yok edilmesi, zayıf bırakılması veya erişilmez kılınması halinde, uzun dönemde, ulusun sosyal ve ekonomik sağlığı üzerinde olumsuz etki bırakacak veya ulusal güvenliği sağlama kabiliyetini etkileyecek fiziksel tesisler, tedarik zincirleri, bilgi teknolojileri ve iletişim ağları [1] olarak tanımlanabilir.

Bütün altyapıların, teknolojik gelişmelerin etkisiyle, birbiriyle bağlantılı ve birbirine bağımlı hale geldiği günümüzde, kamu düzeni, güvenliği ve sağlığı toplumsal refah ve kamu hizmetlerinin sürdürülebilirliği açısından kritik altyapıların korunması hayati önem arz etmektedir. Bir ülkenin kritik altyapısında meydana gelen saldırılar ülkenin diğer kritik altyapılarını da etkileyebilmektedir.

Kritik Altyapılar ülkeden ülkeye farklılık göstermekle birlikte temel olarak Şekil 1.'deki başlıklar altında sıralanabilir [2,3,4].



Şekil 1.Kritik Altyapılar

Kritik altyapıların bilgi teknolojilerinin en önemli özelliği ülkelere coğrafi olarak birbirinden çok uzakta bulunan sistem ve araçları tek bir merkezden daha maliyet etkin bir biçimde kullanmayı sağlamasıdır. Bu kapsamda kullanılan temel sistem dağıtık denetim ve kontrol sistemleri olan SCADA sistemleridir. Bu sistemler en yalın olarak bir merkezden iletim kanalları kullanılarak uzaktaki birimlerin etkinleştirilmesi şeklinde tanımlanabilir. Örnek bir SCADA sistemi Şekil 2.'de gösterilmektedir.

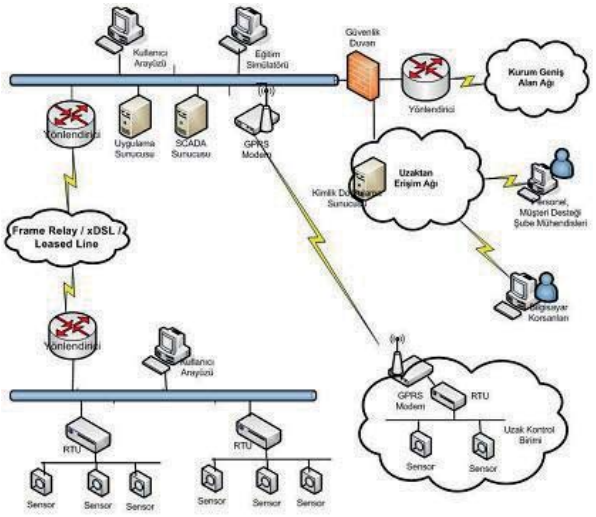
Bir SCADA sistemi,

- Kontrol edilen (makine, tezgâh ya da ardışık işlemlerden oluşan bir sistem),
- Kontrol eden (mikrodenetleyiciler, PLC ya da bilgisayar kumandalı sürücüler),
- SCADA yazılımı (merkezî bir bilgisayara yüklenmiş),
- Ağ elemanları (çoklu sistemler için) olarak özetlenebilir [6].

Melih Durak, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: melihdurak@gmail.com.

İnan Semiz, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: inansemiz@gmail.com.

Selçuk Sönmez, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: selcoksonmez@gmail.com.



Şekil 2. SCADA Sistemi Konfigürasyonu [5].

II. LİTERATÜR TARAMASI

BOME'ler ise bilgisayar ve şebeke güvenliğini izleyen ve siber saldırı mağdurlarına olaylara müdahale hizmeti sunan teknik birimlerdir. BOME'ler, açıklıklara ve tehditlere ilişkin uyarılar ve bilgisayar ve şebeke güvenliğini geliştirmeye yönelik bilgiler yayımlar; farkındalık oluşturma, güvenlik danışmanlığı gibi hizmetleri ve teknolojiyi izleme, güvenlik araçları geliştirme gibi proaktif hizmetlerin yanısıra, siber saldırılara karşı koyma ve bunların yol açtığı zararın azaltılması gibi reaktif hizmetler de sunarlar [7].

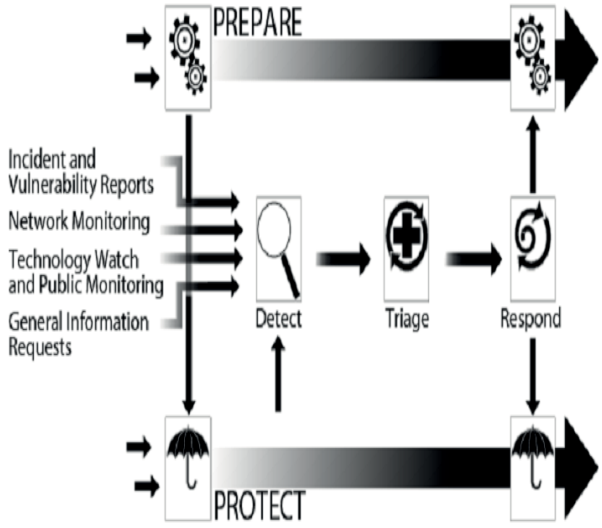
BOME'lerin görev ve sorumlulukları bakacak olursak en yeni tehditlere ilişkin güncel bilgiler sunmak ve ihtiyaç duyan paydaşlara siber saldırılarla mücadele konusunda teknik destek sağlamaktır. BOME'ler tarafından sunulan hizmetler Tablo 1'de gösterilmiştir.

TABLO 1
BOMELER TARAFINDAN SUNULAN HİZMETLER [8].

Reaktif Hizmetler	Proaktif Hizmetler	Güvenlik Kalite Yönetimi Hizmetleri
• Uyarma • Saldırılara müdehale • Saldırı Analizi • Açıklıklara müdehale • Açıklık analizi	• Bilgilendirme • Teknolojiyi İzleme • Güvenlik denetimi ve değerlendirme • Güvenlik yönetimi • Güvenlik araçları geliştirme • Saldırı tespit hizmetleri	• Risk Analizi • İş sürekliliği ve felaket kurtarma • Güvenlik danışmanlığı • Farkındalık oluşturma • Eğitim verme • Ürün değerlendirme veya belgelendirme

Literatürdeki bilgisayar olaylarına müdahale süreçlerine incelediğimizde genel olarak birbirine benzer süreçler ele alınmıştır.

Şekil 3'te beş aşamalı 'Hazırlama, Koruma, Tespit/Tanımlama, Önem derecesine göre ayırma ve müdahale' süreci görülmektedir. Bu temel müdahale süreci olarak literatürde, US-CERT dokümanlarında da belirtilmiştir [9,10].



Şekil 3. Beş Yüksek Seviyeli Olay Yönetim Süreci [9].

Avrupa Birliği'ne baktığımızda bilgisayar olaylarına müdahale süreci Şekil-3'e benzer model aldığı görülmüştür [11].

III. BOME'LERİN KRİTİK ALTYAPILARIN GÜVENLİĞİNİN SAĞLANMASINDA KULLANIMININ ETKİNLEŞTİRİLMESİ

A. *Çalışmanın Amacı*

Kritik altyapılar ülkeler için son derece önemlidir. Dolayısıyla ulusal boyutta siber olaylara müdahale edebilecek yetenekte birimlerin etkin bir biçimde kullanılması siber güvenliğin sağlanmasında en önemli gereksinimlerden bir tanesidir. Bu maksatla bu çalışmada amaç, ulusal boyutta kabul edilmiş kritik altyapıların siber güvenliğinde gerek kritik altyapıyı yöneten kurumların gerekse de BOME'leri yönlendiren kuruluşların etkin bir iletişim içinde siber saldırılara en hızlı biçimde çözüm bulmasına yönelik bir model önerisi sunmaktır.

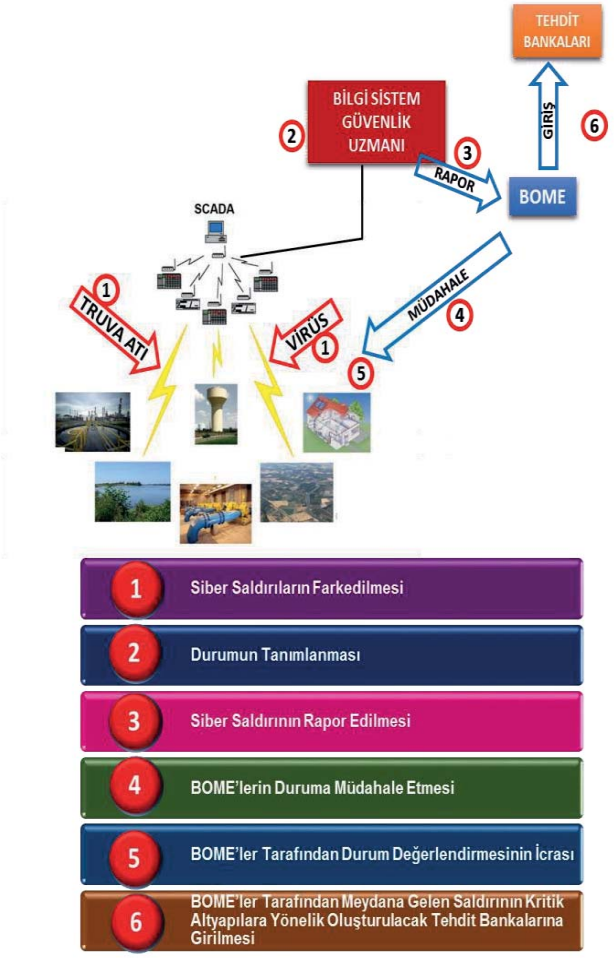
B. *BOME'lerin Kritik Altyapıların Siber Güvenliğinin Sağlanmasında Etkin Kullanım Modeli*

Kritik altyapıların siber güvenliğinin sağlanmasında altı basamaklı model ile siber saldırıların öncelikle fark edilmesi sağlanmış olacak daha sonra da çözüm bulma süreci en kısa sürede tamamlanacaktır. Aşağıdaki Şekil 4.'te süreç adım adım gösterilmektedir.

(I) Siber Saldırıların Fark Edilmesi:

İlk basamak tehdidin farkına varmaktır. Siber saldırı kaynakları ve metotları her geçen gün artmakta ve çeşitlenmektedir. Bu nedenle şüpheci olmak ve sistemde meydana gelen değişimleri iyi gözlemlemek gerekmektedir. Bu maksatla kontrol merkezlerinde vardiya değişimleri büyük önem taşımaktadır.

Ayrıca basit siber saldırıları önleyen ve rapor sunan DDOS Mitigator gibi savunma araçlarının kullanılması bu süreci daha kolay hale getirecektir [12].



Şekil 4. Kritik Altyapıların Siber Güvenliğinde BOME'lerin Kullanım Modeli

(II) Durumun Tanımlanması:

Sistemde meydana gelen aksamanın fark edilmesinden sonraki süreç aksaklığın tanımlanmasıdır. Kritik altyapıların kontrol merkezinde bilgi sistem güvenliğinden sorumlu uzman personelin bulunması tanımlama sürecinde meydana gelen duruma Siber saldırı tanımı konabilmesini sağlayacaktır.

(III) Siber Saldırının Rapor Edilmesi

Eğer meydana gelen aksama ve olay fiziksel ve sistemden kaynaklanmadığı fark edilirse ve bilgi sistem güvenlik personelinin tespiti siber saldırı olabileceği değerlendirilerek bir an önce bu saldırı şüphesinin Ulusal BOME'lere aktarılması gerekecektir. Bu kapsamda Ulusal seviyede belirlenen kritik altyapılar ile BOME'ler arasında bir iletişim altyapısının kurulu olması gerekmektedir.

Bu bildirilerin oluşturulacak olay bildirim formları ile iletilmesi sağlanarak eksik bilgi iletilmesinin önüne geçilecektir.

(IV) BOME'lerin Duruma Müdahale Etmesi:

Sağlanan iletişim kanallarından durumun rapor edilmesi sonucu BOME'ler duruma müdahale eder ve saldırının siber kaynaklı olduğunu tespit ederlerse sorunun çözümüne yönelik aşağıdaki faaliyetleri icra ederler.

- Olay sırasınca olay ile ilgili kanıtların toplanması
- Olay sonrasında kanıtların incelenmesi
- Olay ile ilgili sorumluların belirlenmesi
- Olaya sebep güvenlik problemlerinin (saldırgan tekniği veya açıklık) belirlenmesi [13].

(V) BOME'ler Tarafından Durum Değerlendirmesinin İcrası:

Siber tehditin ortadan kaldırılmasından sonraki aşama bir daha böyle bir saldırının gerçekleşmemesi için alınması gereken tedbirler ve yapılacak işlemlerin değerlendirilmesidir.

Bu süreçte saldırıdan zarar gören kaynakların kurtarılması ve hasarın telafisi yolları araştırılır. Kritik altyapının risk haritası güncellenebilir.

(VI) BOME'ler Tarafından Meydana Gelen Saldırının Kritik Altyapılara Yönelik Oluşturulacak Tehdit Bankalarına Girilmesi

Kritik Altyapılara yönelik saldırıların sınıflandırılması ve daha kolay takibinin ve çözümünün sağlanması maksadıyla meydana gelen saldırılar ve alınan tedbirler oluşturulacak ulusal tehdit bankalarına eklenmelidir. Bu bilgi uluslararası tehdit bankaları ile paylaşılıp diğer ülkelerin tecrübelerinden de istifade edilmelidir. Böylece benzer saldırılarda çözüm bulunması daha kolay olacaktır.

Bu aşamada dünyadaki diğer tehdit bankalarından faydalanılabilir. Örneğin;

- FIRST
- TF-CSIRT
- European Government CERTs [14].

IV. SONUÇ

Bu çalışmada BOME'lerin kritik altyapıların siber güvenliğinin sağlanmasında nasıl kullanılacağı bir model üzerinde gösterilmiştir. Kritik altyapıları yöneten kurumlar tarafından öncelikli olarak yapılması gereken husus sistemin yönetildiği merkezlerde siber farkındalığın yüksek olması ve siber olaylara tanım koyabilecek yetenekte personelin sürekli bulundurulmasının sağlanmasıdır.

BOME'lerin ulusal düzeyde kritik altyapı olarak belirlenen kurumlarla gerek idari gerekse de teknik olarak en hızlı iletişim kanallarını tesis etmesi durumun rapor edilmesi sürecini hızlandıracaktır. BOME'lerin uluslararası tecrübelerden de istifade ederek bir tehdit bankası oluşturması ve bunun sürekli güncel tutulmasının sağlanması karşılaşılacak saldırılarda çözüm adına ışık tutacaktır.

BOME'lerin siber olaylara sistematik bir şekilde müdahale etmesi, durumun en erken şekilde tanımlanarak reaktif ve proaktif önlemlerle tedbir getirilmesi ile kritik altyapılarımız korunmuş olacaktır.

KAYNAKLAR

[1] M. Ünver, C. Canbay, B.H. Özkan, Kritik Altyapıların Korunması, Bilgi Teknolojileri ve koordinasyon Dairesi Başkanlığı Ankara,2010, s.4

[2] National Infrastructure Protection Plan, s.19 , http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[3] Avrupa Komisyonu, "Kritik Altyapıların Korunması için Bir Avrupa Programı,Rapor", http://eurlex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

[4] Bilgi Güvenliği Politika Konseyi, "Kritik Altyapılar için Bilgi Güvenliği Önlemleri Üzerine Eylem Planı, Karar", s.2, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf

[5] D.J. Gaushell, W.R. Block, SCADA communication techniques and standards. Computer Applications in Power, IEEE, 1993, 6.3: s.45-50.

[6] Endüstriyel Otomasyon teknolojileri Scada Sistemleri s.4 http://ytumekatronik.files.wordpress.com/2012/12/scada-sistemleri-1.pdf

[7] S. A. Boyer, SCADA: supervisory control and data acquisition. International Society of Automation, 2009.

[8] M. Ünver, C. Canbay, A.G. Mirzaoğlı, Siber Güvenliğin Sağlanması, Bilgi Teknolojileri ve koordinasyon Dairesi Başkanlığı Ankara,2009, s.41

[9] C. Alberts, A. Dorofee, Georgia Killcrece, R. Ruefle, M. Zajicek, Defining Incident Management Processes for CSIRTs: A Work in Progress,2004, s.25

[10] M. Brown, D. Stikvoort, P. Kossakowski, G. Killcrece ,R. Ruefle, Handbook for Computer Security Incident Response Teams (CSIRTs),2003, s.189

[11] A step-by-step approach on how to o set t up a csırt, European Network and information Security Agency (ENISA), 2006, s.66

[12] http://www.tubitak.gov.tr/tr/haber/siber-saldirilara-karsi-yerli-savunma-araci-gelistirildi,Erişim Tarihi:12.07. 2013

[13] H. Bahşi, Ulusal Bilgi Sistemleri Güvenlik Programı, TÜBİTAK UEKAE İstanbul,2008.s.11

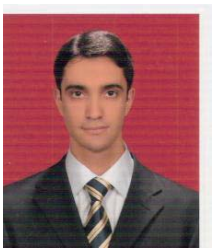
[14] M.Eriş, Bilgisayar Güvenlik Olayları Müdahale Çalışmaları, TÜBİTAK UEKAE İstanbul,2008,s.33



Melih DURAK lisans eğitimini 2004 yılında Sistem Mühendisliği dalında Kara Harp Okulu'nda tamamlamıştır. Yüksek Lisans Eğitimini 2007 yılında Beykent Üniversitesinde Uluslararası İlişikiler dalında yapmıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, Orta Doğu, ve siber savaş konularına ilgi duymaktadır.



İnan SEMİZ lisans eğitimini 2004 yılında Sistem Mühendisliği dalında Kara Harp Okulu'nda tamamlamıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, Avrupa Birliği, ve siber savaş konularına ilgi duymaktadır.



Selçuk Sönmez lisans eğitimini 2004 yılında Sistem Mühendisliği dalında Kara Harp Okulu'nda tamamlamıştır. Yüksek Lisans Eğitimini 2009 yılında İstanbul Üniversitesi'nde Uluslararası İlişikiler dalında yapmıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, Avrupa Birliği, ve siber savaş konularına ilgi duymaktadır.

Data and Endpoint Security in Mobile Computing

Sait Murat GİRAY

***Abstract*—Nowadays laptops, tablets and smartphones have capabilities and abilities once have only been dreamed. Mobile platforms and mobile computing became an inseparable part of daily and professional life. Their widespread use is motivated by the flexibility and productivity they provide as well as rich options of accessing and processing content with them. This new trend and different form factors also present several security risks for the devices and data stored in and/or accessed via them. Data and endpoint security is particularly challenging in corporate world. Current study discusses data on mobile endpoints and provides a comparison of security mechanisms on the basis of convenience, security efficiency and deployment cost against several threats to provide a baseline for mobile network use and deployments.**

***Index Terms*—Cost, Convenience, Efficiency, Endpoints and data security**

I. INTRODUCTION

MOBILE computing includes all portable computing/communication devices with wired/wireless connectivity. Recent hardware and software advances lead to versatile devices and a productive environment. Communication and computation habits have been transformed and became user location oriented. Mobility is very attractive for both casual users and corporate world because of the flexibility and efficiency in data use along with social and business services. However several issues and constraints [1] based on the characteristics of mobility are introduced in several studies such as are performance, connection variability and short battery life. Major mobility challenges [2,3] are disconnection handling, low bandwidth in wireless connections, network heterogeneity and limited user interaction. When a technology becomes popular it attracts both users and malicious parties. Therefore security of user, device and data became a major concern.

Today mobile devices are able to store and process large amounts of data but they are mostly exposed since it is easy to lose or steal them. As a result, unauthorized access to device, data and private networks is very likely if necessary precautions are not taken. One of the best security practices would be removing unnecessary and sensitive information from mobile devices unless proper and explicit permissions are granted for it within organization. Mobile endpoints can easily become a security liability if they are not properly managed. The value of a mobile device stems from the data stored in it and installed applications that enable dedicated services through it. Thus security outshines other challenges considering the proliferation of mobile devices in individual and business use. Mobile devices and data are essentially prone to security risks based on mobility and usage patterns. Typical security concerns of traditional stationary systems such as authentication, authorization, confidentiality, privacy and integrity are also valid in mobile endpoints with resource constraints, battery and connectivity [4, 5] issues.

Threat models are mainly loss, theft or physical damage, unauthorized use, malware vulnerabilities and data leak through eavesdropping or sniffing. Backup, password protection, encryption, authentication, remote management, trusted computing approaches and physical precautions are major countermeasures for end user devices. A combination of them at different levels is required for overall security. Focus of this study is corporate users considering more attractive data on their mobile devices. Awareness and employee training are also a part of security. Reference [6] describes this aspect as "the stage of prescriptiveness, i.e. that users should be intrinsically committed to the security objectives of the organization". Proper security policy management and continuous training will realize this capability.

This paper provides a comparison and an evaluation of security mechanisms for mobile endpoints and data based on convenience, cost and security efficiency from the perspective of a decision authority who would answer the following questions:

-Is it easy for users to adopt the security system?

-Do the solutions provide sufficient security?

-Do the value of data and device justify the incurred costs?

Section 2 describes mobile computing environment while Section 3 details challenges and issues of mobility. Security management challenges are handled in Section 4 and the reasoning for comparison criteria with evaluation of techniques are presented in Section 5 while Section 6 includes the final remarks and the conclusion.

II. MOBILE COMPUTING ENVIRONMENT

All kinds of mobile communication /computation devices and portable data storage are considered in this context. Mobile computing provides almost uninterrupted processing of data and it is more utilized every day because of novel and productive communication, data/service access, processing and storage means. Reference [7] shows a global

Sait Murat Giray is with Turkish Naval Forces Command and Middle East Technical University Computer Engineering Department, Ankara (email: giray.s1778@dzkk.tsk.tr or giray.murat@metu.edu.tr)

surge in smartphone usage. In particular, companies heavily use mobility to keep up with market pace. This fact also reminds us that mobile devices store very precious user and employee data [8] as shown in Fig.1.

Mobility did not yet reach to Weiser's "Ubiquitous computing" concept of full-fledged integration and interaction of information technology (IT) devices and humans [9]. However, current era has several examples of ubiquity such as Google Glass Project [10]. Nowadays it is common to instruct mobile devices with voice command to perform tasks like web searching, making calls and navigating. Schools are equipped with interactive boards, public and private sectors digitize and mobilize their services. Different transactions take place over dozens of mobile applications. Order management, delivery tracking, mobile payment [11], e-mail exchange, marketing, advertising, banking and customer relationship management (CRM) [12] are some examples of what mobility can achieve The list of what we can with mobile services introduces various restrictions and threats in mobile environment.

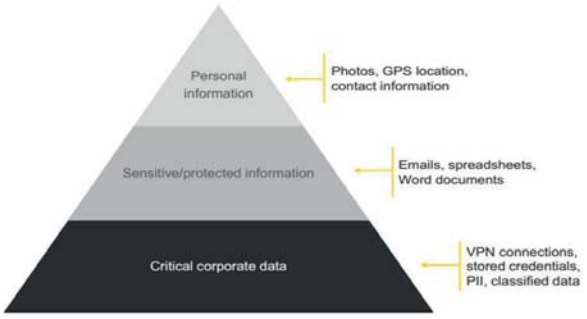


Fig. 1. Mobile devices in corporate environment contain very sensitive data.

III. CONSTRAINTS IN MOBILE COMPUTING

Nowadays smaller, thinner and more powerful devices are at premium. All the efforts in progress serve to eliminate the limitations and obviate inherent challenges of mobile equipment which cause security concerns.

A. Insufficient Resources

Although contemporary mobile devices reached a standard of 2 GHz plus multi-core processor units, tens/hundreds gigabytes of storage along with several gigabytes of memory, they are still considered as resource poor due to size, weight and power consumption limitations [1] which would thwart utilization of a strong security mechanism on the device.

B. Network Heterogeneity

Mobile devices support different communication protocols (Bluetooth, Wireless Fidelity (Wi-Fi), 3G/4G and etc.) and they can rapidly face connection changes. Those shifts may occur within same or different overlapping networks. A marketing agent can talk with a customer on the phone while downloading files simultaneously over a public Wi-Fi with the same device. If it is configured automatically switching to faster/known networks then this endpoint may be exposed to threats in an uncontrolled environment.

C. Connection Fluctuations and Bandwidth Restrictions

Distance to base stations or hotspots and surroundings heavily affect signal quality. Indoors hampers strong signal reception while outdoors puts the device away from the wireless router. Low speeds and connectivity variation may also lead to security threats. An employee may prefer a fast but insecure public Wi-Fi internet rather than intermittent 3G service to send some data. In this scheme, it is apparently easier to interfere with the traffic or impersonate an access point. Therefore employee is more vulnerable to network attacks such as phishing [13] and spoofing [14].

D. Limited User Interaction

User-device interaction is still restrictive on mobile devices mainly because of small sizes and lack of physical input (keyboard, mouse etc.) even though several enhancements such as sliding keypads, touch screens, high resolution displays, voice recognition and customizable user interfaces are introduced. Lack of fast and responsive user interfaces can cause security breaches by making users ignore protections like screen locks.

E. Reliance on External Power

Usability, performance and computation duration of mobile devices depend on battery. Although battery life times are substantially enhanced, they are still in the order of hours and they are heavily affected by usage pattern. For example Wi-Fi is a dominant factor in battery consumption as stressed in CoolSpots study [15] and 3G/4G networks also drain the battery rapidly. Since one cannot always control the environment that he/she plugs in the mobile device, frequent recharges would yield physical threats to device.

IV. SECURITY MANAGEMENT

Since mobile devices became pervasive and affordable, companies hand them out to almost each of their employees. In current market conditions, mobility became a high value asset and a resort to reduce delays and to accelerate service delivery. Neither personnel nor data are any more office bound. Widespread use of mobility is exceeding the organizational boundaries and spanning into ad hoc context which brings a lot of security risks and management problems.

Think about e-mails and financial figures on a smartphone, details of a new state of the art engine in a laptop or a heedless user who saves login credentials of company Virtual Private Network (VPN) client for convenience. In these situations, possession of the device (locally or remotely) directly refers access to private network and/or sensitive data. Necessity of tight security originates from high exposure to different environments. Appropriate management of devices requires clearly specified boundaries between hierarchical levels. A distinctive classification of personnel on an authority and responsibility scale is assumed to exist throughout this study. Otherwise it would be hardly possible to distinguish security exigencies of devices and data at different levels.

A. Threat Model and Countermeasures

Consider an employee who is working at home with a laptop connected to corporate systems. Some data residing only at a company server are required for a report and employee downloads those data to speed up the work. This employee has also a plane to catch so he/she keeps on working at the cab by sharing 3G connection over the smartphone. The report has been completed before getting onboard and it was sent to colleagues over public Wi-Fi as it is faster. Employee used different networks either with some degree of control or none. Considering this scheme, several measures should be utilized for security of the devices and data. Raw data has been processed and became a valuable asset on the go while device was a free pass to the corporate systems. Security of mobile wireless carriers is beyond the scope of this paper.

Major security risks can be classified as physical threats (robbery, loss, damage and unattended use) and cyber threats (unauthorized disclosure or remote access through malware). Since smartphones allow third party applications, malware risk is now valid for them. Countermeasures have a similar categorization too. Physical protection measures consist of being a prudent user, carrying or keeping devices in locked areas and fastening them with cable locks if possible. Mechanisms of cyber domain include encryption, authentication, backup, remote wipe and feature killing, device tracking, anti-malware, system patches and firmware updates.

