

A Proposal for Modular Multiplication

Ali Şentürk and Mustafa Gök

Department of Computer Engineering
Cukurova University Balcalı, 01330, Turkey

Abstract—Modular multiplication is an important operation used in cryptography. This paper presents a novel modular multiplication algorithm that uses mainly multiply-accumulate operation. The proposed algorithm uses a small-size look-up table that can be stored into a general-purpose processor's cache. The algorithm can be used in any microarchitecture that has high-performance multiply-add hardware units in their datapaths.

Index Terms—RSA algorithm, modular multiplication.

I. INTRODUCTION

RSA and elliptic curve cryptography algorithms mostly rely on modular multiplication [1], [2], [3]. RSA algorithm encrypts a plain text T as $T^E \bmod M$ where E is the public key and M is a large modulus. RSA decrypts a cyphertext, C , as $C^D \bmod M$ where D is the private key. Since the exponentiation operation can be performed by executing a series of modular multiplications, the efficient execution of this operation improves the performance of the algorithm. Direct computation of the modular multiplication requires one multiplication and one division operations. To compute modular exponent, most algorithms use the result of the modular multiplication iteratively which causes a data dependency. Because of the data dependency, hardware may waste many cycles if a division instruction is used in the computation. The previous work favored the Montgomery's algorithm [4], since it does not require trial divisions. Over the years it is also accepted that the Montgomery's algorithm is the best fit for hardware implementations and significant research effort is dedicated on efficient hardware implementation of this algorithm [5], [6], [7]. Efficient hardware implementations are important because they decrease the time needed for the decryption of the cipher by brute force. To make brute force attacks difficult, the preferred bit sizes for the modulus, public key, and private key are increased. Recently, applications that use 1024 to 2048 bit sizes have come to scene. On the other hand this trend introduces an important drawback. Public users do not have special hardware for cryptography applications and general purpose processors do not have arithmetic units that can directly operate on large operands. A strategy to process the large operand sizes is dividing the operand into sub-operands equal to the processor's word size and operating on them and combining the sub-results to get the final result. Though this method causes significant performance degradation, it is the only choice if there is no special hardware support.

Modern general purpose processor architectures have multiple high-performance multiply and multiply-add units in their datapaths due to extensive use of this operation in all kinds of applications. Thus, significant research effort is dedicated to decrease the latency of these instructions. For

example, current Intel Core Duo processor family that uses 65nm technology has a 32-bit integer multiply instruction with 3 cycle latency whereas the addition instructions in this processor family have 1 cycle latency [8]. Including popular Montgomery algorithm most modular multiplication algorithms rely on addition instruction. This study presents a modular multiplication algorithm that uses multiplication operation to fill this gap. The rest of the paper is organized as follows: Section 2 presents the proposed algorithms, Section 3 discusses the efficiency of the algorithm. Section 4 presents the conclusion.

II. THE PROPOSED ALGORITHM

Modern general purpose processor architectures have multiple high-performance multiply and multiply-add units in their datapaths. The proposed algorithm uses these units to perform modular multiplication for large moduli. The steps of the proposed algorithm are given below.

Algorithm

Assume A and B are two n -bit numbers and M is the moduli.

- Multiply A and B , $P = A \cdot B$. Perform $Q = W(1)$ where Q is used to accumulate modular equivalent of the constant values that are discarded in this step. $W(1)$ is obtained from a look-up table (LUT) as $W(1) = LUT(P_{(n+k-1):n})$. The LUT has 2^k rows where each row contains an n -bit precomputed $P_{(n+k-1):n} \bmod M$ value.
- Test if $PL(1) = P_{2n-1:(n+k)}$ is equal to zero, if the test fails, do $(PL1 \cdot W(2)) + P_{(n-1):0}$ where and $W(2) = LUT(2^k)$, otherwise, go to the final step.
- Repeat computation until $PL(i+1) = 0$ when this occurs sum the value of the accumulated Q with $PL(i)_{(n-1):0}$ to get the final result.

The flow chart of the algorithm is given in Figure 1. The algorithm requires pre-computation of moduli values for a selected range of values as explained above. These elements are computed only once for each new moduli. An important challenge is the size of the look-up tables since very large look-up tables create memory bottleneck. However, for practical operand sizes look-up tables can be small enough to fit in L1 caches. In the worst case, the algorithm computes the modular multiplication in $\lceil n/k \rceil$ iterations and requires one multiply-add, one addition and one access to LUT for each iteration. A numerical example that demonstrates the worst case for an 8-bit moduli is given below.

$$A^2 \equiv (7F)_{16}^2 \bmod (81)_{16}$$

is computed using the presented algorithm. To demonstrate the algorithm more clearly hexadecimal representation of the

TABLE I
A COMPARISON OF MODULAR MULTIPLICATION METHODS

Operation	M.A. [4]	P. A.
Add	64	4
Multiply-Add	-	4
Shift	32	-
LUT Access	-	4

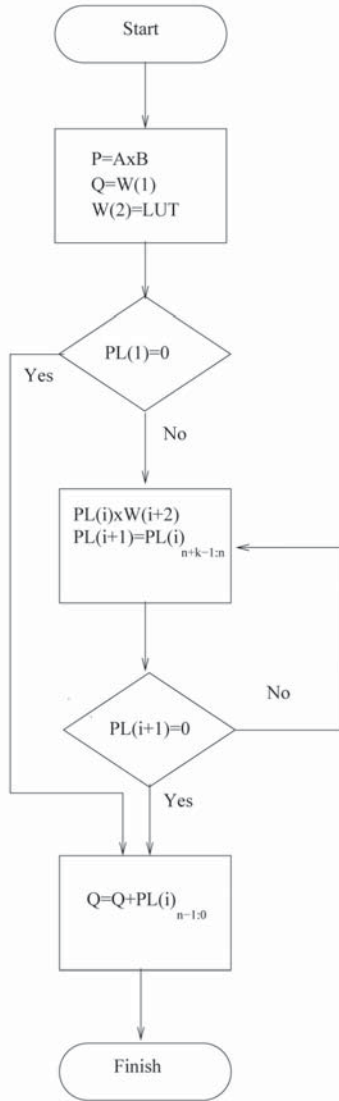


Fig. 1. The Flow Chart.

numbers are used.

Example

- Step 1:
 $P = A^2 = 3F01$
 $PL1 = 0F$
 $Q = W1 = 7B, W2 = 79.$
- Step 2:
 $(PL1 \cdot W2) + P_{(n-1):0} = (F \cdot 79) + 01 = 718$
 $W3 = 73, W4 = 0$
 $PL2 = 0$
- Step 3:
 $Q \equiv Q + W3 \bmod 81 \equiv (7B + 73) \bmod 81 \equiv 6D$
 $Q \equiv (Q + PL1_{(n-1):0}) \bmod 81$
 $\equiv (6D + 18) \bmod 81 \equiv 4$

III. ANALYSIS OF THE ALGORITHM

Most modern processor's support 32-bit operand sizes. The proposed algorithm can be adjusted to perform 32-bit modular

multiplication. As it is stated before, the number of the required iterations to generate the result mainly depends on the size of the LUT. For 32-bit applications, to keep the look-up table small enough to fit in a processor's cache a look-up table that has 256 rows with 32-bit row size is used. Total size of the LUT is 8KBs which can easily be stored even in an L1 cache of a modern general purpose processor. In this setup, the proposed algorithm computes the result in $32/8 = 4$ iterations when the worst case occurs. Table 1 presents number of operations required to compute a 32-bit modulus with the proposed method and with Montgomery's method. In both methods, there is a data dependency between each iterations. This means the operations cannot be executed in parallel. An estimate for processors that has 65 nm Intel Core is given based on the worst case latencies for the operations [8]. The latency for a memory access is accepted as one cycle assuming the look-up table is stored in L1 cache. The latency for add and shift operations are one cycle, the latency for multiply instruction is three cycles. There is a packed multiply-add instruction (PMADDWD) among MMX instructions for this family with three cycles latency. Based on these latency values Montgomery algorithm computes the product of 32-bit modular multiplication in 96 cycles whereas the proposed algorithm generates the same result in 20 cycles. On the other hand it should be noted that there is extra overhead for the proposed algorithm due to the computation of the LUT values. A fair concern about the applicability of the algorithm may arise considering the large operand sizes used in practice such as 1024 bits or 2048 bits. Since the available operations are dictated by the processor's word size, the large size operands have to be split into word size suboperands. For example a 128-bit operand must be splitted into four 32-bit operands, to be processed which is true for all algorithms.

IV. CONCLUSION

This paper presented a straightforward algorithm to compute modular multiplication. The algorithm exploits the current improvements in the performance of multiply-add implementations. Preliminary analysis shows that it has potential to speed-up the computation of modular multiplication in general-purpose architectures. The proposed algorithm can be combined with Montgomery's algorithm in order to increase the instruction level parallelism, since these two algorithms use different resources. Planned future work will search the direct applicability of the proposed algorithm on hardware and more specifically on FPGA platforms.

REFERENCES

- [1] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, p. 126, 1978.
- [2] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.
- [3] V. Miller, "Use of elliptic curves in cryptography," in *Advances in CryptologyCRYPTO85 Proceedings*. Springer, 1986, pp. 417–426.
- [4] P. Montgomery, "Modular multiplication without trial division," *Mathematics of computation*, vol. 44, no. 170, pp. 519–521, 1985.
- [5] S. Eldridge and C. Walter, "Hardware implementation of Montgomery's modular multiplication algorithm," *IEEE Transactions on Computers*, vol. 42, no. 6, pp. 693–699, 1993.
- [6] E. Brickell, "A survey of hardware implementations of RSA," in *Advances in CryptologyCRYPTO89 Proceedings*. Springer, 1986, pp. 368–370.
- [7] N. Nedjah and L. Mourelle, "Three hardware architectures for the binary modular exponentiation: Sequential, parallel, and systolic," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 3, pp. 627–633, 2006.
- [8] "Intel 64 and IA-32 architectures optimization reference manual," Intel Corporation, November 2009.

Türkçe Telaffuz Edilebilir Parola Üreteci

R. Engür PİŞİRİCİ, Aslı Çankaya PİŞİRİCİ

Özet — Bilişim Teknolojileri alanında kimlik doğrulama da kullanılan “bildiğiniz bir şey” - parola – konseptinde kullanıcılar için rastgele ve güvenilir sözcükler üreten uygulamalar mevcuttur. İnsanlar, rastgele anlamsız ancak telaffuz edebildikleri sözcükleri daha rahat ezberleyebilmektedirler. Bu makalede yurt dışında yabancı diller için geçerli telaffuz edilebilir parola üreticileri gibi ülkemizde üzerinde pek çalışma olmayan, Türkçe’imiz için bir dizayn modeli ve yaklaşımı önereceğiz. Bu makalenin sonunda ise, önerdiğimiz dizayn modeli ve yaklaşımının uygulanabilir alanlarından bahsedeceğiz.

Anahtar — Bilişim Güvenliği, Kimlik Doğrulama, Parola, Telaffuz edilebilir Parolalar, Türkçe Telaffuz Edilebilir Parola Üretici, FIPS 181, FIPS 112, CSC-STD-002-85

Abstract—In the field of information technologies, “something you know” - passwords- which are used at authentication concept, there are some applications which generates safe and random pass phrases. Humans can easily remember randomly produced but pronounceable phrases. In this paper, we will offer a design model for Turkish Pronounceable password generation and application. At the end of this paper, We will give some examples for how to apply this design model for today's information systems.

Index Terms—Information Security, Authentication, Password, Pronounceable Passwords, Turkish Pronounceable Password Generator, FIPS 181, FIPS 112, CSC-STD-002-85

1. GİRİŞ

Kimlik Doğrulama, bir varlığın, bu doğrulamayı yapacak, karşı tarafta bulunan ve daha önceden kimlik doğrulama için tanımlanmış **veri kümesinden**, kendisine ait **alt kümeyi doğrulamasıdır**[1]. Bu alt kümeler mümkün olduğu kadar tekil olabilmeli, kolaylıkla tahmin edilememelidir. *Bir insanın, başka birisini yüzüne bakarak tanıması, sesini dinleyerek kim olduğunu anlaması veya bir arslanın, eşinin bir kaya üzerine bıraktığı kokusu ile bulabilmesini* örnek olarak verebiliriz. İnsanların kalıcı hafızasında yüz binlerce surattan oluşan bir **kütüphane** mevcuttur. Bunları kullanarak karşımızdakini ismini dahi *hatırlayamaz* durumda iken tanıyabiliriz.

İnsanlar için bilişim sistemlerinde kimlik doğrulama 3 (üç) yolla olur[2]. *Kullanıcılar, kendilerine ait, doğrulama için kullanacakları veri kümesini bilişim sistemine iddia ettikleri kimlik tanımları ile beraber sunarlar*. Bu kimlik tanımları kullanıcı ismi olabileceği gibi anlamsız gözükene bir sayı topluluğu da olabilir. Yahut bu kimlik tanımını bilişim sisteminin onlara sunduğu listeden seçebilirler. Ayrıca, bilişim

sistemi, bu iddia da bulunan kullanıcının, **insan olup olmadığını** da burada bahsetmeyeceğimiz[6] çeşitli methodlarla sınayabilirler.

Kullanıcılara ait bu veri kümelerini 3 (üç) gruba toplayabiliriz.

- **Bildiği bir şey.** (Something you know)[3]
- **Sahiplendiği / envanterinde olan bir şey.** (Something you have)[4]
- **Olduğu bir şey.** (Something you are)[5]

“**Bilinen**” yani bildiği bir şey, *kullanıcının bildiği, bilişim sistemine ait bir terminal aracılığı ile girebileceği veri kümesidir*. Parolalar, kimlik tanımları iddiasını değerlendirecek bilişim sisteminin göstereceği *resimlerin sırası, bir koordinat, pi sayısının ilk 10 basamağı, pasifte konuşulan bir dildeki sözcükler olabilir*. Bu örnekler çoğaltılabilir, ancak bu örneklerle “**şifre**”[7] kavramını eklemek yanlış olacaktır. Dilimize yanlış geçirdiğimiz bir kavramda budur.

Bu “**bilinen**” lerin bir takım ortak özellikleri mevcut olabilir.

- Tekil olabilecekleri gibi bir gruba da ait olabilir. (*Bir grup kullanıcının ortak parolası gibi*)
- Kolay ve tahmin edilebilir (kimliklerle ilişkilendirilebilmesi gibi) olmaması gerekir. (*Doğum yılı, isim/soy isim de bulunan sözcükler gibi*)
- En sık karşılaşılan ortak özelliklerden birisi de **kolaylıkla unutulabilir** olmalarıdır. Bir kullanıcının parolasını unutmaması, iddia ettiği kimliği *doğrulamaması* anlamına gelir. Bu makale de ise buna karşı bir önlem sayılabilecek bir yöntemi Türkçe’imiz için uygulanabilir bir model önermekteyiz.
- En büyük dezavantajlarından biri de, **başkaları** tarafından öğrenilmesi durumu anlaşılmayabilir.

“**Sahiplenilen**” yani envanterindeki bir şey, kullanıcının sahip olduğu, bilişim sistemine ait bir terminal aracılığı ile “sunabileceği” ve bünyesinde, kimlik doğrulama için gerekli olan veri kümesini içeren bir nesnedir. *RFID kartlar, banka kartları, SIM kartları, kredi kartları, yaka kartları, sinema biletleri* gibi örnekler verilebilir.

- Bu “**sahiplenilen**” lerin bir takım ortak özellikleri mevcut olabilir.
- Tekil olabilecekleri gibi bir gruba da ait olabilir. (*Bir grup seyircinin tek bileti olması gibi*)
- **Kopyalanabilir** oldukları için bu yöntemlerin risk yönetimleri dahilinde olabildikçe zorlu olarak dizayn edilmeleri gerekir. Örnek vermek gerekirse *fiyatı ucuz olan bir sinema biletinin hazırlanması ile Büyük Millet Meclise giriş sağlayacak yaka*

• Bu makale 19 Nisan , 2010 tarihinde gönderilmiştir. Versiyon 1.1.3

Bu teknoloji için patent başvurusunda bulunulmamıştır. Araştırmacılar diledikleri gibi kullanabilirler.

R. E. Pişirici, FREELANCE, Ankara, TURKEY, engur@uzay.eu

A. Ç. Pişirici, EMTA A.Ş., Ankara, TURKEY, asli@uzay.eu

kartlarının hazırlanması aynı şekilde olmamalıdır.

- **Kaybedebilme** yahut **çaldırma** gibi olaylar olabilir. Bunların kaybeden ve çaldıran kullanıcı tarafından **fark edilmesi** kolaydır ancak kopyalanması durumunda gene anlaşılmayabilir.

“**Olunan**” yani olduğu bir şey, kullanıcının, kimlik iddiasında bulunduğu bilişim sistemine uygun bir terminal aracılığı ile veriler kümesi biçiminde iletebilecek bir olgudur. Bu olgular kullanıcının doğumu ile beraber gelebileceği gibi sonradan kazandığı özellikleri de olabilir.

Önemli olan bu olguların kişilere göre belirleyici ve veriler kümesi şeklinde ifade edilebilir olmasıdır. *DNA, Kan grubu, yüz izi, retina taraması, vb. BIOMETRİK olgular olabileceği gibi, imza, yazı karakter biçimleri gibi sonradan KAZANILAN olguları da örnek verebiliriz.* Bu örneklerle ıslak imza, elektronik imza gibi kavramları ekleyebiliriz.

Ancak **elektronik imza** ile **sayısal imzanın** aynı olmadığını, *sayısal imzanın matematiksel bir örüntü olduğunu*, elektronik imzanın da genel anlamı itibarı ile ıslak imzanın elektronik bir cihaza atılarak verilere dönüştürüldüğünü belirtmek gerektiğini önemle vurgulamak isteriz.

Bu “**olunan**” ların bir takım ortak özellikleri mevcut olabilir.

- Terminallerin kandırabilir olması durumu vardır. Örnek olarak vermek gerekirse *Parmak izi okuyucularını kandırmak için bir çok yol bulunabilmektedir.*
- Amacına göre güvenliği en iyi sağlanabilecek yöntemleri içermektedir. Kimliklerin doğrulamasında birbirleri ile aynı çıkmayacak **en güvenilir** veri kümelerini bu yolla alabiliriz.

Makalemizde inceleyeceğimiz kısım **PAROLA** konusudur. **Bilinen** türü içinde yer alan **PAROLA**, ezberleyip **UNUTMAMAMIZ** gereken bir veri kümesidir. Bu veri kümesini bir *terminal* aracılığı ile direkt olarak kullanıcının kendisi girmektedir. Unutulmadığı halde girmek bazen doğru şekilde olmayabilir. Fiziksel anlamda bir etkileşim mevcuttur. Örnek olarak, *tuş takımı – parmaklar ikilisi verebiliriz. Bozuk bir tuş takımı, yanlış basılan bir tuş, gibi etkenler bu sistemi etkilemektedir.*

Bir diğer konuda, parola seçimi ve seçilmiş parolaların yönetimidir. Günümüzde bir kullanıcı, birçok bilişim sistemine bu yolla girmektedir. Kullandıkları *banka kartları, kredi kartları, eposta hesapları, izledikleri forumlar, üyelikler gibi sunulan bütün hizmetler için* akılda kalıcı olması açısından bir zafiyet yaratacak da olsa ezberlenmesi kolay ancak güvensiz parolalar seçilmektedir. Parola yönetimi olarak bakıldığında, her ne kadar bu zayıf parolaların değiştirilmesi yönünde kullanıcı zorlansa da kullanıcı ilk fırsatında bunlar gene zafiyet yaratacak biçimde seçmekte ve kullanmaktadır.