B. Security Mechanisms

1) Authentication:

It is the process of verifying user identity before granting access to device, data and services. Reference [16] presents a clear classification of authentication by coining the terms "knowledge, possession and property".

a) Single Phase Authentication:

Passwords are the simplest- also cheapest- form of identity confirmation and the most basic component of authentication. Presumably all mobile devices have this function. Password protection may vary among platforms and mobile operating systems but alphanumeric phrases, numerical codes and pattern drawings are commonly used. In addition, visual confirmation with predetermined pictures and prerecorded question-answer pairs are available. Several combinations can be applied to meet the required level of security. A four digit code may suffice to hold some curious friends away from the phone while a banking application deservedly requires a customer ID, a passkey and then combine them with preselected images and location/IP address information.

b) Multi-Phase Authentication:

Passwords can be compromised by guessing, brute force search or over–the–shoulder pries. Multi-phase approach requires possession of a specialized hardware or software as an extra step. USB tokens and credit cards are common examples of physical cards while one time pass code generator applications provide software aided multi-phase authentication. One major disadvantage of them is the very same risks of being forgotten, stolen or lost.

c) Biometrics:

Biometric authentication use unique physical feature such as fingerprint, eye (iris, retina) and voice to verify identity. This concept is explained in four steps as capturing sample, extracting unique data, comparing templates and determining matches and no matches in [17]. It provides top level security and they are generally preferred by high profile organizations like law enforcement, government offices, military services and large industrial enterprises. Biometrics is also used in mobile devices as built-in fingerprint readers or facial recognition software using integrated camera.

2) Encryption:

This procedure converts clear text into unintelligible format which requires a decryption key to reverse the process. It is one of the core pillars of the security. Considering high value data accessed, stored, processed and transmitted on the mobile devices; encryption is crucial for companies and individuals. British government's loss of two password-protected but unencrypted computer disks [18] which include personal records of 25 million individuals is a good example about how correct implementation of a measure is a sharp edge. Encryption can be applied at two levels with respect to location where data rest. First level is full disk encryption (FDE) [19] and the other is file system level encryption (FSLE) [20]. FDE encrypts entire storage of the device and it requires correct user credentials to authorize access [21]. FDE can be implemented in software or hardware. Latter one has a separate encryption processor. In FSLE, files and directories are encrypted instead of the entire disk. Both are the last line of defense if device falls into hands of illegitimate users.

3) Remote Management:

A remote administration can protect the devices and data in case of a loss or theft is by remote data removal and/or feature lockdown. Those features are Bluetooth, Wi-Fi, infrared, camera, microphone, USB or memory card mount, synchronization, messages and e-mail [22].

4) Trusted Computing:

In trusted computing concept, devices always perform as expected and this is it is enforced both by hardware (Trusted Platform Module-TPM) and encryption software. Use of mobile IT entities such as mobile payment, ticketing, portable gaming, multimedia and cloud computing is increasing [23]. They include sensitive data so needs protection. Customer and fiscal data in mobile payment or digital rights management (DRM) in content streaming to the authorized mobile players are a few examples. Trusted Computing Group (TCG) defined Mobile Trusted Module (MTM) [24] to provide a specification of encryption/decryption, signature generation and sensitive data storage to deliver functions such as secure boot, data integrity, device authentication and remote attestation.

5) Security Awareness:

Human instincts drive individuals disregarding tools unless one believes it is useful and bypass rules even if they

are deduced from unquestionable facts but they do not make any sense at the very moment. Extensive security policy training is not only a solid requirement to create awareness but also it is a lucrative investment on the employees. It should teach or remind what type of data they need to carry or not; how and why they secure their devices properly; appropriate reactions against incidents; possible consequences of security breaches and finally their responsibilities. Reference [25] highlights that "learning is a continuum; it starts with awareness, builds to training, and evolves into education". The cost of these trainings proves its worth in the form of reduced number of security breaches and decreased damage. Technical and social elements of security awareness include putting a label onto device with identifiable information, updating the operating system and installed applications regularly, using only official manufacturer firmware and application markets as software sources, avoiding processes like "rooting" or "jailbreaking" the device and using remote device finder services.

V. SECURITY ASSESSMENTS

A. Assessment Criteria Reasoning

Main assessment criteria are convenience, cost and security efficiency. Convenience outweighs others while choosing and implementing a security system in author's perception which is a decision made upon human nature. An advanced but not user friendly security system is likely to be ignored or improperly used by employees. Most of them will prefer being "insecure" instead of using this intricate system. Cost and security efficiency do not matter if/when users do not adopt this solution. Instructing users about strong passwords is much cheaper and convenient than carrying a code generator. Training employees makes this trade-off more manageable in.

Cost is the most crucial one from a business owner's perspective and it is in the same level with security efficiency within this study. A cheap but efficient system may deliver better solutions than an expensive system but it is not the case in real life as you get what you pay for and real cyber security is not cheap. The challenge is justifying incurred costs and showing expensive one is actually more cost effective in the long run. In the end, cost of a security mechanism must match the desired security efficiency within the budget.

B. Convenience

Convenience observes adoptability and acceptance by users. Key consideration is the extent of an applied mobile security mechanism which influences user preferences since it would inevitably introduce some inconvenience while safeguarding.

Password protection is practical and successful when it is properly used but this assumption does not always hold. Employees generally choose simple combinations to facilitate recollection, note down enforced sophisticated passcodes or renew them with a similar one. Eventually ease of use becomes a short circuit in the security mechanism. Two–phase authentication is also integrated into daily life. However, carrying an extra key card is not that much convenient and the card itself is subject to very similar risks of any other mobile device.

Biometrics has an edge over others because of organic integrity. Users do not need to remember surreptitious codes or plug in extra hardware. Fingerprint recognition particularly has an increasing popularity as reported in [26]. Privacy is an unsolved issue for biometrics as it requires recording unique individual features and employees may resist using it daily. Acceptance and legal matters regarding to privacy in biometric authentication are highlighted in [27].

FDE performs transparently as long as mobile device has sufficient resources to support full storage encryption and handle extra I/O. FSLE depends on either system wide policy stipulations or individual data significance perception. It may also require more complex key management [28]. FDE saves users from such intervention but FSLE provides more flexibility and granular control on the data while encrypting.

Trusted computing is criticized in several ways such as privacy, loss of anonymity, inability of device owner to fully control the device, remote validation abuse and manipulating users' choice of software [29,30]. These restrictions would be acceptable in a company environment since IT departments aim to ensure overall security for the registered devices. MTM and TPM do a good job in servicing these needs at a rational enterprise level but they may cause inconvenience too.

C. Efficiency

In security efficiency, main concern is whether the applied system provides sufficient security or not. This measurement requires a classification of devices and data. A password may prevent others using a smartphone but it is not enough to secure unencrypted e-mail attachments. An efficient mechanism prevents breaches before they occur instead of plugging holes later. Ineffective one inflicts costs with frequent replacements, confidence loss and reputation damage.

Simplicity of password protection brings several shortcomings and supported length or character variety is very important. Security of single phase falls behind because of the tendency of choosing easy to remember (so guess) codes or keeping default passwords [31]. Multi-phase authentication provides considerably more security with extra steps. Two key factors generally use one-time valid code and they carry a time synchronization property [17]. Since smart cards or tokens might be stolen or misplaced, this extra step in security has a potential of turning into total disability of using system as well.

Biometrics eclipses previous techniques in performance since it utilizes absolute metrics which are almost impossible to forge or reproduce. Two main factors should be taken into account on the accuracy and efficiency of biometrics. They are "False Rejection Ratio (FRR)" and "False Acceptance Ratio (FAR)". Former one indicates the number of valid users to whom access is denied while the latter one gives the number of illegitimate users who obtain access [17].

FDE overpowers FSLE in terms of security efficiency because it ensures that no unencrypted data will be written

[21]. Critical data may exist or be copied in multiple locations and FDE eliminates data selection at user's discretion. In FSLE, plaintext data can be discovered in page or temp files with keyword search even after encryption. Vulnerability of FDE against cold boot attacks [32] should be kept in mind and it cannot secure data if a careless employee leaves device unsupervised while a session is open. In terms of efficacy, TPM delivers better protection with hardware and software control while making devices more tamper-resistance but it is not perfect either [33].

D. Cost

Security cost mainly comprises of three elements; initial deployment, training and maintenance (updates/renewals). When selecting a solution, time and fiscal issues must be considered. Value of data/device should justify the incurred costs and it should not outweigh the benefits. It does not make sense to protect a regular smartphone with biometrics while depriving of a hardware security from a laptop which is storing very sensitive government data. Expenses are proportional with desired security.

Passwords are considered free since presumably all mobile operating systems have them. Its cost is covered at the initial procurement. Password management has an IT labor cost since it would erode IT staffs' work hours with frequent password resets. Multi-phase authentication has three components and it is more expensive. First one is the special hardware/software, second item is the hardware reader and the last one is the software which manages identities and keys. There are several factors which cover the cost of biometric security such as hardware, recognition software and employee training as emphasized in [34]. As a result, such deployments should be based on a need basis. Biometrics is also beneficial in saving security management expenses by reducing help desk requests.

Cost evaluation of FDE and FSLE would be performed for worst case scenarios in which the device is lost or stolen. FDE has more overhead and more deployment cost per unit but it delivers better protection for unauthorized data disclosure. TPM and MTM are gaining popularity and major manufacturers are embedding them into their solutions. In most cases, no extra costs are incurred for them unless a specific application of trusted computing is required. In terms of cost, loss of customer trust and reputation upon a breach cause much more than a good initial protection mechanism.

VI. CONCLUSION

Proper implementation and deployment of security methods are vital for avoiding data loss or leaks from a mobile device. Author of this paper evaluated the security measures that provide end–user device and data security by performing comparisons based on convenience, security efficiency and cost. This triplet delivers a strong basis in order to map an extensive organizational ramification of required security at the right level. Challenges about measures are determined upon whether they are easy to adopt or lead to ignorance; whether they provide enough security or result in breaches and whether cost of the applied solution is justified or not. Advantages and disadvantages of mobile operating systems are provided in Appendix. Biometrics and FDE are the strongest but most expensive mechanisms which verifies the notion of "you get what you pay for" in security. It is also concluded that single or multi-phase solutions are sufficient for most of the mobile devices when a meaningful hierarchy is established but biometrics is required if devices store mission critical data. In addition to that, FDE should be preferred over FLSE when mobile devices can run stable without hampering productivity. Use of TPM and MTM provides better protection in overall device security with respect to software modification, authorized use of device and data alterations. Remote administration tools should be considered and their integration with business solutions provides very strong control on mobile devices, data and services. Since humans are the weakest ring in the security chain, their training has great importance in end device and data security.

APPENDIX

Following tables provide insights about the security features of popular mobile operating systems [35].

TABLE I
MOBILE OPERATING SYSTEM COMPARISON-ADVANTAGES

Operating System	Advantages
BlackBerry	Proprietary encryption Enterprise-level features allow setting security policies Secure application installation methods
iOS	Strong device and application security framework Remote GPS location and wipe App Store heavily vetted Data encryption, policies, secure VPN and Wi-Fi
Windows Phone 7	Sandbox with isolated application runtime and storage architecture Central policy management for passwords, remote wipe All apps installed from Windows phone marketplace Mobile IE ensures no malicious code launch from a website
Symbian	SMS remote lock Secure Exchange ActiveSync support
Android	Secure sandbox approach apps Native encryption Remote security management APIs Remote GPS and wipe Openness fosters innovative security products

TABLE II
MOBILE OPERATING SYSTEM COMPARISON-DISADVANTAGES

Operating System	Advantages
BlackBerry	Not many alternative devices supported Business base an attractive target for hackers
iOS	Can't lock mobile device management profiles to prevent end-user opting out Jailbroken devices are a risk Wildly popular platform makes malware more worthwhile
Windows Phone 7	Security policies and management not on par with Windows Mobile Not really new, same concerns as old architecture
Symbian	Dying platform casts shadow over security investment
Android	No way to stop users from opting out of management profiles Too open in terms of application market

TABLE III
MOBILE OPERATING SYSTEM COMPARISON-DECISION

Operating System	Decision for Security
BlackBerry	Very good candidate for corporate world
iOS	Acceptable security for the audience
Windows Phone 7	Promising but requires more work
Symbian	Going to disappear but considered secure
Android	Application policies need discipline but security features are developing fast and rigorously.

REFERENCES

[1] M.Satyanarayanan,"Fundamental Challenges In Mobile Computing.", In Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing Philadelphia, Pennsylvania, United States, May 23 - 26, 1996). PODC '96. ACM, New York, NY, 1-7.

[2] G.H.Forman, and J. Zahorjan,"The Challenges of Mobile Computing.", Computer 27, 4 (Apr. 1994), 38-47.

[3] J. Landay,"User interface issues in mobile computing." In Proceedings of the Fourth Workshop on Workstation Operating Systems (WWOS-IV), 40-47. IEEE, October 1993.

[4] S. Ravi, A. Raghunathan, and N. Potlapally, "Securing Wireless Data: System Architecture Challenges",In Proceedings of the 15th International Symposium on System Synthesis (Kyoto, Japan, October 02 - 04, 2002). ISSS '02. ACM, New York, NY, 195-200.

[5] A.Jøsang and G.Sanderud."Security in mobile communications: challenges and opportunities.",In Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21, pp. 43-48. Australian Computer Society, Inc., 2003.

[6] M.T. Siponen,"Five Dimensions of Information Security Awareness." SIGCAS Comput. Soc. 31, 2 (Jun. 2001), 24-29.

[7] Germany, Ipsos MediaCT."Mobile Internet & Smartphone Adoption." Google Mobile Ads Blog, 2012.

[8] J.Y.Chee,"Security Issues In Mobile Computing",IT Governance Conference,2012

[9] M.Wieser," The computer for the 21st century". Scientific American 9,(1991), 933–940.

[10] D.Goldman,"Google unveils 'Project Glass' virtual-reality glasses". Money (CNN). 4 April 2012.

[11] Q.Li, X. Zhang, J.P.Seifert and H.Zhong,"Secure Mobile Payment via Trusted Computing", In Proceedings of the 2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference(APTC '08),IEEE Computer Society, Washington, DC, USA, 98-112,2008.

[12] B.Holtz,"CRM for the Mobile Workforce – The Past, the Present, The Future", Customer Interaction Solution, Vol.22, No.5, pp.44-47, 2003.

[13] A.P.Felt, and D.Wagner. "Phishing on mobile devices." University of California, Berkeley (2011).

[14] J.Yang,Y.Chen and W.Trappe. "Detecting spoofing attacks in mobile wireless environments.",In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, pp. 1-9. IEEE, 2009.

[15] T. Pering, Y. Agarwal, R. Gupta, and R. Want, "CoolSpots: Reducing the Power Consumption of Wireless Mobile Devices with Multiple Radio Interfaces." In Proceedings of the 4th international Conference on Mobile Systems, Applications and Services (Uppsala, Sweden, June 19 - 22, 2006). MobiSys '06. ACM, New York, NY, 220-232.

[16] W.Jansen,"Authenticating Users on Handheld Devices", Proceedings of the Canadian Information Technology Security Symposium, May 2003.

[17] N.Boertien, E.Middelkoop,''Authentication in Mobile Applications'', CMG, Telematica Instituut, Netherlands, January 2002.

[18] Wikinews,"UK government loses personal information of 25 million people.",November 20, 2007. Available:http://en.wikinews.org/wiki/UK_government_loses_personal_information_of_25_million_people

[19] C. Fruhwirth."New Methods in Hard Disk Encryption". Technical report, Vienna University of Technology, June 2005.

[20] S.Ludwig and W.Kalfa."File system encryption with integrated user management". SIGOPS Oper. Syst. Rev. 35, 4 (October 2001), 88-93.

[21] PGP Corp. White Paper,"How Whole Disk Encryption Works", 2008.

[22] Microsoft White Paper, "A Technical Comparison of Mobile Management Solution Features and Functions", 2008.

[23] Trusted Computing Group, Mobile Phone Work Group. "Selected Use Case Analyses – v 1.0",2009

[24] TCG, "TCG MPWG Mobile Trusted Module Specification", version 1.0, Revision 7.02 29 April 2010.

[25] M.Wilson and J.Hash,"Building Information Technology Security Awareness and Training Program", National Institute of Standards and Technology, NIST Special Publication 800-50, Oct. 2003.

[26] Farpoint Group Technical Note, Document FPG 2008-435.1, "The Broad Reach of Biometrics:Fingerprint Recognition and Mobile Security", November 2008.

[27] T.Greene,"Biometric Security:Practical and Affordable", Global Information Assurance Certification Paper,17 January 2001.

[28] C.J.Kolodgy and G.Pintal, "Securing Laptops with Full Disk Encryption",IDC White Paper, February 2008.

[29] R.Anderson, "Cryptography and competition policy: issues with trusted computing". In Proceedings of the twenty-second annual symposium on Principles of distributed computing (PODC '03). ACM, New York, NY, USA, 3-10.

[30] S.Schoen,"Trusted computing: Promise and Risk.",Electronic Frontier Foundation Article (October 2003).

[31] W.Jansen, K. Scarfone,"Guidelines on Cell Phone and PDA Security", NIST Special Publication 800-124, 2008, page 3-3.

[32] J.Halderman, J. Alex, et al., "Lest we remember: cold-boot attacks on encryption keys." Communications of the ACM 52.5 (2009): 91-98.

[33] E.R.Sparks,et al.,"TPM reset attack.", Available: http://www.cs.dartmouth.edu/~pkilab/sparks/.

[34] D.Polemi,"Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication", Institute of Communication and Computer Systems, National Technical University of Athens, April 1997.

[35] D.Turney,"The Best Mobile OS:Security Showdown",ZDNET,23 May 2011.

Kritik Altyapıların Siber Güvenliğinin Sağlanmasında Üçlü Boyut Yaklaşımı

İnan Semiz, Kerim Göztepe, Recep Kılıç

***Özet*—Kritik altyapılar ülkeler için hayati öneme sahip sistemlerdir. Bu sistemlerin önemi arttıkça korunmasına yönelik çaba da bir o kadar artmaktadır. Sistemlerin gün geçtikçe karmaşıklaşması, altyapısında bilgi sistemlerinin yoğun kullanılması ve her geçen gün artan siber tehditler bu noktadaki güvenlik çalışmalarını arttırmıştır. Yapılan çalışmalar kritik altyapıların siber güvenliğinin sağlanmasında temel üç boyutu ön plana çıkarmıştır. Bunlar; kurumların sistemlerinin teknik altyapısını ilgilendiren teknik boyut, kritik altyapıların yönetimini ilgilendiren kurumsal boyut, ve siber güvenliğin sağlanmasında önemli bir konu olan ulusal ve uluslararası işbirliği boyutudur.**

***Anahtar Kelimeler*—Supervisor Control and Data Acqusition Systems (SCADA) Kritik Altyapı, Siber Güvenlik**

***Abstract*—Critical infrastructure systems are of vital importance for the countries. As the importance of these systems increasing the protection effort is also increasing. Today the complexity of the systems and the intensive use of information systems cause growing cyber threats for security efforts. Ensuring the security of critical infrastructure, cyber studies have highlighted the main three dimensions. These are technical infrastructure of institutions and systems, institutional dimension that concerns the management of critical infrastructures, and cyber security which is an important issue in maintaining the size of the national and international co-operation.**

***Index Terms*—SCADA, Critical infrastructure, Cyber security**

I. GİRİŞ

KRİTİK altyapılar insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve herhangi bir aksama, yok edilme veya bu fonksiyonları sürdürmede yetersiz kalma sonucunda belirgin etki gösterecek varlık, sistem veya ilgili parçaları [1] olarak tanımlanabilir. Sağlık, enerji, su, ulaşım, bilgi ve iletişim, finans, gıda, kamu düzeni ve güvenlik, nükleer biyolojik kimyasal ve radyoaktif madde endüstrileri gibi çok değişik alanlar ülkeler tarafından kritik altyapılar olarak kabul edilmektedir [2].

Teknolojinin baş döndürücü bir hızla gelişmesi coğrafi olarak birbirinden ayrı sistem altyapılarının birbirine entegrasyonuna imkan sağlamıştır. SCADA sistemleri [2,3] olarak da adlandırılan, entegrasyonun temelini oluşturan bu kontrol yapıları teknolojinin gelişimi ile paralel olarak mimari yapısı itibariyle;

- birinci nesil monolitik,
- ikinci nesil dağıtık (distributed)
- ve üçüncü nesil ağ tabanlı (networked) olarak üç nesile ayrılabilir [4].

İlk geliştirilen SCADA sistemlerinde hem üreticiye özel protokoller kullandığı hem de diğer ağlarla bağlanmadığı için daha çok fonksiyonellik ön plana çıkmıştır [5]. Bu nedenle çok fazla güvenlik özelliği eklenmemiştir [6]. Fakat süreç içerisinde SCADA sistemleri için standart protokollerin [7] yaygınlaşması sistemlerin internet ya da kapalı bilgisayar ağları üzerinden kontrol edilmesi güvenlik risklerini de artırmaya başlamıştır. Bu riskler SCADA sisteminin internete bağlılık düzeyine göre artmaktadır[8,9]. Geniş alan ağına bağlı kontrol sistemlerinin üçüncü nesilde yoğun biçimde kullanılması sistemlerin yönetiminde büyük kolaylıklar sağlarken dış tehditlere karşı da hassasiyeti aynı oranda arttırmıştır. Son dönemde siber saldırıların öncelikli hedefi haline gelen bu sistemlerin güvenliğine yönelik ülkelerin ulusal ve uluslararası çalışmaları yoğunlaşmıştır [10,11]. Ancak her ne kadar bu konuda birçok çalışma yapılmış olsa da ortak bir yöntem ortaya konamamıştır.

II. KRİTİK ALTYAPILARIN SAĞLANMASINDA ÜÇLÜ BOYUT YAKLAŞIMI

A. *Çalışmanın Amacı*

Kritik altyapıların siber güvenliğinin sağlanmasında ülkeler ve uluslararası kuruluşlar birçok çalışma gerçekleştirmiş ancak bunlar arasında ortak ve çözüm sağlayan bir yöntem belirlenememiştir. Bu maksatla ortaya konacak bu yaklaşımla ülkelerin kritik altyapılarının siber güvenliğinde kullanabilecekleri temel ve sade bir yöntemin oluşturulması amaçlanmıştır.

B. *Üç Boyut Yaklaşımı*

Kritik altyapıların siber güvenliğinin sağlanmasında üç boyut yaklaşımı teknik boyut, kurumsal boyut, ulusal ve uluslararası işbirliği boyutlarından oluşmaktadır (Şekil 1).

İnan Semiz, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: inansemiz@gmail.com.

Kerim Göztepe, Ph.D. Harp Akademileri Komutanlığı, Kara Harp Akademisi, Harekat Ana Bilim Dalı, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: kerimgoztepe@gmail.com.

Recep Kılıç, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: rkilic40@gmail.com.

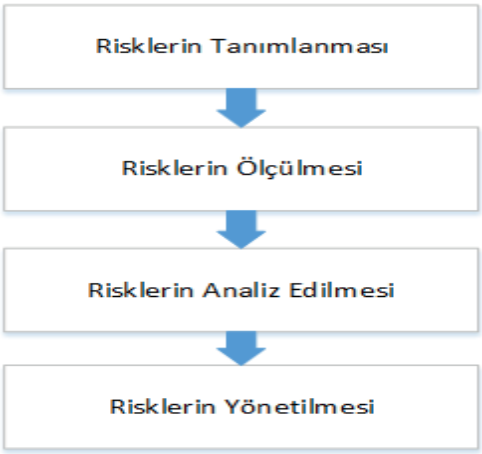


Şekil 1. Üç boyut yaklaşımı

(I) Teknik Boyut

Birinci ve en temel boyut teknik boyuttur. Sistemi oluşturan alt sistemlerin hassasiyetleri aynı zamanda tüm sistemin hassasiyetidir. Bütüncül olarak sistemin güvenliğinin sağlanması ve alt sistemlerin güvenliğinin sağlanmasında sistematik bir yaklaşım önemli bir konudur.

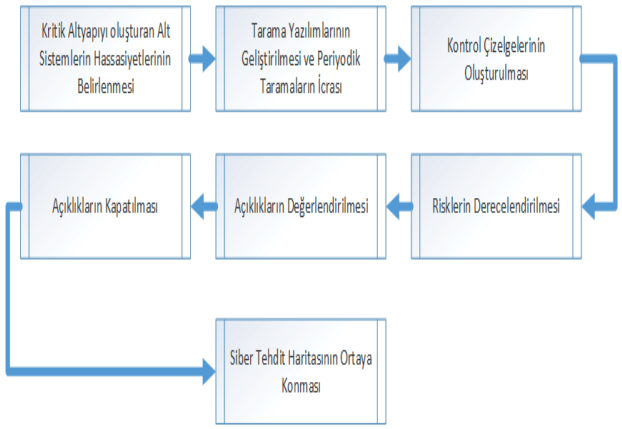
Kritik altyapının yönetilmesini sağlayan sistemin tüm yapısı incelenerek risk yönetimi aşağıdaki basamakları izleyerek uygulanmalı ve sistemlerin risk haritası ortaya çıkarılmalıdır (Şekil 2).



Şekil 2. Risk yönetimi

Teknik boyutta önemle üzerinde durulması gereken bir diğer konu da teknik açıklık yönetimidir. Kısaca, bilgi sistemlerinde var olan teknik açıklıkların tespit edilmesi, açıklıkların değerlendirilip önlemlerin ortaya konması, uygun önlemlerin seçilerek uygulanması ve uygulama sonuçlarının gözlenmesi [3],[12]olarak tanımlanan bu yöntem, kritik bir altyapıdaki temel bilgi güvenliği konularından birisidir ve sürekli işlemesi gereken bir süreçtir. Her ne kadar açıklık yönetimi dendiğinde bazen penetrasyon testlerinin belirli aralıklarla icra edilmesi veya ortaya çıkan açıklıkların kapatılması, bir diğer deyişle yamalanması olarak algılansa da bu yöntemler teknik açıklık yönetiminin sadece bir bölümünü oluşturmaktadır. Kritik altyapıların siber güvenliğinin sağlanmasında teknik açıklık yönetiminin kurumsal olarak belirlenecek bir metodoloji ile işletilmesi büyük önem taşımaktadır. Bu sürecin de en önemli basamağını hassasiyetleri itibariyle korunması gereken sistem veya alt sistemlerin belirlenmesi oluşturmaktadır.

Bir diğer önemli basamak da sistem altyapılarının sürekli olarak taranmasıdır. Teknik açıklık yönetimi aynı zamanda risk yönetimi süreci ile paralel işletilmelidir [8],[12]. Açılıklardan ortaya çıkan risklerin derecelendirilmesi gerekmektedir. Tespit edilen açıklıklar mutlaka yönetim tarafından değerlendirilmeli ve doğrulanmalıdır. Son olarak da açıklıkların ortadan kaldırılması için gerekli yöntemler uygulanmalıdır. Teknik açıklık yönetimi ile kuruma kazandırılması gereken en önemli çıktı da güncel siber tehdit haritasıdır. Bu sayede ihtiyaç duyulan koruma sistemlerinin geliştirilmesi ve gerektiğinde satın alınması sağlanacaktır. Aşağıda teknik açıklık yönetiminin sistematik ve sade biçimde akış diyagramı yer almaktadır (Şekil 3).



Şekil 3. Teknik açıklık yönetimi

Teknik boyutun önemli bir diğer basamağı da sisteme müdahil olan yönetici ve kullanıcıların erişiminin kontrol altında bulundurulmasıdır. Kritik altyapıların yönetiminde grid bir yapı olmalı ve hiçbir zaman bilgi sadece tek noktadan ve kişiden akmamalıdır. Sistemin kontrol edilmesi ile personele güven ayrı konulardır dolayısıyla kontrol güvene mani değildir ve aynı zamanda herkes sisteme ait bilmesi gerektiği kadar bilgiye ulaşmalıdır. Ağ denetimi de bu kapsamda gerek yerel ağlarda gerekse de geniş alan ağında uygulanması gereken bir yöntemdir.

Çoğu zaman gözden kaçan ve etkin uygulanmayan teknik boyutun bir diğer basamağı da ağ topolojilerinin ve sistem konfigürasyon yönetiminin sağlıklı yapılması hususudur. Sisteme giren altyapıların ve yazılımların sürümlerinin sistem envanterine dahil edilmesi veya çıkarılması konfigürasyon yönetiminin en basit tanımıdır.

Kritik altyapıların yönetiminde kullanılan SCADA sistemlerin güvenliğinin sağlanmasında yukarıda ifade edilen teknik boyutun basamaklarının yanında sistemlere kazandırılan bir diğer güvenlik tedbiri de sistemlerin kendini koruma yazılım ve sistemleridir. Bunları sıralarsak [13,14]; güvenlik duvarı (firewall), antivirüs yazılımları, saldırı tespit sistemi (intrusion detection system), alarm zayıflık tarama yazılımları, ağ dinleme ve yönetim yazılımları, kütükleme (log) yazılımları ve yedekleme araçlarıdır. Teknik Açıklık yönetimi ile ortaya çıkacak siber tehdit haritasına göre sahip olunan bu yazılım ve sistemler güncellenmelidir.

(II) Kurumsal Boyut

Kritik Altyapıların kurumsal olarak yönetimi güvenliğin bir diğer boyutudur. Kritik altyapıların yönetiminde kurumsal olarak en önemli basamak kurumun siber güvenlik politikasına sahip olmasıdır. Bu kapsamda kurum olarak siber farkındalığın tüm personel tarafından kanıksanması, kullanıcı, uzman ve yönetici olmak üzere her seviyede eğitimin personele verilmesi gereklidir. Teknik boyuttaki tedbirlerin uygulama kriterlerini içeren, bilginin erişimini, korunmasını ve değişimini belirli kriterlere bağlayan konular yazılı olarak kurum içinde personele bildirilmelidir.

Kritik altyapıların yönetimi siber tehditler haritasına uygun olarak kendi kurumsal yapısı bünyesinde uygun savunma teşkilatı kurmalı, bu yapı ile ulusal ve uluslararası kuruluşlarla gerekli koordinelerde bulunmalıdır.

Kurumsal olarak ulusal ve uluslararası siber güvenlik yapılanmaları ile işbirliği sağlanmalı ve icra edilen siber güvenlik tatbikatlarında kritik altyapı en etkin biçimde test edilmelidir. Teknik boyut ile kurumsal boyutun kesiştiği risk yönetimi, erişim yönetimi, konfigürasyon yönetimi ve teknik açıklık yönetimi gibi süreçlerde yönetim olarak mümkün olan en üst seviyede şeffaf olunmalı ve sistemlerin eksikliklerinin üzerinin kapatılması yerine en ivedi şekilde çözüm için gerekli işlemler yapılmalıdır.

SCADA sistemlerinde yer alan alt sistemlerin üreticilerine yönelik değişiklikler izlenmeli, kullanılan bu altyapının dünyada maruz kaldığı saldırılardan gerekli dersler çıkarılmalıdır. Bazı ülkelerin SCADA sistemlerine saldırı yapılmış ve çok ciddi zararlar verilmiştir. Burada kullanılan sistem altyapısı ile aynı sistemi kullanan altyapının aynı tehditle yüzyüze olduğu aşikardır. Bu durumda üretici firmanın sorgulanması gerektiğinde firma tarafından önleyici ek tedbirler üretmesi beklenmelidir.

(III) Ulusal ve Uluslararası İşbirliği Boyutu

Siber Tehditler saldırı kaynakları ve yöntemleri göz önünde bulundurulduğunda çok farklı ve kapsamlı bir güvenlik anlayışını kurumlar için zorunlu kılmaktadır. Bundan dolayı gerek ulusal gerekse de uluslararası boyutta kurumlar kritik altyapılarının güvenliğini sağlama noktasında her türlü işbirliği yoluna başvurmalıdır.

Ülkeler kritik altyapıların siber güvenliğini sağlama noktasında ulusal boyutta yapmaları gereken ilk adım kritik altyapıları belirlemektir. Kritik altyapıların önem derecesine gore önceliklendirilmesi ve buna uygun yasal çerçevenin çizilmesi gerekmektedir. Dünyada bu konuda çeşitli çalışmalar yapılmıştır. "Kritik Altyapı Belirleme, Önceliklendirme ve Koruma" başlıklı HSPD–7, kritik altyapıların korunması konusundaki ana düzenlemelerden biridir. Bu direktif, kurumlara ve bakanlıklara terörist saldırılardan korunmak için kritik alt yapıları ve önemli kaynakları belirleme ve önceliklendirme yükümlülüğü getirmektedir [15].

Ülke içinde her kurumun kendi sistemlerini siber saldırılara karşı korumak için uyguladıkları politikalar ve metodlar bulunmaktadır. Tüm bu politikaların üstünde bir politika ve kurumlar arası oluşturulacak bir sinerji ile tüm kabiliyetlerin bir havuzda toplanması ulusal olarak atılması gereken bir adımdır. Bu kapsamda kurumların oluşturduğu siber güvenlik teşkilatlarının işbirliği de sağlanmalıdır.

Ulusal sinerjinin oluşturulması sonucunda tüm kritik altyapı ve diğer sistem altyapılarının siber güvenlik tatbikatları ile test edilmesi ve ortaya çıkan açıklıkların ortak elde edilen tecrübelerle yönetilmesi siber tehditlerle mücadele etmede ulusal bazda ülkelere büyük güç katacaktır.

Kritik altyapılarda geniş alan ağının kullanılmaya başlanması nedeniyle bir ülkenin zarar görmesi diğer ülkeleri de etkileyecek ve ülkeler bu konuda birbirine bağımlı olacaktır. Bu nedenle ülkeler ortak bir biçimde kritik altyapıları koruma çabalarını ve prensiplerini, genel kabul gören kılavuzları/standartları, tanımlamaları, kritik altyapı önceliklerini tam olarak belirlemelidir.

Kritik Altyapıların siber güvenliğinde en can alıcı noktalardan bir tanesi de uluslararası işbirliğinin sağlanmasıdır. Siber uzay ülkeler arasındaki sınırları kaldırmıştır. Sınırların ortadan kalktığı bu ortamda birleşme ve işbirliği yapma bir zaruret halini almıştır. Her an ülkelerin en önemli yapılarının zarar görebileceği bu yol ve yöntem üzerinde beraber hareket etmek, güvenlik seviyelerinin ve tecrübelerinin paylaşımına imkan sunan tatbikatları icra etmek bu yapıların güvenliğinin sağlanmasında önem taşıyan uygulamalardan bir tanesidir. Uluslararası işbirliği boyutunda bir diğer önemli aşama da siber saldırılara uluslararası hukuk çerçevesinde uygulanacak yaptırımlardır. Ülkelerin bu aşamada uzlaşıya varması kritik altyapıların güvenliğinin sağlanmasında en önemli adımlardan bir tanesi olacaktır.

III. SONUÇ

Bu çalışma ile kritik altyapıların siber güvenliğinin sağlanmasında ortaya konacak tedbirleri çerçeveleyen idarelerin daha kolay sistemlerini kontrol edebilecekleri bir yapı oluşturulması hedeflenmiştir.

Kritik altyapıların yönetimi ve izlenmesi büyük oranda teknoloji ile bütünleşen SCADA sistemleri ile yapılmaktadır. SCADA sistemlerinin bilgi sistemleri ile bütünleşmesi birçok kolaylık ve esneklik sağlaması yanında ciddi güvenlik risklerini de beraberinde getirmiştir. Bu kapsamda ulusal ve uluslararası boyutta kritik altyapıların güvenliğinin nasıl sağlanacağı sorusu gün geçtikçe önem kazanmaktadır.

Bu konuda Dünya'da birbirinden bağımsız yapılan birçok çalışma biraraya getirildiğinde dikkat çeken en çarpıcı husus çalışmada ortaya konan üç temel boyutun kritik altyapıların güvenliğinin sağlanmasında esas hatlar olduğudur. Ortaya konacak her türlü güvenlik tedbiri ve uygulaması bu üç boyuttan herhangi biri içinde değerlendirilebilecektir. Teknolojik gelişmeler sonunda ortaya çıkan bilişim dünyasında siber tehditlerle mücadele ancak kapsamlı bir yaklaşımla gerçekleşebilir. Üç boyut yaklaşımı bu mücadelede etkin bir şekilde kullanılabilir.

KAYNAKLAR

[1] Avrupa Komisyonu, 702 sayılı "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması,"Konulu Tebliğ, 2004, s. 3.
[2] D.J. Gaushell, W.R. Block, SCADA communication techniques and standards. Computer Applications in Power, IEEE, 1993, 6.3: s.45-50.
[3] S. A. Boyer, SCADA: supervisory control and data acquisition. International Society of Automation, 2009.
[4] R.L Krutz, Securing SCADA systems. John Wiley & Sons, 2005.
[5] J. Pollet, Developing a solid SCADA security strategy. In: Sensors for Industry Conference, 2002. 2nd ISA/IEEE. IEEE, 2002. s. 148-156.
[6] V. M. Igure, S.A. Laughter, R.D. Williams, Security issues in SCADA networks. Computers & Security, 2006, 25.7: s.498-506.
[7] G. Clarke, D. Reynders, E. Wright, Practical modern SCADA protocols. IDC technologies, 2004.
[8] M. Kara, S. Çelikkol, 4. Ağ ve Bilgi Güvenliği Sempozyumu Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği, Kocaeli Üniversitesi, 2011.
[9] C. Nan, I. Eusgeld, W. Kröger, Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. Reliability Engineering & System Safety, 2013, 113: s.76-93.
[10] N. Cai, J. Wang, X. Yu, Scada system security: Complexity, history and new developments. In: Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on. IEEE, 2008. s.569-574.
[11] T. Brown, Security in SCADA systems: How to handle the growing menace to process automation. Computing & Control Engineering Journal, 2005, 16.3: s.42-47.
[12] H. Bahşi, Teknik Açıklık Yönetimi, 2008.
[13] P.A.S. Ralston, J.H. Graham, J.L. Hieb, Cyber security risk assessment for SCADA and DCS networks. ISA transactions, 2007, 46.4: 583-594.
[14] C. P. Pfleeger, S. Pfleeger, Lawrence. Security in computing. Prentice Hall PTR, 2006.
[15] M. Ünver, C. Canbay, B.H. Özkan, Kritik Altyapıların Korunması, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı Ankara,2010, s.14.

A Decision Framework for Combat Cloud Computing Strategy

Kerim Goztepe, Ismet Cehreli, and S. Eyup Sensoy

***Abstract*— Cloud computing presents a significant technology trends not only in public sector but also in military works. Cloud computing has become a vise solution for providing a flexible computing environment for military applications. This work proposes a new decision framework provided by military experts for cloud computing in combat. The purpose of this study is to demonstrate main steps for basics of Combat Cloud Computing (CCC). CCC framework may simplify the data management in the combat environment.**

***Index Terms*—Combat Cloud Computing (CCC), Decision framework.**

I. INTRODUCTION

CLOUD computing is an evolutionary outgrowth of prior computing approaches, which builds upon existing and new technologies [1]. Cloud computing represents a new era for delivering resources and services [2]. Mell and Grance [3] is defined cloud computing as follows: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction."

Cloud computing technologies started with Arpanet and changed over a number of years [4,5,6]. The mainstream of this change is in Figure1.[4,7]. Cloud computing is based on Internet [8]. It is possible to deliver information and data in real time. This is the most important feature of the cloud system. There is a tendency among the companies to use the clouds today [9,10,11]. While cloud computing offers cost reduction, elasticity, reliability, availability and energy-saving, companies want to join cloud computing.

Kerim Goztepe, Ph.D.War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100/1321, İstanbul-Turkey, e-mail: kerimgoztepe@gmail.com.

İsmet Cehreli, War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Turkey, e-mail: ismetcehreli@gmail.com.

S. Eyüp Sensoy, War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Turkey, e-mail: eyupsensoy@gmail.com.

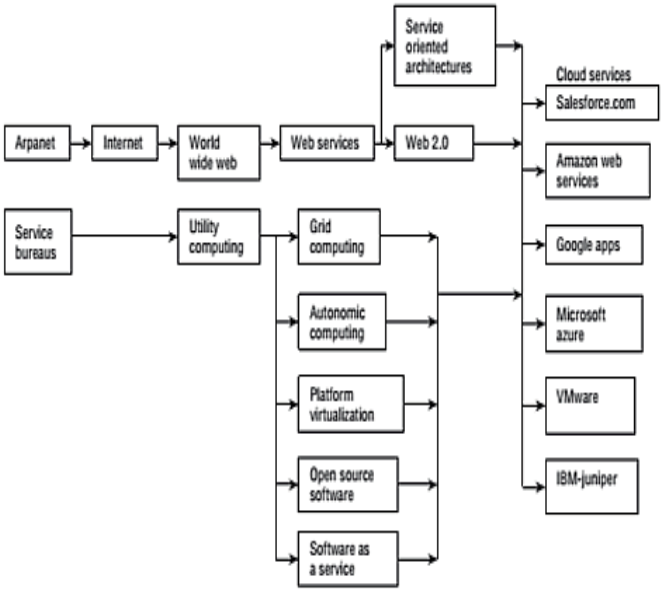


Figure 1: Origins of cloud computing [4].

II. COMBAT CLOUD COMPUTING FRAMEWORK

A. Purpose of the Study

Requested data support of the maneuver operation is a continuous process. It begins with the receiving the task by the maneuver commander and continues until the mission is completed. It is one of the key issue in combat in order to gain success. Therefore, a real-time mannered solution to intelligence or battlefield data is a critical component of tactical warfare [12].

A new decision framework for combat cloud computing strategy for deciding on combat cloud computing environment is proposed in this paper. This study addresses the design of a CCC establishment in order to access the best data management plan in battlefield. Initially, steps that are determined for the problem are formed by applying military cyber experts. Then, decision framework structure is built up by using the data related to CCC. The decision framework is demonstrated by flow chart.

B. CCC Decision Framework Main Steps

Four main steps have been used for CCC decision framework. They are given below.

Step 1. Determine combat cloud computing basics: In the first step, objectives of CCC are determined by CCC decision team. Main principles of framework are estimated.

Then estimated principles are approved. The proposed factors that affect framework are obtained from military cyber experts, combat units, stuff officers and literature on cloud computing studies [13] (See Figure 1).

Step 2. Determine CCC type and users: Three cloud computing type are evaluated for CCC framework. These are external, internal and hybrid cloud computing. Users are important for cloud computing security in combat environment. Thus, three groups of users are capable to enter combat cloud computing systems; developers, active CCC users in battlefield and CCC users in headquarter (Figure1).

Step 3. Decide applications for CCC: Combat environment needs different type of computer applications. Developing necessary applications for CCC is a must for related users. Integrating these applications with CCC users should also done for an efficient system (Figure 2).

Step 4. CCC vendor selection process: After conclusion on CCC basics, CCC type, applications and integration a vendor should selected. Vendors have to be appropriate and have security clearance for CCC. Following request for information process, vendors need to be evaluated by military experts. If vendor has sufficient quality then purchasing process can start (Figure3).

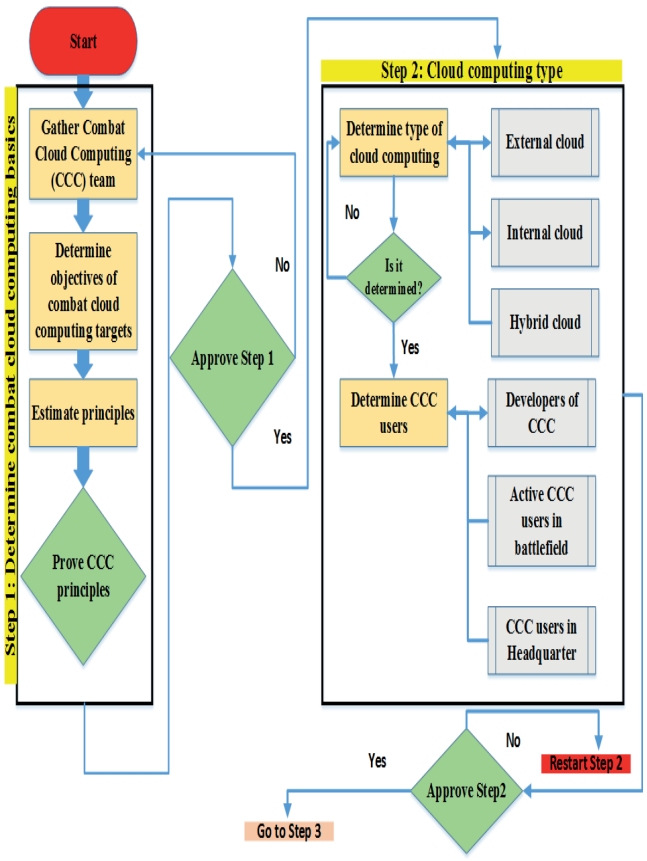


Figure 2. CCC decision framework, Step 1 and Step 2.

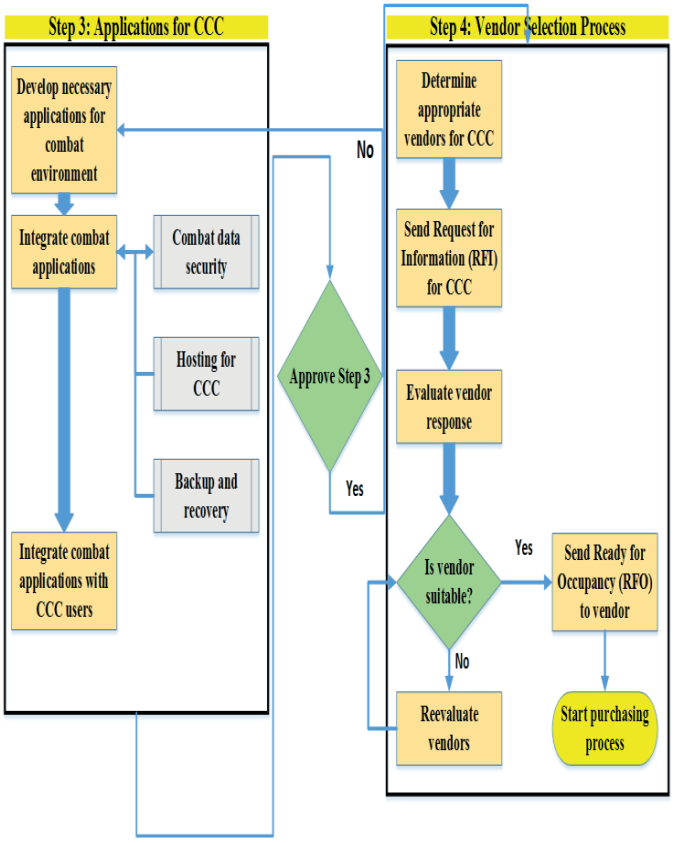


Figure 3. CCC decision framework, Step 3 and Step 4.

III. Conclusion

Proposed CCC decision framework depicts how CCC can be for a better battle environment. Deciding for CCC is important and of great interest because successful cloud computing may provide us an efficient battle management.

A new decision framework for deciding on CCC basics then purchasing process is proposed in this paper. The proposed CCC process designed on MS-Visio. It is believed that CCC decision framework may works well when sufficient military cyber experts are gathered. The framework's goal is to control every steps of CCC before purchasing process. The proposed framework can be used also by CCC suppliers in order to support best devices and applications needed in battlefield.

Appendix

A sample structure of cloud computing [14] is given APPENDIX.

Acknowledgement

We thank to War Colleges Command, Army War College, Dept. of Combat Tactic staff officers for their valuable contribution.

REFERENCES

[1] P.E. Johnson,. A Review of "Cloud Computing for Libraries" Breeding, M.(2012). Chicago, IL: ALA TechSource. *Journal of Access Services*, 2013, 10.1: pp.71-73.

[2] Vic Jr. Winkler,. Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier, 2011.

[3] P.Mell, T. Grance, Effectively and securely using the cloud computing paradigm. NIST, Information Technology Lab, 2009

[4] R.L. Krutz, R.D. Vines, Cloud security: A comprehensive guide to secure cloud computing. Wiley., 2010.

[5] D.G. Feng, M. Zhang, Y. Zhang, and Z. Xu, Study on cloud computing security. Journal of Software, 22(1), 2011, pp.71-83.

[6] C. Hoffa, G. Mehta, T. Freeman, E. Deelman, K. Keahey, B. Berriman and J. Good, On the use of cloud computing for scientific workflows. In eScience, 2008. eScience'08. IEEE Fourth International Conference, 2008,pp. 640-645.

[7] S. Bhardwaj, L. Jain, S. Jain, Cloud computing: A study of infrastructure as a service (IAAS). International Journal of engineering and information Technology, 2010, 2.1: pp.60-63.

[8] B. Furht, A. Escalante, Handbook of cloud computing. Springer Publishing Company, Incorporated, 2010.

[9] A. Lin, N-C. Chen, Cloud computing as an innovation: Percepetion, attitude, and adoption. International Journal of Information Management, 2012, 32.6: pp.533-540.

[10] P. Mathur, N. Nishchal, Cloud computing: New challenge to the entire computing industry. InProceeding of parallel distributed and grid computingSolan, India, 2010, pp. 223-228.

[11] M. Miller, Cloud computing: Web-based applications that change the way you work and collaborate online. IN, Indianapolis: Que Publisher, 2008.

[12] R.J. Bunker, J. Robert, Five-dimensional (cyber) Warfighting: Can the Army After Next be Defeated Through Complex Concepts and Technologies?. DIANE Publishing, 1998.

[13] V. Kundra, Federal cloud computing strategy. 2011.

[14] Cloud computing structure, http://www.zuraidin.com/2010/04/cloud-computing.html, reach time, 04 July, 2013.



Kerim Goztepe received the B.S.degree in System Engineering from Turkish Military Academy in 1998. He was accepted in Marmara University and received M.S. degree in Engineering Management in 2003. He started doctoral education in Industrial Engineering, Institute of Science and Technology at Sakarya University and graduated in 2010. He is interested in fuzzy logic, neural network, multicriteria decision making and cyber security for open source systems. Dr. Kerim Goztepe is an author of 22 refereed papers, associate editor of "International Journal of Cryptography and Security" and in editorial board of International Journal of Engineering.

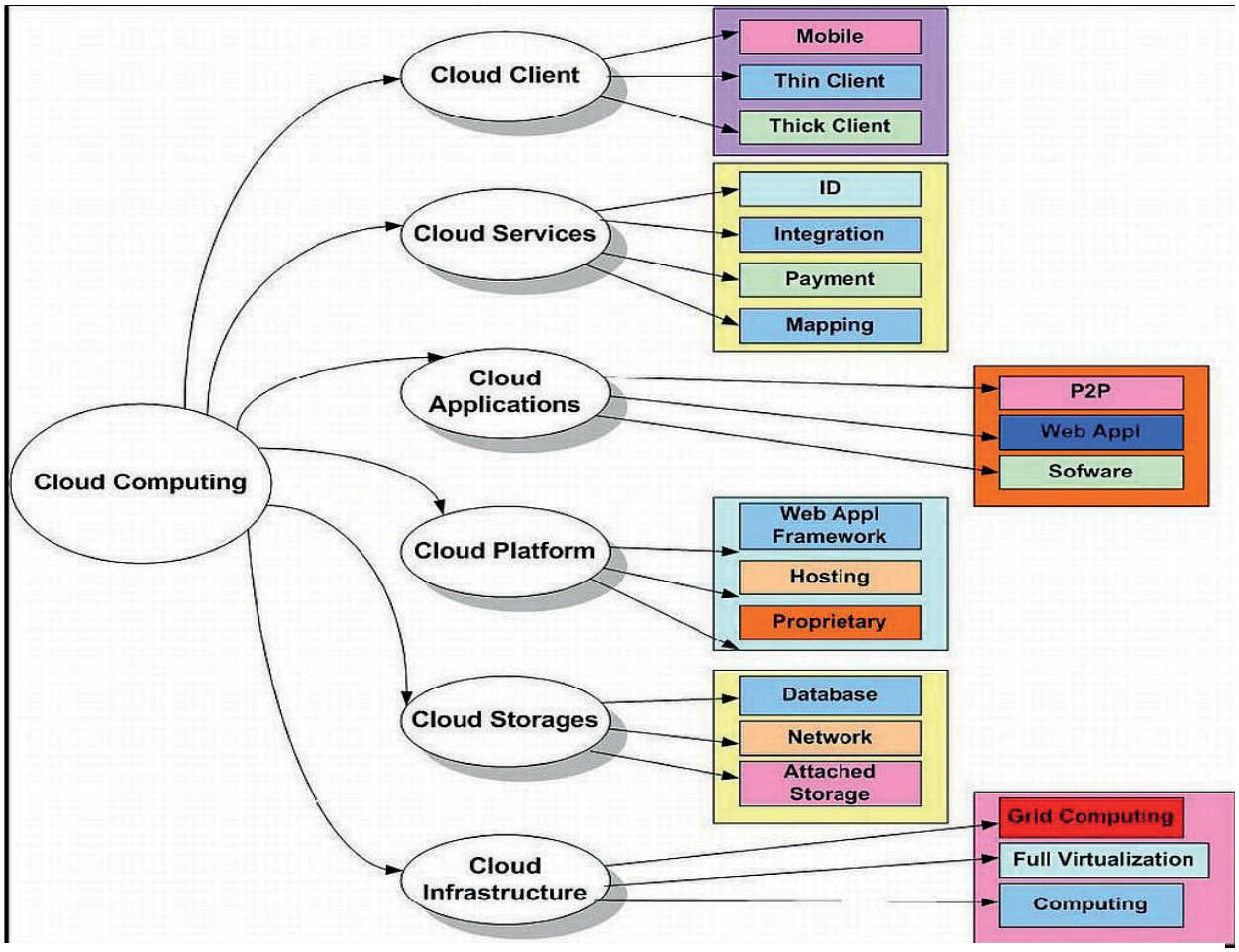


İsmet Cehreli received the B.S.degree in System Engineering from Turkish Military Academy in 1997. He started doctoral education in Spain. He is interested in Combat Control and Communication, Operations and Higher Military education.



S. Eyüp Şensoy received the B.S.degree in System Engineering fromTurkish Military Academy in 1998. He was accepted in European University of Lefke (MBA) in 2000; Yuzuncu Yil University (Msc Applied Sociology) in 2003 and Turkish War Academy (Msc National and International Security Strategies) in 2008. His major interest is conflicts in all levels and in all disciplines (conflict management in small businesses; village, city, migration and analytical approach to the migration and conflict between immigrant and government; analyzing of conflict as an organizational behavior at the small army units).