A. Getirdiğimiz Yenilik

1980 li yıllardan beri kullanıcılar için parola seçimi, bilişim sistemlerinde parola yönetimi gibi konularda çalışmalar

olmuştur[8]. Bu makalede bahsettiğimiz telaffuz edilebilir parola kavramı yeni olmamakla beraber, Modern Türkçe yazım dili için hazırlanmış bir model yoktur. Getirdiğimiz yenilik, Türkçe kullanan kullanıcıların zafiyet yaratacak bir biçimde zayıf parola seçmesi yerine daha güçlü parolalar seçebilmesini sağlayacak telaffuz edilebilir parola üretebilecek bir model ve yaklaşım önerceğiz.

B Makalenin Organizasyonu

Makalenin ikinci kısmında PAROLA kavramının dayandığı EZBERLEME konseptine bakacağız. Sembolik bilincimizin olduğundan ve ezberlemeyi semboller üzerinden yaptığımızdan bahsedeceğiz. Bu konseptde yer alan kısa süreli hafızamızla ilgili **yedi (7) sembol** kavramına değindikten sonra telaffuz edebilmenin sembolik bilincimizle ilgisine değineceğiz. Üçüncü kısmında Türkçe telaffuz edebilmenin modeline bakacağız. Hece gruplarına değinecek, ayrıca telaffuz edebildiğimiz ancak anlamı olmayan sözcükler ile harflerin yan yana geldiği gene anlamsız sözcükleri kıyaslayarak semboller şeklinde tuttuğumuz parolaların gerçek uzunluklarına örnekler göreceğiz. Dördüncü kısımda bu konuda dünyadaki örnek uygulamalara değinecek ve çalışma örneklerine bakıp modelimizi ve yaklaşım methodlarımızı tamamlayacağız. Beşinci ve son kısımda anlatılanları özetleyip ortaya koyduğumuz model ve yaklaşım ile bilişim sistemlerinde yapabileceğimiz değişiklikleri tartışarak makaleyi tamamlayacağız.

II. EZBERLEMEK

A Bilinç Tanımı

Beyin ve bilinç kavramı hala üzerinde çalışılan ve tamamı tam olarak anlaşılmamış konulardır. Anlayabildiklerimiz üzerinde duracak olursak, insan beyni bilinç üzerinde her şeyi “*ezberleyerek*” yapmaktadır. Basit gibi görünen bir matematik işlemini bile aslında ezberleyebildiğimiz için yapabilmekteyiz. Örnek olarak verirsek, **5 ile 8 in çarpımında sonucu 40 olarak buluruz.** Bu sonucu bir matematik işlemi yaptığımız için değil ezberlediğimiz için verebilmekteyiz. Yüz hafızamız içinde aynı şekilde, onları “ezberleyip” beynimizin bu iş için ayırdığı “bölmelere” koymaktayız.

Okumak bize ne kazandırıyor? sorusuna baktığımız vakit, yazıları harf harf olarak değilde “kalıplar” şeklinde algıladığımız ortaya çıkıyor. Çok okuyan birisinin bu kalıpları çok harf içerdiğinden az okuyup sadece harf kalıplarını algılayan bir insandan daha hızlı okuyabilmesini sağlayan mekanizma, konuşma işlemi içinde geçerlidir.

Bilincimiz sembolik olarak işler. Her veriyi sembolleştirerek saklamaktadır. Kısa süreli hafızamız yedi (7) sembolü hemen işleyebilmektedir.[9] Bizden hatırlamamız istenen bir telefon numarasını rakam rakam olarak değilde **gruplanmış semboller olarak** tutabilmek daha kolay olmaktadır. O yüzden bazı numaraları daha rahat hatırlarken bazı numaralar da bir türlü aklımız kalmaz.

Bireylerdeki bu farklılık sembolik bilincimizin semboller konusunda farklılığından kaynaklanmaktadır. Buna örnekler verebiliriz. “*Mehmet*” ismi bizler için *tek bir sembol haline*

dönüşmüşken, dilimize yahut bu isme yabancı birisi, bunu hatırlamakta zorluk çekecektir. Çünkü sembolik bilinci orada kendi dil yapısına uymayan altı (6) adet harf yan yana durmaktadır.

1453 sayısı, bizim nesil için **tek** bir sembol olabilirken, muhtemelen yeni nesildeki birçok birey için dört (4) haneli bir sayı yani muhtemel olarak **dört** (4) sembolden oluşan bir sayı olacaktır.

B. Okuduğumuz Kelimeler ve Telaffuz Edebilmek

Daha öncede değindiğimiz gibi, okuyabildiğimiz kelimeleri aslında **harf harf olarak değilde** sembolik bilincimizde olan **semboller** olarak algılamaktayız. Bunların en basiti ise okumayı öğrenirken bize öğretilen **HECE** gruplarıdır. O yüzden bir anlam ifade etmese bile telaffuz edebildiğimiz kelimeleri harf harf hatırlamak yerine sembol sembol yani hece hece olarak hatırlamamız mümkün olacaktır. Örnek olarak, “*zxlqo*” u beş (5) sembol olarak algılayabilirken “*konrof*” kelimesini sadece iki (2) sembol olarak algılayabiliriz. Sembolik bilincimizde telaffuz edebildiğimiz minimum kalıplar mevcuttur. “*kon*” - “*rof*” bu kalıplardan ikisidir.

Sonuç olarak, “**PAROLA**” yı nasıl *sakladığımızı* bakacak olursak;

Beynimiz sözcükleri harf olarak değilde, gruplanmış semboller olarak tutabilmektedir[10]. (“*konrof*” kelimesi gibi)

Sembol grupları kullanıldıkça tek sembole olmaya doğru yakınsar, yani kalıplaşır. (“*Mehmet*” ismi örneği gibi)

Telaffuz edebildiğimiz sözcükleri harf olarak değilde, hece grupları olarak tutabilmekteyiz. Hatta bu hece grupları beynimizde kendi aralarında sembol oluşturmaları durumunda *daha az sayıda sembol olarak tutabilmemiz gerçekleşebiliyor*.

III. PAROLA VE TELAFFUZ EDİLEBİLİR PAROLA

A. Bilinç Tanımı

Parolalar harf ve sayılar ve giriş yapılacak **terminal** üzerinde bulunabilen şekillerden oluşan sembol gruplarıdır. Kullanıcı bunları terminal aracılığı ile belirli bir sürede, belirli bir sıralamada giriş yapmalıdır. Hemen hemen her terminal de (*klavye, tuş takımları, bilgisayar faresi veya dokunmatik ekran üzerinde tıklayarak, vb.*) hata yapma olasılığına karşı **birkaç** kez tekrarlama hakkı verilmiş ancak fazla tekrarlama yapmak ise kimlik doğrulama istenen kullanıcı tanımının belirli bir süre boyunca o terminal üzerinden girişini **engellemeyi** sağlamışlardır.

Telaffuz edilebilir parolaların çıkışı dünya üzerinde yeni değildir[11]. Bilişim sistemlerinde türkçe telaffuz edilebilir parola üretimi konusunda makale yazarlarından birisinin 1995 de bir çalışması olmuş bunla ilgili bir bilgi notunu 1995 de bir sunumda dipnot olarak bahsetmiştir.[12] Türkçe üzerinde bu konuda yapılan bir başka çalışmaya rastlanmamıştır. Ancak İnternet ve hypertext tabanlı medyanın yaygınlaşması, bu konularda yapılmış çalışmaların literatürlere girilmesini zorlaştırmış, o yüzden Türkçe telaffuz edilebilir parola

kavramını “yeni” olarak sunmak açıkçası doğru gelmemiştir.

Bu bilgiler ışığında, en azından bizler için yeni sayılabilecek bir kavram olarak Türkçe telaffuz edilebilir parolaları incelerken öncelikle **dil yapısına** bakmamız gerekmektedir.

B. Türkçe ve Telaffuz edilebilir Kelimeler

Türkçe, okunduğu gibi yazılabilen bir dildir. Ayrıca bir fonetik alfabesine ihtiyaç duymaz! O yüzden Türkçe telaffuz edilebilir parolalar, okunduğu gibi yazılabilen kelime-sayı ve şekilsel sembollerden oluşabilir.

Türkçe telaffuz edilebilir kelime üretmek için kullanılabilecek bir yaklaşım yazılı metinlerden **markov modeli** kullanarak bir yöntem belirlemek olabilir[13]. Bu yöntem çok rahatça kullanılabilmektedir çünkü yukarıda bahsettiğimiz gibi fonetik diline ihtiyaç duyulmadığı için taranacak yazılı metinlerle oluşturulacak markov veritabanında çok ufak düzeltmeler yaparak, düzgün bir model ortaya konulabilir.

Ancak bu makale de bu yöntem üzerinde durulmayacaktır. Araştırmacıların bu yöntemle ilgilenmesini özellikle Türkçe dili için bir markov modeli geliştirilmesini hararetle tavsiye ederiz.

Türkçe’de kelimeler hece topluluğudur. Heceler harf topluluğudur. Dilimizde birkaç yazım ve/veya okuma kuralı hariç (*sesli uyumu, bazı harflerin kelime başına veya sonuna gelememesi gibi*) telaffuz edilebilir kelime üretebilmek için **üç (3) temel kural** içerir.

- **Her hece bir sesli harf içermektedir.** Bu kural Türkçe fonetiği için kaçınılmaz bir kuraldır. İki veya daha fazla sesli harf içermez. Birçok dilde olduğu gibi bazı kelimelerimizde bazı hecelerin sesli harf içermediğini görebiliriz. Ancak bu kelimeleri de sesli harf içerecek şekilde okuduğumuz için bunların yazımı da sorun teşkil etmeyecektir. Örnek olarak “*tren*” kelimesini verebiliriz. Bu kelimeyi “*ti-ren*” şeklinde okuruz. Tek heceden oluşmuş gibi gözükse de, bunu fonetik olarak iki hece şeklinde kelimeyi söyleriz.
- **İlk hece hariç, bütün hecelerde ikinci harf sesli harfidir.** Bu kuraldan, bir kelimeyi oluşturan heceler için şu alt kuralları çıkarabiliriz.
 - İlk hece tek harften oluşabilir. (bir tane sesli harf)
 - Diğer heceler minimum iki harften oluşabilir. Daha önceden belirttiğimiz gibi heceler harf topluluğudur.
 - Fonetik dil yapımız gereği bir hecedeki maksimum harf sayısını dört (4) ile sınırlandırmış olursak, bu kural kapsamında kelimeleri hecelerine ayırabilir, uygun hecelerle telaffuz edilebilir kelimelerde üretebiliriz.

Örnek olarak “*aza, ilk, ilkin*” kelimelerini verebiliriz. “*Aza*” kelimesini “*a-za*” olarak okuruz, “*az-a*” olarak okumayız. “*İlk*” kelimesini tek hece olarak “*ilk*” şeklinde telaffuz ederiz. “*İlkin*” kelimesini “*il-kin*” olarak söyleriz, “*i-lkin*” veya “*ilk-in*” şeklinde telaffuz etmeyiz.

- Üçüncü kural olarak rahatlıkla türetebileceğimiz gibi, ilk hecenin sesli harf ile başlayabilmesidir. ("a-ma")

C. Hece Gruplarının Tanımlanması

Öncelikle **hecenin tanımına** bakacak olursak, kelimeleri oluşturan en küçük birimi harf olan ve **ağzın tek hareketinde sarf edilebilen ses modelidir**[14]. Türkçe de **en fazla 4 harfli** hece vardır. Türkçe de hece ve seslem konuşma ve yazma dilinde aynıdır. O yüzden yukarıda bahsettiğimiz gibi ayrıca bir fonetik abecesine ihtiyaç duymaz. Modeli oluşturmak için gerekli tanımları ortaya koyarken, hece gruplarını tanımlamadan geçemeyiz. Yaklaşımımızda alfabeyi oluşturan sembollerden rastgele seçerken uygun bir hece oluşturabilmek için kelimeyi oluşturan hece gruplarına uygunluğuna bakmamız gerekir. Bu gruplamayı hecenin, kelimedeki pozisyonuna göre yaparız. Buna göre, Tablo-I de gösterilen üç (3) çeşit hece grubundan bahsedebiliriz.

TABLO I
HECE GRUPLARI

Kod	İsim	Açıklama
H1	Başlangıç Hece Grubu	Kelimelerin başında bulunan ve Türkçe kurallarına göre üretilen grup.
H2	Orta Hece Grubu	Kelimelerin ortasında bulunan grup. Bu gruptaki hecelerin komşu hecelerle uyumlu olması sağlanabilir.
H3	Bitiş Hece Grubu	Kelimelerin sonlarında bulunan ve Türkçe kurallarına göre üretilen grup.

Bu gruplar, yukarıda geçen kurallara ve ilk başta belirttiğimiz Türkçenin diğer (sesli uyumu, *Ğ* ile *başlamama*, vb.) uygun olarak üretilirler.

Örneğin H1 grubundan bir hece, başlangıç grubu olduğu için tek harf olarak üretilebileceği gibi "**Ğe**" şeklinde bir H1 hecesi de olmayacaktır.

D. Kelime Gruplarının Tanımlanması

Model için hece gruplarının tanımını yaptıktan sonra kelime gruplarının da tanımını yapabiliriz. Bu kelimeleri veya sözcükleri direkt parola olarak kullanabileceğimiz gibi ileride değineceğimiz şekilde kelime gruplarından bütünselik elde edeceğimiz grupları da kullanabiliriz.

Kelime gruplarını Tablo-I deki hece gruplarına göre Tablo-II de göstertildiği gibi üç (3) şekilde yapılandırabiliriz.

TABLO II
KELİME GRUPLARI

KOD	İsim	AÇIKLAMA
KT	Tek heceli Kelime Grubu	Bu grupta, H1 ve H3 gruplarına uyan yani ortak kümelerinde kesişen heceleri sayabiliriz. KT = H1∩H3 olarak formül biçiminde ifade edebiliriz.
Kİ	İki heceli Kelime Grubu	Burada iki heceden oluştuğu için H1 ve H3 gruplarından heceleri sayabiliriz. Kİ = H1+H3 olarak ifade edebiliriz.
KÇ	Çok heceli Kelime Grubu	Bu kelime grubunda tanımladığımız bütün hece gruplarını kullanacağız. KÇ = H1+H2+...(H2)...+H3

Bu tablo da belirtilen hece grupları Tablo-I den alınmıştır.

TABLO III
SEMBOL GRUPLARINA EKLENTİLER

Kod	İsim	Küme
S1	Rakam Tablosu	{0,1,2,3,4,5,6,7,8,9}
S2	Çarpım Tablosu	{...,25,...,81,...}
H1	Alfanümerik Karakter Tablosu	{A,...,Ξ,Ψ,Z}
T1	Terminal üzerinde bulunan sembol Tablosu	{.,!,^,%,&,...}
...	...	...

Tablo bilincimizde yeralan sembollere göre rahatlıkla uzatılabilir.

E. Sembol Gruplarının Genişletilmesi

Telaffuz edilebilir Parola modelinde temel olarak şekilleri değil insan beyninde oluşan sembollerini temel almıştık. Bu semboller hece grupları olduğu kadar başka şekillerden oluşan sembollerde olabilir. Sembol gruplarımızı, kelime-hece gruplarına ekleyerek sembol havuzumuzu genişletebiliriz. Böylece hece gruplarının arasına, kelime gruplarının başına ve/veya sonlarına bu sembol gruplarını da ekleyebiliriz. (Yukarıdaki Tablo-III'e bakınız.)

Bu örnekler çoğaltılabilir. Dikkat edilmesi gereken en önemli şey, bu kümelerde bulunan elemanların insan beyninde ve özellikle Türkçe düşünen bir bilinçte sembol olarak bulunmasıdır. İlkokulu bitiren herkes 81 sayısını tek sembol olarak hatırlayabilecekken, 1453 gibi bir tarihi tek sembol olarak hatırlanamayabilir.

Bunların dışında, bu sembol gruplarına yapılabilecek bazı özellikleri de tek başına bir sembol olarak kabul edebiliriz. Örnek vermek gerekirse, büyük-küçük harf farkı tek başına bir semboldür.

F. Zorluk Dereceleri

Modelimizi oluştururken, üretilebilecek parolalar için bir hatırlanma zorluk derecesi (HZD) tanımlayabiliriz. Buna göre, Tablo-IV de HZD'ler tanımlanmıştır.

TABLO-IV HATIRLANMA ZORLUK DERECELERİ		
HZD	PAROLANIN İÇERDİĞİ SEMBOL SAYISI	ÖRNEK
Kolay	1—2 arası	a1, alsa
Orta	3—5 arası	konzartok, yandurkurtsa
Zor	6—7 arası	kardıçakkoznayopnok
İstisna	7'nin üstü	21tur%kantRonXkay!

Bu tanımlamalar üzerine, kullanıcıların bu model doğrultusunda istedikleri bir zorluk derecesinde parola üretebilmeyi veya sistemin güvenlik kriterleri bakımından minimum bir zorluk derecesinde parola ürettirmeyi yapabiliriz..

G. Parola Örnekleri

Parola ve telaffuz edilebilir parolalara örneklere yukarıda yaptığımız tanımlar doğrultusunda geçebiliriz. Örnekleri 1-7

HZD sırasında ele alacağız. Örnekleri incelerken, hatırlanması aynı zorlukta olan ve sembollerini aynı sayıda barındıran ancak karakter olarak (harf, sayı veya sembol digitleri) birbirlerinden çok farklı sayıda içeren parolalara rastlayacağız.

Bir tane sembol içeren örnekler; “zon, ka, a, 21, 5, kart, 1976, aslı”. Bu örneklerde tek heceli grupları görebiliriz. Ayrıca bir doğum yılı veya bir isim birileri için tek sembol haline gelmiş olabilir.

İki tane sembol içeren örnekler; “Zon, aü, on21, aslı1975”. Burada “Zon” örneğini, “z si büyük – zon” olarak anlarız. “aslı1975” ise bir isim ve bir doğum tarihinden oluşan aslında toplam iki tane sembol içeren bir paroladır. Bu tip parolalara sıkça rastlayabiliriz. Uzun gözükmesine rağmen aslında “kolay” olduklarını fark etmemiz gerekmektedir. Parolalar asla ama asla karakter **uzunluklarına göre incelenmemelidir**

Üç tane sembol içeren örnekler; “kazOn, aüv, akazon, engüraslı1975”. Örnekleri incelersek, “ka-o'su büyük-zon, üç tane harf, üç hece, ve iki isim artı bir tane tarih” olarak görebiliriz. Aynı seviyedeki örnek verdiğimiz bu parolalarda üç karakterli de on üç (13) karakterli parolada olmaktadır.

Son olarak yedi tane sembol içeren bir örneğe bakalım; “kaRt%1976zon%engür”. Bu örneği “r'si büyük kart-% işareti-1976 tarihi-zon-ünlem-isim” olarak ele alabiliriz. Bunu ezberlemeye başladıktan sonra bir takım yakınsamalar olabileceği gibi sembol sayısı zamanla bire (1) doğru yaklaşacaktır.

Dikkat edilmesi gereken bir hususta, sembollerini birbirine benzeyen grupların yan yana gelmemesidir. Örnek olarak *çarpım tablosundan 21 ve rakam tablosundan 3 'ü yanyana kullanırsak ortaya çıkan “213”ü iki sembol olarak değilde, başlangıçta “2-1-3” olarak algılayabiliriz*

IV. YABANCI DİLLER İÇİN VAR OLAN UYGULAMALAR VE MODELİMİZ

Dünyadaki örnekleri incelemeye çalıştığımız vakit, yukarıda belirttiğimiz sebepler yüzünden, daha çok İngilizce kaynaklar ve patent arama motorları üzerinden bulabildiklerimizi inceleyebildik.