APPENDIX
A sample structure of cloud computing [14]



Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala

Osman Akın, Işıl Çınar, Muhammer Karaman, Fatih Bilekyiğit

Özet— Bilgi teknolojilerinin her geçen gün yaygınlaşması ve sayısal ortamda hem kişisel hemde kamusal verinin günden güne katlanarak artması beraberinde siber tehditlerin getirdiği riskleri artırmaktadır. Siber güvenlik alanında önemli adımlardan birisi durumsal farkındalık oluşturmaktır. Bu çalışmada siber durum farkındalığını artırmaya yönelik bayrağı yakala (BY) yarışmaları ayrıntılı olarak incelenmiş ve bu kapsamda kurum içi farkındalık çalışması olarak uygulanan bir yarışma sonrasında elde edilen sonuçlar ve alınan dersler paylaşılmıştır. Sonuçlar göstermiştir ki siber güvenlik alanında çalışan ve gerçek sistemlere saldırı yapma imkanı olmayan personel için düzenlenecek bayrağı yakalama yarışmaları ile bilgi düzeyi ve farkındalık artırılabilir. Yine bu çalışma göstermiştir ki siber güvenlik alanında çalışsa dahi bir personel için bizzat yaşanacak tecrübeler teorik olarak öğrenilen bilgiden çok daha etkili bir şekilde farkındalık oluşturmaktadır.

***Anahtar Kelimeler*— Siber güvenlik, bayrağı yakala, siber güvenlik farkındalığı, siber oyun.**

An Effective Method of Increasing the Situational Awareness of Cybersecurity: Capture the Flag

***Abstract*— The spread of information technologies and the exponential growth of both personal and public data in digital media increase the cyber threats risks. One of the main important issue in the field of cyber security is to create situational awareness. In this study, capture the flag contests that help improve situational awareness are studied in detail. As a part of in-house awareness study, a capture the flag contest is implemented, the results and lessons learned have been shared. The results have shown that the level of knowledge and awareness can be advanced among cyber security personnel who do not have an opportunity to attack real systems. This study has also demonstrated that the real experiences, which are gained by attending capture the flag contest, can increase the level of awareness a lot more than theoretical knowledge for cyber security personnel.**

***Index Terms*— Cyber security, capture the flag, cyber security awareness, cyber game.**

I. GİRİŞ

BİLGİ teknolojilerinin kullanımının yaygınlaşması ve günümüzde kurumların bilgi ve verilerinin büyük bir bölümünün sayısal ortamda bulundurulması ile siber tehditlerin oluşturduğu risk her geçen gün bir kat daha artmaktadır. Özellikle sosyal ağların sayısının ve kullanıcısının artması, birçok devlet uygulamasının internet ortamından sunulması, sanal ortamdaki verinin artmasını beraberinde getirmiştir. Bu durum birçok kötü niyetli kişilerin ve çoğu devletin iştahını kabartmaktadır. Tıpkı gerçek savaşlarda olduğu gibi siber güvenlik konusunda önceden almış olduğunuz güvenlik tedbirleri, yapmış olduğunuz testler, yaşadığınız tecrübeler, kurumlar arası işbirliği ve en önemlisi oluşturmuş olduğunuz durumsal farkındalık sistemlerinizi korumaya yardımcı olacaktır. Siber güvenlik farklı adımları barındıran bütünleşik bir olgu olmasına rağmen, en temel adımlardan bir tanesi bu alanda çalışan personelin farkındalığıdır. Siber güvenlik alanında farkındalığı artırmak için farklı yöntemler ve çalışmalar önerilmiştir. Barındırdığı sistemler ve kritik veriler açısından farkındalığın en yüksek olması gereken alanların (organizasyonların) başında kamu kurumları gelmektedir. Bu alanda kamu algısı 2010 yılında yapılan bir çalışmada [1] ele alınmış ve birçok kamu kurumunda siber güvenlik farkındalığının çok zayıf olduğu, sadece güvenlik duvarı kurulmasıyla sistemlerin güvenli kabul edildiği ortaya konmuştur. Türkiye'de kamu kurumlarında siber güvenliğin sağlanması noktasında ortaya çıkan ve çıkacak olan teknik, idari, hukuki, yönetimsel vb. alanlarda zayıflıkları öngörmek, tespit etmek ve gidermek maksadıyla ulusal çapta politika, strateji ve eylem planlarından oluşan ve Haziran 2013'de yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda "Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri" başlığı altında siber güvenlik farkındalığı ele alınmış ve artırılmasına yönelik vurgular yapılmıştır [2]. Siber güvenlik alanında farkındalıkları artırmak için yapılan çalışmalardan bir tanesi de BY yarışmaları düzenlemektir. BY, beyaz şapkalı hackerlar arasında oynanan öğretici bir oyundur. BY'de yarışmacılar dijital labirentler içinde bir hedefin başarılı bir şekilde tamamlandığını gösteren bir bayrağı yakalamaya çalışırlar. Bir başka ifadeyle hacker timlerinin belirli yazılımlar ve ağ yapılarını kullanarak bilgisayarlar ve ağlara saldırmaya veya savunmaya çalıştığı bir yarışmadır [5]. Belirlenen hedefe ulaşmak ve bayrağı(hedef sistemlerde gizli metin dosyası) önce kapmak için sistemlerdeki güvenlik açıklıkları değerlendirilerek bayrağa ulaşılır [3]. Bu bayraklar; gizli bir parola, bir veriye ulaşma, veya bir resim bile olabilir. Bayraklar her yarışmacı için ayrı veya farklı da olabilir.

BY yarışmasının temel amacı proaktif güvenliğin faydalarının gösterilmesidir. Diğer bir ifadeyle önlem alınmayan basit güvenlik hatalarının sonuçlarının nelere mal olacağını uygulamalı olarak göstermektir. Burada dikkat edilmesi gereken husus bu oyunun yıkıcı bir hacking anlayışından ziyade katılımcının teorik bilgilerini uygulamaya koymasını sağlamak ve çeşitli sistemler arasındaki güvenlik sorunlarını hızlıca bulup değerlendirmesini yapmaktır [4].

Bu alanda bir çok çalışma önerilmesine rağmen genellikle yapılan yarışmalar belli platformları gerektirmekte ve katılımcıların belli bir ön bilgi seviyesine sahip olması gerektiği ön koşul olarak sunulmaktadır. Bu çalışmanın temel amacı bu tür yarışmaların küçük ölçekli işletmelerde ve kamu kurumlarında öğretici ve siber güvenlik farkındalığını artırıcı olarak uygulanabilirliğini göstermektir. Bu çalışmada BY yarışması bir kurum içi eğitim kapsamında ele alınmış, yarışmacılar siber güvenlik alanında çalışanlardan herhangi bir ön kriter uygulanmadan seçilmiş, elde edilen sonuçlar anket

O.Akın Hacettepe Üniv.Bilg.Müh., e-mail: (oakin@hacettepe.edu.tr).
I.Çınar Gazi Üniv.Bilg.Müh., e-mail: (isil.cinar@gazi.edu.tr).
M.Karaman, Siber Güv.Uzmanı, e-mail: (muammerkaraman29@gmail.com).
F.Bilekyiğit, Siber Güv.Uzmanı, e-mail: (fatihbilekyigit@gmail.tr).

yöntemiyle değerlendirilmiş ve bu alanda yapılacak çalışmalara bir fikir oluşturması için alınan dersler özetlenmiştir. Bu çalışma göstermiştir ki gelişmiş sistemlere sahip olmadan yaklaşık 20 günlük bir sürede basit bir ağ ortamında bu şekilde bir yarışma hazırlanabilmektedir. Yine bu yarışmanın sonuçları ve elde edilen tecrübeler göstermiştir ki siber güvenlik çok geniş bir olgudur ve her bir alanda mutlaka çok tecrübeli olunması gerekmektedir. Yarışma sonucunda elde edilen bilgilerle katılımcıların kendilerine olan güvenlerinin ve tecrübelerinin arttığı gözlemlenmiştir.

Bu makalenin bundan sonraki kısımları şu şekilde ele alınmıştır:Bir sonraki bölümde bu alanda yapılan çalışmalar özetlenmiş ve çalışmaların artıları eksileri tartışılmıştır. Üçüncü bölümde soruların nasıl ve ne amaçla oluşturulduğu, yarışmanın nasıl dizayn edildiği, nasıl gerçeklendiği konuları detaylı olarak ele alınmıştır. Bir sonraki bölümde ise yarışma sonucunda değerlendirmenin nasıl yapıldığı ve sonuçları özetlenmiştir. Beşinci bölümde yarışma ile kazanılan deneyimler ve alınan dersler paylaşılmıştır. Son olarak bu şekilde bir yarışmayı gerçekleştirmenin artı ve eksileri değerlendirilerek sonuçlar ortaya konmuştur.

II. İLGİLİ ÇALIŞMALAR

Akademik ve farkındalık artırma amaçlı yapılan birçok siber güvenlik çalışması BY'yi oluşturmaktadır. Bu alanda şimdiye kadar birçok çalışma yapılmıştır ancak önerilen her farklı yöntem yeni bir farkındalık oluşmasına olanak sağlamaktadır. BY çalışmaları, güvenlik alanında söz sahibi bir eğitim kurumu olan SANS'ın yayınladığı dokümana [3] göre temel olarak 3 farklı grupta toplanmıştır. Bunlar sadece saldırı(only offensive) olanlar, saldırı veya savunma olanlar(ofensive/defensive) bir de saldırı ve savunmanın bir arada olduğu karışık saldırı/savunma (mixed offensive/defensive) olanlar şeklinde belirtilmiştir. BY ilk olarak 1996 yılında, 4'üncü DefCon Konferansında yapılmıştır. Söz konusu yarışmanın katılımcılarını, bilgisayar güvenlik uzmanları, köşe yazarları, hukukçular, hükümet çalışanları, güvenlik araştırmacıları ile; yazılım, bilgisayar mimarisi, telefon sistemlerine yasadışı girme, donanım değişikliği ve hacklenebilecek herhangi bir konuda ilgisi olan hackerlar oluşturmuştur [5].

Müteakiben DefCon yarışmaları her yıl düzenlenmeye devam edilmiştir. Bu yarışma dünya çapında herkese açık olmasına rağmen öncesinde belirli eleme aşamalarından geçildiği için bir bakıma profesyonellerin katıldığı bir yarışmadır. Elemelerde başarılı olan sekiz takım DefCon konferansında daha önce oluşturulmuş olan tecrübeli bir takıma karşı yarışmaktadır [6].

Düzenlenen yarışmaların uygulama şekli de farklılık gösterebilmektedir. Örneğin yine DefCon'un düzenlediği ve amacı DARPA'nın 5 yıllık birikmiş Ar-Ge dayanıklılığının etkisini test etmek olduğu yarışmada [6] her takımın hem saldırı hem de savunma yeteneği bulunmakta ve her takım kendi bayrağını savunurken diğer takımların bayrağına ulaşmaya çalışmaktadır. DARPA'nın "kırmızı takım" ismi verilen ve gelenekselleşen yarışmalarında ise takımların sadece saldırı yetenekleri ölçülmektedir.

Bu alanda yapılan başka bir çalışmada [7], BY farklı altyapılara sahip öğrenciler için siber güvenlik farkındalığı ve tecrübesi oluşturulması amacıyla uygulanmıştır. Yarışmanın farklı bilgi birikimine sahip öğrenciler için ele alınmasının temel nedeninin çok daha fazla öğrencinin bu deneyimi yaşamasını sağlamak olduğu ifade edilmiştir. Bu yarışmada öğrencilerden farklı takımlar oluşturulmuş ve her bir takım, oluşturulan sanal sunucularda kendi web sitesini korurken başka takımın web sitesinde yer alan bayrağı ele geçirmeye çalışmıştır.

Benzer yapılan bir diğer çalışmada [8], BY için farklı okullardan öğrencilerle farklı takımlar oluşturulmuştur. Bu çalışmada yine her bir takım kendi web sitesini korurken diğer takımların web sitesinde yer alan bayrağı ele geçirmeye çalışmaktadır. Bu çalışma siber güvenlik alanında her bir açıklık için çok iyi derecede spesifik bilgiye sahip olunması gerektiğini ortaya koymuştur.

Bu alanda en çok bilinen diğer iki yarışma da Amerikan Ulusal Kolejler Arası Siber Savunma Yarışması (National Collegiate Cyber Defense Competition-NCCDC) [9] ve Kaliforniya Üniversitesinin Uluslararası Bayrağı Yakala Yarışmasıdır(International Capture the Flag Competition - iCTF) [10]. Her iki yarışma da hem ulusal hem uluslararası olarak yüzlerce öğrencinin katılımıyla ve ön elemeleri ile birlikte çok büyük organizasyonlar şeklinde icra edilmektedir.

Bu alanda daha spesifik ve farklı formata sahip askeri okullar için kullanılan çalışmalardan bir tanesi de Military Academies Cyber Defense Exercise (CDX) [11,12,13] yarışmalarıdır. Bu yarışma, öğrencilerin kendi ağlarını(network) kırmızı bir takıma karşı savunmaları bakımından NCCDC yarışmasına benzemektedir. Bu yarışmadaki farklılık kırmızı takımın National Security Agency (NSA) ve bu alanda uzman askeri personelden oluşturulması ve öğrencilerin var olan bir ağı kullanmak yerine verilen bir bütçe kapsamında kendi ağlarını kurmaları ve savunmalarıdır.

Büyük ölçekli yarışmaların yanında bu konuyu bizim yaptığımız çalışmaya benzer olarak küçük boyutta ele alan çalışmalar da mevcuttur [14]. Bu yarışmada öğrencilerden altışarlı gruplar şeklinde dört masa oluşturulmuş ve her bir masa kendi ağını(web sitesi, veritabanı, firewall, DNS vb. içermekte) kurarak ve savunarak diğer ağlara saldırı düzenlemiştir. Bu çalışmada BY yarışmalarının küçük boyutlu olarak etkin bir şekilde yapılabileceği gösterilmeye çalışılmıştır.

BY yarışmaları öğrenme amaçlı hazırlandığı için daha sonrasında yıkıcı amaçlı kullanılmaması önemlidir. Bununla ilgili bir çalışmada [15] bir BY yarışmasının amacının öğrencilerin eğitimine katkı sağlamak olduğu ve yarışma sorularının etik olarak hazırlanması gerektiği vurgulanmıştır. Bazı yarışmacıların konuyla ilgili yetenek ve bilgilerini zararlı faaliyetlerde kullanabileceği; bu sorunu aşmak için yarışma soruları içeriği ve genel müfredatın etik olması gerektiği belirtilmiştir. Yarışma sorularının kapsam ve içeriği belirlenirken bu durum kurum içi hazırlanan yarışmalarda da göz önüne alınmalı ve konunun hassasiyeti ve yarışmanın amacı katılımcılara çok iyi bir şekilde aktarılmalıdır.

İncelenen çalışmalarda önemle üzerinde durulan bir diğer husus ise yarışma icrası için kaynak kullanımı ve maliyet konusudur. Hoffman, L. ve ark. yaptıkları çalışmada [16] tedarik/temin (özellikle sadece yarışma için gerekli ise uygun donanım/yazılım tedariki zor ve maliyetli olabilmektedir), bakım (yarışmaların bütçeleme ve planlaması uzun süreye yayıldığında ve düzenli olarak her yıl uygulandığında teknik güncellemeler gibi bakım ihtiyacı doğmaktadır), personel ihtiyacı (bu tarz yarışmalarda yönetimsel ve teknik personel desteğine her zaman ihtiyaç duyulmaktadır), dış destek (iç destek seviyesine göre saldırgan, hakem veya denetçi gibi davranabilmek için dış bilgi hizmetinin alınması da önemlidir), yönetim (çeşitli sponsorlardan destek almak yarışma geliri

açısından önemlidir) ve imkanlar konularına dikkat çekmişlerdir.

Türkiye'de de son yıllarda artmakla birlikte farklı zaman ve formatlarda çeşitli BY yarışmaları düzenlenmektedir. Bu oyunlara zaman zaman çevrimiçi katılım sağlanabildiği gibi farklı platformlar da kullanılabilmektedir. Son yıllarda yapılan yarışmalardan bir tanesi de Prodaft şirketi tarafından düzenlenen, siber güvenlikle ilgili analitik düşünme ve teknik bilgi gerektiren 25 adet görevin verildiği "Dünyayı Kurtaran Hacker" adlı siber savaş oyunudur. Oyunun amacı Türkiye'de siber güvenliğin önemini duyurmak ve bu konudaki yetenekli gençleri bir araya getirmek olarak açıklanmıştır. Soruların web sayfası üzerinden yayımlandığı yarışmaya toplam 1599 kişi katılım sağlamıştır [17].

Bilgi Güvenliği Akademisi, İstanbul Bilgi Üniversitesi ve ADEO Bilişim ve Danışmanlık şirketi işbirliğiyle İstanbul Bilgi Güvenliği Konferansı'nda 2009 ve 2011 yıllarında düzenlenen konferaslarda yine BY yarışması icra edilmiştir. İlkinde BY yarışması iki ana kategoriye ayrılmış ve yarışma 5 farklı adımdan oluşmuştur [18]. İkinci yarışmada ise 38 farklı konuda 35 farklı uzman yer almış ve hem internet üzerinden hem de etkinlik alanında "Capture The Flag Ethical Hacking" yarışması gerçekleştirilmiştir. Yarışmaya ait detaylı çözümleri içeren doküman web üzerinden yayımlanmıştır [19].

Düzenlenen başka bir etkinlik, Bilgi Güvenliği Akademisi tarafından Nisan 2012 tarihinde genele açık BY ve Beyaz Şapkalı Hacker (Ethical Hacking) yarışmasıdır. Yarışma toplam 6 adımdan oluşmuş ve her bir adımda bir sonraki adım ile bağlantı kurulmuştur [20]. Yarışmaya yaklaşık 500 kişi katılmıştır. Sorular web uygulaması ortamında sunulmuş veya e-posta ile gönderilmiştir. Soruların çözümlerine ait teknik doküman ise yarışma sonrasında yayımlanmıştır.

Başka bir faaliyet olarak, TÜBİTAK ve Bilgi Güvenliği Akademisi, Türkiye'de siber güvenlik uzmanı eksikliğinin giderilmesine destek olmak ve kapasite geliştirilmesini sağlamak amacıyla üniversite öğrencilerine yönelik "Siber Güvenlik Yaz Kampı" düzenlemektedir. İlki 2012 yılında Gebze'de düzenlenen kampın ikincisi 2013 yılında düzenlenmiştir. Kamp süresince bilişim sistemleri güvenliği konusunda öğrencilere farklı konularda eğitimler verilmesinin yanısıra uygulamalı, eğitim amaçlı ve ödüllü BY yarışmaları düzenlenmektedir [21].

Katılımcıların çoğu kamu kurumu olmakla birlikte, içlerinde özel sektör ve sivil toplum kuruluşları da bulunan 2. Ulusal Siber Güvenlik Tatbikatı 2013 yılında düzenlenmiş; daha önceki yıllardan farklı olarak bu tatbikatta BY yarışması icra edilmiştir. Yarışmaya 5'er kişilik 4 farklı takım katılmıştır. Yarışmada önceden tasarlanmış, belirli açıklıkları olan sistemleri aşamalı olarak ele geçirmek üzere oyun senaryoları kurgulanmıştır [22].

Yine 2013 yılında İstanbul'da gerçekleştirilen ve amacı araştırmacılar, hackerlar ve geliştiriciler arasında fikir ve tecrübelerin öğrenilmesi ve paylaşılmasını sağlamak olan "NOPcon Güvenlik Konferansı"nda NOPcon BY yarışması düzenlenmiş ve çözümleri sunulmuştur [23].

Bir başka çalışma da, Web Güvenliği Topluluğu (Owasp Türkiye) tarafından geliştirilen "Davshan" isimli BY projesidir. Projede güvenlik konusunda kendini test etmek isteyen kişiler, sistem üzerinde bilerek bırakılmış olan açıklıkları tespit etmeye çalışmaktadırlar [24].

Bu noktadan hareketle; Türkiye'de icra edilen Siber Güvenlik Tatbikatları, Siber Güvenlik Yaz Kampları ve benzeri kapsamda yapılan diğer çalışmalar incelendiğinde son yıllarda düzenlenen bu gibi organizasyonlarda ciddi artış olduğu; ulusal, kurumsal ve doğal olarak bireysel farkındalığın arttığı ve buna paralel olarak BY yarışmalarının da bu farkındalığın artmasında, siber güvenlik alanında ihtiyaç duyulan motivasyonun sağlanmasında ve yeteneklerin keşfedilmesinde önemli bir etken olduğu görülmektedir.

Bu alanda özellikle Amerika kaynaklı çok fazla çalışma önerilmesine rağmen, bu yarışmaya hazırlanırken ve sonrasında bu çalışmayı oluştururken yapmış olduğumuz taramalarda BY'nin küçük ölçekli olarak kamu kurumlarında hizmet içi eğitim kapsamında uygulanmasına rastlanmamıştır. Amerika kaynaklı birçok yarışma özellikle öğrencilerin eğitimi için önerilmiştir. Bunun yanı sıra yaptığımız yarışma formatına benzer yarışmalar Türkiye'de yapılmışsa da bu yarışmalarla ilgili herhangi bir değerlendirme yapılarak paylaşılan herhangi bir çalışma bilgimiz dahilinde yoktur. Yaptığımız bu çalışma kamu kurumlarında BY'yi hizmet içi eğitim kapsamında ele alması anlamında bir ilki oluşturmaktadır. Bu çalışmada ayrıca farklı soru çeşitleri kullanılarak siber güvenliğin çok kapsamlı konuları barındırdığı ve farkındalık oluşturulurken bu durumun göz önünde bulundurulması gerektiği ortaya konmaya çalışılmıştır.

III. YARIŞMANIN DİZAYN EDİLMESİ VE UYGULANMASI

Yarışma tasarlanırken siber güvenliğin önemi göz önüne alınarak, hem alanın ne kadar geniş olduğu hem de bu alanda yetişecek kişilerin temel konulara çok iyi hakim olması gerektiği hedeflenmiştir. Bu yarışmanın amacının savunmaya yönelik farkındalık oluşturmak olduğu katılımcılara özellikle vurgulanmıştır. Yarışmanın hazırlanması ve uygulanması prosedürel konular ve teknik konular olmak üzere iki farklı alt başlık altında toplanmıştır. Prosedürel konularda yarışmanın nasıl yapılması gerektiği, süresi, kullanılacak platform ve donanım gibi konular ele alınırken; teknik konular kısmında yarışmada kullanılan sorular ve çözümleri ayrıntılı olarak incelenmiştir.

A. Prosedurel Konular

Sorular hazırlanırken, kurum içi alınan eğitimlerin katılımcılara faydası, katılımcıların çalışma alanları, yarışma sırasında kullanılacak donanım/yazılım yeterliliği, katılımcıların siber güvenlik konusundaki farkındalığının test edilmesi gibi hususlar göz önünde bulundurulmuştur.

Yarışmacılara donanım ve yazılım kullanımı kapsamında herhangi bir kısıtlama getirilmemiş, yarışmaya bireysel veya iki kişilik takımlar halinde katılabilecekleri belirtilmiş ve yarışmanın süresi 2 gün olarak kısıtlanmıştır. Süre yönünden kısıtlama getirilmesinin sebebi kullanıcıların daha iyi performans göstermelerini beklemektir. Yarışma için belirli sistemler oluşturarak katılımcıların bu sistemlere saldırmalarını beklemek yerine belirli formatta hazırlanan soruları içeren dosyalar gönderilerek yarışmanın yapılması kararlaştırılmıştır. Yarışmayı bu şekilde dizayn etmemizdeki temel amaç minumum donanım ve çaba ile yarışmanın yapılmasını sağlamaktır.

Yarışmanın içeriği, amacı, soru başlıkları, puanlaması gibi yarışmayla ilgili genel bilgiler Wordpress kullanılarak yarışma öncesinde katılımcılarla paylaşılmıştır. Katılımcılar siber güvenlik alanında çalışan personelden herhangi bir ön kriter uygulanmadan seçilmiştir.

Yarışmaya katılacak kişilere birer adet bilgisayar tahsis edilmiş ve bu bilgisayarlar bir yerel ağ oluşturacak şekilde bir sunucu ile internete irtibatlandırılmıştır. Kullanıcılar kendi bilgisayarlarında yönetici yetkisine sahiptirler ve internet

ortamında gerekli yazılımları indirerek kullanabilmişlerdir. Yarışma puanlamasında cevap veren kişi sıralaması dikkate alınmış ve ilk üç kişiye cevap verme sırasına göre 10, 8 ve 6 puanları verilmiş, sonraki yarışmacılardan cevap veren her kişiye beşer puan verilmiştir. Puanlama Wordpress kullanılarak online olarak kullanıcılara iletilmiştir. Yarışmaya toplam 16 kişi katılım sağlamıştır.

Yarışma sorularının cevapları yarışma sonunda paylaşılmış; farklı teknik ve yöntemlerle sonuca giden yarışmacılar da soruların çözümüne katkı sağlamıştır. Böylece yarışmacıların sorularda hangi aşamaya kadar geldikleri, eksikliklerinin neler olduğu ve farklı çözüm yöntemleri öğrenilmiştir.

B. Teknik Konular

Yarışmada sorular; stegonagrafi, internet üzerinden bilgi toplama yöntemleri, sosyal mühendislik, şifre kırma bilgisi (Truecrypt, Winrar vb.), web uygulama güvenliği (SQL injection), parola kırma saldırıları (hash, md5 , rainbow table vb.), kriptolama bilgisi kullanma, ağ trafiği analizi , e-posta güvenliği gibi konuları içermektedir. Sorular hazırlanırken daha önce Türkiye'de ve dünyada gerçekleştirilmiş olan yarışmalardan faydalanılmıştır [3,17,20]. Sorularla ilgili ayrıntılı bilgiye ve değerlendirmeye aşağıda yer verilmiştir.

- E-posta Güvenliği

Yarışmacılardan yahoo, mynet ve gmail e-posta hesapları istenmiştir. Bu hesaplara kendilerine ait diğer e-posta adreslerinden gelmiş gibi görünen sahte e-posta gönderilmiştir. Metin içeriğinde şifreli bir şekilde flag bilgisi verilmiştir. Yarışmacının gelen e-postanın sahte olduğunu anladığı anda tespit etmek üzere gelen e-postanın başlık bilgisini kontrol etmesi gerekmektedir. Böylelikle yarışmacı sahte postanın hangi posta sunucusu kullanılarak gönderildiğini tespit etmektedir. Yarışmacıya bayrak olarak sahte posta göndermek için kullanılan sunucunun adı şifreli olarak verilmiştir.

- Web Uygulama Güvenliği

Bu senaryoda SQL Injection ile yerel olarak kurulmuş olan bir web tabanlı uygulamaya yetki olmadan ve herhangi bir parolaya sahip olmadan giriş yapılması istenmiştir. SQL Injection ile sisteme yönetici yetkisiyle giriş yapıldığında listedeki tüm personelin bilgilerine erişilebilecektir. Listedeki belirli bir kaydın bilgilerinin değiştirilmesi, silinmesi veya yeni kayıt girilmesi gibi SQL işlemlerinin gerçekleştirilmesi beklenmiştir. Bu işlemleri gerçekleştiren kullanıcı ekran görüntüsünü cevap olarak gönderecektir.

- Stegonagrafi

Stegonagrafi kullanılarak herhangi bir resim içerisine gizlenen metnin çözülmesi istenmiştir. Burada kullanılan orjinal resim ve içerisine metin gizlenmiş olan resim (Şekil 1) yarışmacıya e-posta ile gönderilmiştir.

Burada önemli olan nokta; herhangi bir resme bir stego aracı ile metin gizlendiğinde bu metni çözmek için yine aynı stego aracı kullanmak gerektiğidir. Sadece ticari birkaç ürünle herhangi bir araçla gizlenmiş olan metinlerin çözülebildiği iddia edilmektedir. Dolayısıyla katılımcıya kullanılan stegonagrafi aracı (Quick Stego) ipucu olarak verilmiştir. Yarışmacılar Şekil2'de yer alan sonuca ulaşmışlardır. Bu yarışma sorusu, siber güvenlik açısından bazı dosyaların göründüğünden farklı bilgiler içerebileceğini göstermiştir. Stegonografi teknikleri ile ilgili detaylı bilgi için Tatar ve ark.'nın çalışmasına [25] bakılabilir.