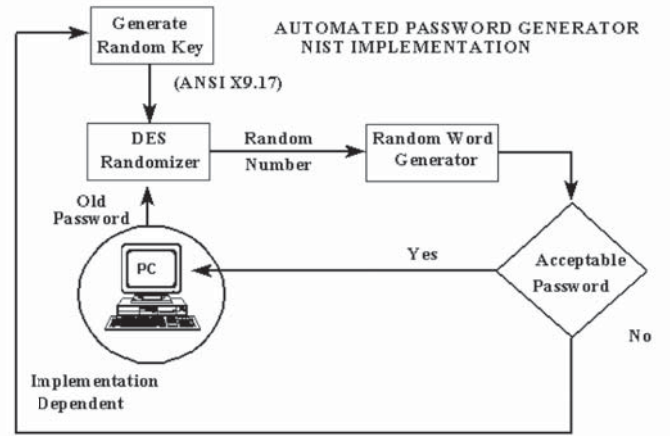
İlk rastladığımız belge FIPS-181 deki telaffuz edilebilir parola üretimindeki yönlendirmeleri idi[15]. Rastladığımız birçok uygulamada FIPS-181 deki direktiflere uygun olarak yapılmıştı.

Diğer bulabildiklerimiz, genellikle markov modeli kullanarak oluşturdukları ağaç yapısından yola çıkarak bir takım diller için telaffuz edilebilir parolalar kullanmaktadırlar[16]. O dilde yazılmış ne kadar çok metin bulunabilirse, oluşturdukları modeller daha etkin telaffuz edilebilir ancak anlamsız kelimeler üretebilmektedirler[17].

A. FIPS-181 ve Digram Modeli

FIPS-181'de bahsedilen model üç ana parçadan meydana gelir. Birim tablosu, **digram** tablosu ve rastgele üretici alrutini. Şekil – 1 de geçen rastgele kelime üretici (Random Word Generator), telaffuz edilebilir hece /seslem grupları oluşturarak ve bunları birbirlerine bağlayarak kelime üretir[18]. Telaffuz edilebilme kuralları birim ve digramlar için bir tabloda tutulur. Bu kurallar birimler yani alfabe de bulunan harflerin hece/seslem içinde bulundukları pozisyon

için geçerli yahut geçersiz şeklindedir.



Şekil. 1. Rastgele kelime üretici önceden üretilmiş rastgele sayıyı kullanarak FIPS181 de tanımlanmış kurallara uygun olarak telaffuz edilebilir parola üretiyor.

B. Markov Modeli ve Diğerleri

Aşağıda örnek olarak inceleyeceklerimiz dışında bizim modele yakınsayanlarını bulamadık. Genellikle hedefledikleri diller dolayısı ile yahut markov modeli sayesinde genelleştirebildikleri için bu yöntemi tercih etmişlerdir. Fonetik dile ihtiyaç duymayan dil sınıfında sadece Türkçe yi araştırdığımızdan dolayı, dünya üzerinde bizim modele benzeyen başka bir yapıt dan haberimiz olamadı. Ancak aklın yolu birdir. Spesifik olarak, fonetik dile ihtiyaç duymayan bir dile uygulanabilecek bu yöntem, genelleşmiş markov modelinden daha iyi sonuç vereceği ortadadır. Unutulmaması gereken, diğer uygulamalarda ortak olarak kullanılan markov modeli, bir sistemin eğitilmesine ve eğitildiği veriler üzerine inşasına dayanır.

Üzerinde çalışılan dilden çıkarılacak markov modelinde dikkat edilmesi gereken birçok konu olabilir. Fonetik dile ihtiyaç duyan yapılarda telaffuz edilemeyecek kelimeler ortaya çıkabilir. Hem bizim önerdiğimiz yaklaşım çerçevesince araya başka semboller konularak üretilecek parola güçlendirilebilmektedir. Bunu markov modeli uygulamalarda araya konulmasından çok başına yahut sonuna eklenebilmektedir.

Ayrıca, fonetik dil-yazım dili çevrimi yapabilen, böylece fonetik dile ihtiyaç duymasına rağmen markov modeli oluşturmadan yapabilen bir uygulamaya rastlamadık.

C. Örnek Uygulamalar

İnceleyeceğimiz uygulamaların hakları taraflarca saklıdır. Bu paragraf dan başlayarak beşinci kısma kadar olan bahsedilenler kendi fikirlerimiz değildir ancak yorumlar bize aittir, sahiplerini bağlamaz.

KeePass Pronounceable Password Generator[23]

Projenin dokümanlarında nasıl telaffuz edilebilir parolaları nasıl ürettiğine dair ayrıntılı bilgi yoktur. FIPS-181 direktiflerine uyduğunu proje dosyalarından bir metinde deklare etmiş, ancak nasıl uyduğuna dair ek bilgi koymamıştır.

Method and System for generating pronounceable security passwords / US Patent No: 5588056[19]

Projenin dokümanlarında nasıl telaffuz edilebilir paroları nasıl ürettiğine dair ayrıntılı bilgi yoktur. FIPS-181 direktiflerine uyduğunu proje dosyalarından bir metinde deklare etmiş, ancak nasıl uyduğuna dair ek bilgi koymamıştır.

A Simple Pronounceable Password Generator for PHP[20]

Projenin dokümanlarında nasıl telaffuz edilebilir paroları nasıl ürettiğine dair ayrıntılı bilgi yoktur. FIPS-181 direktiflerine uyduğunu proje dosyalarından bir metinde deklare etmiş, ancak nasıl uyduğuna dair ek bilgi koymamıştır[21].

V. SONUÇ

Bu makale kapsamında, **Türkçe telaffuz edilebilir parola** üretimi incelenmiş, dünyada diğer diller için var olup Türkçe için uygun sayılabilecek, önceden hazırlanmış tablolar kullanma sureti ile (**FIPS** modeli) veya daha önceden bulunmuş metinlere dayalı olarak oluşturulan **markov modelleri** yerine, kurallarına uygun bir biçimde tablolara Ya da **markov modeli'ne** ihtiyaç duymadan **sınırlanmamış** parola üretebilmeyi sağlayacak bir model ortaya konmuş ve yaklaşımı incelenmiştir.

Önerilerimiz, çeşitli işletim sistemleri için tasarlanabilecek **uygulamalarda** kullanılmak üzere bu konuda bir **kütüphane** geliştirmek, böylece bu kütüphane yi olabildiğince çok **platformda** destekleyerek halkın kullanımına açmaktır. Bir **kütüphane** ve birkaç **platformda** çalışan uygulamalarımız mevcut dur ve paylaşıma açıktır. Bir fikir alınması açısından araştırmacılar alıp **inceleyebilir**.

Ayrıca, önceden parola atanması konusunda, bilişim sistemlerine bu tip bir kütüphane eklenerek, kullanıcıya hiç olmazsa akılda daha çok kalıcı parola atanabilir. **Kullanıcıya** parola **seçtirirken**, bu kütüphane yardımı ile bunlara uygunluğu test ettirilebilir.

Bu konseptin içinde, başka sembol grupları da eklenebilir. Örneğin *klavye komşuluk grubu* gibi. ("asd", "qwe", "hjk")

Son olarak da, yukarıda bahsedilen durumun **tam tersi** de uygulanabilir. Kullanıcının seçtiği parolanın telaffuz edilebilir olup olmadığına bakılarak, *telaffuz edilemeyecek* daha **zor** parolalar için yönlendirilebilir. Unutmamak gerekir ki, telaffuz edebilmek, akılda daha kalıcı olur. Bu da bir takım görüşlere göre bir **zafiyet yaratmaktadır**[22].

EKLER

Makalede bahsi geçen kodları baş yazarla irtibata geçerek alabilirsiniz. Ayrıca bu makaleye ait hazırlanan sunumu <http://engur.uzay.eu/sunumlar> adresinden indirebilirsiniz.

TEŞEKKÜR

Sayın **Emre Karalarlı**'ya ve **Hidayet Doğan**'a bu makalenin hazırlanması esnasındaki değerli katkılarından dolayı teşekkür ederiz.

KAYNAKÇA

- [1] Pişirici, R., E., Unix de Güvenlik. 1. Türkiye'de İnternet Konferansı. Kasım 1995.
- [2] Authentication. Wikipedia. <http://en.wikipedia.org/wiki/Authentication> (01.04.2010).
- [3] Schneider, F., B., Ders Notları. Something You know, are and have. <http://www.cs.cornell.edu/Courses/CS513/2005FA/NNLauthPeople.html> (01.04.2010). 4
- [4] Usb and Tokens. Entrust. <http://www.entrust.com/tokens/> (01.04.2010)
- [5] Ahuja, V., A., Dallas-Texas Üniv. Bilişim IT ve Yönetim http://citm.utdallas.edu/research/Publications/white_papers_source/Bio_metrics.pdf (01.04.2010)
- [6] Ahn, L., V., M. Blum. ve J. Landford. Captcha: Telling Humans and Computers Apart. http://www.captcha.net/captcha_cacm.pdf (01.04.2010).
- [7] Pişirici, R., E., Güvenlik ve Kavramlar. 11. Akademik Bilişim Konferansı. Şubat 2009.
- [8] The Federal Information Processing Standards. Password Usage. FIPS 112. Mayıs 1985
- [9] Erden F., Kocaeli Üniversitesi Farmakoloji Anabilim Dalı Yayınları, <http://tip.kocaeli.edu.tr/docs/farmakoloji/bizogrenirken.ppt> (01.04.2010)
- [10] Erden F., Kocaeli Üniversitesi Farmakoloji Anabilim Dalı Yayınları, <http://tip.kocaeli.edu.tr/docs/farmakoloji/bizogrenirken.ppt> (01.04.2010)
- [11] The Federal Information Processing Standards. Password Usage. FIPS 112. Mayıs 1985
- [12] Pişirici, R., E., Unix de Güvenlik. 1. Türkiye'de İnternet Konferansı. Kasım 1995.
- [13] Passkool, SourceForge, <http://passkool.sourceforge.net/> (01.04.2010)
- [14] Sesbilim, Vikipedi, <http://tr.wikipedia.org/wiki/Sesbilim> (01.04.2010)
- [15] The Federal Information Processing Standards. Automated Password Generator Standard. FIPS 181. October 1993.
- [16] Randomness Requirements for Security. RFC- IETF. <http://www.ietf.org/rfc/rfc4086.txt?number=4086> (01.04.2010)
- [17] Pişirici, R., E., Güvenlik ve Kavramlar. 12. Akademik Bilişim Konferansı. February 2010.
- [18] E. H. National Technical Information Service (NTIS) AD A 017676, *A Random Word Generator for Pronounceable Passwords.*, pp. 123–135.
- [19] Online Patent Search Engine. <http://www.freepatentsonline.com/5588056.html> (01.04.2010)
- [20] Jesus nickli yazar. PhpBuilder Website. <http://www.phpbuilder.com/columns/jesus19990502.php3> (10.01.2010)
- [21] Gasser, M., *A Random Word Generator for Pronounceable Passwords*, MTR-3006, The MITRE Corporation, Bedford, MA 01730, ESD-TR-75-97, HQ Electronic Systems Division, Hanscom AFB, MA 01731. NTIS AD A 017676
- [22] Password Strength. Wikipedia. http://en.wikipedia.org/wiki/Password_strength (01.04.2010)
- [23] KeePass Pronounceable Password Generator at SourceForge WebSite. <http://sourceforge.net/projects/pronouncepwgen/files/> (01.04.2010)

Yazarlar

R. Engür Pişirici – <http://engur.uzay.eu>
Aşlı Ç. Pişirici – <http://asli.uzay.eu>

An Implementation of Kerberos Captive Portal

Cihat TOMBAK, Natan ABOLAFYA, Tugkan TUGLULAR

Abstract— A widespread example usage of wireless networks, a technology which gets more and more employed every single day thanks to its simplicity of utilization and deployment, and high accessibility, is captive portal, software for hotspots. However, developed security solutions for wireless communications are not suitable for captive portals. Problems and solutions for captive portals are mainly based on authentication because primarily the main task of a captive portal is authentication. Even though it's primary, it is also highly vulnerable to session hijacking for most of the captive portal implementations. This paper proposes a solution against session hijacking. It explains negotiation based Kerberized captive portal model for secure authentication. In this model, captive portal is proposed as a proxy with Kerberos authentication and negotiation. This model is worked up into an application with participation of key distribution center.

Index Terms—Captive portal, Kerberos authentication, proxy.

I. INTRODUCTION

AFTER growth popularity of IEEE 802.11 a, b, g, n based wireless communication, securing wireless communication and authentication became an important issue. This security is provided by many protocols in terms of different TCP/IP layers.

Home and small business wireless networks can be protected by WEP, WPA or WPA2 encryption methods. These methods are used via a single password. Any of these methods is not feasible for network systems that has huge amount of clients like hospitals, universities, and hotels. Single password is not convenient for these systems because security of single password in a crowded environment is not reasonably achievable. Therefore, wireless hot spots are used for these environments. Captive portal is the application that operates on wireless hot spots. Captive portals are preferred for short time authentication because of their functionality. They do not require any installation on client machine and authentication is easy via web interface. Also user management is very simple. However, it has many security

vulnerabilities open to exploitation by intruders. We propose a new approach and implementation to secure these vulnerabilities.

Kerberos is introduced as an authentication and authorization method for local networks. We merged the power of Kerberos with functionality of captive portal structure. For this purpose, there are a lot of studies including usage of Kerberos authentication for secure captive portals. These implementations use Kerberos authentication for only login process of captive portals. We propose a model including fully kerberized authentication and communication called negotiation.

The content of this document is organized as follows. Second section mentions existing captive portal implementations, their vulnerabilities and consequences of these vulnerabilities. Section three introduces our approach and its advantages. Finally, fourth section presents details of our implementation as an application.

II. EXISTING IMPLEMENTATIONS AND THEIR VULNERABILITIES

As in Figure 1 and 2, the common authentication occurs as following [3,4]:

1 - "Client" selects and connects the network which captive portal is employed. Client requests DHCP lease, and gets its IP address.

2 - Client requests an HTTP service from the exterior network via a web browser. (Figure 1 – Step I)

3 - Gateway firewall cannot recognize the IP and MAC address of the request owner and redirects client to the login page of the captive portal. (Figure 1 – Step II)

4 - Client signs-up and/or signs-in with credentials, agrees some terms, types numbers from a pre-paid ticket, enters credit card number or any kind of authentication that captive portal is employed for.

5 - The captive portal software verifies this information locally or externally and adds the according firewall policy with regard to MAC and IP address. (Figure 2 – Step IV)

6 - Client gets response for the HTTP request it sent originally. (Figure 2 – Step III, V)

Unless specified, client is allowed to use network resources afterwards.

A. Current captive portal Implementations

All of the current captive portal implementations are based on registering client's IP and MAC address to gateway firewall. This registration means updating the firewall policy, thus client is allowed to communicate with the exterior network. However, this model is remarkably vulnerable to

Manuscript received April 1, 2010.

Cihat Tombak is with the Department of Computer Engineering, İzmir Institute of Technology, İzmir, 35430 Turkey, (e-mail: cihatombak@std.iyte.edu.tr).

Natan Abolafya is with the Department of Computer Engineering, İzmir Institute of Technology, İzmir, 35430 Turkey, (e-mail: natanabolafya@std.iyte.edu.tr).

Asst. Prof. Dr. Tugkan Tuglular is with the Department of Computer Engineering, İzmir Institute of Technology, İzmir, 35430 Turkey, (e-mail: tugkantuglular@iyte.edu.tr).

session hijacking [2]. Three variations of this implementations are explained below.

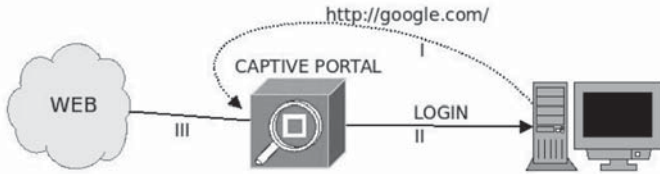


Figure 1: captive portal web access request.

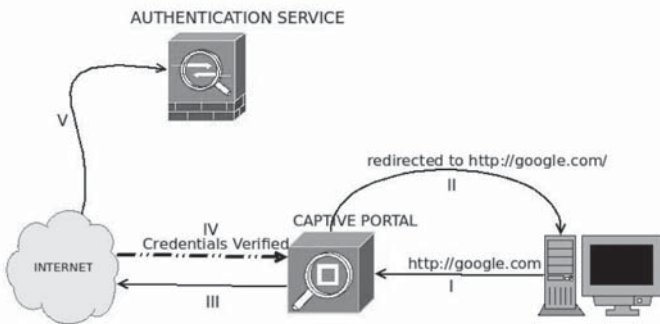


Figure 2: captive portal Authentication Process.

First implementation is based on only basic web authentication. Client meets the requirements to authenticate on the web interface and if accepted, its IP and MAC address is registered. Unless encrypted, for instance by SSL, credentials are easily eavesdropped or used by replay attack.

Second implementation supplements RADIUS or suchlike which provides centralized Authentication, Authorization and Accounting (AAA) to first implementation [5]. This protocol offers more secure authentication and flexible services (accounting, etc.) for captive portals. However, it is still ineffective to session hijacking.

Third and yet the most effective implementation is a periodic authenticator [9]. After client signs in, the web browser creates a new page or runs a background process called authenticator which sends encrypted messages to gateway periodically. If these encrypted messages aren't received by gateway on time, it deletes the corresponding policy which lets the specified MAC and IP address owner access to the exterior network.

B. Security Vulnerabilities of Current Captive Portal Implementations

Current captive portal implementations have all the vulnerabilities a wireless local network without any security measurements like WPA/WEP [2]. This results in all network traffic on the local network being broadcast to anyone. This enables attackers to perform eavesdropping, man-in-the-middle attacks, and replay attacks.

The most significant exploit for captive portals is session hijacking. Any intruder that sniffs the wireless network traffic, is able to easily obtain MAC and IP addresses of authorized clients since there is no encryption. With MAC and IP

addresses they can easily act as if they are authorized clients. Therefore, they can get access to restricted services without permission.

Less common, yet a dangerous attacks for captive portals are man-in-the-middle attacks. In these attacking methods, the attacker puts itself between client and gateway by creating a trojan access point or ARP Poisoning or any other MITM methods. If mutual authentication isn't employed in the captive portal environment, client cannot know captive portal is the actual captive portal, therefore sends its credentials, which might be even of a credit card, to the attacker unconsciously.

III. OUR APPROACH AND ITS ADVANTAGES

General structure of fully kerberized captive portal is examined under three headings; authentication, negotiation and web access. Clients connect to wireless network without network password as is classic captive portals. Whenever they attempt to browse web, that request is handled by firewall which is configured to route requests to captive portal information page. This page displays the configurations that client must do and software to install in order to authenticate. Furthermore, it is possible to create a PHP page to display an interface for signing-up or creating users (principles for Kerberos). Figure 3 shows kerberized captive portal implementation.

A. Authentication

Authentication process is done with Authentication Server (AS) as in conventional Kerberos authentication model.