Şekil 1. İçerisine Metin Gizlenmiş Olan Resim



Şekil 2. Resim İçindeki Çözülmüş Gizli Metin

- Şifre Kırma

Bu soruda amaç TrueCrypt ile şifrelenmiş dosyanın parolasını bulup içerisindeki gizli mesajı ortaya çıkarmaktır. Yarışmacılardan öncelikle istenen özel bir wordlist oluşturarak şifrelenmiş olan dosyanın parolasını bulmalarıdır. TrueCrypt ile şifrelenmiş dosyanın parolasının ilk 5 karakterinin "siber" kelimesi olması, bu kelime hariç sadece rakamlardan oluşması ve toplam 10 karakter içermesi ipucu olarak verilmiştir. Bu senaryoda kullanıcılardan yukarıda yer alan ipuçlarını kullanarak oluşturdukları bir şifre listesi(wordlist -Bactrack ile birlikte gelen "Crunch" vb.) ile veya çoğu uygulamanın sağladığı "password pattern" seçeneğini kullanarak düzenli ifadeler (regex) ile TrueCrypt şifresini açık kaynak uygulamalardan birini (örneğin; OTFBrutus adlı araç hem "wordlist" hem de "password pattern" kullanımını sağlamaktadır) kullanarak kırmaları ve gizli mesajı ortaya çıkartmaları istenmiştir. Gizli mesaj içerisinde bayrak yer almaktadır. Bu soru ile basit parolaların kısa sürede kırılabilirliği ve kişisel hayatımızla ilgili bilgilerin parolalarda kullanılmasının tahmin edilebilirliği(word list oluştururken) kolaylaştırdığı katılımcılara gösterilmeye çalışılmıştır.

- İnternet Üzerinden Bilgi Toplama

Bu soruda yarışmacılara jpeg formatında bir fotoğraf ve bir senaryo verilmiştir. Yarışmacılar öncelikle bu fotoğrafı kullanarak internet üzerinde görsel arama yapacaklar ve fotoğrafın ait olduğu web sitesini keşfedeceklerdir. Bu web

sitesinde uygun kelimelerle arama yapacak ve kullanıcı bilgilerinin(kullanıcı adı, şifre vb.) yer aldığı bir excel dosyasına erişeceklerdir. Sonrasında ise yarışmacıların toplamış oldukları bilgileri kullanarak web sitesinin veritabanına sızmaları ve bu veritabanında yer alan bir makaleye erişmeleri istenmiştir. Buradaki bayrak veritabanına sızıldığını kanıtlayan, veritabanındaki makalelerden bir tanesinin kimlik bilgisidir. Sisteme giriş yapıldıktan sonra araştırma yöntemiyle web tabanlı uygulamada gerekli bilgiler elde edilebilecektir. Bu soruda katılımcıların "google hacking" ve arama motorunda görsel arama sayfasından resim arama özelliğini kullanmaları beklenmiştir. Bunun yanısıra katılımcılar, kullanıcı bilgilerini ve şifrelerini içeren herhangi bir dosyanın web sunucuda saklanmaması ya da unutulmaması gerektiğinin farkına varmışlardır.

- Farkındalık ve Biliçlendirme

Bu alanda iki adet soru kullanılmıştır. İlk olarak katılımcılara sadece bir fotoğraf gönderilerek bayrağa erişmeleri istenmiştir (Şekil 3). Fotoğrafın parlaklık ve karşıtlık ayarlarıyla oynandığında içine yerleştirilmiş bir metin ortaya çıkmaktadır (Şekil 4). Bu soru katılımcılara bir dosyanın göründüğünden farklı bilgileri de barındırabileceği gerçeğini göstermiştir.

İkinci soru notlarımızı çöpe atarken ne kadar çok dikkat etmemiz gerektiğini hatırlatmak maksatlı hazırlanmıştır (Şekil 5). Soruda kağıt parçaları uygun şekilde birleştirildiğinde bayrağa erişilmektedir (Şekil 6) Birleştirme işlemi çeşitli yazılımlarla (photoshop vb.) kısa sürede yapılabilmektedir veya fotoğrafın çıktısının alınıp uygun şekilde birleştirilmesi de bayrağa ulaşmayı sağlayacaktır.



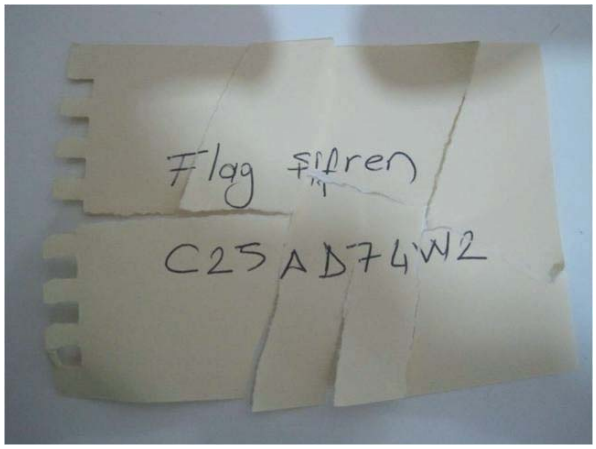
Şekil 3. İçerisine bayrak gizlenmiş resim



Şekil 4. Ayarları ile oynanarak bayrağın elde edilmesi



Şekil 5. Yarışmacılara gönderilen parçalı fotoğraf



Şekil 6. Parçaların uygun şekilde birleştirilmiş hali

- Parola Kırma Saldırıları (hash, md5 , rainbow table vb)

Bu soruda katılımcılara Winrar kullanılarak şifrelenmiş bir dosya içerisinde kullanıcı adlarının ve şifrelerinin hash kayıtları verilmiştir. Katılımcıların öncelikli olarak kaba kuvvet (Brute force) atak ile Winrar şifresini kırmaları istenmiştir (ör: Winrar Password Cracker, Rar Pasword Recovery). Yarışmacılar şifreyi kırdıktan sonra eriştikleri dosyada kullanıcı adları ve hash kayıtları bilgilerine erişeceklerdir. Sonrasında ise "Flag" adlı kullanıcının hash kaydını, online md5 kaydı kıran web sitelerinde [26] deneyerek şifreye ulaşmaları hedeflenmiştir. Bu senaryo ile katılımcılara şifrelerin zorlaştıkça kırılmasının daha zor olduğu ve uygulamalarda şifrelerin açık olarak (clear text) tutulmaması gerektiği anlatılmaya çalışılmıştır.

- Kriptolama

Katılımcılara Sezar Şifreleme yöntemi kullanılarak hazırlanmış bir metin gönderilerek kriptolama alanındaki bilgileri ölçülmüştür. En eski şifreleme yöntemlerinden biri olan Sezar algoritmasını yarışmacılara bir kez daha hatırlatmak için hazırlanan bu soruda amaç katılımcıların online şifre çözen web sitelerinin [27] ve araçların (crank v0.1.3 vb.) farkında olup olmadıklarını ölçmektir.

- Ağ Trafiği Analizi

Katılımcılara bir pcap (ağ sniff edilerek elde edilmiş dosya) dosyası gönderilerek; trafik analizinin yapılması istenmiştir. Katılımcılar analiz sonucunda flag olarak analiz

dosyası içinde yer alan şifre bilgisine ulaşmışlardır. Bu senaryoda amaç katılımcıların Wireshark, Networkminer, Tcpdump vb. trafik analiz araçlarını kullanmalarını sağlamaktır. Bu soru ayrıca yarışmacılara ağ üzerinden açık olarak gönderilen bilgilerin başkalarının eline geçme ihtimalinin çok yüksek olduğunu göstermiştir.

IV. DEĞERLENDİRME

BY yarışmasının etkinliği yapılan anket ile değerlendirilmiştir. Kullanıcılara yarışmadan önce ve sonra siber güvenlik alanında kendilerine güvenlerinin nasıl olduğu sorulduğunda, katılımcılar ortalama olarak %50 oranında güvenlerinin arttığını belirtmişlerdir. Buna ek olarak böyle bir yarışmaya tekrar katılmak ister misiniz ya da yarışmanın hazırlanması aşamalarında yer almak ister misiniz sorularına katılımcıların hepsi "Evet" cevabını vermişlerdir. Ayrıca katılımcılar yarışma için kullandıkları donanım ve yazılımların yeterli olduğunu, yarışmanın formatının ve yayımlanma şeklinin uygun olduğunu belirtmişlerdir. Katılımcılara yarışmanın siber güvenlik farkındalığına katkısı sorulduğunda tamamından "çok iyi" cevabı alınmış ve tekrarlanması istenmiştir. Başka bir soruya cevap olarak katılımcılar yarışmanın alınan eğitimlerin uygulanması için kendilerine bir fırsat sunduğunu dile getirmişlerdir.

Bunun yanı sıra katılımcılarla yüz yüze yapılan görüşmelerde yarışmanın güvenliğe bakış açısını nasıl değiştirdiği sorulmuştur. Yarışmacılardan bir tanesi kişisel bilgisayarında eksik olan yamaları yüklediğini, bir diğeri virüs programını güncellediğini ve bir başkası da şifresiz olarak açılan bilgisayarına şifre koyduğunu belirtmiştir. Bunun yanı sıra kullandığı şifrenin basit olduğunun farkına varan başka bir yarışmacı şifresini güçlendirdiğini dile getirmiştir. Bir başka etkinlik olarak yarışma sonrasında soruların cevapları yarışmacılarla paylaşılmış ve yarışmacıların kullandıkları farklı yöntemler öğrenilmiştir. Bu sayede çok farklı ve özgün çözümlerin de olabileceği diğer yarışmacılar tarafından tecrübe edilmiştir. Yarışma sorularından elde edilen tecrübenin yanında katılımcılar bu paylaşım sayesinde birbirlerinin tecrübelerinden de faydalanma imkanı bulmuşlardır.

V. ALINAN DERSLER VE GELECEK ÇALIŞMALAR

Bu şekilde bir yarışma dizayn etmek ve uygulamak bizim açımızdan bir ilk olduğu gibi katılımcılar açısından da bir ilki oluşturmaktadır. Bu anlamda bu yarışmadan öğrenmiş olduğumuz ve paylaşılmaya değer bulduğumuz konuları paylaşmak istedik. Öncelikle böyle bir yarışmayı icra edebilmek için çok büyük miktarda bir veri kaynağını taradık ve böyle bir yarışmanın nasıl icra edilmesi gerektiği konusunda bilgi sahibi olduk. İlk adım olarak bu faaliyet siber güvenlik konusunda öncelikle bizim farkındalığımızın artmasını sağladı.

Özellikle kurumsal bir BY gerçekleştirilmesi sebebiyle, yarışmanın hem mesai saatlerini hem de sonrasını kapsıyor olması kurum işlerinden dolayı zaman zaman yarışmacıların ara vermelerine ve puanlamada geriye düşmelerine neden olmuştur. Yarışmanın gerçekleştirileceği tarihlerin, katılımcılara haftalar öncesinden bildirilmesi, iş yükünün daha az olduğu haftaların seçilmesi, yarışmaya katılacak personele mesai sırasında imtiyaz gösterilmesi gibi hususların sonraki yarışmalarda dikkate alınması gerektiği sonucuna varılmıştır.

Yarışmada kullanılan donanım/yazılım alt yapısı her ne kadar iyi seviyede olsa da daha karmaşık soruların hazırlanıp uygulanması ve yarışmanın kapsamının genişletilerek daha çok personelin katılımının sağlanması için her yıl düzenlemeyi planladığımız yarışmalara özel laboratuar çalışması yapılması gerektiği sonucuna ulaşılmıştır.

Yarışma öncesinde yarışmacıların kullanacakları araçlarla ilgili gerekli kontrolleri yapmaları konusunda bilgilendirme yapılması ve yarışma öncesi destek verilmesi gerektiği sonucuna varılmıştır. Örneğin sanal makine kullanan bazı yarışmacılar konfigürasyon konusunda sıkıntı yaşamış ve zaman kaybetmişlerdir.

Yarışma yapı itibari ile birbirinden bağımsız sorulardan ve bayraklardan oluşmaktadır. Soruların yarışmacılara başlangıçta bütün olarak verilmesi, zorluk derecesi bakımından aynı seviyede olmayan sorulara yarışmacıların farklı sırada cevap verebiliyor olması, puanlamadaki dengeleri değiştirmiştir. Bundan sonra gerçekleştirilecek olan yarışmalarda yapı değiştirilerek, bir önceki sorudan elde edilen bayrakla sonraki sorulara geçiş yapılmasının daha uygun olacağı düşünülmektedir. Bu şekilde basit sorudan zor soruya doğru bir hiyerarşik yapı oluşturulmuş olacak ve herkes aynı zamanda aynı soru için çaba harcayacaktır.

VI. SONUÇ VE ÖNERİLER

Bu yarışma hem katılımcılar hem de yarışmayı hazırlayanlar için üst düzeyde bir öğrenme tecrübesi oluşturmuştur. Öncelikle bu yarışmaya katılanlar siber güvenlik alanında ne derecede bilgi birikimine sahip olduklarının farkına varmışlar ve bu alanda ne tür yeteneklerini geliştirmeleri gerektiğini daha iyi kavramışlardır. Bunun yanı sıra bu yarışma hem katılımcılara hem de hazırlayanlara siber güvenliğin ne kadar karmaşık bir yapıda olduğunu ve çok geniş bir bilgi alanını içine aldığını göstermiştir. Bu yarışma için oluşturulan altyapı, kurulması düşünülen siber güvenlik test laboratuarı için bir ön çalışma niteliği taşıyabilir. Yapılan yarışmanın daha da geliştirilerek bir sonraki adımda daha çok personel ile ve daha farklı konuları içerecek şekilde yapılması planlanmaktadır. Bu alanda ülke ve kurumlar çapında yapılacak bayrak yarışmalarının; ulusal ve kurumsal farkındalığın artırılmasına, bireysel yeteneklerin ortaya çıkarılmasına, siber güvenlik alanında dinamikliğin sağlanması açısından faydalı olacağı değerlendirilmektedir. Bunun yanı sıra üniversitelerin de bayrak yarışmaları adı altında yarışmalar düzenlemesinin büyük öneme sahip olduğunu düşünülmektedir. Bayrak yarışmalarının kapsamlarının genişletilerek bireysel ve kurumsal katılımın da artırılmasıyla siber güvenlik tatbikatlarından ayrı olarak "Ulusal Bayrak Yarışmaları" düzenlenmesinin, bu ve benzer faaliyetlerin icra edildiği haftanın da "Ulusal Siber Güvenlik Farkındalık Haftası" olarak ilan edilmesinin siber güvenlik farkındalığına ve eğitimine katkı sağlayacağı değerlendirilmektedir.

KAYNAKLAR

[1] Adnan Yılmaz, M. Akif Bakır: *Kamu Kurumlarında Bilgi Güvenliğine Yönelik Bir Durum Tespiti,* ISCTurkey'10,. pp.97-101

[2] http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm (Karar Sayısı : 2013/4890 Ekli "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nın kabulü; Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 18/2/2013 tarihli ve 412 sayılı yazısı üzerine, Bakanlar Kurulu'nca 25/3/2013 tarihinde kararlaştırılmıştır.)

[3] http://www.sans.org/reading_room/whitepapers/casestudies/capture-flag-education-mentoring_33018, Haziran 2013

[4] CTF, http://www.istsec.org/ctf/, Kasım 2009

[5] Gavas, Efstratios, Nasir Memon, and Douglas Britton. "Winning Cybersecurity One Challenge at a Time." Security & Privacy, IEEE 10.4 (2012): 75-79.

[6] Cowan, Crispin, et al. "Defcon capture the flag: Defending vulnerable code from intense attack." DARPA Information Survivability Conference and Exposition, 2003. Proceedings. Vol. 1. IEEE, 2003.

[7] Werther, Joseph, et al. "Experiences in cyber security education: The MIT lincoln laboratory capture-the-flag exercise." Cyber Security Experimentation And Test 8 (2011).
[8] Ho, Jun-Won, Nayantara Mallesh, and Matthew Wright. "The Design and Lessons of the ASCENT Security Teaching Lab." Proceedings of the 13th Colloquium for Information Systems Security Education. 2009.
[9] The National Collegiate Cyber Defense Competition. Web Site, Haziran 2013: http://www.nationalccdc.org/
[10] The UCSB iCTF. Web Site, February 2012: http://ictf.cs.ucsb.edu/
[11] Mullins, Barry E.; Lacey, Timothy H.; Mills, Robert F.; Trechter, Joseph E. and Bass, Samuel D. *How the Cyber Defense Exercise Shaped an Information- Assurance Curriculum*. IEEE Security and Privacy, 5(5) (September 2007), pp. 40-49
[12] DeLooze, Lori L. Counter Hack: *Creating a Context for a Cyber Forensics Course.* In Frontiers in Education Conference 2008 (FIE 2008), Saratoga Springs, NY, October 2008.
[13] Fanelli Robert L. and O'Connor, Terrence J. *Experiences with practice-focused undergraduate security education. In Proceedings of the 3rd international conference on Cyber security experimentation and test* (CSET'10). Washington, DC, August 2010.
[14] O'Leary, Mike. "*Small-Scale Cyber Security Competitions.*" (2012).
[15] Conti, Gregory, Thomas Babbitt, and John Nelson. "*Hacking competitions and their untapped potential for security education*." Security & Privacy, IEEE 9.3 (2011): 56-59.
[16] Hoffman, Lance J., Timothy Rosenberg, Ronald Dodge, and Daniel Ragsdale. "*Exploring a national cybersecurity exercise for universities*." Security & Privacy, IEEE 3, no. 5 (2005): 27-33.
[17] www.dunyayikurtaranhacker.com, 2012
[18] http://www.istsec.org/ctfdetay/, 2009
[19] http://blog.bga.com.tr/2011/05/istsec-istanbul-bilgi-guvenligi.html,2011
[20] http://www.bga.com.tr/calismalar/BGACTF2012_Cozumleri.pdf , 2012
[21] *Siber Güvenlik Yaz Kampı Duyurusu*, Http://www.uekae.tubitak.gov.tr/home.do?ot=5&rt=&sid=0&pid=0&cid=9365, 2013
[22] Ulusal Siber Güvenlik Tatbikatı 2013, http://www.tk.gov.tr/bilgi_teknolojileri /siber_guvenlik/usgt2013.php, Haziran, 2013
[23] http://www.signalsec.com/nopcon-ctf-cozumleri-ve-sunumlari ,6 Haziran 2013, nopCON Security Conference
[24] http://www.davshan.com/, Haziran 2013
[25] Ünal Tatar, Tolga Mataracıoğlu: *Analysis and Implementation of Distinct Steganography Methods*., ISCTurkey'12, pp.298-303
[26] www.md5decrypter.co.uk, Mayıs 2013
[27] http://rumkin.com/tools/cipher/caesar.php, Haziran 2013

Osman Akın, Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümünde doktora öğrencisidir. Şimdiye kadar web tabanlı uygulama geliştirme, web güvenliği konularında çalışmış olup şu anda siber güvenlik konusunda çalışmalarını devam ettirmektedir. Doktora programında tez aşamasında olup Bilgisayarlı Görme alanında nesne takibi(object tracking) konusunda çalışmaktadır.

Işıl Çınar, Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde yüksek lisans yapmaktadır. Bilgi Sistemleri Güvenliği, Veri Madenciliği, İnsan Bilgisayar Etkileşimi alanlarına ilgi duymaktadır.

Muhammer Karaman, Siber güvenlik üzerine 2 yıldır uzman olarak çalışmaktadır. Kurumsal ve ulusal Siber Güvenlik yol haritaları belirleme, siber savaş, siber-elektronik savaş, siber güvenliğin milli güvenliğe entagrasyonu ve siber savaş hukuku konularına ilgi duymaktadır.

Fatih Bilekyiğit, Bilgi Sistemlerinin İşletmesi ve Ağ topolojileri üzerine yaklaşık 10 yılı aşkın bir süre çalışmış olup şu an siber güvenlik üzerine çalışmaktadır.

Test Suite Study for Security Analysis of Digital Signature Applications

Tamer Ergun, Ferruh Özbudak, Ferda Topcan

***Abstract*—Digital signature technology is used widely for security and trust in electronic business and communications. Nowadays it becomes commonly used especially in government agencies. At this point of view, it is crucial to implement correct applications to create and verify digital signatures.**

CEN [1] has introduced the security requirements for signature creation [1] and signature verification [2] applications but neither proposed a PKI model nor implemented a test suite to evaluate the accuracy of signature applications. This is a real necessity, because a signature application have to be hardly tested and the responses of the application to a wide range of wrong scenarios have to be well analyzed.

With this work, we aimed to design a unique PKI model and state whole problematic scenarios both in signature creation and verification and address the lack of such a suite by designing *E-Signature Test Suite*. *E-Signature Test Suite* is a detailed tool, formed by a huge set of certificates and signatures, designed to analyze the accuracy of digital signature applications working mechanism both in signature creation and verification.

***Index Terms*—CAdES[2], Digital Signature, PKI[3], Time Stamp, X509 Certificate.**

I. Introduction

DIGITAL signature is a world wide used technology for security and trust in electronic business and communication. This technology is based on cryptography and more particularly public key cryptography, but the management of the system, and stating a clear identification of the parties are also very important. Such necessities bring out a famous concept, known as public key infrastructure (PKI).

An end-entity needs signature creation and verification applications to get a role and use PKI services. Even though all the PKI components work well, we have to be sure of the security of the application. This shows that, secure PKI is a necessary step of reliable transaction but beside this step, signature creation and verification applications must be also reliable. These applications must be capable of detecting each security ring of the PKI chain and must be strongly analyzed. For this aim, European Committee for Standardization (CEN) has introduced guidelines CWA 14170 [1] and CWA 14171 [2] and defined some security criterias for signature creation and verification applications but these guidelines do not define each occurable wrong scenarios in PKI explicitly and open to interpretation. European Telecommunications Standards Institute (ETSI) has also released a guideline ETSI TS 102 853 [8] for security criterias in signature verification but, similar to CWAs, this guideline does not define each wrong scenarios explicitly and even does not offer a PKI model for testing signature applications. Therefore it is an open problem to design a unique PKI model which includes all the occurable problematic scenarios for each PKI component. Besides, it is important to implement this model and create the whole certificate set which is capable to interact with all the problematic components of designed PKI model. Last step is creating the signature set which includes error scenarios coming from the certificate set mentioned above and further structural error cases in each signature types defined by ETSI [5].

In this work, we aimed to address the lack of such a PKI model and a detailed tool for analyzing signature applications. We focused on analyzing applications seperately by means of signature creation and verification. First we stated the occurable wrong scenarios in a PKI hierarchy and designed our PKI model for our test suite. After this step we created root, subroot and end-entity certificates. While creating these certificates, we paid attention to create one error case from root to end-entity certificate to analyze each error case individually. Beside the certificates, we created the occurable wrong scenarios in online certificate status protocol (OCSP) servers and certificate revocation lists (CRLs) to analyze if the application validates the required properties of revocation datas. Since time stamp is an important invariant of PKI, we also designed and created the necessary error cases for time stamp servers. After all, a big PKI model with not all but most of the wrong scenarios established.

In this paper we will present our unique PKI model and the error scenarios designed to create *E-Signature Test Suite*. The structure of the paper is as follows. In Sec. 2, some definitions and basic PKI concepts are reviewed. In Sec. 3, we present our test scenarios and scetch the hierarchical certificate chain structure of Test Suite. Finally, In Sec. 4, we present the statistical results of our work and the future work plan.

II. Preliminaries

In this section we collect necessary definitions and cover some PKI concepts.

T. Ergun is with the TÜBİTAK-KamuSM, Bilim, Sanayi ve Teknoloji Bakanlığı Ek Bina, GMK Bulvarı 128/B Kat:3, Tandoğan, Çankaya, Ankara, Turkey.

F. Özbudak is with the Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bulvarı No. 1, 06800 Ankara, Turkey.

F. Topcan is with the TÜBİTAK-KamuSM, Bilim, Sanayi ve Teknoloji Bakanlığı Ek Bina, GMK Bulvarı 128/B Kat:3, Tandoğan, Çankaya, Ankara, Turkey.

Manuscript revised August 22, 2013.

[1]European Commitee for Standardization

[2]CMS Advanced Electronic Signatures

[3]Public Key Infrastructure

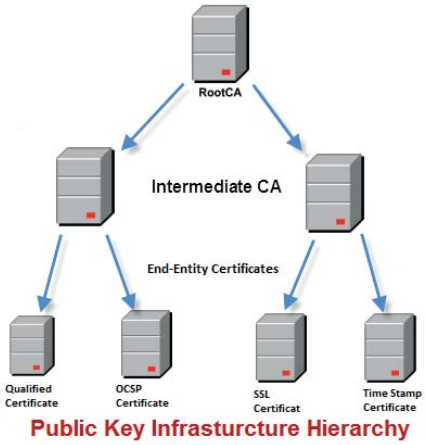


Fig. 1: CA Hierarchy

Public-Key Key of a user's key pair which is publicly known.
Private-key Key of a user's key pair which is known only by that user, and responsible for the use of it.
Certificate Digitally signed data, binding identity with public key.
Qualified Certificate A certificate which meets the requirements in [4], [17], [15].
CA Certificate An authority authorized legally to create and assign public-key certificates.

More definitions on certificates can be found in [11] and [12].

PKI hierarchy is an other important issue. Along the path from end entity certificate to a RootCA, every component of PKI is signed by an authorized signer. In this signature chain, signer is known as issuer and the signed component is known as subject. Therefore the word 'hierarchy' indicates the total issuer-subject relation of the whole system. In figure 1, a hierarchical two-level chain structure is shown. In order to trust an end entity certificate, one should verify its respective intermediate CA (issuer) and lastly the RootCA. All necessary verification items will be covered in section III. Beside the PKI hierarchy, we should care of two important concepts about certificate revocation check:

CRL is the abbreviation of Certificate Revocation List and includes all revoked certificates with serial number and revocation date.
OCSP is a response data signed by an OCSP certificate. This response data contains the revocation status of the requested certificate.
OCSP Certificate is the certificate authorized to sign OCSP responses.

Both in CRL and OCSP response, the revocation date of a revoked certificate is crucial. Since revocation date is so crucial, date used for revocation check must be trusted. As stated before, trusted concept means accurate data signed by a trusted CA. Therefore time stamp is used to indicate the accurate date.

Time Stamp is a token containing a specific information and a date such that, that specific data exists before the date in token. Time stamp token is also a signed data issued by a time stamp certificate.
Time Stamp Certificate is the certificate authorized to sign time stamp tokens.

Lastly we should cover electronic signature formats. ETSI defined 10 signature formats [5]. In signature verification part of *E-Signature Test Suite*, we implemented scenarios, derived from our unique PKI model, in these 10 formats. Now we briefly define frequently used ones.

CAdES-BES namely the basic electronic signature containing signer's document, some signed attributes and the digital signature.
CAdES-T CAdES-BES with time stamp.
CAdES-XL CAdES-T with complete certificate and revocation references and values.

Beside of ETSI signature types, signature files can be splitted into two groups as attached and detached signatures.
Attached is the type of signature where tha actual content (message) is stored in the signature files.
Detached is the type of signature where the actual content (message) is not stored in the signature files. In this case both the signature file and the content have to be stored for validation.

III. Test Suite

In this section we shall study the details of our unique PKI model designed for test suite and define the error cases, nodes of PKI tree, both in signature creation and signature verification parts.

A. Signature Creation

This part of the suite defines the error cases designed to construct the PKI model and to analyze the signature creation accuracy of signature applications. The aim is to create verifiable signature by means of applying certificate validation prior to signing process. While designing, we stated the wrong scenarios and grouped them with respect to their natures. There exists five types of wrong scenarios:

1) Certificate Self Check: Certificate self check section includes the scenarios related with the structure of end entity certificates with respect to the directives coming from [4], [6], [13], [14], [15], [17] in Turkey. Self check scenarios can be grouped into three groups as qualified certificate checks, certificate expiration check and certificate signature check.

Qualified Certificate Checks:

- **Non-Repudiation Absent:** Non-Repudiation is a MUST field in a qualified certificate. In this scenario, a qualified certificate without Non-Repudiation field is designed. We aim to determine if the application checks certificate's Non-Repudiation field to accept it as a qualified certificate.
- **ETSI[4] QC Statement ID Absent:** In this scenario, a qualified certificate without ETSI QC Statement ID

[4]The European Telecommunications Standards Institute

(0.4.0.1862.1.1) is designed. We aim to determine if the application checks certificate's ETSI QC Statement ID field to accept it as a qualified certificate.

- **ICTA[5] QC Statement ID Absent:** In this scenario, a qualified certificate without ICTA QC Statement ID (2.16.792.1.2.1.1.5.7.1.1) is designed. We aim to determine if the application checks certificate's ICTA QC Statement ID field to accept it as a qualified certificate.
- **ICTA QC Statement Info Absent:** In this scenario, a qualified certificate without ICTA QC Statement Info ("Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır.[6]") is designed. We aim to determine if the application checks certificate's ICTA QC Statement Info field to accept it as a qualified certificate.
- **CP User Notice Statement Absent:** ICTA QC Statement Info has to be also stated in Certificate Policies [11] field of a qualified certificate. In this scenario, a qualified certificate without CP User Notice Statement is designed. We aim to determine if the application checks certificate's CP User Notice Statement field to accept it as a qualified certificate.

Last three items are specific for applications in Turkey but the others are global.

Certificate Expiration Check: Every public-private key pair has a cryptographic life time. Since certificate is defined as a digital data binding public key of an end-entity with his id, every certificate has a life time. In this scenario, an expired certificate is designed. We aim to determine if the application checks certificate's expiration date and do not permit to sign the document.

Certificate Signature Check: In the PKI hierarchy we stated that every evidence is signed by a trusted authority. Hence, an end entity certificate is also a signed data and is signed by its issuer, which is the intermediate CA (SubRootCA) illustrated in figure 1. The intermediate CA is also signed by RootCA and RootCA is self-signed, means RootCA signs itself. In this scenario, a signature forged end entity certificate is designed. We aim to determine if the application checks certificate's signature and if not valid, do not permit to sign the document.

2) Certificate Revocation Check: In daily life, like credit cards, a certificate may be revoked for some reasons. After the exact date of revocation, it is expected that no signature can be constructed with this certificate. Revocation status of a certificate is published in two ways. One of them is CRL and the other one is OCSP. Clients use these services by using access points stated in certificates. CRL for a specific certificate can be obtained by using CDP[7] field of the certificate. Similarly, OCSP response for a certificate can be obtained by using AIA[8] field of the certificate. In revocation check scenarios, revocation check form CRL and OCSP have to be checked seperately to determine that an application is able to deal with these services clearly. For this reason we designed two certificates such that both of them are revoked. Certificates differ from each other as one of them has just CDP field but not OCSP address and the other one has the reverse. We aim to determine if the application checks certificates' revocation info accurately in both ways.

3) Revocation Info Check: In section III-A2 the issue was to evaluate, the accuracy of getting revocation status of a certificate and the clearness of interaction with the CRL and OCSP services. In this part we examine the validity of a CRL file and an OCSP response and state in which situations they become invalid.

CRL Validation Checks:

- **Expired CRL:** As certificates, CRL files have also life time. This life time is restricted between thisUpdate and nextUpdate [11] fields of CRL file. In revocation control of a certificate from CRL, nextUpdate has to be greater than validation time. If not, in mean time, this CRL can not be used to validate a certificate since a fresh CRL has to be released before nextUpdate date of older CRL. In this scenario an expired CRL is designed. Aim is to determine if the application compares nextUpdate date of a CRL used for a specific end entity certificate with validation time.
- **Signature Forged CRL:** CRL is also a signed data and the signer CA of the CRL, used to be informed about revocation status of a specific certificate, has to be same with the signer (issuer) CA of that specific certificate [4]. If the signature of a CRL is forged than CRL file becomes invalid. In this scenario a signature forged CRL file is designed. Aim is to determine if the application verifies the signature of the CRL file.

OCSP Response Validation Checks:

- **Expired OCSP Response:** Similar with CRL, OCSP responses are expired for some reasons. OCSP responses have thisUpdate, nextUpdate and producedAt fields [9]. nextUpdate field indicates the time at or before which newer information will be available about the status of the certificate. This field is optional and if not set it means that newer revocation information is available all the time. producedAt indicates the time at which the OCSP responder signs the response. Therefore if nextUpdate is null then it means producedAt is the time after which newer information will be available about the certificate. At validation time, producedAt field has to be greater than validation time and if not, signature creation application must interpret the OCSP response as expired. In this scenario an OCSP server producing expired OCSP responses with null nextUpdate field is designed. Aim is to determine if the application compares producedAt with validation time.
- **Signature Forged OCSP Response:** OCSP response is also a signed data and is signed by an OCSP

[5]Information and Communications Technologies Authority

[6]This certificate is a quailified certificate according to e-signature law numbered 5070

[7]Certificate Distribution Point

[8]Authority Information Access

certificate. Issuer of the OCSP certificate has to be same with the issuer of the certificate to be informed about its revocation status [9]. If the signature can not be validated, the OCSP response becomes invalid. In this scenario an OCSP server producing signature forged responses is designed. Aim is to determine if the application verifies the signature of the OCSP response.

- **Expired OCSP Certificate:** An OCSP certificate has also a life time. In this scenario an OCSP server with an expired OCSP certificate, producing responses is designed. A signature application has to verify both the OCSP response and the OCSP certificate. Aim is to determine if the application checks the expiration status of the OCSP certificate.
- **Signature Forged OCSP Certificate:** An OCSP certificate is a signed data, signed by its issuer. In this scenario an OCSP server with a signature forged OCSP certificate is designed. Aim is to determine if the aplication checks the signature of the OCSP certificate.
- **Revoked OCSP Certificate:** As other certificates, an OCSP certificate can be revoked for some reasons. In our PKI model, revocation status of OCSP certificates are published via CRL. In this scenario an OCSP server with a revoked OCSP certificate, producing responses is designed. Aim is to determine if the application checks the revocation status of the OCSP certificate.

4) Issuer Check: So far we defined wrong scenarios related with end entity certificates. Beyond end entity certificates, most of the stated wrong scenarios can be applied to the subCA and RootCA certificates. We aimed to determine if the applications accurately handle necessary controls for subCA and RootCA authorities. In the case where just end entity certificates are concerned, we have a tree path with a valid root, valid subroot and defined problematic end entity certificates but while creating problematic scenarios for also subroots and roots, our PKI model became enlarged.

5) Time Stamp Check: In digital signature technology, time stamp is used for different reasons [5]. Time stamp token (response) is a signed data, signed by a trusted time stamp certificate. A signature application MUST check all necessary controls and verify the token. From this point of view we created negative scenarios that make a time stamp token invalid and embed the sources of these scenarios as new time stamp servers to our PKI model.

Time Stamp Validation Checks:

- **Signature Forged TS Token:** As all evidences used in PKI technology, time stamp token is a signed data. It is signed by a time stamp certificate with a trusted issuer. A malicious user of PKI may try to edit the token and change the time or the digest of the event. For resisting such a situation, signature creation applications must be capable of validating the signature of the token. In this scenario a time stamp server producing signature forged tokens is designed. Aim is to determine if the application verifies the signature of the time stamp token and informs the user about this issue.
- **Expired TS Certificate:** A time stamp certificate has also a life time. In this scenario a time stamp server with an expired time stamp certificate, producing tokens is designed. Signature application has to verify both the time stamp token and the time stamp certificate. Aim is to determine if the application checks the expiration status of the time stamp certificate.
- **Signature Forged TS Certificate:** Time stamp certificate is a signed data, signed by its trusted issuer. In this scenario a time stamp server with a signature forged time stamp certificate is designed. Aim is to determine if the application checks the signature of the time stamp certificate.
- **Revoked TS Certificate:** As other certificates, a time stamp certificate can be revoked for some reasons. In our PKI model, revocation status of TS certificates are published via CRL. In this scenario a time stamp server with a revoked time stamp certificate, producing time stamp tokens is designed. Aim is to determine if the application checks the revocation status of the TS certificate.
- **TS Root CA Scenarios:** All the scenarios with time stamp servers so far were about tokens and the time stamp certificates but a signature creation application must also validate the issuer of the time stamp certificate. From this point of view we designed 10 more time stamp certificates whose issuers are problematic because of different reasons. Each root CA has an individual mistake and aim is to determine if the application makes the issuer controls beyond the self check of time stamp token.

B. Signature Verification

This part of the suite is designed to analyze the signature verification accuracy of signature applications. Verification part of the suite includes signature files created in 10 signature types defined in [5]. These types are:

- BES (Basic Electronic Signature),
- EPES (Explicit Policy Based Electronic Signature),
- ES-T (Electronic Signature with Time),
- ES-C (Electronic Signature with Complete Validation Data References),
- ES-X-Type 1 (Extended Electronic Signature with Time Type 1),
- ES-X-Type 2 (Extended Electronic Signature with Time Type 2),
- ES-X-Long (Extended Long Electronic Signature),
- ES-X-Long-Type 1 (Extended Long Electronic Signature with Time Type 1),
- ES-X-Long-Type 2 (Extended Long Electronic Signature with Time Type 2),
- ES-A (Archival Electronic Signature).

Each of the signature files has one error case derived from our unique PKI model defined in section III-A and signature

type specific issues extending from type BES to type ES-A. From this point of view, each set of signatures for a particular type is equally or more detailed then the previous one and so has further analysis criterias. We can group our signature verification specific wrong scenarios in 5 groups.

1) Signature File Format Check: In these scenarios wrong formatted, do not compatible with ETSI [5], signature files are designed and aim is to determine if the signature verification application checks the format of the signature file.

2) Signature Verification Check: It means cryptographic validation of raw signature data files. In this scenario, we forged the signature of either signature file, time stamp token, CRL or OCSP response. Aim is to determine if the signature verification application verifies the signature of all signed datas used in the signed file.

3) Certificate Path Verification Check: Certificate path consists of a root certificate, an intermediate certificate and an end entity certificate. End entity certificates are either qualified certifices, OCSP certificates or time stamping certificates. For all certificates in the path one of the following errors may occur:

- **Signature Forged Certificate:** Aim is to determine if the signature verification application checks the signature of each certificate forming the path from the qualified end entity certificate to the trusted root certificate in the signature file.
- **Revoked Certificate:** Aim is to determine if the signature verification application checks the revocation status of each certificate forming the path from the qualified end entity certificate to the trusted root certificate in the signature file.
- **Expired Certificate:** Aim is to determine if the signature verification application checks the expiration status of each certificate forming the path from the qualified end entity certificate to the trusted root certificate in the signature file.
- **Certificate usage constraints does not match:** This scenario is for qualified end entity certificates. Aim is to determine if the signature verification application checks the qualified certificate properties of each signer certificate in the signature file.

4) Validation Data Access Check: Validation datas are certificates and revocation informations (CRL or OCSP responses) to validate the certificate path due to the signature time. Validation data must be collected within a short period after the signing time and stored on a local store or attached to the signature file. For signature types ES-C and above, validation datas, its references or both are attached to the signature. For all validation datas one of the following errors may occur:

- **Missing Validation Data:** In this scenario we omitted a revocation-certificate reference [5] or a revocation-certificate value from the signature. Aim is to determine if the signature verification application realizes the missing data.
- **Corrupted Validation Data:** In this scenario we corrupted a revocation-certificate reference [5] or a revocation-certificate value from the signature. Aim is to determine if the signature verification application realizes the corrupted data.
- **Expired Validation Data:** In this scenario we attached an expired validation data derived from our PKI model, defined in section III-A3. Aim is to determine if the signature verification application realizes the expired data.

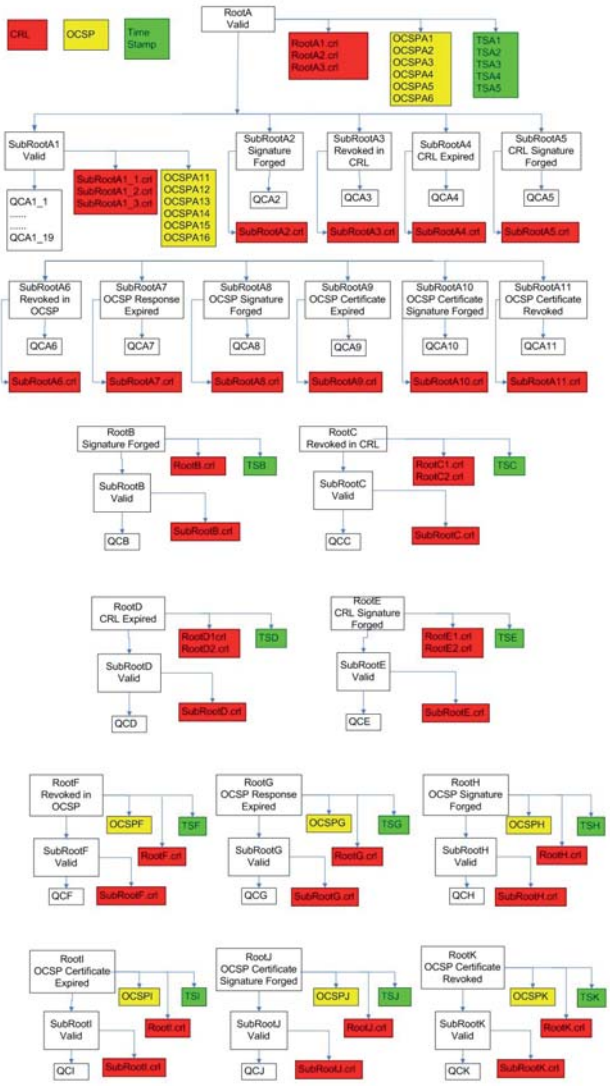


Fig. 2: E-Signature Test Suite Hierarchy

5) Archive Signature Check: ES-A, archival form, is a signature type extending from ES-XL, ES-XL Type 1 or ES-XL Type 2 where the whole signature is time stamped, known as archive time stamp. It is against to protect breaking of encryption algorithms and hashing algorithms. These tests are designed to check e-signature archiving verification process of signature verification applications.

IV. Conclusion

In this work we aimed to solve an important lack of digital signature process, security and reliability of signature creation

PKI Element Type	Total Amount
Root Certificates	11
Sub Root Certificates	21
Qualified End Entity Certificates	39
Time Stamp Servers	15
OCSP Servers	18
Released CRLs	39

Fig. 3: Signature Creation Suite

and verification applications. CEN [1], [2] and ETSI [8] has introduced some security concepts on both signature applications but these concepts are general and neither propose a PKI model nor an implementable design theory on these subjects. In order to fill this gap, we studied on designing a unique PKI model and implemented this model to produce certificate and signature set of *E-Signature Test Suite*. Our PKI model is shown in figure 2. As we stated before, each path from an end entity certificate to its root certificate contains just one faulty. Thus we succeed to evaluate the accuracy of signature applications to individual error scenarios independently.

Since we aimed to design each occurable error scenarios in a PKI model, signature creation part of the suite, defined in section III-A composed a huge public key infrastructure statistically charted in figure 3. We have established 18 OCSP Responders and 15 Time Stamp services. These services are available online and accessible during the signature creation tests. SubRoot certificates, root certificates and CRL's are also published online and accessible through the web.

In the signature verification part, we created wrong scenarios in 10 signature types defined in III-B. While creating these signatures, we used TUBITAK[9]-BILGEM[10] digital signature libraries. Types of signatures and the total amount of signature files created are shown in figure 4. Our design philosophy for creating signature files is same as signature creation hierarchy structure such that each signed file has just one error for the same reason. As seen in figure 4, from type BES to ES-A, the number of signature files created are increasing. This is because the details of the signature files are extending as signature type tends to ES-A.

In Turkey, digital signature applications used by government agencies are controlled by TUBITAK-BILGEM-KAMUSM[11]. This task is given to TÜBİTAK-BİLGEM-KAMUSM by the prime ministry [3], [16]. The output of this work is used to evaluate government agencies applications since December, 2012. During these period, we realized different kinds of mistakes that the signature applications do and correct them.

Also in this period we realized that some applications have efficiency loss. Even if they apply the validation rules successfully, the path they follow is time consuming. The order of validation for a particular issue, say OCSP response validation, affects the time spent considerably. As future work, we plan to design an efficient verification path for some

Signature Type	Attached	Detached
BES	46	46
EPES	46	46
ES-T	70	70
ES-C	78	78
ES-X TYPE 1	93	93
ES-X TYPE 2	93	93
ES-XL	95	95
ES-XL TYPE 1	110	110
ES-XL TYPE 2	110	110
ES-A	110	110
	851	851
Total	1702	

Fig. 4: Signature Validation Suite

evidences used in electronic signatures and assist signature application developers in terms of efficiency.

Acknowledgment

This research project would have been possible with the support of TUBITAK-BILGEM-KAMUSM.

References

[1] CEN, *CWA 14170 - Security requirements for signature creation applications,* May 2004.
[2] CEN, *CWA 14171 - General guidelines for electronic signature verification,* May 2004.
[3] Doç. Dr. T. K. Bensghir, F. Topcan, *E-imza: Türkiye'de Kamu Kurumlarında Uygulanması,* TODAİE Yayın No:356, Ankara, Turkey, December 2010.
[4] Committee Decision, *Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberine İlişkin Kurul Kararı, 2007/DK-77/207,* 18 April 2007.
[5] ESI, *ETSI TS 101 733 - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES),* November 2009.
[6] ESI, *ETSI TS 101 862 - Electronic Signatures and Infrastructures (ESI); Qualified Certificate profile,* March 2004.
[7] ESI, *ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES),* June 2009.
[8] ESI, *ETSI TS 102 853 - Signature verification procedures and policies,* July 2012.
[9] IETF, *RFC2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,* June 1999.
[10] IETF, *RFC3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP),* August 2001.
[11] IETF, *RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* May 2008.
[12] ITU-T, *Rec. X.509 - Information technology - Open systems,* November 2008.
[13] Official Gazette, *Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, 25692,* 06 January 2005.
[14] Official Gazette, *Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, 25692,* 06 January 2005.
[15] Official Gazette, *E-signature law No. 5070, 25355,* January 2004.
[16] Official Gazette, *Kamu Sertifikasyon Hizmetlerine İlişkin Usul ve Esaslar, 2006/13,* 19 April 2006.
[17] Official Journal, *Directive 1999/93/EC of The European Parliement and of The Council,* December 1999.

[9]The Scientific and Technological Research Council of Turkey
[10]Informatics and Information Security Research Center
[11]Government Certification Authority

Genetik Algoritma ve Tekil Değer Ayrışımı Tabanlı Yeni Bir Kırılgan Resim Damgalama

Veysel Aslantaş, Mevlüt Doğru

***Özet*—Bu çalışmada, Genetik Algoritma (GA) kullanarak Tekil Değer Ayrışımı (Singular Value Decomposition - SVD) tabanlı yeni bir kırılgan resim damgalama tekniği geliştirilmiştir. Çoklu ölçekleme faktörleri (scaling factors - SFs) kullanarak damganın her bir satırı ölçeklenmiştir. Orijinal resim de bloklara ayrılmıştır. Bu blokların tekil değerlerine (singular values - SVs) sırasıyla farklı bir damga satırı gömülerek damgalanmış resim elde edilmiştir. Önerilen metotta, maksimum saydamlık için ölçekleme faktörleri GA ile optimize edilmiştir. Deneysel sonuçlar, maksimum saydamlığa ulaşıldığını göstermektedir. Damgalanmış resme çeşitli saldırılar uygulanarak da kırılganlık tespiti yapılmıştır. Saldırı olmadan damga olduğu gibi elde edilirken, saldırı olması durumunda ise gömülen damga oldukça bozulmaktadır.**

***Anahtar Kelimeler*—Genetik Algoritma, Kırılgan Resim Damgalama, Tekil Değer Ayrışımı.**

***Abstract*—In this paper, a novel fragile image watermarking scheme based on SVD using GA is presented. Watermark of every line is scaled by using multiple SFs. Host image is divided into blocks. Watermarked image is obtained by embedding a different line of watermark to SVs of the every block. In this proposed method, the SFs are optimized using GA to achieve maximum transparency. Experimental results indicate that reached the highest transparency. Fragility detected under various attacks. When an attack does not occur exactly the original embedded watermark is achieved or else the embedded watermark is intensely corrupted.**

***Index Terms*—Genetic Algorithm, Fragile Image Watermarking, Singular Value Decomposition.**

I. GİRİŞ

SAYISAL damgalama; ses, resim ve video gibi sayısal verilerin korunmasında yaygın olarak kullanılan tekniklerden biridir. Bu teknikte amaç, bir sayısal verinin damga olarak başka bir sayısal verinin içerisine gizlenmesidir. Telif hakkının korunması, veri doğruluğunun ispatı, doküman arşivleme, dokümana ait bilgilerin saklanması ve dijital parmak izi korunması gibi birçok işlemler için sayısal damgalama kullanılmaktadır [1,2]. Resim damgalama genel olarak; gömülme ortamına, görülebilirliğe ve kalıcılığa göre sınıflandırılabilir [2-4].

Gömülme ortamına göre damgalama; resim ve frekans uzayı teknikleri olarak iki guruba ayrılabilir. Resim uzayı tekniklerinde damgalama işlemi doğrudan orijinal resmin piksellerine eklenerek gerçekleştirilirken, frekans uzayı tekniklerinde ise Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform - DCT), Ayrık Dalgacık Dönüşümü (Discrete Wavelet Transform - DWT) ve SVD gibi dönüşüm teknikleri aracılığıyla frekans uzayı katsayılarına damga eklenerek gerçekleştirilmektedir [1,2]. Genellikle, frekans uzayı metotları birçok saldırıya karşı resim uzayı metotlarına göre daha dayanıklı ancak bir dönüşüm uygulandığından hesaplama maliyeti olarak daha yüksektir [2,5-7].

Görülebilirliğine göre resim damgalama; görünür ve görünmez (saydam) olarak iki guruba ayrılabilir. Görünür damgalar, televizyon yayınlarına eklenmiş logolar gibi insan gözüyle rahatlıkla görülebilmektedir. Görünmeyen damgalar ise insan görme sistemince algılanamayacak şekilde sayısal verinin içerisine eklenen damgalardır. Görünür damgalara göre daha güvenli ve dayanıklıdır [2].

Kalıcılığa göre damgalama teknikleri; dayanıklı, kırılgan ve yarı-kırılgan olmak üzere üç gurupta sınıflandırılabilir. Dayanıklı damgalamada damga, çeşitli saldırılardan (filtreleme, gürültü ekleme vb.) etkilenmemelidir. Kırılgan damgalamada, damgalanmış resme basit bir işlem uygulandığında damga kolaylıkla bozulmalıdır. Bu tür damgalar genellikle veri doğrulama amacıyla kullanılır. Yarı-kırılgan damgalamada ise, belirli saldırılara maruz kaldığında damga bundan etkilenmemeli, ancak içerik değişikliği gibi kötü niyetli saldırılara karşı damga yok olabilmelidir [6,8,9]. Kırılgan damgalama yönteminde damgalanmış resimdeki damga insan gözüyle fark edilemez. Güvenlik açısından doğrulama amacına uygun olarak da resimler yetkisiz kişiler tarafından değiştirilmemelidir. Bunun için, kırılgan damgalama yöntemi kullanılarak orijinal verinin bozulup bozulmadığı hakkında bilgi alınabilmektedir.

SVD, uyarlaması kolay olduğundan damgalama dahil bir çok alanda güçlü bir nümerik analiz tekniği olarak kullanılmaktadır. Literatürde, farklı yapay zekâ teknikleri kullanılarak DCT dönüşümüyle kırılgan damgalama teknikleri [10-12], SVD dönüşümüyle de maliyet fonksiyonu değiştirilerek dayanıklı, kırılgan ve yarı-kırılgan damgalama tekniği [13] geliştirilmiştir. Ayrıca, herhangi bir yapay zeka tekniği kullanmadan DCT tabanlı [14] ve DWT-SVD tabanlı [15] dayanıklı damgalama teknikleri de mevcuttur. Optimizasyon algoritması kullanarak geliştirilen bazı kırılgan damgalama metotları ve bu makalede önerilen metodun karşılaştırılması ise Tablo I'de verilmiştir.

Bu çalışmada, gri seviye resimler için GA kullanılarak SVD tabanlı kırılgan damgalama tekniği geliştirilmiştir. Ölçekleme faktörleri kullanılarak satırları ölçeklenmiş olan damganın her bir satırının, bloklara ayrılmış orijinal resmin her bloğun tekil değerlerine farklı bir damga satırı gömülecek şekilde eklenmesiyle damgalanmış resim elde edilmiştir. Damga ekleme sırasında ölçekleme faktörleri en yüksek saydamlığa ulaşacak şekilde GA ile belirlenmiştir. Deneysel sonuçlar, saydamlık ve saldırı olmadan damganın

Veysel Aslantaş, Erciyes Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Kayseri, Türkiye (e-mail:aslantas@erciyes.edu.tr).

Mevlüt Doğru, Maliye Bakanlığı, Milli Emlak Genel Müdürlüğü, Bilgi İşlem Daire Başkanlığı, Ankara, Türkiye (e-mail:mevlut_dogru@milliemlak.gov.tr).

TABLO I
ÖNERİLEN METOT VE LİTERATÜRDEKİ BAZI METOTLARIN KARŞILAŞTIRMASI

Kullanılan Teknik ve Algoritma	*Özellik*	*Yayımlama*
DCT Klonal Seçme Algoritması (KSA)	Kırılgan	Aslantas vd. (2007)
DCT Parçacık Sürü Algoritması (PSO)	Kırılgan	Aslantas vd. (2008)
DCT GA, PSO, KSA, Diferansiyel Gelişim Algoritması (DGA)	Kırılgan	Aslantas vd. (2009)
SVD GA	Kırılgan Yarı-kırılgan Dayanıklı	Modaghegh vd. (2009)
SVD GA	Kırılgan	Önerilen Metot

geri elde edilmesi bakımından geliştirilen tekniğin başarılı olduğunu, saldırı olduğunda ise damganın oldukça bozulduğunu göstermektedir.

II. SVD TABANLI DAMGALAMA

SVD ile *NxN* boyutlarındaki bir *A* matrisi $A=USV^T$ olacak şekilde üç ayrı matrisin çarpımına eşitlenebilir. Burada *NxN* boyutlarındaki *U* ve V^T ortogonal matris, *NxN* boyutlarındaki *S* ise köşegen (diagonal) matristir. Köşegen elemanları dışındaki elemanları sıfır olan *S* matrisi, *A* matrisinin tekil değerleri olarak adlandırılır [5,6].

A. Damga Gömme

Orijinal resim (*I*) ile damganın (*W*) boyutlarının sırasıyla *NxN* ve *Mx2M* (N>2M) olduğu, *k*'nın da ölçekleme faktörü olduğu varsayılırsa, damga gömme işleminde aşağıdaki adımlar uygulanmıştır. Burada, W_i damganın *i.* satırı, $I_{(m,n)}$ ise bloklara ayrılmış orijinal resmin *m.* satır ve *n.* sütun bloğunu ifade etmektedir.