Authentication occurs as following:

- 1 - Client selects and connects the network without providing any password as in standard captive portals.
- 2 - When Client requests an HTTP service from the exterior network via a web browser, gateway redirects the request to the information page of the captive portal.
- 3 - Guided by the page, client configures its system and installs the necessary software. Client authenticates itself to Key Distribution Center (KDC) with an AS request via Kerberos client software. (Figure 3 – Step I)
- 4 - Client receives a Ticket Granting Ticket (TGT) along with additional information encrypted with client master key (password hash). Client decrypts the additional information to extract a session key which will be used for further communications with Ticket Granting Server (TGS). This ticket is valid for a specified period and it's cached on the file system. (Figure 3 – Step II)

B. Negotiation

Negotiation is done with TGS as in conventional Kerberos authentication model.

Client sets up its web browser for proxy according to Information Page. After authentication, client browses web over proxy without any interference until TGT expires. Behind these procedures system simply proceeds in following sequence:

5 - After gateway redirection and proxy configuration, HTTP requests are handled by proxy server. Client sends an HTTP Request to proxy server.

6 - Proxy Server responds with the status message of "HTTP/1.1 401 Authorization Required". This message includes what kind of authentication method is required, which is "Negotiate".

7 - When the configured web browser encounters this message, it automatically handles it with the following procedures.

7a - Client sends a Service Principal Name (SPN) for the service along with its cached TGT to TGS with a request for a Service Ticket in order to be authorized by proxy server. (Figure 3 – Step III)

7b - TGS decrypts the TGT to extract the session key and validate client. TGS prepares the service ticket for SPN and encrypts using service master key, which is the key for the service account of the web browser. TGS sends the service ticket to the client. (Figure 3 – Step IV)

7c - Client receives the Service Ticket and sends HTTP request again with ticket to proxy server. (Figure 3 – Step V)

7d - Proxy Server uses its master key to decrypt the ticket and extract the session key. Proxy Server checks the extracted session key to validate client. Then it sends the HTTP respond. (Figure 3 – Step VI)

This procedure is called "Negotiation". Negotiation ensures the authentication is neither stolen or imitated by an attacker so session hijacking wouldn't prove successful.

C. Web Access

After Negotiation, since proxy server is not restricted by firewall and client only interacts with proxy (internal network) instead of exterior network which is restricted by firewall, client gets to connect web smoothly [6].

Finally, communication between client and proxy server can be secured against network sniffing, by Secure Socket Layer (SSL) or Internet Protocol Security (IPSec). This is highly recommended.

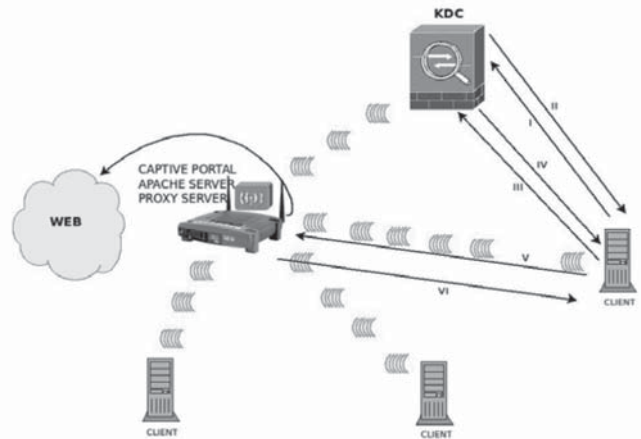
IV. IMPLEMENTATION

The application consists of three participants, "Kerberos Server", "Gateway" and "Client". Kerberos Server consists of a Key Distribution Server (KDC), which consists of AS and TGS, and KADM5 Administration Server. KDC provides necessary tickets for Authentication and Negotiation. Gateway is responsible for intercepting packages via firewall and redirecting clients to the "Welcome Page", presenting the "Welcome Page" and "Admin Page", providing proxy service to offer Internet access to internal clients that are restricted by the firewall and implementing the Kerberos Negotiation for the proxy. Client is responsible for installing Kerberos client software and configuring web browser if needed.

A. Deployed Software

MIT Kerberos V5 [7] as Kerberos Server is installed on an Ubuntu 9.10. The server can be located either in local area

network (LAN) or on the Internet. If it is not located in LAN, the respective firewall policy to permit the communication with it must be added. KDC is installed for the operations of ticket exchanges. An NTP Time Server is installed on the same system to provide timestamps for the ticket exchanges. Finally, an Admin Server is installed to manage principles, policies and keytabs.



Gateway is built on OpenWRT, an open-source Linux-based firmware for embedded devices. This firmware is flashed on a "Linksys WRT54GL" wireless gateway. OpenWRT has a build system that gives us opportunity to extend related modules for Linux kernel. It also offers a package manager (ipkg), which supplies libraries and software packages from its repository like some Linux distributions. For firewall configuration, OpenWRT comes with "iptables" to administrate Linux kernel firewall, Netfilter. Via the software repository of OpenWRT "Apache2 HTTP Server" version 2.2 is installed to provide HTTP and proxy services. To provide HTTP proxy server, mod_proxy and mod_proxy_http is built onto Apache2 HTTP Server. To provide Kerberos authentication and negotiation mod_auth_kerb [10] is built on Apache2 HTTP Server and MIT Kerberos client is compiled. Furthermore, PHP is installed in order to provide "Welcome Page" and PHP KADM5 extension package to make "Admin Page" capable of managing principles and policies. Finally, a DNS server called Berkeley Internet Name Domain (BIND9) is installed in order to define realm name and gateway name.

Client is supposed to install a Kerberos client software onto its system and a negotiation and proxy capable web browser. MIT offers Kerberos client software for Windows NT, Linux and Mac-OS operating systems.

- Windows NT: MIT offers a GUI client-side software for Windows OS. This software provides necessary libraries and bash commands as well. This software is called MIT Kerberos for Windows (KfW). We use version 3.2.2.
- Linux-based OS: Debian offers a package called krb5-user for authenticating to MIT Kerberos Servers.

- Mac-OS: Since Mac-OS X 10.3, MIT Kerberos for Macintosh 5.0 comes with the distribution in default. Also extra tools can be downloaded from MIT website.

Known Kerberos capable web browsers are Mozilla Firefox (since 1.7b), MS Internet Explorer (since 5.0), Safari and Konqueror.

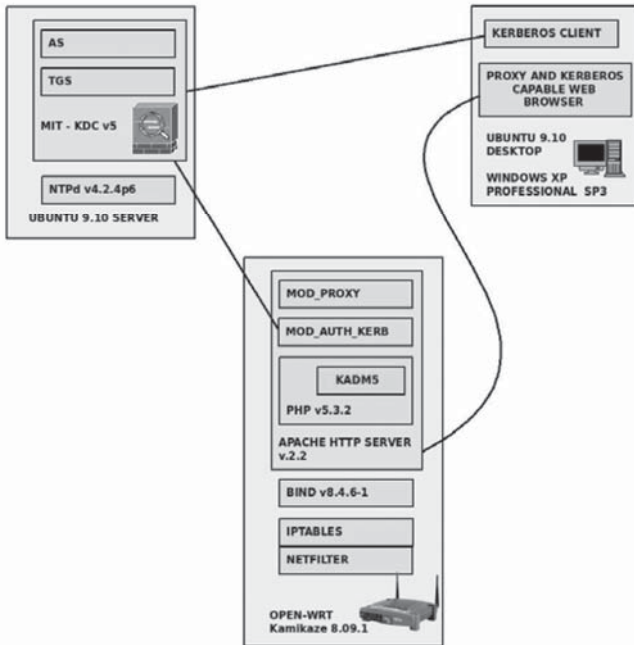


Figure 4: System Software Architecture

B. Configuration

Following fields are configured for Kerberos Server in corresponding files.

1 - krb5kdc: Principles are added for users. Instances are defined for service and special administrative principals. Realm is identified as the domain name in BIND9 converted to uppercase (LOCAL.NETWORK). Access Control List (ACL) permissions are defined for principles. KDC Realm DNS Records for supported protocols are defined for KDC Server as BIND9's forward zones.

2 - NTP Server: Lookup location of NTP Server is added. Also a "Cron" (scheduled task) entity is recorded for updating the NTP Server daily.

Gateway is the governor of this system. Configuration of the gateway can be divided into four parts. All but firewall and BIND9 are configured by Apache2 HTTP Server configuration files.

1 - Firewall policies: Following policies are added to the firewall via iptables :

- Drop all forwarded packets.
- Accept all local traffic.
- Redirect all local clients to Welcome Page.
- Accept traffic with KDC if it's in the exterior network.

2 - BIND9: Forward Zone Entity records are added to designate KDC and Apache2 HTTP Server in LAN. Reverse Zone Entity records are added for resolving names of KDC

and Apache2 HTTP Server from their IP addresses.

3 - Proxy: mod_proxy and mod_proxy_http is enabled for Apache2 HTTP Server. Port number of 8080 is configured for Proxy Server for listening. Forward Proxy mode is enabled.

4 - Kerberos Module for Apache2 HTTP Server: mod_auth_kerb is enabled for Apache2 HTTP Server. Authentication type for all proxy requests is configured to "Kerberos". Negotiation mode is enabled and K5Password mode is disabled. Authentication realm is configured as arranged on BIND9. A service name of "HTTP/fully qualified domain name (fqdn)" and the location of the keytab to be used is given to the Authentication mode. The corresponding keytab is added to the specified location via kadmin interface. This keytab file is arranged to be permitted to used only by Apache2 HTTP Server. Keytabs are the files that can be extracted from the KDC principal database and contain the encryption key for a service or host.

5 - Welcome and Admin Pages: These PHP pages are settled on Apache2 HTTP Server. Welcome Page is designed to give detailed guide for client-side configuration and software to download depending on the operating system and web browser. Admin page is capable of create, read, update, delete operations for principles and policies. Also, scheduled tasks are available in order to give clients permission for limited time if specified.

Clients' configuration depends on the operating system and web browser. Client downloads and installs the Kerberos client software for the corresponding operating system. Only web browser that is supposed to be configured in order to negotiate is Mozilla Firefox. All others are always ready to be used with a TGT.

V.CONCLUSION

To authenticate and authorize captive portal users, negotiate Kerberos authentication model is applied. By means of this model, clients' sessions are secured against many common attacks, primarily session hijacking, that is applied to captive portal. Others can be secured with encryption methods like SSL or IPSec. Users login the system with kinit process to get access right to web. Kerberized captive portal is implemented on a Linux based firmware named OpenWRT that can run on a programmable wireless gateway thus it doesn't require an extra server rather than KDC to accomplish its job. This model also gives us the opportunity to use Kerberos user database that is pre-installed in aforesaid network to authenticate captive portal users along with other systems that requires the same system for authentication.

REFERENCES

- [1] A. Lockhart. "Wireless security" in *Network Security Hacks*, 2nd ed. Sebastopol, Calif. : O'Reilly, 2006, pp. 236-249, ch 7
- [2] P. Mateti. Hacking techniques in wireless networks. Dayton, Ohio: Wright State University [Online] Available: <http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm> March 30, 22010
- [3] T. Sondag, J. Feher, "Open source wifi hotspot implementation", *Information Technology & Libraries*. June 2007, Vol. 26 Issue 2, p35-43

- [4] M. Lenczner Wireless portals with wifidog. [Online] Available: <http://www.linuxjournal.com/article/8352>. October 31, 2005
- [5] H. Xia, J. Brustoloni. "Detecting and blocking unauthorized access in Wi-Fi networks", *NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications*. Springer Berlin, Heidelberg : 2004, Vol. 3042/2004, p795-806
- [6] B. Clifford Neuman. "Proxy-Based authorization and accounting for distributed Systems". *Proceedings of the 13th International Conference on Distributed Computing Systems*, May 1993, p283-291.
- [7] B. Clifford Neuman and T. Ts'o. "Kerberos: an authentication service for computer networks". *Communications Magazine, IEEE*, September 1994, Vol.32 Issue.9 p32-38.
- [8] Interlink Networks, Inc. (2004, February 10) Securing hotspots with Radius [Online] Available: http://www.lucidlink.com/media/pdf_autogen/Securing/Hotspots_White_Paper_021004.pdf. March 30, 2010,
- [9] Zeroshell. Captive portal for hotspot authentication [Online] Available: <http://www.zeroshell.net/eng/captiveportal/details/>, March 30, 2010.
- [10] Kerberos module for apache [Online] Available: <http://modauthkerb.sourceforge.net>, March 30, 2010.
- [11] R.T. Fielding, G. Kaiser. "The Apache HTTP Server project". *Internet Computing, IEEE*. Jul/Aug 1997, Vol.1 Issue.4, p88-90.
- [12] Yun-Yu Lee, Ing-Ye chen, Sy-Yen Kuo, His-Hai Liu, Yuh-Rong Leu. "Implementation of OpenWrt-based IP PnP gateway", *International Conference On Mobile Technology, Applications, And Systems, 2008*.
- [13] Mauro Brunato, Danilo Severina. (2008) "WilmaGate: a new open access gateway for hotspot management" *Proceedings of the 3rd ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, 2008.

NATO ve Siber Savunma

Mehmet MERAL

Özet-Bilgi ve iletişim teknolojileri günümüzde yaygın olarak kullanılmaktadır. Söz konusu sistemlerin kullanımı her geçen gün artarken, bu sistemlere yönelik, kişisel veya politik amaçlı saldırıların sayısında da sürekli artış gözlemlenmektedir. Bu saldırıları ülkesine yönelik tehdit olarak gören ülkeler siber savunma politikalarını belirleme yoluna gitmişlerdir. Dünyanın en büyük savunma örgütü NATO ise karşı karşıya kaldığı bir dizi olaylarla birlikte Müttefiklerini siber tehditlere karşı korumak için çalışmalar yapmaktadır. Bu bildiride NATO'nun siber savunma alanında yaptığı çalışmaların gelişimi incelenmiştir.

Anahtar kelimeler: Siber savunma, siber güvenlik, siber saldırı, NATO

MEHMET MERAL, Ataşe, T.C. Bükreş Büyükelçiliği Romanya -
(e-mail: mehmet.meral@mfa.gov.tr)

I. GİRİŞ

Soğuk Savaşın sona ermesinin ardından teknolojik gelişmelerle birlikte yeni asimetric risk ve tehditler ortaya çıkmıştır. Geleneksel risk ve tehditlerden daha karmaşık olan sınıraşan nitelikli bu tehditlerin en önemlilerinden biri de kritik altyapılarda yoğun olarak kullanılan bilgi sistemlerine yönelik gerçekleştirilen siber saldırılardır.

Söz konusu sistemleri hedef alan bu saldırılar, devletlerin toplumsal, ekonomik ve siyasal fonksiyonlarının yerine getirilmesini engelleyerek büyük zararlara yol açabilir. Bu nedenle, siber saldırılardan kaynaklanan risk ve tehditlerin modern dünyada devletler ve diğer uluslararası örgütler tarafından en az geleneksel risk ve tehditler kadar ciddiye alınarak uygun politikaların geliştirilmesi gerekmektedir.

1949 yılında Soğuk Savaş döneminin ihtiyaçları çerçevesinde kurulan NATO da savunma politikalarını terörizm, iklim değişikliği, enerji güvenliği ve siber saldırılar gibi 21. yüzyılda ortaya çıkan yeni asimetric risk ve tehditlere göre biçimlendirmek durumunda kalmıştır. Temmuz 2009 yılında hazırlanmaya başlanan ve 2010 sonbaharında yapılacak NATO Zirvesine sunulması beklenen NATO'nun yeni stratejik konseptinin hazırlıkları da bu çerçevede yürütülmektedir.

Bu bildirinin diğer bölümlerinde, siber savunma kavramının NATO tarafından ele alınış biçimi, İttifakın karşı karşıya kaldığı siber tehditler ve bu tehditlerden sonra İttifak içerisinde gelişen Siber Savunma mekanizmalarına ilişkin süreçlere değinilmektedir.

II. NATO AÇISINDAN SİBER SAVUNMA KAVRAMI

NATO belgelerinde siber saldırı, bilgi ve iletişim sistemlerinin beklenen işlevini durdurmak, geciktirmek,

değiştirmek ve etkilemek için elektronik sistemlerin kullanılması olarak tanımlanmaktadır. [1] Bilgisayar ağı saldırısı ise, NATO Terimler ve Tanımlar Sözlüğünde, bir bilgisayar ve/veya bilgisayar ağında yerleşik bilgiye, ya da bir bilgisayar ve/veya bilgisayar ağının kendisine kesinti, tahrip ve niteliğini bozma amaçlı yapılan eylemler olarak ifade edilmektedir. [2]

Günümüzde NATO üyeleri ve ortak ülkeler, bilgi temelli varlıklarını tahrip etmeye yönelik siber saldırı riskleriyle karşı karşıyadır. Bu tip saldırılar, yanlış bilginin yayılması ve askeri alandaki hassas bilginin ele geçirilmesi gibi sonuçlara yol açarak bir milletin küresel rekabet gücünün zayıflamasına neden olabilir. Ayrıca, bir ülkenin toplum düzenini ve ekonomisini devam ettirmek için gerekli olan kritik altyapı olarak isimlendirdiğimiz enerji, su, iletişim ve ticari varlıklarının zarar görmesine yol açabilir. Bu saldırılar politik amaçlar için gerçekleştirilebileceği gibi, suç teşkil eden sıradan adli olaylar da olabilir. Bireyler tarafından, devletler tarafından veya devletlerin desteklediği bireyler tarafından işlenebilir. Bu tür siber saldırılar içerdiği etmenler ve hareket noktasına bağlı olarak, siber suç, siber terörizm ve siber savaş olarak adlandırılabilir.

NATO üyesi Estonya, 2007 Nisan ve Mayıs aylarında kritik internet alt yapısını tahrip etmeye yönelik büyük saldırılara maruz kaldı. Saldırıların süresinin uzunluğu ve yıkımı, NATO'yu harekete geçirdi. İttifak krize hızlı bir şekilde karşılık verdi ve üyelerine karşı yapılacak saldırılarda savunmak için araçlar ve yetenekler geliştirdi.

Estonya'ya yapılan söz konusu saldırılar çok kutuplu dünyada İttifakın karşı karşıya kaldığı yeni dinamik tehditleri de açığa çıkardı. Aynı zamanda bu saldırılar NATO'nun 5. Maddesini yoruma açtığından diplomatik ilgiyi de üzerine çekti. 5. Madde'de "Müttefiklerden birine yapılan saldırı İttifakın tümüne yapılmış kabul edilir" olarak vurgulanan husus 11 Eylül saldırılarından sonra bir kez daha gündeme geldi.

Konunun kapsamının genişliğine ve karmaşıklığına rağmen, NATO bir Siber Savunma Politika belgesi ortaya koymayı başardı ve söz konusu belgede konu edilen iki önemli kilometre taşına hayata geçirdi:

1. Gerçek zamanlı operasyonel kabiliyeti olan Cyber Defence Management Authority (CDMA-Siber Savunma İdari Makamı)
2. Uzun dönemde, siber alandaki strateji ve doktrinlerin tartışıldığı, geliştirildiği bir fikir platformu olan Estonya temelli Cooperative Cyber Defence Centre of Excellence (CCDCoE-Siber Savunma İşbirliğine Ait Mükemmelliyet Merkezi) [3].

III. İTTİFAKA KARŞI TEHDİTLER VE SİBER SAVUNMA PROGRAMININ GELİŞİMİ

NATO, 1990'ların sonunda Balkanlarda Sırbistan'a karşı askeri operasyonlara başladığında, çok sayıdaki Sırp bilgisayar korsanı, NATO'nun savaş yeteneklerine zarar vermek amacıyla, NATO'nun internet alt yapısına saldırdı. Çatışmanın durumunu güncel haberlerle aktaran kamu ilişkiler web sitesi 'Distributed Denial-of-Service (DDoS)' saldırılarından dolayı günlerce işlevini yerine getiremedi. DDoS ataklarının hazırlığında, saldırgan, dünya üzerindeki çok sayıdaki güvenliksiz bilgisayarı zararlı yazılımlarla ilerdeki hedeflerinde kullanmak üzere zehirler. Atak süresince, saldırgan ele geçirdiği güvenliksiz bilgisayarlara ufak veri paketleri göndererek kurban bilgisayarı ziyaret etmesi için komutlar gönderir. Bir anda milyonlarca istekle karşı karşıya kalan kurban bilgisayar, bu istekleri karşılayamaz düzeye gelir ve sistemleri etkisiz olur. Bu saldırıların neticesinde NATO'nun e-posta sunucuları, milyonlarca e-mail akışına tabi tutuldu.

Bu deneyimin sonucu olarak, 2002 Prag Zirvesinde NATO liderleri teknik bir "NATO Siber Savunma Programı"nın devreye girmesini ve NATO Computer Incident Response Capability (NCIRC) kurulmasını kararlaştırdı. NCIRC'in Koordinasyon Merkezi'nin Brüksel'de kurulmasıyla, NATO, bu alandaki kritik görevleri organizasyon içinde dağıtma yeteneğinden, bilgisayar virüslerinin tespit edilmesine, NATO ağına yetkisiz sızmalardan, kriptografik cihazların internette yönetilmesine kadar birçok konuda donanımlı hale geldi. Bunlara ek olarak NATO uzmanları bilgisayar güvenliği alanında teknik desteğin yanında politik ve hukuki konularda da katkı sağladılar. NCIRC Koordinasyon Merkezi'nin Başkanı Süleyman Anıl, özellikle NATO makamlarını hedef alan karmaşık casusluk saldırılarının sosyal profillerini belirlemeyle ilgilendi.

Siber tehditleri önlemek için yapılan çabaların önemi, Estonya'nın Nisan-Mayıs 2007 tarihlerinde karşı karşıya kaldığı DDoS saldırılarıyla daha da ortaya çıkmıştır. Ülkenin bütün iletişim sistemleri, iki büyük bankası birkaç gün boyunca iş göremez durumda kaldı. Estonya yüksek düzeyde gelişmiş elektronik altyapısından dolayı, bu türden bir saldırı için özellikle kırılgandı. Dünyada ilk parlamento seçimlerini elektronik ortamda yapan, kimlik tanımlama için ulusal e-kimlikler, elektronik imzalar kullanan Estonya, elektronik bankacılık, sağlık sektörüne yönelik bilgi teknoloji hizmetleri gibi uygulamaları halen yoğun bir şekilde internet üzerinden yapmaktadır.

Ekim 2008'de, resmi ve ticari bilgisayar sistemlerine karşı yapılan DDoS saldırılarından yaklaşık bir buçuk yıl sonra, Estonya dört önemli ayağı olan bir siber savunma stratejisi yayınladı:

1. Estonya'da siber güvenlik önlemleri uygulaması,
2. Eston uzmanlığının geliştirilmesi,
3. Ulusal boyutta yasal ve düzenleyici çerçevenin genişletilmesi,

4. Küresel siber güvenliği güçlendirmek için uluslararası işbirliğinin artırılması. [4]

Estonya aynı zamanda, kamu ve özel sektörü eğitmek amacıyla yüksek kalitede ve erişilebilir seviyede bilgi sağlamaya odaklandı. Güvenlik uzmanlarına yüksek seviyede bilgi sağlama ihtiyacının önemini fark etti. Bu ihtiyacı karşılamak için araştırma geliştirme çalışmalarına yöneldi. Tüm bu çalışmalar ilerleyen bölümlerde daha ayrıntılı bahsedilecek olan bir merkezin, Cooperative Cyber Defence Centre of Excellence (CCDCoE-Siber Savunma İşbirliğine Ait Mükemmelliyet Merkezi)'nin kurulmasına giden yolu açtı. Bu merkez, 2008 yılında NATO ve Müttefiklerin siber savunma yeteneklerini geliştiren bir araştırma organı oldu.

NATO, Estonya'ya yapılan siber saldırıları ciddi bir "operasyonel güvenlik" sorunu olarak gördü ve uzmanlarını bu benzersiz saldırıda Estonları desteklemek üzere görevlendirdi. Saldırı öncesine kadar, NATO siber savunma konusunda, Müttefiklerine yardım etmekten çok, öncelikle kendi iç sistemini korumaya odaklanmıştı. Saldırıları, İttifak üyelerinin karşı karşıya kalabileceği büyük bir dinamik tehdidi gözler önüne serdi. Aynı zamanda NATO merkezinin kriptolu ağının güvenliğinin korunmasının ötesinde, kritik iletişimi korumak için işbirliği ihtiyacını ortaya çıkardı.

Sözkonusu saldırılardan sonra uzmanlar, saldırıların gelişmiş ülkeler için "uyanma çağrısı" olduğunu belirtmişlerdir. Estonya aynı zamanda NATO'nun siber savunma politikasının geliştirilmesinde, siber saldırıların İttifaka karşı yapılan askeri bir saldırı olup olmadığının tartışılmasında temel bir rol oynamıştır.

2008 yılında ise, Rusya Gürcistan'a girdiğinde Rus kaynaklı web sitelerinde, interneti olan herkesin kullanabileceği, Gürcü hükümetinin ve Tiflis'teki Amerika ve İngiltere Büyükelçiliklerinin web sitelerini hedef alan yazılımlar dağıtıldı. Gürcü hükümeti ve bağımsız birkaç kaynak, bu saldırıların St. Petersburg kaynaklı "Rusya İş Ağı" adındaki organizasyon tarafından yapıldığına işaret etmişlerdir. Saldırıların Rus hükümeti tarafından yapıldığını teyit eden bir kanıt bulunmamakla birlikte, sözkonusu hükümetin saldırıları durdurmak için çaba harcadığına ilişkin bir işaret de mevcut değildir.

Estonya ve Gürcistan makamları sözkonusu saldırılar nedeni ile daha çok Rusya'ya odaklanırken, Amerikan kaynakları Hamas ve Hizbullah gibi örgütlerin Amerika'ya yönelik siber saldırı planları bulunduğunu gündeme getirmiştir. Aynı kaynaklar, Rusya ve Çin'in de Amerika'ya karşı ciddi siber saldırı kaynaklarını barındırdığını iddia etmiştir.

Bütün bu gelişmelerin sonucunda, 2008 yılında Bükreş'te yapılan NATO Zirvesi'nde, Müttefikler siber savunma kavramını ilk defa resmi bir zirve çerçevesinde ele almışlardır. Bükreş Zirvesi ile eşzamanlı olarak gerçekleştirilen NATO ve Siber Savunma konulu toplantının sonuç raporunda "Global bilgi ekonomisinde, interneti iş dünyası için açık ve büyük tehlikelerden uzak tutmak,

denizleri ve hava koridorunu açık tutmakla eşdeğerdir” cümlesi vurgulanmıştır. [5]

Zirve boyunca NATO uzmanları ve yetkililer Estonya’nın yaşadığı deneyimden öğrenilen dersleri gözden geçirdiler. Bükreş Zirvesi Sonuç Bildirisinin 47. maddesinde Siber Savunma’ya yer verilerek konunun önemi resmi olarak vurgulanmıştır;

“NATO, siber saldırılara karşı İttifakın temel bilgi sistemlerinin güçlendirilmesi konusundaki taahhütlerine bağlıdır. Siber Savunma Politika Belgesini kabul ettik ve sözkonusu politikayı yürütecek yapı ve makamları geliştirmekteyiz. Siber Savunma konusundaki politikamız, NATO ve üye ülkelerin kendi sorumlulukları çerçevesinde temel bilgi sistemlerinin korunmasına, örnek uygulamaların paylaşılmasına ve siber saldırıları önlemek için Müttefiklerin istekleri doğrultusunda yardım sağlamaya vurgu yapmaktadır. NATO’nun siber savunma yeteneklerinin gelişmesinin ve NATO ile ulusal makamlar arasındaki bağların güçlendirilmesinin sürdürülmesini umuyoruz.”. [6]

Sözkonusu Zirve’de onaylanan NATO Siber Savunma Politikasının iki önemli sonucu ise operasyonel seviyede “Cyber Defence Management Authority”nin (CDMA) kurulması ve stratejik seviyede ise “Cooperative Cyber Defence (CCD) Centre of Excellence”ın (CoE) açılmasıdır.

IV. CYBER DEFENCE MANAGEMENT AUTHORITY (CDMA-SİBER SAVUNMA İDARİ MAKAMI)

İsminden de anlaşıldığı gibi CDMA, siber savunma faaliyetlerinin koordine edildiği NATO kapsamında görevli bir idari makamdır. CDMA, bir siber saldırı durumunda talep etmeleri halinde müttefiklere yardım ve işbirliği sağlamak üzere hazır bulunmaktadır.

Brüksel’de yeni bir idari makamın kurulması, siber savunma alanında operasyonel yeteneklerin merkezileştirilmesi için büyük bir gayreti temsil etmektedir. NATO açıklamalarına göre, Brüksel temelli CDMA’nın amacı, müttefiklerin siber saldırılara verecekleri tepkileri koordine edecek merkezi bir otorite oluşturmaktır. Yetenekleri konusunda sınırlı bilgi paylaşımı bulunmakla birlikte, CDMA’nın, siber tehditleri belirlemek için gerçek zamanlı ileri elektronik izleme kapasitesinin bulunduğu ve istihbarat paylaşımı gibi konuları kapsayan çalışmalar yaptığı bilinmektedir. Önümüzdeki birkaç yılda CDMA’nın, NATO siber savunması için taktiksel yanıtların hazırlandığı “savaş odası operasyon merkezi”ne dönüşmesi beklenmektedir. En azından, Estonya’daki saldırıların tersine, şu an üye ülkelerin gerçek bir siber acil durumda arayabilecekleri bir numaraları bulunmaktadır.

Nisan 2008’ten bu yana aktif olan CDMA, alanında birçok ilerleme kaydetmiştir. Şimdiye kadar yönetici komitesi beş defa toplanmış ve operasyonel politikalar geliştirmiştir. İki defa siber savunma tatbikatı gerçekleştirilmiş, Kasım 2008’te yapılan ilk tatbikattan sonra Kasım 2009’da yapılan ikinci tatbikata 21 NATO üyesi ülke katılmıştır. CDMA,

siber savunmanın yasal boyutlarından, Ortaklarla işbirliğine kadar pekçok konuda politika geliştirmiştir.

V. COOPERATIVE CYBER DEFENCE (CCD) CENTRE OF EXCELLENCE (COE) - SİBER SAVUNMA İŞBİRLİĞİNE AİT MÜKEMMELİYET MERKEZİ

Bükreş zirvesinin ikinci sonucu ise Tallin merkezli “Cooperative Cyber Defence Centre of Excellence (CCDCoE- Siber Savunma İşbirliğine Ait Mükemmeliyet Merkezi)”dir. NATO Mükemmeliyet Merkezleri (Center of Excellence – CoE), NATO’nun dönüşüm sürecini kolaylaştırmakla görevlidirler. CoE’lar, NATO ve Barış için Ortaklık üyesi devletlere açıktır ve birlikte çalışabilirliğin ve yeteneklerin ilettilmesi, doktrinlerin geliştirilmesi, deneylerle operasyonel kavramların onaylanmasını için imkânlar sağlar. Hâlihazırda Mart 2010’da Romanya’da açılan Human Intelligence Center of Excellence ile birlikte 18 tane mükemmeliyet merkezi bulunmaktadır.

Siber mağdur statüsünü tersine çevirmek için, bilgi ve iletişim teknolojilerini en yoğun kullanan Avrupa ülkesi olan Estonya, NATO’nun ilk siber savunma mükemmeliyet merkezine evsahipliği yapma konusunda da liderliği üstlendi. CDMA, NATO’nun operasyonel seviyede siber savunmasını koordine etmekle görevli olmasına karşın, Estonya’daki Mükemmeliyet Merkezi, NATO’nun siber savunma doktrin ve stratejilerinin uzun dönemde gelişimini sağlayacaktır. Resmi olarak Mayıs 2008’de kurulan ve NATO’nun tam akreditasyonunu Ekim 2008’te alan merkez, Müttefiklerin uzun dönemde siber savunma kabiliyetlerini nasıl geliştirebileceği konusundaki çalışmalara başlamıştır. Web sitesinde de belirtildiği gibi, Merkez özel sektörden kamu sektörüne, İttifak üyelerinden ve ortak ülkelere geniş bir kitle için seminerler, etkinlikler ve çalıştaylar düzenlemektedir. Merkezin ana görevleri;

1. İttifak için siber savunma ile ilgili doktrin ve stratejiler üretmek,
2. NATO üyeleri için çalıştaylara, kurslara, tatbikatlara ev sahipliği yapmak,
3. Araştırma-geliştirme faaliyetlerini yürütmek,
4. Geçmiş ve gelecek saldırıları değerlendirmek, çıkarılan dersleri belirlemek,
5. Devam eden saldırılarda istendiği takdirde, danışmanlık sağlamaktır. [7]

Tamamen sponsor ülkelerle finanse edilen CCD CoE, en iyi örneklerin geliştirildiği ve paylaşıldığı bir araştırma ve öğrenme merkezi olarak düşünülebilir.

VI. NATO SİBER SAVUNMA POLİTİKASI

Estonya’nın karşı karşıya kaldığı ilk siber saldırılardan yedi hafta sonra Haziran 2007’de yapılan NATO Savunma Bakanları toplantısında, NATO uzmanları son olaylardan çıkarılan dersleri içeren ve siber savunma alanında gelecekte yapılması gereken işlerin çerçevesini çizen bir rapor hazırladılar. Ekim 2007’de bir sonraki NATO Savunma Bakanları toplantısında ise, Bakanlara İttifakın siber

savunmaya yaklaşımını belirleyen daha detaylı bir rapor sunuldu. Raporda, siber saldırılara karşı yeni önlemlerin uygulanması amacıyla Müttefiklere tavsiyelerde bulunuldu. NATO Siber Savunma Politika Belgesi olarak isimlendirilen rapor Ocak 2008’de kabul edildi ve Nisan 2008’de Bükreş Zirvesinde Devlet ve Hükümet Başkanları tarafından onaylandı.

NATO müttefikleri arasında, siber tehditlerin ciddiyeti ve NATO’nun bu alandaki potansiyeli konusunda görüş birliği bulunduğundan, Siber Savunma Politikası üzerinde hızlı bir anlaşma sağlanmıştır. İttifakın ilgili askeri ve teknik organları politikayı uygulama konusunda hali hazırda çalışmalarına devam etmektedirler. NATO’nun Siber Savunma Politikasının tam ayrıntıları ise gizli tutulmaktadır.

VII. SONUÇ

Siber saldırılar; nükleer yayılma, iklim değişikliği, terörizm ile birlikte hali hazırda, İttifakın karşı karşıya kaldığı en ciddi asimetrik tehlikelerden biridir. İnternetin açık doğası, siber saldırılardan korunmayı zorlaştırmaktadır. Etkili uluslararası işbirliği siber saldırılarla mücadelede kritik bir önem arz etmektedir. Dünya’nın en büyük savunma örgütü olan NATO’nun, üyelerinin siber savunmalarına katkı sağlama, savunma önlemlerini koordine etme ve bu tür

eylemleri caydırma gibi sorumlulukları bulunmaktadır. NATO’nun hazırlanmakta olan yeni stratejik konseptinde de yirmi birinci yüzyılın en önemli güvenlik tehditleri arasında bulunan siber saldırılarla mücadeleye geniş bir yer verilmesi beklenmektedir. Ulusal parlamentolar ise, siber savunma önlemlerini yürürlüğe koymak, ulusal seviyede uygulamak ve NATO’nun siber savunma politikalarının uygulanma sürecini hızlandırmak konularında önemli bir role sahiptir.

KAYNAKLAR

1. “NATO and Cyber Defence”, Sverre Myrli, Raportör, 2009
2. NATO Glossary of Terms and Definitions
3. “Partnering to Defent Aganist Cyber Attacks”, Tasnif Dışı NATO Raporu, Haziran 2009
4. “Cyber Security Strategy”, Estonya Savunma Bakanlığı, Ekim 2008
5. “NATO and Global Cyber Defence” Rex B. Hughes, Romanya Dışişleri Bakanlığı Bükreş Konferansı Sonuç Bildirisi, Mayıs 2008
6. Bükreş Zirvesi Sonuç Bildirisi, 3 Nisan 2008
7. NATO CCD CoE web sitesi, <http://www.ccdcoe.org/37.html>

Elektronik Haberleşme Sektöründe Veri Gizliliği Düzenlemeleri

Güneş KOCA, Ayhan TÖZER¹

Abstract — The use of digital technologies is overturning traditional publicly available communications market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Electronic communications services over the digital networks open new possibilities for users but also new risks for their personal data and privacy. In this context, related EU legislation is evaluated in general terms in the first part, following with the evaluation of the situation in Turkey. In the study, it is emphasized that like EC Member Countries Turkey also should make legal, regulatory and technical provisions in order to protect rights and freedoms of natural persons and legitimate interests of legal persons.

Keywords — EU Directives, Electronic Communication, Data Privacy, Data Security.

Özet — Elektronik haberleşmenin ve dijital teknolojilerin artan oranda kullanımı geleneksel anlamda telekomünikasyon piyasaları ve bu ortam kullanılarak gerçekleştirilen işlemlerde yapısal değişimlere yol açmıştır. Söz konusu yeni teknolojiler kullanıcılara pek çok imkan ve farklı uygulamaları sunarken, aynı zamanda veri güvenliği ve gizliliği hususlarında daha önce öngörülmemiş risklerin ortaya çıkmasına neden olmaktadır. Bu çerçevede makale kapsamında elektronik haberleşme sektöründe veri gizliliği hususunda yapılan hukuki düzenlemelere yer verilmektedir. İlk bölümde ilgili AB mevzuatı genel hatlarıyla değerlendirilmiş, müteakiben de ülkemizde konuyla ilgili mevzuat ve yeni düzenleme çalışmaları ele alınmıştır. Çalışmada, Türkiye’de veri gizliliği konusunda AB mevzuatının uygulanması sürecinin tamamlanmasının önemi vurgulanmaktadır.

Anahtar Kelimeler — AB Direktifleri, Elektronik Haberleşme, Veri Gizliliği, Veri Güvenliği.

I. GİRİŞ

Günlük hayatımızda kişiler arası iletişimin artmasıyla birlikte kişilere ait verilerin kullanılması da artış göstermiştir. Örneğin herhangi bir spor salonuna üyelikte isim, soy isim yanında, yaş, cinsiyet, telefon numarası, resim, spor yapmaya ilişkin sağlık bilgileri gibi özel bilgiler dahi üye olduğumuz kulüp tarafından istenmektedir. Belirli ya da kimliği belirlenebilir kişilere ait bütün bilgiler “kişisel veri” olarak tanımlanmakta olup, bu bilgiler doğrudan kişinin kendisinden alınabildiği gibi mevcut bir veri tabanından da elde edilebilmektedir. Herhangi bir kayıt, başvuru, abonelik sırasında vermiş olduğumuz bu bilgiler daha sonra başka amaçlarla da kullanılabilir hale gelebilir.