1) Orijinal resim *M/2xM/2*'lik bloklara bölünür.

$$I = \bigcup_{m=1}^{2N/M} \bigcup_{n=1}^{2N/M} I_{(m,n)} \tag{1}$$

2) Orijinal resmin her bloğuna SVD uygulanır.

$$I_{(m,n)}^{SVD} = U_{(m,n)} S_{(m,n)} V_{(m,n)}{}^T \tag{2}$$

3) Blokların $S_{(m,n)}$ matrisine damganın satırları gömülür.

$$S_{(m,n)}^{*} = \bigcup_{m=1}^{2N/M} \bigcup_{n=1}^{2N/M} S_{(m,n)} + k * \bigcup_{i=1}^{4N^2/M^2} diag(W_i) \tag{3}$$

4) Damgalanmış resim blokları hesaplanır.

$$I_{(m,n)}^{D} = U_{(m,n)} S^{*}{}_{(m,n)} V_{(m,n)}{}^T \tag{4}$$

5) Damgalanmış resim blokları birleştirilerek damgalanmış resim (I_W) elde edilir.

$$I_W = \bigcup_{m=1}^{2N/M} \bigcup_{n=1}^{2N/M} I_{(m,n)}^{D} \tag{5}$$

B. Damga Çıkarma

SVD ile damgalanmış resimden damga çıkarma işleminde aşağıdaki adımlar sırayla uygulanmıştır.

1) Damgalanmış resim, bloklarına ayrıldıktan sonra her bir bloğa SVD uygulanır.

$$I_{(m,n)}^{DSVD} = U'_{(m,n)} S'_{(m,n)} V'_{(m,n)}{}^T \tag{6}$$

2) Her bloktan, gömülen damga çıkarılır.

$$W_i^{*} = \bigcup_{m=1}^{2N/M} \bigcup_{n=1}^{2N/M} diag(S'_{(m,n)} - S_{(m,n)}) / k \tag{7}$$

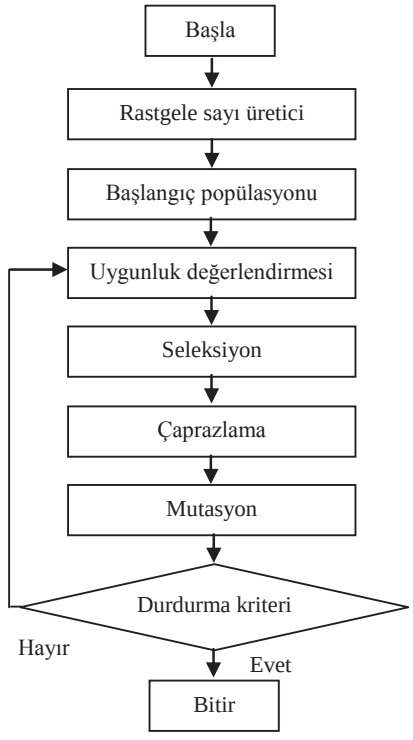
3) Her bloktan çıkarılan damga satırları birleştirilerek çıkarılan damga (W^*) elde edilir.

$$W^{*} = \bigcup_{i=1}^{4N^2/M^2} W_i^{*} \tag{8}$$

III. GENETİK ALGORİTMANIN TEMEL YAPISI

Şekil 1'de özetlenen temel GA [16]; rastgele sayı üretici, uygunluk değerlendirmesi ve genetik operatörler (seleksiyon, çaprazlama ve mutasyon) bileşeninden oluşmaktadır. Başlangıçta; algoritma tasarımcısı tarafından durdurma kriteri, maliyet fonksiyonu ve parametreler belirlenir. Durdurma kriteri sağlanıncaya kadar da optimizasyon işlemi devam eder.

Başlangıç popülasyonu, algoritmanın başlangıcında rastgele sayı üretici tarafından oluşturulan sayı dizisidir. Her bir dizi, optimizasyon problemi için muhtemel çözümü gösterir. Sonraki aşamada her bir dizinin uygunluk değerlendirmesi, maliyet fonksiyonuna göre hesaplanır.



Şekil 1. GA'nın temel akış şeması.

Uygunluk değeri, mevcut çözümlerin en iyisinin ölçümü için kullanılan bir değerdir. Seleksiyon operatörü, doğal seleksiyon fonksiyonunu yerine getirir. Bireyleri temsil eden dizilerden uygunluk değeri daha yüksek olan sonraki nesillere aktarılır.

Çaprazlama operatörü ile rastgele birey çiftleri seçilir ve yeni bireyler oluşturulur. En temel çaprazlama işlemi, ebeveynin rastgele seçilen bir noktasından kesilerek diğer ebeveynin aynı kesme noktasından sonraki elemanları ile yer değiştirmesidir. Ebeveynlere uygulanacak çaprazlama işleminin miktarı çaprazlama oranına (crossover rate - CR) göre belirlenir. Mutasyon operatörü, rastgele olmak üzere mutasyon oranına (Mutation rate - MR) göre bireyi temsil eden sayı değerlerinin değiştirilmesini sağlamaktadır. Genetik operatörlerin amacı, mevcut çözümleri daha kaliteli uygunluk değerine sahip çözümlere dönüştürmektir [5].

IV. GA VE SVD TABANLI KIRILGAN DAMGALAMA

GA, başlangıçta rastgele üretilen SF'lere uygulanarak saydamlık açısından optimum damgalama elde edilmiştir. Bu çalışmada geliştirilen GA tabanlı damga gömmenin blok diyagramı Şekil 2'de gösterilmektedir.

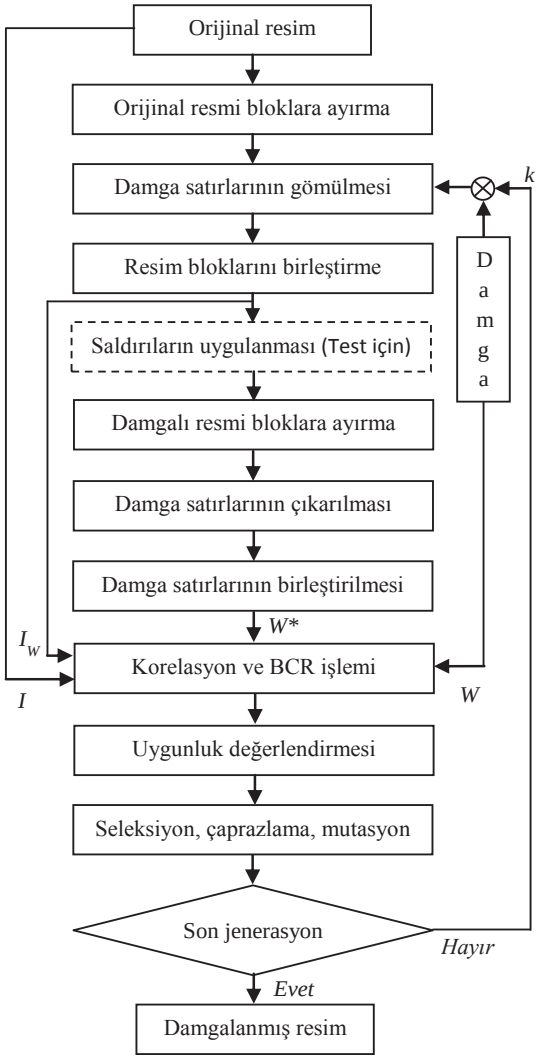
Gömme işlemi, Bölüm II. A'da verilen bilgilere göre yapılmaktadır. Saldırıya uğramış veya uğramamış damgalanmış resimden damgalar da Bölüm II. B'de verilen bilgilere göre çıkarılmıştır. Bu işlemler sonucunda çıkarılan ikili (binary) damganın piksellerinde SF'lerin etkisiyle değişimler olabileceğinden; çıkarılan damganın piksel değerleri 0.5'den daha küçük olanlara 0, 0.5 ve daha büyük olanlara ise 1 atanarak yeniden ikili damga elde edilmiştir. Çeşitli veri doğrulama işlemleri için farklı damgalama uygulamaları kırılganlık testi gerektirebilir. Bu çalışmada damganın kırılganlığını test edebilmek için yeniden ölçekleme (YO), döndürme (DN), gausian gürültü (GG) ve ortalama filtreleme (OF) saldırıları uygulanmıştır. Damgalanmış resimlere bu saldırılar uygulanarak kırılganlık tespiti yapılmıştır. Geliştirilen modelin esnekliğinden dolayı farklı saldırılar da uygulanabilir.

İki boyutlu korelasyon değeri ($corr_I$) sayesinde orijinal resim ile damgalanmış resim arasındaki benzerlik (saydamlık amacıyla), denklem 9'da gösterilen *"Bit Doğruluk Oranı" (Bit Correct Rate - BCR)* sayesinde de orijinal damga ile çıkarılan damga arasındaki farklılık (kırılganlık amacıyla) hesaplanmıştır. Denklemde; W_t orijinal damgayı, W_t^* çıkarılan damgayı, M_W damganın satır sayısını, N_W damganın sütun sayısını, $\oplus$ simgesi ise lojik *XOR* operatörünü göstermektedir. *BCR* %100 olduğunda gömülen damga tamamen doğru bir şekilde çıkarılabilmiştir [17].

$$BCR = \left(1 - \frac{1}{M_W \, x \, N_W} \sum_{t=1}^{M_W \, x \, N_W} \left(W_t \oplus W_t^*\right)\right) . 100\% \quad (9)$$

Korelasyon ve *BCR* kullanılarak önerilen maliyet fonksiyonu denklem (10)'da gösterilmektedir. Bu denklem, saydamlık ve kırılganlık için durdurma kriteri sağlanıncaya kadar GA tarafından minimize edilmiştir. Durdurma kriterine örnek, maksimum jenerasyon sayısı verilebilir. Burada *t* jenerasyon sayısını, f_i ise *i.* jenerasyondaki maliyet fonksiyonunun değerini ifade etmektedir.

$$f_i = BCR_{i=1}^{t} - corr_I(I, I_W) \quad (10)$$



Şekil 2. GA tabanlı damga gömme ve çıkarmanın blok şeması.

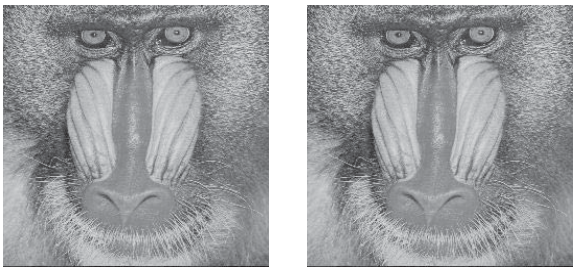
V. DENEYSEL SONUÇLAR

Geliştirilen metodu değerlendirmek için damga olarak, Şekil 3 (a)'da gösterilen 32x64 boyutundaki orijinal ikili resmin 32x8'lik bloklar halinde sırayla alt alta yerleştirilmesiyle oluşturulan ve Şekil 3 (b)'de gösterilen 256x8'lik ikili resim kullanılmıştır. Kaynak resim olarak da 256x256 boyutlarındaki Şekil 4 (a)'da gösterilen Baboon ve Şekil 5 (a)'da gösterilen Gemi resimleri kullanılmıştır. Şekil 3 (b)'deki damga gömülerek oluşturulan damgalanmış resimler Şekil 4 (b) ve Şekil 5 (b)'de gösterilmektedir. Her iki damgalı resme de herhangi bir saldırı uygulamadan çıkarılan damgalar ise Şekil 6'da verilmiştir. Görsel analizle de görüleceği gibi damgalı resimlerde ve çıkarılan damgalarda herhangi bir bozulma gözükmemektedir. Test aşamasında yöntemin saldırılara karşı kırılganlığını ölçmek için YO (bilineer: 256→128→256), DN (bilineer: 3^0), GG ve OF işlemleri uygulanmıştır. Saldırılar sonrasında Baboon ve Gemi damgalanmış resimlerinden çıkarılan damgalar Şekil 7'de verilmiştir. Bu resimlerden, orijinal damgaya göre çıkarılan damganın tamamen bozulduğu görülmektedir. GA'nın kontrol parametreleri; jenerasyon sayısı 500, seleksiyon şekli "rulet", çaprazlama şekli "iki noktalı", çaprazlama oranı 0.4, mutasyon şekli "düzenli", mutasyon



(a) (b)

Şekil 3. (a) Orijinal damga, (b) Oluşturulan yeni damga.



(a) (b)

Şekil 4. (a) Orijinal Baboon, (b) Damgalanmış Baboon.



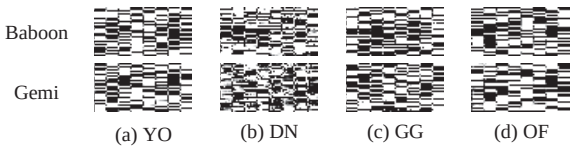
(a) (b)

Şekil 5. (a) Orijinal Gemi, (b) Damgalanmış Gemi.



(a) (b)

Şekil 6. Saldırı olmadan çıkarılan damga, (a) Damgalanmış Baboon'dan, (b) Damgalanmış Gemi'den.



(a) YO (b) DN (c) GG (d) OF

Şekil 7. Saldırılar sonrası damgalanmış resimlerden çıkarılan damga.

TABLO II
FARKLI RESİMLERİN KORELASYON VE BCR DEĞERLERİ

	$corr_I$	*BCR*				
			YO	DN	GG	OF
Baboon	1	100	56,1523	54,9316	56,1523	54,8340
Gemi	1	99,6582	56,3477	54,8828	54,9805	55,5664

TABLO III
SABİT SF'LER İLE OPTİMUM SF'LERİN PERFORMANS KARŞILAŞTIRMASI

			$corr_I$	*BCR*
Baboon	GA SF'ler		1	100
Gemi			1	99,6582
Baboon	Sabit SF'ler	1	1	42,1875
		20	0,9983	93,7988
		40	0,9938	88,1836
Gemi		1	1	44,3359
		20	0,9985	89,3066
		40	0,9943	84,7309

oranı 0.04, popülasyon büyüklüğü 128 ve başlangıç popülasyon aralığı da [-15;15] olarak seçilmiştir. 500 jenerasyon sonucunda optimizasyon işlemi sonuçlanmaktadır.

Geliştirilen GA tabanlı yöntemin korelasyon ve *BCR* değerleri Tablo II'de verilmiştir. Tablo sonuçları incelendiğinde, her iki resimde $corr_I$ değerinin 1 çıkması maksimum saydamlığın sağlandığını göstermektedir. *BCR* değerinin ise saldırı uygulamadan Baboon resminde 100 çıkarak orijinal ve çıkarılan damga arasındaki benzerliğin %100 olduğunu, Gemi resminde de "99.6582" çıkarak bu benzerliğin oldukça yüksek olduğunu göstermektedir. Saldırının türüne göre *BCR* değeri "54-57" arasında değişerek de çıkarılan damganın oldukça bozulduğunu ve bu tekniğin kırılgan bir damgalama olduğunu göstermektedir. GA ile elde edilen sonuçlar aynı zamanda "1, 20, 40" sabit ölçekleme faktörleri kullanılarak karşılaştırılmıştır. Tablo III'deki bu sonuçlara göre, SF değeri 1 verildiğinde $corr_I$ 1 çıkmakta fakat *BCR* oldukça düşük çıkmaktadır. Sabit SF değerini artırınca ise $corr_I$ düşmekte ve *BCR* de %100 başarı seviyelerine ulaşamamaktadır. GA tabanlı yöntemde ise hem maksimum saydamlık sağlanmakta hem de saldırı olmadan orijinal ve çıkarılan damga arasındaki benzerlik korunmaktadır.

VI. SONUÇLAR

Bu çalışmada, GA kullanılarak SVD tabanlı yeni bir kırılgan resim damgalama tekniği sunulmuştur. Çoklu ölçekleme faktörleri kullanılarak ölçeklenen damga resmin her bir satırı, bloklara ayrılmış orijinal resmin her bloğun tekil değerlerine farklı bir damga satırı gömülecek şekilde eklenmesiyle damgalanmış resim elde edilmiştir. Önerilen metotta, resmin kalitesini değiştirmeden olabildiğince yüksek saydamlık için çoklu ölçekleme faktörleri GA ile elde edilmiştir. Deneysel testler, GA ile optimize edilen SF'lerin sabit SF'ye göre çok daha kaliteli sonuçlar ürettiğini göstermektedir. Ayrıca orijinal resim ile damgalanmış resmin aynı çıkması, damgalanmış resmin en yüksek saydamlığa ulaştığını belirtmektedir.

Kırılgan damgalama tekniği sayısal verilerin bozulup bozulmadığının testi için kullanıldığından, kırılganlığı tespit etmek amacıyla YO, DN, GG ve OF saldırıları damgalanmış resme uygulanmıştır. Saldırılar sonucunda çıkarılan damgalar incelendiğinde, damganın oldukça bozulduğu görülmektedir.

KAYNAKLAR

[1] F. Hartung, and M. Kutter, "Multimedia watermarking techniques", Proc. IEEE 1999; 87: 1079–107.

[2] V. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques", Proceedings of the 3rd international IEEE conference on industrial informatics (INDIN 2005), Perth Western Australia, 10-12 Aug. 2005.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey", Proceedings of IEEE 1999; 87:1062–78.

[4] B. L. Gunjal, and R. R. Manthalkar, "An overview of transform domain robust digital image watermarking algorithms", Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no 1, CIS Journal 2010-2011.

[5] V. Aslantas, "An SVD based digital image watermarking using genetic algorithm", International Conference on Information Sciences, Signal Processing and its App., ISSPA2007, Sharjah, U.A.E., 2007.

[6] V. Aslantas, "An optimal robust digital image watermarking based on SVD using differential evolution algorithm", Optics Communications 282, 769–777, 2009.

[7] D. Arya, "A survey of frequency and wavelet domain digital watermarking techniques", International Journal of Scientific & Engineering Research, vol. 1, iss. 2, Nov. 2010.

[8] E. Hussein, and M. A. Belal, "Digital watermarking techniques, applications and attacks applied to digital media: A survey", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, vol. 1, no 7, Sep. 2012.

[9] M. H. Hassan, and S. A. M. Gilani, "A semi-fragile watermarking scheme for color image authentication", World Academy of Science, Engineering and Technology 19, 2006.

[10] V. Aslantas, S. Ozer, and S. Ozturk, "A novel clonal selection algorithm based fragile watermarking method", LNCS, 4628, pp. 358-369, 2007.

[11] V. Aslantas, S. Ozer, and S. Ozturk, "A novel fragile watermarking based on particle swarm optimization", IEEE Int. Conf. on Multimedia and Expo, Hannover, Germany, 269-72, 2008.

[12] V. Aslantas, S. Ozer, and S. Ozturk, "Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms" Optics Commun., vol. 282, no 14, 2806-2817, 2009.

[13] H. Modaghegh, R. H. Khosravi, and M. R. Akbarzadeh-T, "A new adjustable blind watermarking based on GA and SVD", Innovations'09: 6th International Conference on Innovations in Information Technology, Dec. 2009.

[14] M. B. Abugharsa, M. A. Sullabi and A. M. Taher, "Digital watermarking enhancement for satellite images using a DCT algorithm", 5th International Conference on Information Security & Cryptology, Turkey, May. 2012.

[15] M. Agoyi and D. Seral, "An imperceptible watermarking scheme based on double density dual-tree discrete wavelet transform in combination with singular value decomposition", 5th International Conference on Information Security & Cryptology, Turkey, May. 2012.

[16] J. H. Holland, "Adaptation in natural and artificial system: an introductory analysis with applications to biology, control and artificial intelligence", Cambridge, MA: MIT Press, 1992.

[17] S. C. Chu, H. C. Huang, Y. Shi, S. Y. Wu, and C. S. Shieh, "Genetic watermarking for zerotree-based applications", Digital Watermarking and Multimedia Security, Circuits Syst Signal Process, 27: 171–182, 2008.

Veysel Aslantaş Erciyes Üniversitesi Elektronik Mühendisliği Bölümünden 1988 yılında mezun oldu. 1988 yılında aynı üniversitenin Elektronik Mühendisliği bölümünde Araştırma Görevlisi olarak göreve başladı. İngiltere Galler Kardiff Üniversitesinde Zeki Sistemler üzerine yaptığı Doktorasını 1997 yılında tamamladı. 2010'da ise Doçent ünvanını aldı. İlgi alanları; bilgisayarla görme, resim işleme, bilgisayar grafik, yapay sinir ağları ve zeki optimizasyon teknikleridir. Halen Erciyes Üniversitesinde Öğretim Üyesi olarak görevini sürdürmektedir.

Mevlüt Doğru Erciyes Üniversitesi Bilgisayar Mühendisliği Bölümünden 2007 yılında mezun oldu. 2010 yılında aynı üniversitenin Bilgisayar Mühendisliği Ana Bilim Dalında Yüksek Lisansını tamamlayarak Doktora eğitimine başladı. SGK Bilgi Sistemleri ve Güvenliği Daire Başkanlığında Sistem Mühendisi olarak 2010'da başladığı görevini, 2011 yılından itibaren Maliye Bakanlığı Milli Emlak Genel Müdürlüğünde sürdürmektedir. Aynı zamanda Doktora eğitimine de devam etmektedir.

A Data Security System Design for Hybrid (Cloud & Volunteer) Global Computing

Emrah Dönmez, and Akif Kutlu

***Abstract*—In this study; we aimed to develop a data security infrastructure (DSI) for a hybrid global computing system which consists of cloud and volunteer computing. This performed work has put forth potential capacity of a global computing system which is also known as network computing based method, in terms of data security. Each computer performed computing operations on network has named as "volunteer contractor". The entire computing network is named as "volunteer cloud". We obtained data security analysis on volunteer contractors via designed framework. These analyses have been examined as response time, performance loss and delay time. While global computing system's operating power is 13488 GFLOPS without DSI, it has been discovered that it loss about average 4.67% performance with operating DSI.**

***Index Terms*—Cloud computing, Data security, Global computing, Volunteer computing.**

I. Introduction

GLOBAL computing is a computing technique that provides operating of process suitable to distributed computing by utilizing computing power of computers located on the internet as a distributed or server farms manner. As computing process can be performed on one or more server in computing environment known as cloud computing, on the other hand, it can be performed on distributed computers by allocating workloads in different or similar proportions in computing environment known as volunteer computing.

Data security ensured on computing network is a quite significant element in aspect of computations performed affect total result. Especially, this situation is much more salient in mathematical models implemented with sensitive data. Thus, each computed function or other different process can be at a level where whole computation processes are affected.

In this study, since the effects of security is major concern, during the execution of computation operations such as processing of data-intensive applications in hybrid computing environment, emerging effects of the data security to the potential computing power are examined.

Manuscript received March 01, 2013.

Emrah Dönmez, Computer Engineering Department & Graduate School of Science, Engineering and Technology at İstanbul Technical University, Maslak, İstanbul, 34467 Turkey (corresponding author to provide phone: +90-542-309-9325; fax: 212-285-6169; e-mail: donmezemr@.itu.edu.tr).

Akif Kutlu, Computer Engineering Department at Süleyman Demirel University, Çünür/Central, Isparta, 32260 Turkey (e-mail: akutlu@hotmail.com).

II. Related Works

Train et al. [4] made a study upon challenges in cloud computing and security solutions. Santos et al. [6] indicated required approaches for reliable cloud computing. Chonka et al. [8] performed a study upon developed attacks against cloud architectures and counter measures. Lombardi at al. [9] implemented studies on security virtualization processes in cloud computing systems.

SETI@home [1] project is a significant implementation in terms of revealing potential power of a volunteer computing project. Bayanihan [3] is a volunteer computing project implemented by using JAVA programming language. It has allowed users to participate volunteer computing network via a web browser.

This study is the first study used volunteer and cloud computing systems as a hybrid computing network and examining changes in a global computing mechanism in terms of data security.

III. Computing Infrastructure

Volunteer Cloud Computing: It is a distributed computing network which can be participated by users to contract computation processes. At the same time, it can be used to take only computation results from servers (contractors) by using user computers without contracting any computation process.

The first definition in above paragraph refers to volunteer computing, and the second definition refers to cloud computing, by using advantages of both computing infrastructure, a flexible computing model has been obtained.

A. Volunteer Cloud Model

Structure of computation network working with respect to volunteer computing fundamentals, is demonstrated in figure 3. In this figure, contractor computers consist of singular volunteer hosts and server farms including multiple numbers of computers.

Server farms connect to computation environment through proxy host. This situation reveals apparent distinction of these host communities from singular volunteer contractors. Hosts which employ only computation processes without taking any workload on computing network are named as computation clients. The structure that consists of all contractor hosts constitutes global computing itself.

IV. Computing System Resources

The performance and major QoS (Quality of Service) requirements of computing cloud has been measured according to hardware resources via designed application and Dhrystone synthetic benchmark micro-software by operating them at different time intervals.

A. Data Processing Power

68% of the total participant hosts that are located as volunteer contractors and server farms have constituted the multicore single processor computers in the volunteer cloud computation environment. 27% of the total participant hosts, located on the computing network, has actualized participation as single-core single processor computers. A method resembling to the one used in [12] study has been used to compute data processing power as following.

$$C_P = H_{eff} * N_{eff} * C_{back} * H_{shr} * C_{flops} * C_{life} * C_{ncpu} \quad (1)$$

In this formula, C_p stands for computing power, H_{eff} hardware resources efficiency, N_{eff}; average performance of network efficiency, C_{back}; average exhausted resources by back-up unit, H_{shr}; average shared hardware resources, C_{flops}; average floating point operations per CPU, C_{life}; average life time of contractors and C_{ncpu}; average number of CPU per contractor host.

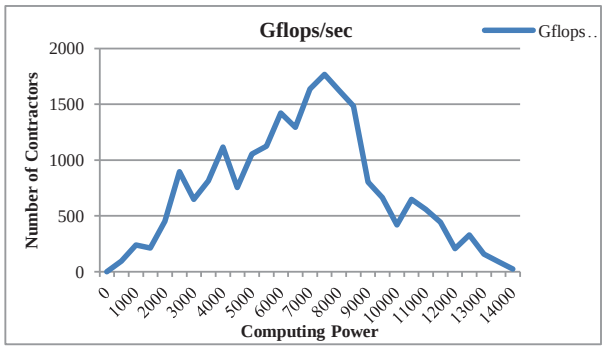


Fig. 1. Floating point operations power (Number of contractors-Gflops/sec).

Total CPU performance values have been obtained with data taken from global computing network periodically. Results make possible observations to be interpreted CPU performance as number of contractor host against floating point operations, figure 1. Given values belong to average performance values in total execution time.

Average processing power per host in GFLOPS for each CPU type of total 1762 pcs hosts demonstrating participation to the cloud have been compared in table 1. Number of CPU core situation has been given for only hosts which have Intel or AMD architecture. Total processing power has been specified approximately 13488 GFOLPS.

At the same time, 63% of contractor hosts have consisted of two processor node and 5% of contractor hosts have consisted of three or more processor nodes.

TABLE I
CPU Types

CPU Type	Number of hosts	GFLOPS per host	Total GFLOPS
Intel	1137	8.504	9668.5
-Multi-core	*853*	*9.885*	*8432*
-Single-core + HT	*284*	*4.354*	*1236.5*
AMD	532	6.647	3536.2
-Multi-core	*351*	*8.079*	*2835.7*
- Single-core	*181*	*3.870*	*700.5*
Power PC	53	3.212	170.2
Others	40	2.837	113.5
TOTAL	1762	7.656	13488.4

B. Network Bandwidth

Average network communication speed has been measured as 352 Kbps in tests actualized by taking into account whole computation cloud. This speed has been measured at higher values than average in some contractors; on the other hand, it has been measured at lower values than average because of their locations. File download speeds in network against number of contractors have been demonstrated in figure 2.