üçüncü kişilerle de paylaşılabilmektedir. Özellikle elektronik haberleşmenin² yaygınlaşması ve bilgisayar teknolojisindeki gelişmeler bu verilerin sadece ülke içerisinde değil tüm dünyada da hızla yayılabilmesine imkan vermektedir. Bir ülkede toplanan (kayıt altına alınan) bilgilerin diğer ülkelere gitmesi ya da bir sektörde elde edilen bilgilerin diğer sektörlerde de kullanılması bir diğer ifade ile kişisel bilgilerin hem istihbarat amacıyla hem de ticari amaçlarla artarak kullanımı bu alanda bir düzenleme yapmayı gerekli hale getirmiştir.

II. AVRUPA BİRLİĞİ ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İŞLENMESİ VE GİZLİLİĞİNİN KORUNMASI

Avrupa Birliği (AB)’nde elektronik haberleşme sektörüne ilişkin olarak kişisel verilerin işlenmesi ve gizliliğinin korunması hususunda ilk spesifik (özel) düzenlemeyi Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin korunmasına ilişkin Avrupa Parlamentosu ve Konseyi’nin 15 Aralık 1997 tarih ve 97/66/EC sayılı Direktifi oluşturmuştur [1]. Söz konusu Direktif, Kişisel Verilerin İşlenmesinde Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımına İlişkin Avrupa Parlamentosu ve Konseyi’nin 24 Ekim 1995 tarih ve 95/46/EC sayılı Direktifinde yer alan ilkeleri, telekomünikasyon sektörü için özel kurallara haline getirmiştir [2]. 97/66/EC sayılı Direktifin piyasalar ve elektronik haberleşme hizmetleri teknolojilerindeki ilerlemelere uyumlu hale getirilmesi amacıyla 2002 yılındaki düzenleyici paket içerisinde elektronik haberleşme sektörüne ilişkin Elektronik Haberleşme Sektöründe Gizliliğin Korunması ve Kişisel Bilgilerin İşlenmesine ilişkin 12 Temmuz 2002 tarihli Avrupa Parlamentosu ve Konseyi’nin 2002/58/EC sayılı Direktifi yayımlanmış [3] ve 97/66/EC sayılı Direktif 31.10.2003 tarihinden geçerli olmak üzere yürürlükten kaldırılmıştır.

Elektronik haberleşme alanında mobil teknolojiler gibi pek çok yeniliğin giderek artan oranlarda kullanıldığı günümüz bilgi toplumunda, bu sektöre ilişkin özel düzenlemelerin yapılmasını kaçınılmaz hale getirmiştir. Bu alandaki koruma ve verilerin kullanıcıların kişisel istemleri dışında kullanılmasının engellenmesi, aynı zamanda, bilgi ekonomisinin gelişmesi sürecinde sunulan e-ticaret gibi

¹ Bu yazıda ifade edilen görüşler yazara ait olup, hiçbir suretle Bilgi Teknolojileri ve İletişim Kurumunun görüşleri şeklinde yansıtılamaz.

² Metin içerisinde “elektronik haberleşme” ve “telekomünikasyon” kavramları birbirleri yerine kullanılabilir.

hizmetlere olan kullanıcı güveninin artması açısından da önem taşımaktadır. Bu çerçevede hazırlanan Direktif toplam 21 maddeden ibaret olup, haberleşmenin gizliliğini ve tüketici haklarını koruyucu maddeler önem taşımaktadır. Haberleşmenin gizliliği başlıklı 5 inci madde kullanıcının kendi rızası dışında bir başkası tarafından elektronik haberleşme verisinin (trafik verisi dahil) dinlenmesi ve kaydedilmesinin yasak olduğunu hükme bağlamaktadır. Bu yasağın tek istisnasını ise ortada hukuken geçerli bir yetkilendirme olması durumu oluşturmaktadır. Aynı şekilde trafik verisi başlıklı 6 ncı madde abone verisinin pazarlama amaçlı kullanımı için önceden kullanıcı izni olması gerektiğini belirtmektedir. Yine aynı madde hükümlerine göre bu izin aynı zamanda kullanıcının iradesine bağlı olarak her zaman için geri alınabilecektir. Buna paralel bir düzenleme de istek dışı haberleşmeler başlıklı 13 üncü madde de görülmektedir. Bu başlık altında insan müdahalesi olmaksızın çalışan (sms gönderimi gibi) elektronik sistemler aracılığıyla mesaj gönderilmesine ancak kullanıcı izni varsa müsaade edilebileceği ifade edilmektedir. 7 nci madde abonelerin ayrıntılı fatura alma hakkını düzenlerken, 8 nci madde de kullanıcıların gizli numaralardan aramaları otomatik olarak reddetmeleri imkânını sağlayan hükümlere yer verilmektedir. Direktifin ele aldığı diğer konular arasında ise abone rehberlerine ilişkin düzenleme, otomatik aramayı yönlendirme teknik özellikler ve standardizasyon gibi hususlar bulunmaktadır.

Veri gizliliği konusundaki ikinci düzenlemeyi ise 15.03.2006 tarihinde yürürlüğe giren 2006/24/EC Direktifi oluşturmaktadır [4]. Bu Direktifin hazırlanarak yürürlüğe girmesinde özellikle İngiltere’de 2005 yılında meydana gelen terör olaylarının rol oynadığı görülmektedir. Zira, anılan Direktifin dibacesinde bu duruma değinilerek, bu tür olayların daha etkin bir şekilde takip edilebilmesi açısından telekomünikasyon verilerinin saklanması ile ilgili ortak tedbirlerin en kısa zamanda alınmasının gerekliliği vurgulanmaktadır. Bu çerçevede hazırlanan Direktif topluluk boyutunda elektronik verinin saklanma ve veriye ulaşım hususlarındaki usul ve esasları belirlemektedir. Direktifin temel maddeleri arasında ise veri saklama zorunluluğu, veriye erişim, saklanacak veri kategorileri, saklama süreleriyle bu verilerin korunmasına ilişkin hükümler bulunmaktadır. Örneğin saklanacak veri kategorileri arasında internet yoluyla yapılan haberleşmeler (e-posta) de sayılmış ve bu kapsamda kullanılan IP adresleri, internet erişim hizmetine giriş ve çıkışların tarihleri ve süresi, abone kimliği gibi bilgilerin altı aydan az ve iki yıldan çok olmayacak şekilde saklanması hükme bağlanmıştır. Diğer taraftan, saklanan bu verilerin korunması için yapılması gerekenler de sayılarak, bu tedbirlerin alınmaması ve veri güvenliğinin ihlal edildiği durumlarda geçerli olacak yaptırım ve cezalara da ayrıca yer verilmiştir.

AB tarafından bu konuda getirilen en son düzenleme ise yine 2002/58/EC direktifini tadil eden ve 25.11.2009 tarihinde yürürlüğe giren 2009/136/EC Direktifi olmuştur [5]. Bu Direktifte, evrensel hizmet ve veri gizliliği hususundaki bir

takım ek düzenlemelere yer verilmektedir. Direktifteki maddeler 2002/58/EC direktifinde bulunan maddeleri tadil edici bir şekilde kaleme alınmış olup; veri gizliliği ve güvenliği konusunda tüketici haklarına olan vurgu daha da belirgin bir şekilde yapılarak, telekomünikasyon hizmet sağlayıcılarının bu konuda her türlü tedbiri alması gerektiği belirtilmektedir. Bu kapsamda, özellikle gelişen teknolojiyle birlikte veri güvenliği konusunda yeni risklerin ortaya çıktığı ve bu konuda gerek işletmecilerin gerekse ulusal düzenleyici kurumların her türlü tedbiri alması hususunda yeni düzenlemelere gidilmiştir. Örneğin, işletmeciler yeni Direktif hükümleri çerçevesinde bu konu kapsamındaki (örneğin veri tabanına girme teşebbüsü vb.) bilgiyi düzenleyici kuruma sağlayacak ve bu kurumlar da toplanan veri ışığında gerekli çalışmaları yapacaktır. Diğer taraftan, kullanıcıların ekipmanlarına (bilgisayar, cep telefonu vb.) sızarak veri toplayan yazılımların (dolayısıyla bu tip faaliyetleri yürüten şahısların) da veri güvenliği hususunda ciddi bir tehlike oluşturduğu ve bu konudaki önleyici tedbirlerin alınması hususu da vurgulanmaktadır. Sonuç itibarıyla son Direktifin, önceki Direktifte yer alan hükümlerin gelişen teknoloji karşısında tüketici haklarını koruma konusunda yetersiz kalmaması adına hazırlandığı ifade edilebilecektir.

Ancak, diğer bütün hususlarda da görüldüğü gibi, her zaman mevzuatın bulunması istenilen sonuçların alınması açısından yeterli olmamaktadır. Buna güncel bir örnek olarak AB üyesi bir ülkede yaşananlar gösterilebilecektir. İtalya’da telekomünikasyon hizmetlerinden yararlanan abonelerin bulunduğu veri tabanları tele pazarlama amaçları için kullanılmakta olup, bunun için aboneden önceden izin alınmadığı belirtilmektedir. Komisyon bunun yanı sıra, abonelerin isteseler dahi bu haklarını kullanmada yeterince etkin bir prosedür geliştirilip geliştirilmediği konusunda da şüpheler bulunduğunu ifade etmektedir. Bu nedenlerden ötürü Komisyon 28.01.2010 tarihinde veri gizliliğine ilişkin mevzuata uyum sağlanmadığını içeren resmi bir mektup iletmış olup, İtalyan hükümetine cevap için iki aylık bir süre tanımıştır [6]. Daha önce de ifade edildiği gibi söz konusu Direktiflerde; abonelerin kendileriyle ilgili bilgilerin rehber hizmetleri veri tabanında yer alıp almamasına ilişkin karar verebilmeleri, karar vermeden önce bu bilgilerin ne amaçlarla kullanılacağı gibi hususlarda bilgilendirme yapılması zorunluluğu bulunmaktadır.

III. ÜLKEMİZ ELEKTRONİK HABERLEŞME SEKTÖRÜNDE VERİ GİZLİLİĞİ

TÜRKİYE’DE elektronik haberleşme sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin ilk düzenleme; AB’nin 2002/58/EC Direktifi temel alınarak ve 2813 sayılı Telsiz Kanununa dayanılarak hazırlanan 06.02.2004 tarih ve 25365 sayılı Resmi Gazete’de yayımlanan “Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında

Yönetmelik” (Veri Gizliliği Yönetmeliği)³ olmuştur [7]. Veri Gizliliği Yönetmeliğinin AB müktesebatındaki gelişmelerle birlikte, Ülkemizde teknik ve hukuki alanda meydana gelen gelişme ve değişimlere cevap verebilir hale getirilmesi amacıyla Yönetmeliğin yürürlüğünden sorumlu olan Telekomünikasyon Kurumu⁴ tarafından çalışmalar başlatılmış ve başlatılan çalışma sürecinde AB tarafından 2006’da yayımlanan 2006/24/EC sayılı Direktifte öngörülen değişikliklere uyum sağlaması da esas alınarak yeni bir Yönetmelik Taslağı hazırlanmıştır. Taslak Yönetmelik Kurum tarafından diğer kişi ve kurumların görüşüne de açılmıştır. Ancak, Taslak Yönetmeliğe son hali verilmek üzere aynı dönemde TBMM gündeminde olup, henüz yasalaşarak yürürlüğe girmemiş olan Taslak Elektronik Haberleşme Kanununun yürürlüğe girmesinin beklenmesi uygun görülmüştür. 10.11.2008 tarih ve 27050 (Mükerrer) sayılı Resmi Gazete’de yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu’nun (EHK) [8] yürürlüğe girmesiyle “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı”, EHK ile uyumlaştırmak üzere gözden geçirilerek yeniden düzenlenmiş ve Taslak Yönetmeliğin son hali bir kez daha ilgili bütün kurum ve kuruluşlar ile tüm kamuoyunun görüşlerini bildirebilmeleri için, Bilgi Teknolojileri ve İletişim Kurumunun internet sayfasında 25.12.2009 ve 25.01.2010 tarihleri arasında bir ay boyunca yayınlanmıştır.

Taslak Yönetmeliğe dayanak teşkil eden EHK’nın “Amaç” başlıklı 1 inci maddesi “*Bu Kanunun amacı; elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesidir.*” hükmünde olup, “İlkeler” başlıklı 4 üncü maddesinde ise bu amaca uygun olarak ilgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde “*Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi*”nin ilkeler içerisinde gözetilmesi gerektiği belirtilmiştir.

EHK’nın 4 üncü maddesinde belirtilen “ilgili merciler”in Ulaştırma Bakanlığı ve Bilgi Teknolojileri ve İletişim Kurumu olması nedeniyle “Kurumun görev ve yetkileri” başlıklı 6 ncı maddesinin (c) bendinde “*Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.*” hususu yer almaktadır. Kişisel bilgilerin işlenmesi ve gizliliğinin korunması bir yandan EHK’da Kurum’un genel görev ve yetkileri içerisinde sayılmakta iken diğer taraftan “Kişisel verilerin işlenmesi ve

gizliliğin korunması” başlıklı 51 inci maddede “*Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir.*” hükmüne özel olarak yer verilmiştir.

Taslak Veri Gizliliği Yönetmeliğinin yayımlanması için EHK’nın yürürlüğe girmesinin isabetli olduğu değerlendirilmektedir. Nitekim, yürürlükte olan mevcut Veri Gizliliği Yönetmeliği yürürlüğe girdiği zamandaki ihtiyaç nedeniyle ve Avrupa Birliğine uyum sürecinde AB Direktiflerinde belirtilen hususları yerine getirmek amacıyla her ne kadar 2813 sayılı Telsiz Kanununa dayandırılarak çıkarılmış olsa dahi, EHK’da açık ve özel bir hükmün olması Taslak Yönetmeliği daha da güçlü hale getirmektedir.

Taslak Veri Gizliliği Yönetmeliği ile Mevcut Yönetmeliğin benzer hükümler taşıdığı görülmekle birlikte AB’nin 2006/24/EC Direktifi ile getirilen hükümlere uygun olarak yeni maddelerin eklendiği görülmektedir. Taslak ve Mevcut Yönetmelikler karşılaştırıldığında “Tanımlar” maddesine Yönetmeliğin devamında getirilen hükümlerin anlaşılmasına ilişkin olarak “Acil yardım çağrıları”, “Hücre kimliği”, “IMEI”, “IMSI”, “Rıza”, “Tanımlayıcı veri”, gibi tanımlara ilk kez yer verildiği diğer taraftan Mevcut Yönetmelikte bulunan bazı tanımların biraz daha farklılaştırılarak yer aldığı görülmektedir. Taslak Yönetmelikte “Tanımlar” maddesinden sonra Mevcut Yönetmelikte bulunmayan “Kişisel verilerin işlenmesine ilişkin ilkeler” maddesinin ilk kez yer aldığını görmekteyiz. Yönetmeliğin bu maddesi incelendiğinde Adalet Bakanlığı tarafından hazırlanmış olan Kişisel Verilerin Korunması Kanun Tasarısının [9] 5 inci maddesinde yer alan ilkeler ile paralellik gösterdiği görülmekte olup, esas olarak kişisel verileri işlenecek olan kişinin rızasına dayalı olması ve işlenecekleri amacın belirli olması ve bu amaçla saklama süresini aşmaması gerekmektedir. Mevcut Yönetmelikte yer alan ve Taslak Yönetmelikte de yer verilen maddelerden biri ise “Güvenlik” başlıklı maddedir. Mevcut ile Taslak Yönetmelik hükmü arasındaki fark ise; Mevcut Yönetmeliğe göre işletmecilerin hizmetin gerektirdiği hallerde şebekenin güvenliğine ilişkin alacakları tüm gerekli teknik ve yapısal önlemleri Kurumun onayına sunmaları olup, Taslak Yönetmeliğe göre ise işletmeciler tarafından teknolojik imkanlar ve uygulama maliyetleri göz önünde bulundurularak muhtemel riske uygun düzeyde güvenlik tedbirleri alınması öngörülmüş olup, ancak Kurum tarafından gerekli görülmesi halinde bu güvenlik tedbirlerinde değişiklik yapılabilecektir. “Güvenlik” maddesine ilişkin bu maddenin Taslak Yönetmelikteki halinin hem bürokrasiyi azaltacağı hem de daha işler bir hal sağlayacağı düşünülmektedir. Zira, İşletmeci güvenlik tedbiri aldığı her durumu Kurumun onayına sunmayacak Kurum gerekli görmesi halinde alınan tedbirlere ilişkin bilgi isteyecek tedbirin yeterli olmadığını düşünmesi halinde de değişiklik yapılmasını isteyebilecektir. Taslak Yönetmelikte “Riskin bildirilmesi” başlığı altında yer alan hükmün Mevcut Yönetmelikte “Riskli haber verme” başlığı altında bulunduğunu görmekteyiz. Her iki hüküm arasındaki fark ise şu şekildedir; Mevcut Yönetmelikte işletmeci tarafından alınan önlemlerin dışında olağanüstü bir risk söz konusu olduğunda aboneler riskler ve riskin giderilmesi yolları hakkında uyarılacaktır, Taslak Yönetmeliğe göre ise işletmeci

³ “Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik” makalenin devamında kısaca “Veri Gizliliği Yönetmeliği” olarak ifade edilecektir.

⁴ “Telekomünikasyon Kurumu”nun adı 10 Kasım 2008 tarih ve 27050 (Mükerrer) sayılı Resmi Gazete’de yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu ile Bilgi Teknolojileri ve İletişim Kurumu olarak değişmiştir.

belirli bir risk olması halinde abonelerle birlikte Kurumu da bilgilendirecek olup, bu riskin işletmeci tarafından alınan tedbirlerin dışında kalması halinde işletmeci abonelerini etkin ve hızlı bir şekilde riskin içeriği ve giderilme yolları hakkında bilgilendirecektir. Taslak Yönetmeliğin “Riskin bildirilmesi” maddesinden sonra gelen üçüncü bölümde verilerin işlenmesi ve saklanması ile ilgili hükümlere yer verilmiş olup, üçüncü bölümün ilk maddesi “Trafik verisinin işlenmesi”dir. Taslak Yönetmeliğin “Trafik verisinin işlenmesi” başlıklı 7 nci maddesi Mevcut Yönetmeliğin 9 ve 11 inci maddeleriyle paralellik arz etmekle birlikte, Taslak Yönetmelikte Mevcut Yönetmelikten farklı olarak trafik verilerinin bu verilerin saklanması gerekli kılan faaliyetin tamamlanmasından sonra silinmesi ve anonim hale getirilmesinin esas olduğu belirtilmiştir. Aynı maddenin devamında trafik verilerinin hangi amaçlarla işlenebileceği ve bu verilerin katma değerli hizmetlerin sunulması amacıyla işlenmesi söz konusu ise verilerin işleme süreleri hakkında abone ve kullanıcıların bilgilendirilmesinin ardından rızasının alınması neticesinde işlenmesi ve abone/kullanıcıların rızalarını her zaman için geri alabilecekleri ifade edilmiştir. Taslak Yönetmelikte de Mevcut Yönetmelikteki şekilde “Trafik verisini işleme yetkisi” maddesine yer verilmiş ve Mevcut Yönetmelikteki hüküm “yolsuzluk tespitleri” ifadesinin uygulamada kavram kargaşasına neden olacağı düşüncesiyle çıkarılmıştır. Mevcut Yönetmelikte “Yetkili makama bildirim” başlıklı 11 inci madde Taslak Yönetmelikte “Trafik verisinin bildirilmesi” başlığı altında ifade değiştirilerek ancak, içerik muhafaza edilerek düzenlenmiştir. Mevcut Yönetmelikte “Telekomünikasyonun gizliliği” başlığı altında düzenlenen aynı zamanda T.C Anayasası ile de güvence altına alınmış olan haberleşmenin gizliliği ilkesine uygun düzenleme Taslak Yönetmeliğe “Trafik verisinin gizliliği” şeklinde geçmiştir. Mevcut Yönetmelikte “Yer verisi” başlığı altında düzenlenmiş olan Taslak Yönetmelikte ise “Konum verisinin işlenmesi” başlığı altında yer alan hükmün uygulama açısından farklılık getirdiği düşünülmektedir. Mevcut Yönetmeliğe göre katma değerli hizmetlerin işlenmesi için aksi başvurusu olmayan abonenin konum verisi işlenebilecek iken Taslak Yönetmeliğe göre ancak abonenin önceden rıza göstermesi halinde konum verisi işlenebilecektir. Aboneler konum bilgilerinin işlenmesi için vermiş oldukları izni her zaman için geri alabileceklerdir. Aynı madde altında Mevcut Yönetmeliğin “Geçici red” başlıklı 16 ncı maddesine paralel olarak konum verisinin işlenmesine izin verilmesi halinde her bağlantı için iznin reddedilmesine imkan verildiği görülmektedir. Yine aynı maddede konum verisine erişilmesinin istisnası olarak acil yardım çağrıları kapsamında yetkili makamların olduğu belirtilmektedir. Mevcut Yönetmelikte “Kişi sınırlandırması” başlığı altında kimlerin konum verisini işleyebileceğine ilişkin hüküm Taslak Yönetmelikte aynı kapsamda korunmuş olup “Konum verisini işleme yetkisi” başlığı altında düzenlenmiştir. Taslak Yönetmeliğin en büyük farklılıklarından biri ise “Saklanacak veri kategorileri” başlıklı madde olmuştur. Nitekim, madde incelendiğinde hangi işletmecilerin hangi bilgileri saklayacağı detaylı bir şekilde belirtilmiştir. Hangi verilerin hangi işletmeciler tarafından saklanacakları belirlendikten sonra bu verilerin ne kadar süre ile saklanacağı “Veri saklama süresi” başlıklı madde altında bir yıl olarak belirlenmiştir. Taslak Yönetmeliğin bir diğer

önemli yeniliği ise “Saklanan verinin korunması ve güvenliği” başlıklı maddedir. Zira, bu maddede veriler saklanırken işletmecilerin göstermesi gereken özen ve alması gereken tedbirlere yer verilmiştir. Taslak Yönetmelikteki bir diğer yeni maddede “İstatistiki bilgilerin verilmesi” başlıklı madde olmuştur. Bu maddede yetkili makamlar tarafından talep edilen ancak kişisel verileri içermeyen bilgiler ile bu veri taleplerinin karşılanıp karşılanmadığı ve bu verilerin saklandığı tarih ile yetkili makam tarafından talep edildiği tarih arasında geçen sürelerle ilişkin bilgilerin istatistiki amaçla her yılın Ocak ayı içerisinde bir önceki yılı kapsayacak şekilde gönderilmesi hüküm altına alınmıştır.

Yönetmeliğin dördüncü bölümünde AB Direktiflerindeki hususlara uygun olarak işletmeciler tarafından kullanıcılara sağlanan imkanlara yer verildiği görülmektedir. Mevcut Yönetmeliğin 13 ve 14 üncü maddesinde düzenlenmiş olan “Arayan hattın kimliğinin açıklanmasının engellenmesi” ve “Arayan hattın bağlanmasının engellenmesi” başlıklı maddelerin Taslak Yönetmeliğin “Numaranın gizlenmesi” başlıklı maddenin birinci fıkrasında düzenlendiğini görmekteyiz. Aynı maddede yeni bir imkana yer verilmiş ve bağlanan hattın numarasının görünebilir olduğu durumlarda, aranan abonenin talep etmesi halinde işletmeci tarafından, ücretsiz ve basit bir yöntemle aramanın gerçekleştirilmesinin arayan tarafından bilinmesi engellenmesinin sağlanması hüküm altına alınmıştır. Ancak, Mevcut Yönetmeliğin uygulamaya ilişkin esas maddelerinden olan “Arayan Hattın Kimliğinin Açıklanmasının Engellenmesi” (Madde 13), “Arayan Hattın Bağlanmasının Engellenmesi” (Madde 14), maddeleri için Yönetmeliğin yürürlüğe girdiği zamandan itibaren işletmecilere, Telekomünikasyon Kurulu Kararları ile 31.12.2007 tarihine kadar muafiyet tanınmış olduğu düşünüldüğünde yeni hükmün uygulanması için de belirli bir sürenin gerekli olup olmadığının işletmecilerden gelen görüşler sonrasında değerlendirilebileceği düşünülmektedir. Taslak Yönetmelikte numaranın gizlenmesine ilişkin hükümlerden sonra Mevcut Yönetmelikte olmayan “Otomatik çağrı yönlendirme” başlığı altında yeni bir maddenin düzenlendiğini görmekteyiz. Bu yeni madde ile üçüncü kişiler tarafından yapılan yönlendirmelerin bir diğer ifade ile bir kullanıcının diğer kullanıcıya yapmış olduğu yönlendirmelerin ücretsiz ve basit bir yöntemle işletmeci tarafından engellenmesine imkan sağlanmaktadır. Diğer taraftan aynı madde ile abone/kullanıcının rızası olmaksızın kullanıcıya yapılan aramaların otomatik mesaj sistemine yönlendirilemeyeceği açık bir şekilde belirtilmiştir. Taslak Yönetmeliğin beşinci bölümden önce düzenlenmiş bir diğer hükmü de Mevcut Yönetmelikte de benzer şekilde yer alan “Aboneler için hazırlanan rehberler” başlıklı maddedir. Bu maddede ise abonelerin kamuya açık kişisel rehberlerde yer alıp almama istekleri ile kişinin tanımlanabilmesi için gerekli veriler dışındaki kişisel verilerin kullanılarak sorgulama yapılabilmesi için abonenin ek rızasının alınması gibi hususlar yer almaktadır. Mevcut Yönetmelikte “İstek dışı haberleşmeler” başlığı altında yer alan hükümler ise Taslak Yönetmelikte “İstenmeyen mesajlar” başlığı altında düzenlenmiş bulunmaktadır. Mevcut Yönetmelikte otomatik sistemlerin abonenin izni olmaksızın siyasi propaganda amacı ile kullanamayacağı yer almakta iken Taslak Yönetmeliğe

siyasi propaganda eklenmemiştir. Taslak Yönetmeliğin bahsi geçen maddesine ilişkin bir diğer fark ise tüketicinin rızası ile pazarlama amacıyla gönderilen elektronik mesajlarda göndericinin kimliği ve erişim bilgisinin yer alması zorunlu tutulmuştur. Her iki Yönetmelik hükmünde de abonelere istenmeyen mesajların gelmesini engellemelerine imkan sağlanması işletmecilere yükümlülük olarak getirilmiştir.

Taslak Yönetmeliğin beşinci bölümünde işletmecilerin Yönetmelikteki yükümlülüklerine uymamaları halinde uygulanacak idari para cezalarına yer verilmiş olup, bu ceza EHK'nın 60 ncı maddesinde belirtilen azami sınıra kadar (işletmecinin bir önceki takvim yılındaki cirosunun %3'ü) erişebilecektir. Ancak, idari para cezası uygulanmadan önce işletmeciye ihlali sona erdirmesi için Kurum tarafından süre verilerek uyarı yapılması gerekmektedir. Taslak Yönetmeliğin önem arz eden bir diğer maddesi de hızla değişen ve gelişen elektronik haberleşme sektöründe öngörülemeyen durumlar için Yönetmelikte hüküm bulunmayan hallerde tebliğ ya da Kurul Kararı ile işlem yapılabilmesidir.

IV. SONUÇ

Ülkemizde kişisel verilerin korunmasına ilişkin AB'de olduğu gibi genel bir düzenleme (95/46/EC) olmamasına karşın elektronik haberleşme sektörüne ilişkin 2004 yılında Veri Gizliliği Yönetmeliğinin yayımlanması ile özel bir düzenleme yapılmış olması zaman zaman eleştirilmiştir. Ancak, kişisel bilgilerin ihlalinin daha hızlı ve yaygın olabileceği bu alanda yapılan Yönetmelik ve ardından 2008 yılında yayımlanarak yürürlüğe giren Elektronik Haberleşme Kanunu kişisel bilgilerin korunmasında yaşanan boşluğu en azından bu sektöre özgü olarak kapatmıştır. Taslak Yönetmeliğin de yayımlanarak yürürlüğe girmesi ile Mevcut Yönetmelikte yer almayan hususlara ilişkin boşluk da kapatılmış olacak ve daha etkin bir koruma sağlanmış olacaktır.

KAYNAKÇA

- [1] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and protection of privacy in the telecommunications sector, OJ L 024, 30/01/1998, p. 01-08
- [2] 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, OJ L 281, 23/11/1995, p. 31
- [3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002 p. 37-47.
- [4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 13.04.2006 p. 54
- [5] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic

communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

- [6] Cullen International (2010), 'Big Five Update', AB İstatistik Raporları, 27.01-22.02. 2010, s. 5-6
- [7] 06.02.2004 tarih ve 25365 sayılı Resmi Gazete'de yayımlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik
- [8] 10 Kasım 2008 tarih ve 27050 (Mükerrer) sayılı Resmi Gazete'de yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu
- [9] Kişisel Verilerin Korunması Kanunu Tasarısı, <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>,

Güvenlik Sistemlerinde Video Aslının ve Bütünlüğün Doğrulanması için bir Donanım Tasarımı

Ö. Uyanık, A. Z. Alkar, İ. E. Ungan

Öz— İçinde çok sayıda video işlemi gerçekleştiren ve video işareti üzerinde görüntü işleme algoritmaları çalıştıran güvenliğin artırılmış güvenlik sistemlerinde gelen video görüntüsünün, beklenen video kaynağından geldiği varsayılmaktadır. Oysa video kaynağının bir başka kaynak ile yer değiştirilebilme olasılığı sonucunda güvenlik sistemi etkisizleştirilebilmektedir. Bu tür sistemlerde video kaynağı ile iletişimin tek yönlü olması, bilgisayar ağlarında sık kullanılan aslının doğrulanması (authentication) yöntemlerinden farklı çözümler gerektirmektedir. Yüksek video çözünürlüklerinde işlemci hızı yetersizliği yüzünden var olan sistemlerde başarımların düşmesi olabilmektedir. Bu çalışmada, güvenlik sistemine doğrudan eklenebilen, üzerinde video çözümü/kodlayıcı ve FPGA bulunan bir kart tasarlanarak videonun aslının ve görüntü bütünlüğünün doğrulanması işlemlerinin güvenlik anahtarlı özet alma (hash) algoritması (SHA-1) ile gerçekleştirilmesi sunulmuştur.

Anahtar Kelimeler— Güvenlik sistemi, video bütünlüğü, videonun aslının doğrulanması (authentication), özet alma işlemi (hash), SHA-1, FPGA.

I. GİRİŞ

Güvenlik sistemlerinde video uygulamalarının önemi artmakta ve yaygın kullanılmaktadır. Gözlenmek istenen bölgelere, hareketli ya da hareketsiz, çoğunlukla çok sayıda kamera yerleştirilerek video işaretleri gözlem odasına ulaştırılmakta ve çok kanallı video alıcılarından geçirilerek bir ya da daha çok monitör üzerine aktarılmaktadır. Gözlemlerin insan kullanılarak yapılması çok kanallı video görüntülerinin sürekli izlenmesini zorlaştırmakta ve güvenliği azaltmaktadır. Bu sorunun önüne video işlemcilerin çok kanallı video işaretleri üzerinde görüntü işleyerek tehdit olabilecek oluşumları algılayan algoritmalarla geçilmektedir. Bunun yanı sıra yüksek çözünürlüklü kameraların sağladığı video

işaretleri üzerinden nesne belirlemeye yönelik tanımlayıcı veriler elde edilebilmekte ve kayıt altına alınarak delil oluşturabilmektedir. Böylece gelişmiş donanım ve yazılım ile güvenlik seviyesi artırılabilir.

Güvenlik sistemleri ister basit ister karmaşık olsun, video işaretleri üzerinde yapılan basit gözlem ya da karmaşık algılama işlemlerinde, gelen video işaretlerinin güvenilir olduğu varsayımı vardır. Video işaretlerinin kaynakları olan kameralar çoğunlukla güvenlik merkezine uzak yerlerde bulunmaktadır. Böylece işaretlerin taşındığı kablolu ya da kablosuz iletim ortamı erişilebilmekte ve farklı video kaynak işaretleri ile yüklenerek güvenlik sistemi etkisiz duruma getirilebilmektedir. Video işaretinin beklenen kaynaktan geldiğini algılamak için video aslının doğrulanması (authentication) gerekmektedir. Doğrulama için yaygın kullanılan “Watermarking” yönteminde video çerçevesinin görünen bölgesi kullanılmaktadır[1]. Bu yöntemde görüntü gözle anlaşılamayacak kadar bozulsun da özellikle yüksek çözünürlüklü video işaretleri üzerinde çalışan görüntü işleme algoritmalarının bozulmuş görüntü üzerindeki analizleri başarımlarını olumsuz etkilemektedir.

Bu çalışmada, aslının doğrulanması için bir başka yöntem olan anahtarlanmış özet alma (hash) işlemi video çerçevesinin görünmeyen bölgesine yerleştirilen rastgele sayı dizisi ve çerçeve sayısı üzerine uygulanmıştır[2]. Aynı işlem, görünen bölgeye de uygulanarak veri bütünlüğünün (data integrity) kısmen izlenebilmesi sağlanmıştır. Bu işlevler, kimlik oluşturucu ve kimlik belirleyici adı verilen tümdevre tasarımları ile FPGA üzerinde VHDL donanım tanımlama dili kullanılarak gerçekleştirilmiştir. FPGA kullanımı ile her video kaynağı için farklı ve değiştirilebilir gizli anahtar kullanımı sağlanmıştır. Yazılım kullanılmadan ve doğrudan donanım ile yapılarak yüksek tasarım gizliliği sağlanmıştır. Üzerinde FPGA, video çözümü ve video kodlayıcı tümleşikdevreler bulunan “video güvenlik kartı” adlı kart tasarlanıp gerçekleştirilmiştir.

Taslak 01 Nisan 2010’da alınmıştır.

Ö. Uyanık Karel Elektronik San. ve Tic. A.Ş. firmasında İletişim Teknolojileri Ar-Ge bölümünde tasarımlar mühendisi olarak çalışmaktadır. (E-posta: ozlem.uyanik@karel.com.tr).

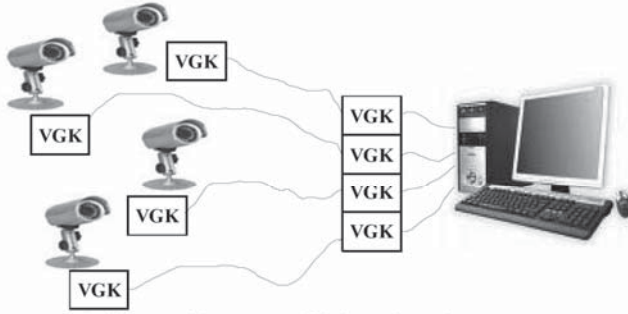
A. Z. Alkar Hacettepe Üniversitesi Elektrik ve Elektronik Bölümünde öğretim üyesidir. (E-posta: alkar@hacettepe.edu.tr).

İ. E. Ungan Karel Elektronik San. ve Tic. A.Ş. firmasında İletişim Teknolojileri Ar-Ge bölümünde teknik lider olarak çalışmaktadır. (E-posta: enis.ungan@karel.com.tr).

verilmiştir.

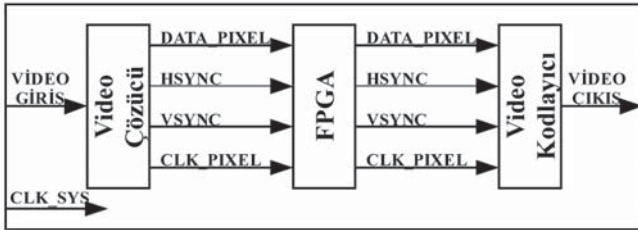
II. SİSTEM YAPISI

Video güvenlik kartı (VGK) video kamera çıkışlarına ve gözetleme odasında toplanan görüntü işleme ünitesi girişlerine yerleştirilir. Kamera çıkışlarında kimlik oluşturma işlevi, görüntü işleme ünitesi girişlerinde kimlik belirleme işlevi kart üzerinde çalışır. Şekil-1'de tipik bir kurulum gösterilmiştir.



Şekil-1: Video güvenlik kartı kurulumu.

Bağlantılarda video, ses ve güç sağlayan yaygın kullanılan ekranlı kablo grubu kullanılır. Video güvenlik kartının yapısı Şekil-2'de verilmiştir. Video kaynağından alınan görüntü video çözücüye girer. Video çözücü analog video işaretini herbiri 8-bit olan parlaklık (Y), mavi (Cb) ve kırmızı (Cr) parçalardan oluşan sayısal 24-bit video benek verisine dönüştürür. Video işaretleri FPGA ile gerçekleştirilen kimlik oluşturma ya da kimlik belirleme işleminden geçip video kodlayıcı ile sayısaldan analog işarete dönüştürülür. Video işaretinin uzak yol alabilmesi için çıkışa güçlendirici yerleştirilmiştir.



Şekil-2: Video güvenlik kartı yapısı.

Video işaretlerin analog ile sayısal bölgeler arası geçiş yaparken genlik değişim ve iletilirken gürültü kapma olasılığına karşı benek verileri için genlik yerine faz farkı ile modüle edilen renk verileri (Cb ve Cr) ve bu verilerin ayarlanabilir sayıdaki (d) en değerli bitleri kullanılmıştır. Bu yapıda (d) en çok 8 değerini alır.

Kimlik oluşturma, kimlik belirleme ve veri bütünlüğü denetim işlemleri FPGA içinde gerçekleşir. Kimlik oluşturma işleminde her video çerçevesi için 128bit çerçeve sıra numarası ve 384bit çerçeve kodu atar. Çerçeve sıra numarası her video çerçevesi gönderiminde bir artarken çerçeve kodu için 511bit sözde rastgele ikili dizi (PRBS) üretilip 384-bit kısmı alınır. Toplam 512bit çerçeve bilgisi FPGA içine

gizlenmiş güvenlik anahtarı kullanılarak SHA-1 özet algoritması (hash) ile kodlanır. 160bit uzunluğundaki "hash message authentication code" (HMAC) ile 512bit çerçeve bilgisini 672bit olarak video çerçevesinin görünmeyen bölgesine yerleştirir.

Benek değerlerinde yalnızca renk bilgilerinin ve bunların da en değerli d sayıda bitlerinin kullanılması veri bütünlüğü denetimini yetersiz kılmaktadır. Bunun yerine, görüntü verilerinin asıl görüntü verisi ile uyumlu olmasına bakarak görsel bir bütünlüğün izlenmesini gerektirmiştir. Bu çalışmada kimlik oluşturma, görünen video bölgesinin her satırından yalnızca 512bit'lik veri toplar, sonraki satır verisi gelmeden video yatay eşzamanlama işaretinin ara bölümünde (blanking interval) SHA-1 işleminin ilkini tamamlar. Tüm satırlara SHA-1 uygulayıp ortaya çıkan 160-bit özet kodu video çerçevesinin görünmeyen satırına yerleştirir.