Average network speed rates have been identified between 0 and 32 Mbps in communication that occurs between contractors, clients and contractor-clients. Though the increase in number of contractor hosts, it has been identified that reflection of increase in computing power to the computation network can be possible with increase in bandwidth in parallel manner. It can be said that bandwidth is a restrictive factor by looking this determination in computation power.

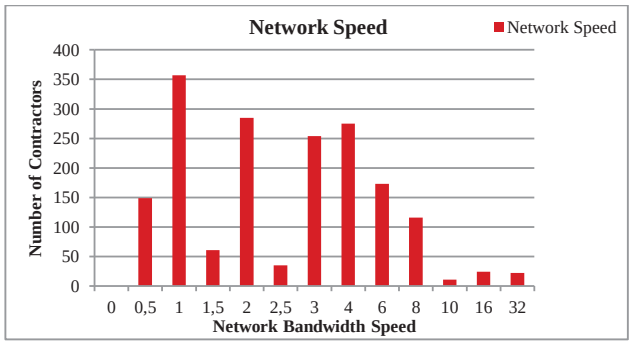


Fig. 2. File download speed distribution in network graph

V. Environmental Design And Findings

A. Dataset

Data used through computation processes have been sent or taken as encrypted on client-server network communication line with starting-up DSI. To be able to synthesize effect of the used data better, it is aimed to obtain a result that is closer to real-world by giving place to different data types. Data have been chosen arbitrarily and any proportion has been not overseen between data types which constitute total amount. It has been minded that data size values are between 1KB-1GB.

Security is a significant element in a computation network designed with respect to global computing structure, since

results obtained from data computation of each contractor host, effects total computation result. Consumption of system resources is desired at a minimum cost level while security is provided at the same time. An optimized data security reduces cost in computation network comparing to a non-optimized data security. Therefore, different security algorithms and designs should be tried by choosing different data types.

Let computation power is expressed with CP (the computation of CP is given section 3) in implemented hybrid global computing cloud and contractors which will operate threaded data are expressed with c1, c2, …, cn. Let computation power of each contractor is denoted with CP_{c1}, CP_{c2}, …, CP_{cn}. Passing time when making only computations without making any encryption, is denoted for each contractor with t_1, t_2, ..., t_n. Let periods passing to encrypt computation data for each contractor while RC6 is using are denoted as t_{r1}, t_{r2}, ..., t_{rn}, while AES is using are denoted as t_{a1}, t_{a2}, ..., t_{an} and while Blowfish using are denoted as t_{b1}, t_{b2}, ..., t_{bn}. In that case, the emerged computing power with actuating DSI on computation cloud;

For RC6;

$$CP_R = CP_{c1}\frac{t_1}{t_{r1}} * CP_{c2}\frac{t_2}{t_{r2}} * \cdots * CP_{cn}\frac{t_n}{t_{rn}} \quad (2)$$

For AES;

$$CP_A = CP_{c1}\frac{t_1}{t_{a1}} * CP_{c2}\frac{t_2}{t_{a2}} * \cdots * CP_{cn}\frac{t_n}{t_{an}} \quad (3)$$

For Blowfish;

$$CP_B = CP_{c1}\frac{t_1}{t_{b1}} * CP_{c2}\frac{t_2}{t_{b2}} * \cdots * CP_{cn}\frac{t_n}{t_{bn}} \quad (4)$$

can be calculated by using these formulas. Average computation power while DSI is used with encryption,

For CP_A;

$$CP_A = \frac{CP_R + CP_A + CP_B}{3} \quad (5)$$

can be calculated with above formula.

The components of the designed hybrid global computation network are demonstrated in figure 3. Workloads actualized in cloud, have been shared between server farms named as sub-cloud and volunteer contractors. The whole network composed of sub-cloud and volunteer contractors named as main hybrid cloud. The computers which stayed out of the main cloud can connect to the computation network to make only calculation together to be able to participating to the cloud.

The management of intercommunication between sub-cloud and volunteer contractors in main cloud and between clients and main cloud in whole network are implemented by main server named Central Computation Management Unit (CCMU). In addition, sub-clouds access to the CCMU located in the main cloud through proxy hosts.

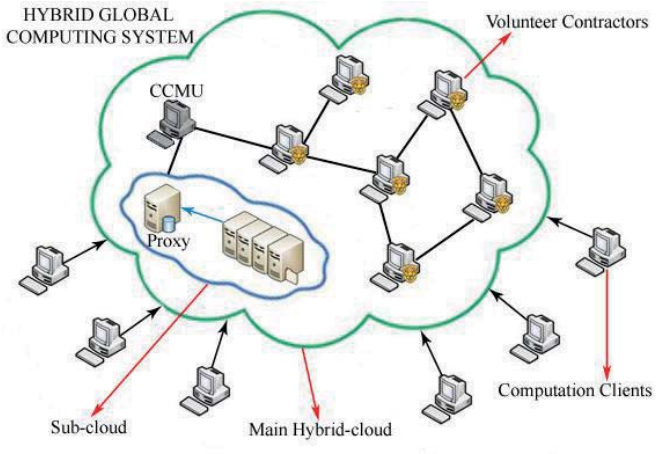


Figure 3. Simplified details of computation environment.

The general name of the process including data encryption methods that are used to prevent accessing, reading and writing the data by other environments, except environments that already use the related data when data security is needed, are called cryptography.

Data Encryption Algorithms

RC6: It is a symmetric switching based encryption technique. It is worked as block based, block size is chosen as 128 bit generally. Generally, suitable to work with 128, 192 and 256 bit switch size. It provides fast and strong encryption.

AES: Advanced Encryption Standard is optimal for 128 – 192 – 256 bit switching sizes. Generally, operates on 128 bit blocks.

Blowfish: It is a symmetric encryption technique operated as block based. Switches between 32 bit and 448 bit are suitable to this encryption technique. Suitable to operate on 64 bit blocks or can be modified to operate on larger blocks.

The comparisons pointing to the speed of algorithms implemented for multi file group (.txt, .jpeg, .png, .avi, .wmv, .mp3, .pdf etc.) about average of three months and occurred changes in performance of global computation cloud in encryption processes are located in the table 2.

In this test, 256 bit switches have been used for all encryption algorithms. While 128 bit blocks have being used for RC6 and AES, 64 bit blocks have being used for Blowfish. Let t denotes the passing time for the calculations made without DSI, t_g denotes the passing time for the same calculations made by using DSI, and t_s denotes encryption time generated by algorithms in system;

$$t_s = t - t_g \quad (6)$$

TABLE II
COMPARISON OF ENCRYPTION ALGORITHMS

Encryption Type	Encryption Time (sec)	Computation Power (GFLOPS)
Blowfish/CTR	0.0064	13263
RC6	0.0112	13125
AES/ECB	0.0081	13087

The time periods identified above, have been obtained from performance report created by using integrated performance measurement tool in ide where the middleware software executed on CCMU is programmed.

Distinct file group has been distributed to the whole computation cloud through CCMU in order to pre-test the available network throughout. Then, each contractor taken these files has sent the data (by assuming that data is processed and ready to sending) to CCMU with encryption modules integrated to the middleware software. The hardware resources of CCMU have been given the following table 3.

TABLE III
CCMU PROPERTIES

	Type	Model	Speed	Other
Mainboard	Intel Ser.	S2600GL	X2 Proc.	I/O Exp.
Processor	Xeon	E5-2643	3.3 GHz	10Mb Ch
Memory	Kingston	HyperX	1600Mhz	64GB
Hard disk	WD SSD	64S-7150	3Gb	8x64GB
GPU	Nvidia	Q-5000	120Gb/s	GDDR5

SSD hard disks have been arranged as x2 RAID5 (2 pcs x 4 unit storage fields) scheme in specified manager workstation (CCMU). Memories have been in the format of x8 8GB. 8 distinct threads can be executed on 4 discrete cores. There are 352 CUDA cores on GPGPU processor and it has 320 bit memory interface.

While network communication is provided through the Internet services, DSI is optimized for only selected data and each message packet including these selected data are subjected to encryption process. This feature has been integrated to the middleware software against the occurrence of the data operated are partially consist of sensitive data in case. User can prevent redundant performance loss that actualized by other general files by encrypting only desired files (.dll, class etc.) in computation environment.

B. Contractor Host Security

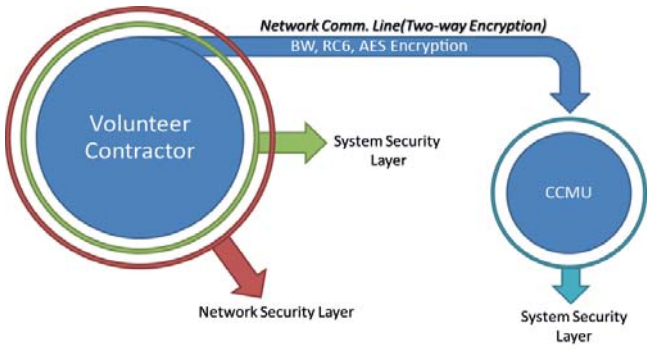


Figure 4. Volunteer contractor security diagram in designed global cloud

Two-way encryption has been implemented in data transfer processes occurred on network communication line between volunteer contractors and CCMU on computation network as shown in figure 4. Three different encryption algorithms; RC6, AES and Blowfish known as prevalent, have been used in two-way encryption processes. Workload occurred by each of them in computation cloud, has been calculated by taking into account parameters of performance criterions (response time, encryption duration and latency duration).

Data security in volunteer contractors has been ensured with a double layer structure designed with respect to a new approach. These layers are system security layer and network security layer respectively.

System security layer: Security modules operating in this layer not only responsible for encryption of data but also responsible for backup to the computer. The general aim is, providing limited accessing authority (such as only reading) or totally preventing accessing to these data from outside by providing data security for users setting calculations with special data in volunteer cloud.

Network security layer: Instead of sending data directly and vulnerably during communication, they have been sent to the CCMU by encrypting with cryptographic encryption modules in this second layer.

C. Server Farms Security

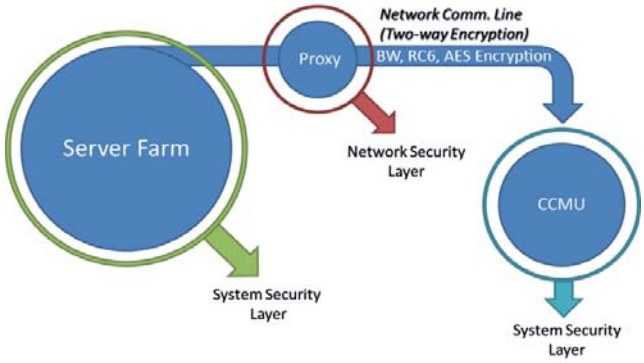


Figure 5. Server farm security diagram in designed global cloud

There is data security structure which is similar to the data security structure of volunteer contractors with a little difference in server farms that are another significant part of computer community in network. The security structure provided for server farms located in computation network has been demonstrated in figure 5. Similarly, two-way encryption structure has been implemented on network communication line. Unlike the security structure of contractor computers, security in server farms has been actualized with operating the double layer structure separately from each of these layer. System security layer has been operated at contractor computers located in server farms. Network security layer has been operated at proxy computer which is the gate of the internet for server farm.

Acquiring performance gain lies at the basic of separately operating security layers from each other. Only the system security layer that is the first layer of security modules has been worked in contractor computers generated server farm. As a result, it has been provided that contractor computers which are already deal with computation processes; have not to enter under the additional workloads. Since, network security layer which is second layer of security has been operated on proxy computer. Providing control of the single flow point of the network is more cleverly method than providing control of the network communication lines on every computer separately.

D. Computation Clients Security

These hosts have only client role. They send requests by entering their own data to make requested computation operations and then take results of these computations as response from network where contractors serve at the end of the period that it was carried out. While defined operations

are executed, the DSI controls all over the communication lines and local files to protect and back-up raw or non-raw data through operations as set-up. Security of network communication lines is ensured as a precaution of data loss in this request-response loop as seen in figure 6. Clients have not any effect on data security in performed computation loop from sending data to the global computation cloud. This operating structure resembles to the classic cloud computing structure in terms of its operating mechanism.

Client-side security is on the carpet only while the data which will be calculated is entered to the computation middleware. Since, security of client data wanted to be processed is ensured by DSI after the related data is entered computation environment via middleware. Ultimately, accurate results can be expected from computation processes by transferring these data to the contractors correctly.

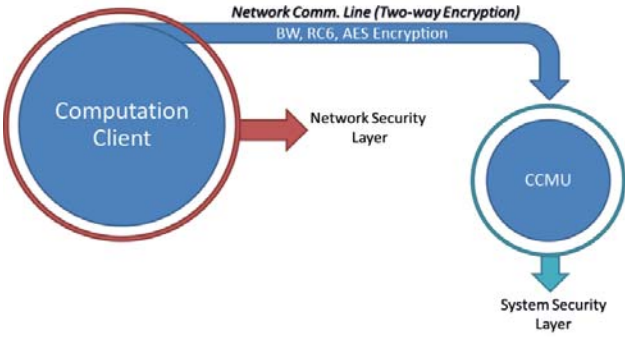


Figure 6. Computation client security diagram in designed global cloud

After the client host entered its own data to the form with desktop application interface, the data are demonstrated to the client user one more time to take approval of user. Before the data transfer processes are performed, the data that were entered at client-side are subjected to the encryption process completely by starting-up of the cryptographic security algorithms as soon as client gives approval for verification process. After encryption processes have done, the data is ready to be sent through DSI.

E. Security Gains

DSI has been created with a triple layered security protocol with regard to other developed or being developed security unit of computation environments. These layers are network security layer, system security layer and client security layer respectively.

Data have been transmitted on both CCMU-Client and CCMU-Contractor communication line by encrypting related data in the first layer defined as network security layer. The data reached to the hybrid computing environment have been protected through system security layer defined as second layer during computations.

The security of data entered to the computation environment from client is ensured in client security layer that is third and last layer. Each data has been subjected to the encryption process through security protocols designed with encryption algorithms which are generated by middleware software.

Performance test has been implemented with three different encryption algorithms in design of security protocols. Analyses have been made on the performance of designed computation cloud from the strongest one to the fastest one in terms of security. The data showing latency time of RC6, AES and Blowfish encryption algorithms against gradual reduction in power of volunteer-cloud computation environment are exhibited in figure 7. The least latency time occurred with Blowfish encryption algorithm as it can be understood from figure. The most latency time occurred with AES. The main reason of faster performing of Blowfish than other algorithms is its block size and *f* function. The other two algorithm; AES and RC6 operates as block-based. 256 bit key (cipher) size is chosen for implementation of general tests.

While computing power is about 13350 GFLOPS on volunteer computation cloud and speed of data exchange (or bandwidth) is about 634.7 Mbps (79.34 MB per second) on network communication line of CCMU, the average latency time of Blowfish algorithm has been actualized approximately 0.1 s (0.098 s), the average latency time of RC6 algorithm has been actualized approximately 0.19 s and lastly, the average latency time of AES algorithm has been actualized approximately 0.21 s according to output of middleware software. This latency is the period occurring only during the communication on between network and CCMU, namely the latencies occurring on the contractors don't fall under to this period. The main reason of lower latency occurred by Blowfish algorithm is that it use smaller block size (64 bit) than others block size (128 – 256 bit), instead of stream it operates as block-based, and accelerated and simple structure of algorithm that is distinctive to itself can be indicated.

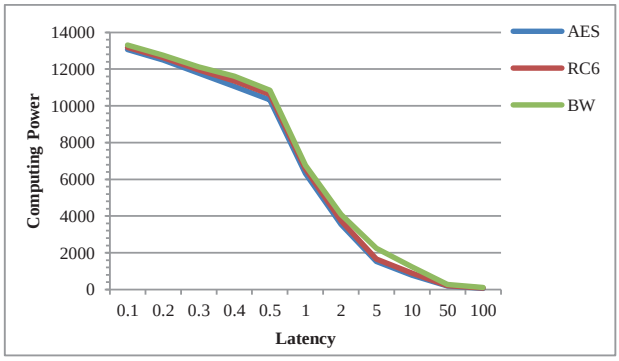


Figure 7. Computing power vs. latency for encryption algorithms

Performance gain is focused factor thus data security in each unit of computation cloud has been handled with distinct principles. Aim approach in here, provide an optimized security with flexibility. In other words; by setting forth from these principles, it is said that the main reason of different design of security in computation units is minimum performance loss while ensuring maximum security.

Both general performance changing and memory performance changing occurred throughout computation cloud against increasing size of the key used for encryption algorithms are illustrated for each algorithm in figure 8. Decreasing is actualized in computation performance (processor, memory, disk unit etc.) while size of the switching increases as it can be understood from figures. Especially starting with use of 256 bit and above keys, decreasing in performance emerges as more significantly. While processor performance is being evaluated in terms of Gflops (floating-point processor power), read – write time and memory frequency is taken into consideration for

memory. During the computations, computing power is observed at level of 13382 Gflops as average while 32 bit switching has been applied. Computation power drops back to level of 12565 Gflops with a loss of 7.86% by 32-fold increasing in the size of switching from 32 bit to 1024 bit. Increasing of switching size at this scale decreases the memory performance from 96.5% to 80.2% with a loss of 16.3%.

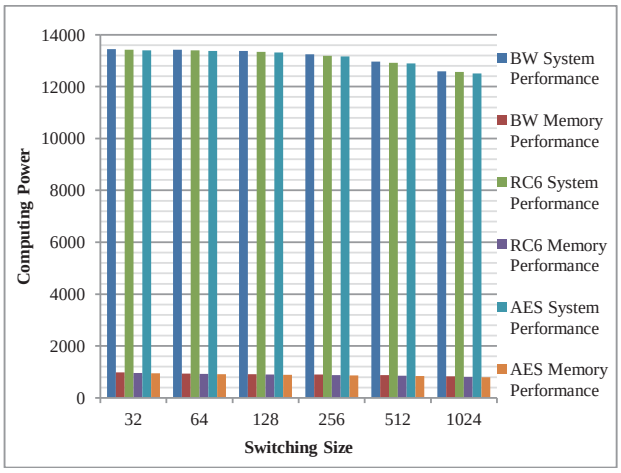


Figure 8. System and memory performance while encryption is being used.

Similarly, effect of encryption block size which is another factor of performance changing in volunteer cloud are illustrated for each encryption algorithm in figure 9. Noticeable declines have been observed when size of block increases. Especially, this decreasing can be observable from 64 bit blocks more clearly. While 32 bit blocks have being used for data during computations, computation power have been about 13389 Gflops. Computation power drops back to level of 12865 Gflops with a loss of 4.62% by 8-fold increasing in the size of switching from 32 bit to 256 bit. Similarly, memory performance is also in a decreasing proclivity. Since, increasing of block size at this scale decreases the memory performance from 96.5% to 74.4% with a loss of 22.1%, approximately. It can be said that block size effects the memory performance more than key size.

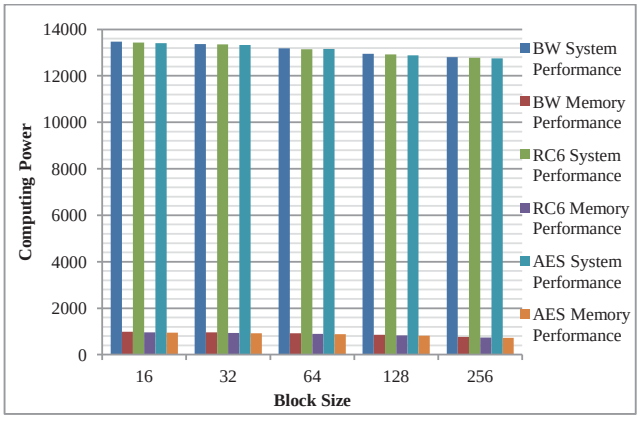


Figure 9. System and memory performance while encryption is being used.

VI. Analyses and Experimental Results

The most important reason of incorporating the data security infrastructure to the global computing cloud is that volunteer contractors and clients are not trustable because of anonym communication is allowed to the computation network. Therefore, security in units (contractor, server farm and client) and back-up modules are used to reduce the worse effect of the malicious and defective hosts to the computation environment performing as volunteer-based. Each task (workload) has been operated on three different contractors with back-up module. If results of these tasks run in with application-defined tolerance values, these results are accepted. Otherwise, a second instance is executed and process continues in this way.

There will be occurred much more data traffic in data secured (means defined encryption algorithms and security modules are worked) volunteer-cloud computing environment according to the pure unsecured computing environment. This situation can cause saturation in network connection of a great number of contractors. If these connections are saturated, computer network connections (shared etc.) opened to the outside can become incapable of working.

Three different encryption techniques known commonly have been used on data security layer designed for volunteer cloud (Data properties have been given in section 5.1). Performance situations are identified when data security is provided or not provided in computation network with these encryption techniques (Table 4). Outputs have been examined as data encryption time, performance loss, and delay time. Average results have been obtained through tests made during approximate time of the entity of computation environment. Network saturation is actualized about average 436,6 Mbps in daytime and 271,3 Mbps in night in tests (daytime, with Turkey time: 08:00 – 17:00, night: 17:00 – 08:00). Saturation is actualized about 43.7% in daytime and 27.1% in night as percentage, if 1000 Mbps data transfer capacity of available CCMU network card is considered. These proportions are found as average values on computation network. Normally, network communication has occurred in a fluctuating course. Encryption time for 1MB granular data have been identified as average 0,0015 sec with AES algorithm, average 0,0012 sec with RC6 algorithm, and average 0,0010 sec with Blowfish in computation network. Performance losses have been identified as average 6,077% with RC6 algorithm, average 4,148% with AES algorithm, and lastly average 3,775% with Blowfish algorithm for particle data (sound, video, text, picture etc.) in computation network. While Blowfish algorithm was being used, the fastest response time has been observed as delay time. Since the least delay time has been identified as average 0,0015 sec with Blowfish. Delay time has been identified as average 0,0018 sec with RC6 and lastly this delay time has been identified as 0,0022 sec with AES which has the latest response time with this value. Computation powers occurred in volunteer-cloud for each encryption algorithm, have been found as in the following table.

TABLE IV
ENCRYPTION TIME OF ALGORITHMS

Encryption type	Average encryption time (sec)	Comparing computing power (GFLOPS)			Delay Time (sec)
		Normal computing power	Encrypted computing power	Difference (%)	
Blow./CT	0.0010	13488	12964	3.775	0.0015
RC6	0.0012	13488	12919	4.148	0.0018
AES/ECB	0.0015	13488	12668	6.077	0.0022

VII. CONCLUSION AND FUTURE WORKS

Computations made as secure as possible and getting results in a fast manner (local + network parallelism) reveal the power of volunteer-cloud hybrid design. The main focusing point is utilizing unused system resources to implement available computations. In this way, unused resources losses are prevented thus cost of computations will be able to be decreased. On the other hand, security mechanisms of computation units are one of the most significant topics in volunteer-cloud computation network. Performance loss has been observed while data security is ensured in a network holding high capacity computing power and employing DSI.

In the future, all user interactive applications will be able to be developed as suitable to the global computing, cloud computing, or hybrid computing systems with the development of applications and the arrival of high-speed network bandwidth through new communication technologies and different techniques. The most important factor will be network bandwidth in development of these kinds of computing technologies. Since when such systems are switched with available ones the reachable speed in reciprocal communication lines will be a determining factor as well as the data processing speed in network elements. Data processed or non-processed may affect the total computation result if these data are changed by external interventions. Thus, security in these communication lines and local environments emerges as an area which should be studied as distinctly in terms of effects on computing performance.

ACKNOWLEDGMENT

We are grateful to volunteer people who allow middleware software to perform tests in their computers, firstly**.** We thank especially cloud service providers allowing integration of volunteer hosts to their platforms. We especially exhibit our thanks to Computer Science Department laboratory at SDU Technology Faculty and CS Department @ITU.

REFERENCES

[1] D.P. Anderson, J. Cobb, E. Korpela, M. Lebofsky, D. Werthimer, "SETI@home: An Experiment in Public-Resource Computing". *Communications of the ACM,45(11)*, Nov. 2002, pp. 56-61.

[2] D.P. Anderson. "BOINC: A System for Public-Resource Computing and Storage". *5th IEEE/ACM International Workshop on Grid Computing*, Pittsburgh, PA, Nov. 8 2004, pp. 365-372.

[3] L.F.G. Sarmenta, "Bayanihan: Web-Based Volunteer Computing Using Java". *Lecture Notes in Computer Science 1368, Springer-Verlag*, 1998. pp. 444-461.

[4] A. Traian, "Cloud Computing Challenges and Related Security Issues". *A project report written under the guidance of Prof. Raj Jain*, 22(6), 2009, pp. 1-10. Available: http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud/index.html

[5] B. Reingold, R. Mrazik, "Cloud computing: the intersection of massive scalability, data security and privacy". *Cyberspace Law*, 14(5), 2009, pp. 1-5.

[6] N. Santos, K. P. Gummadi, R. Rodrigues, "Towards Trusted Cloud Computing". *MPI-SWS*, 11(6), 2009, pp. 1-5.

[7] Z. Dimitrios, L. Dimitrios, "Addressing cloud computing security issues". *Future Generation Computer Systems (Science Direct)*, 10.1016, 2010, pp. 1-10.

[8] A. Chonka, Y. Xiang, W. Zhou, A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks". *Journal of Network and Computer Applications (Science Direct)*, 09-06(004), 2009, pp. 1-11.

[9] F. Lombardi, R. Di Pietro, "Secure virtualization for cloud computing". Journal of Network and Computer Applications (Science Direct), 10-06(008), 2010, pp. 1-10.

[10] R. P. Weicker, "Dhrystone: A Synthetic Systems Programming Benchmark". *Communications of the ACM 27 (10)*, Oct. 1984, pp. 1013-1030.

[11] D. P. Anderson, G. Fedak, "The Computional and Storage Potential of Volunteer Computing". *Seti@HOME, U.C. Berkeley*, Space Science Laboratory, 24(10), 2008, pp. 1-8.

[12] L.F.G. Sarmenta, S. Hirano, S. A. Ward, "Towards Bayanihan: Building an Extensible Framework for Volunteer Computing Using Java". *in Proc. of ACM 1998 Workshop on Java for High-Performance Network Computing, Feb./Mar. 1998.* Also published in Concurrency: Practice and Experience, 1998, pp. 10(11-13).

Emrah Dönmez is a Ph.D. student in the Computer Engineering Department at the İstanbul Technical University. His research areas are: security of cloud computing, data mining with HPC systems, performance optimization in HPC systems, GPGPU acceleration and communication optimization, distributed operating systems, global, grid, volunteer and hybrid computing; problems & solutions. He graduated from the Süleyman Demirel University in 2009 with a B.Sc. in computer science under supervising T. Aydoğan and then he graduated from the Süleyman Demirel University in 2011 with M.Sc. in computer science under supervising of A. Kutlu. He is a student member of IEEE.

Akif Kutlu is a professor in the Computer Engineering Department at the Süleyman Demirel University. His research areas are: microcontrollers, computer networks, microprocessors, industrial control, industrial networks, CAN (Control Area Network), embedded systems, firmware, and engineering education. He graduated from the Sussex University, England in 1998 with a Ph.D. in computer science. His Ph.D. thesis topic is industrial network protocols. He has already published a number of qualified publications as national and international. He is a member of IEEE and IEEE Communication Society. He gives lectures in computer engineering department at SDU nowadays.