Kimlik belirleme işleminde video satırlarından çerçeve sayısı, çerçeve kodu ve HMAC okunur. Çerçeve bilgileri gizli anahtar kullanılarak SHA-1 ile kodlanır. Ortaya çıkan HMAC ile okunan HMAC karşılaştırılıp video kaynağının asıl olup olmadığı denetlenir. Video çerçevesinde görünen her satırdan 512-bit veri okunup tüm satırlardan SHA-1 ile elde edilen HMAC, görünmeyen satırdan okunan HMAC ile karşılaştırılarak görüntü bütünlüğü izlenir. Aslının doğrulanmasında ve görüntü bütünlüğünde sorun çıkarsa video çıkışına okunabilecek hata iletilişi gönderilir.

III. KİMLİK OLUŞTURUCU

Kimlik oluşturma yapısı Şekil-3'te verilmiştir. Video girişinden video çerçevesinin görünen bölgesindeki verileri giriş bloğu alır ve bellek arayüzü ile SHA-1 bloğuna özet bilgi çıkarması için iletir. PRBS bloğu gelen her yeni video çerçevesine sayı ve kod verip çerçeve bilgisinden özet bilgi çıkarması için SHA-1 bloğuna bellek üzerinden iletir. Özet bilgilerin FPGA içine gömülü gizli bir anahtar kullanılarak çıkarılmasını HMAC bloğu sağlar. SHA-1 bloğundan çıkan iki özet bilgi, gelen video çerçevesinin görünmeyen satırlarına video çıkış bloğuna yerleştirilir.

Video çerçevesinin görünen bölgesinin her satırından p benekte bir alınan toplam 512bit veri SHA-1 döngüsünde bir bloklu giriş verisine denk gelir[3]. Görüntü bütünlüğü işlemlerinde video çözünürlüğüne bağlı olarak p değişir:

$$p = 2 * d * b / 512 \quad (1)$$

- p: Satırın görünen bölgesinde atlanacak benek sayısı
- d: Beneğin Cb ya da Cr verisi için en değerli bit sayısı
- b: Satırın görünen bölgesinde benek sayısı

Yukarıdaki (1) eşitliğini kullanan video giriş (*video_grs*) bloğu görünen bölgenin verilerini toplayıp video giriş belleği (*video_bllk*) bloğuna yazar ve 512bit'lik veri bloğunu SHA-1

döngüsü için oluşturur. Bu işlem, görünen bölgede satır sayısı s kere tekrarlanır ve sonucunda 160-bit görüntü özeti ortaya çıkar. Belleğe yazma sıklığı video benek saat sıklığı ile doğru, p değeriyle ters orantılıdır. Okuma sıklığı ise olabilecek en yüksek FPGA sistem çalıştırma saat sıklığıdır. Giriş bloğu için p , d ve s değişken girişlerdir.

sıklığındadır. Okuma sıklığı ise olabilecek en yüksek FPGA sistem çalıştırma saat sıklığıdır.

Yukarıda tanımlanan *video_grs* ve *prbs_grs* bloklarının oluşturduğu 512-bit veri blokları 8bayt uzunluğunda gizli anahtar değeri ile *hmac* ve *sha-1* bloklarınca işlenir ve sonucunda iki adet 160-bit HMAC oluşur. Gizli anahtarın kullanımı [5] için aşağıdaki işlemler yapılır.

$$\begin{aligned} k1 &= \text{ipad64} \oplus (a \parallel \text{sfr56}) \\ k2 &= \text{opad64} \oplus (a \parallel \text{sfr56}) \end{aligned} \quad (3)$$

- $k1$: İlk oluşturulan anahtar değeri 512-bit veri
 $k2$: İkinci oluşturulan anahtar değeri 512-bit veri
 a : Gizli anahtar değeri 8-bayt veri
 ipad64 : 64 kez tekrarlanmış “inner pad” 36h değeri
 opad64 : 64 kez tekrarlanmış “outer pad” 5Ch değeri
 sfr56 : 56-bayt sıfır değeri
 $\oplus$: Karşılıklı bitlerle XOR mantık işlemi

Bu işlemleri *hmac* bloğu gizli anahtar a değerini işleyerek gerçekler ve *hmac_bllk* adlı 1024-bit belleğe $k1$ ve $k2$ değerlerini yazar. *Sha-1* bloğu *hmac_bllk* belleğini $k1$ ve $k2$ değerleri için okur ve diğer 512bit'lik veri blokları ile birlikte işler.

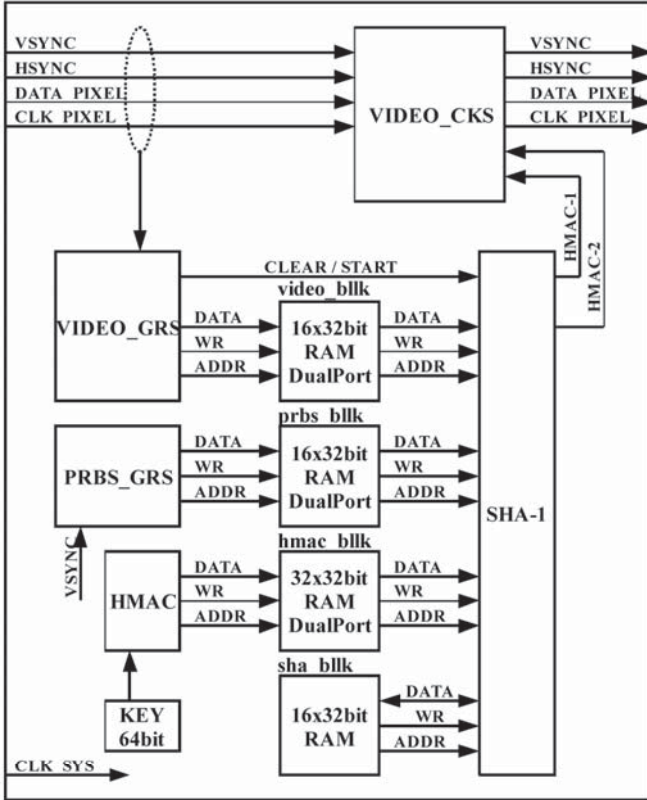
Video aslının doğrulanmasında kullanılacak *hmac1* özet değerinin gizli anahtar kullanılarak elde edilmesi için aşağıda işlem sırası verilmiştir:

$$\begin{aligned} h &\leq \text{sha-1}(k1, \text{hinit}) \\ \text{mac} &\leq \text{sha-1}(\text{prbs}, h) \\ h &\leq \text{sha-1}(k2, \text{hinit}) \\ h &\leq \text{sha-1}(\text{prbs}, h) \\ \text{hmac1} &\leq \text{sha-1}(\text{mac} \parallel 80h \parallel \text{sfr42} \parallel 14h, h) \end{aligned}$$

- h : geçici 160-bit “hash” değeri
 h_{init} : standart başlangıç “hash” değeri
 mac : $k1$ için hesaplanmış 160-bit özet değeri
 sfr42 : 42-bayt sıfır değeri

Buna göre, *sha-1* bloğu $k1$ değerini *hmac_bllk* belleğinden okuyup değişmez ilk özet değeri *hinit*'i kullanarak geçici h özet değerini bulur ve bir yazmaca kaydeder. *Prbs* değerini *prbs_bllk* belleğinden okuyup h özet değerini kullanarak *mac* özet değerini bulur. Benzer şekilde, $k2$ değeri için bulacağı geçici özet değerini *prbs* değerinin geçici özet değeri için kullanır. Bu değeri daha önce bulunduğu *mac* özet değeri için kullanıp *hmac1* değerini elde eder ve yazmacıta saklar. 160-bit (20bayt) *mac* değerinin 512bit'e çıkarılması amacıyla *mac* veri sonuna 80h, ardından 42 adet 00h ve son olarak *mac* uzunluğu olan 20bayt değeri 14h eklenir.

Sha-1 bloğu video görüntü bütünlüğünün izlenmesi için video çerçevesinin *hmac2* özet değerini bulmak için yukarıda



Şekil-3: Kimlik oluşturucu yapısı.

Kimlik bilgisini her çerçeve için oluşturan video çerçeve sıra numarası verisi ve buna bitleştirilen sözde rastgele ikili dizi (PRBS) verisi toplamı olan 512bit veri SHA-1 döngüsünde bir bloklu veridir.

$$k = \varphi \parallel r \quad (2)$$

- k : Kimlik belirleyici kod 512bit veri
 φ : Video çerçeve sayısı 128bit veri
 r : Rastgele sayı 384bit veri
 $\parallel$: Bitleştirme işlemi

Yukarıdaki (2) eşitliğini PRBS giriş (*prbs_grs*) bloğu gerçekleştirir. Blok içinde çerçeve sayısı için doğrusal 128-bit sayaç ve “linear feedback shift register (LFSR)” ile gerçekleştirilmiş 511-bit PRBS üretici bulunur[4]. Blok, kimlik bilgisini her video çerçeve için çıkışındaki PRBS giriş belleği (*prbs_bllk*) bloğuna yazıp 512bit'lik veri bloğunu SHA-1 için oluşturur. Belleğe yazma sıklığı video benek saat

söz edilen benzer işlemleri uygular. 512bit'lik veri bloklarını *video_blk* belleğinden okur. Her video çerçevesi için toplam satır sayısı (s) kadar veri bloğu okur. İşlem sırası;

```

h1  <= sha-1(k1, hinit)
h2  <= sha-1(k2, hinit)
mac <= sha-1(video(i), h1)
h2  <= sha-1(video(i), h2)
h2  <= sha-1((mac || 80h || sfr42 || 14h), h2)
i   <= 1, 2, 3... s için tekrarlar.
hmac2 <= h2

```

olarak belirlenmiştir.

Sha-1 bloğu video ve prbs belleklerinden okunan 16 adet 32-bit sözcükten 80 adet 32-bit sözcük elde eder. 17'nci ve daha sonraki sözcükler kendisinden önce 16'ncı, 14'ncü, 8'inci ve 3'üncü sözcüklerin kullanılmasıyla elde edilir. Bu işlemi gerçekleştirmek için 16*32bit bellek (*sha_blk*) kullanır. Türetilen her yeni sözcük *sha_blk* belleğinde kendisinden 16 sözcük öncekinin üzerine yazılır. *Sha-1* bloğu her video çerçevesi için bulduğu iki adet hmac1 ve hmac2 özet değerinin her birini 80 döngü sonunda ortaya çıkarır ve yazmaçlarına kaydeder.

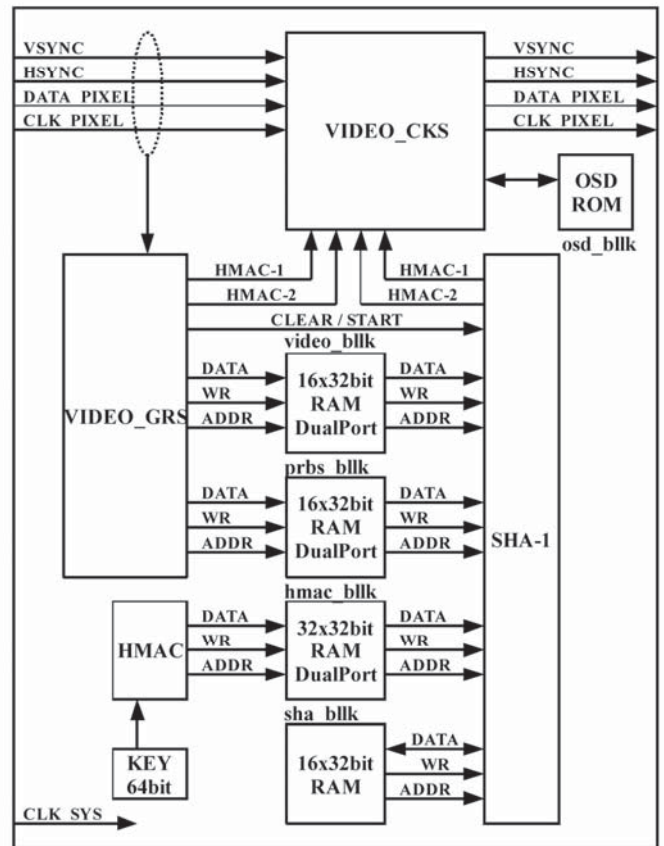
Video çıkış bloğu (*video_cks*), *prbs_grs* bloğundan PRBS değerini, çerçeve sıra numarasını, *sha-1* bloğundan hmac1 ve hmac2 değerlerini alıp çıkacak video çerçevesi içinde görünmeyen video bölgelerine yerleştirir. Blok, d ve p değişkenlerine göre benek adreslerini ve benek değerlerini oluşturur. Kimlik oluşturmada ve görüntü doğrulamada kullanılan veriler için $d = 2$ alınmıştır. Buna göre 672-bit kimlik bilgisi için $672 / (2*d) = 168$ benek kullanılmıştır. Görüntü doğrulama için kullanılan 160-bit hmac2 değeri için 40 benek kullanılır. *Video_cks* bloğu toplam 208 beneği görünen video bölgesinin son satırından sonraki görünmeyen video bölgesinin (front-porch) ikinci satırına yerleştirir.

IV. KİMLİK BELİRLEYİCİ

Kimlik belirleyicinin yapısı kimlik oluşturuçuya benzer. Kimlik belirleme işlevini gerçekleştirmek için gizli anahtar (a) kullanarak gelen veri bloklarından oluşturduğu hmac1 ve hmac2 özet bilgilerini gelen özet bilgileri ile karşılaştırır ve farklılık durumunda video çerçevesinin görünen bölgesine hata iletisi çıkarır.

Kimlik belirleyicinin yapısı Şekil-4'te gösterilmiştir. Video giriş (*video_grs*) bloğu görünen video bölgesinden 512bit'lik bilgiyi *video_blk* belleğine aktarır. Aynı zamanda görünmeyen video bölgesinden PRBS, çerçeve sayısını okuyup *prbs_blk* belleğine yazar. Aynı bölgeden karşılaştırılacak hmac1 ve hmac2 özet bilgilerini okur ve yazmaçlara kaydeder. Gizli anahtarı kullanıp *hmac* bloğu ile oluşturduğu k1 ve k2 değerlerini *hmac_blk* belleğine kaydeder. *Sha-1* bloğu *video_blk*, *prbs_blk* ve *hmac_blk* belleklerinden verileri okuyup işleyerek hmac1 ve hmac2

değerlerini elde eder. Kimlik belirleme ve görüntü bütünlüğü işlemlerinin son basamağı *video_cks* bloğunda gerçekleşir. Blok, *video_grs* bloğundan gelen *hmac1* ve *hmac2* değerlerini *sha-1* bloğundan gelen değerlerle karşılaştırır. Karşılaştırma sonucunda kimlik bilgisinin özeti olan *hmac1* değerinde tutarsızlık olması durumunda hata verir. Görüntü bütünlüğünün doğruluğu için kullanılan *hmac2* özet bilgisinde tutarsızlık olması durumunda ise görüntü bütünlüğü hatası verir. Hata iletileri sözcükler olarak video çerçevesinin görünen bölgesine yerleştirilerek görünmesi sağlanır. Hata tipine göre belirlenen sözcükler *osd_blk* belleğinden *video_cks* bloğunca okunur.



Şekil-4: Kimlik belirleyicinin yapısı.

V. SONUÇ

Kurulu bir güvenlik sisteminin kamera hatlarına kolayca bağlanarak sisteme entegre edilebilen video aslının doğrulanması ve aynı zamanda görüntü bütünlüğü işlevlerini sağlayarak güvenlik sisteminin güvenilirliğini arttıran VGK adlı devre kartı gerçekleştirilmiştir. Sözedilen işlevler kart üzerindeki FPGA içinde, gizli anahtar kullanımına olanak sağlayacak şekilde, standart SHA-1 özet alma algoritmasını çalıştıran donanım tasarımı ile sağlanmıştır. Her VGK kartında faklı anahtar kullanılarak kamera ile kartın bütünlüğü sağlanabilmektedir. Kartın özellikleri Tablo-1'de verilmiştir.

Tablo-1: Video Güvenlik kartı özellikleri.

Video girişleri ve çıkışları:	CVBS
-------------------------------	------

Veri taşıma kanalı:	Grafik RGB Benek'te renk bileşenleri; Cr ve Cb
Benekte kullanılan bit sayısı:	2*d
Satırda kullanılan bit sayısı:	512
Satırda kullanılan benek sayısı:	512 / (2*d)
Kullanılan video satır sayısı:	Tümü
Gizli anahtar bit uzunluğu:	64
Eksik video çerçeve algılayıcı:	Var
Çalışma saat periyodu (Pç):	8 nsn
Çıktı hızı 512 / (85 * Pç):	753Mbit/sn
İşlem süreleri:	
SHA-1 (85*Pç):	0.68 µsn
hmac1(3*85*Pç):	2.04 µsn
hmac2:	s*2.04 µsn

VGK kartının hem bileşik hem de grafik video giriş ve çıkış özelliği arayüzde esneklik sağlamak ve çok çeşitli video kamera bağlantılarına ve kamera çözünürlüklerine olanak sağlamaktadır. Video aslının doğrulanmasında video çözünürlüğünün doğrudan etkisi olmamakta, ancak video benek frekansı belirleyici olmaktadır. Buna göre en yüksek benek frekansı sistem saat frekansı ile aynıdır ve 125MHz'tir. Bu değer yüksek çözünürlükte video işaretlerini kapsayabilecek değerdir[6]. Video veri bütünlüğü için tüm benek değerleri, video üzerinde olabilecek gürültü nedeniyle, kullanılmadığı için görüntü bütünlüğü tanımlanmıştır. Seçilebilir d değeri görüntü bütünlüğünde kullanılabilir renk sayısını belirlemektedir. Görünen satırların her birinde toplam 512-bit kullanılması ve d değeri çözünürlüğe bağlı olarak benek kullanım oranını ortaya koymaktadır. Tablo-2'de bazı video standartlarına göre çözünürlük (Ç), benek frekansı (F), ve çeşitli d değerleri için satırda benek kullanım (kapsama) oranları (K) verilmiştir. Örneğin PAL kamera bağlantısında, görüntü bütünlüğü, 4 renk ve 256'ya 625 çözünürlük ile değerlendirilmektedir.

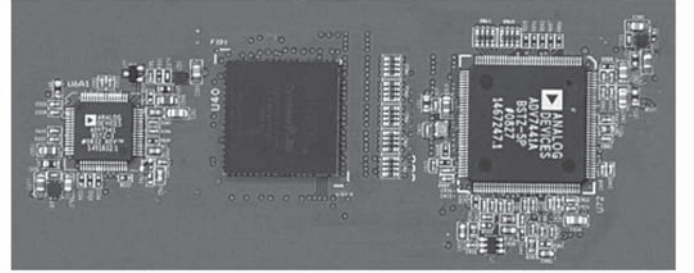
Tablo-2: Uygulanabilen video standartları ve satırda benek kullanım oranları.

Video	Ç	F	K d=1	K d=2	K d=4
PAL	720 / 625	13.5	%36	%18	%9
NTSC	720 / 525	13.5	%36	%18	%9
VGA	640 / 480	25	%40	%20	%10
SVGA	800 / 600	40	%32	%16	%8
XGA	1024 / 768	65	%25	%13	%6
1080p25	1920 / 1080	74.25	%13	%7	%3

VGK'nın temel malzemelerinde ADV7441 video çözücü, ADV7341 video kodlayıcı ve EP3C25F384 FPGA bulunur. Kart boyutları yaklaşık 12cm x 5cm'dir. Kartın görüntüsü Şekil-5'te gösterilmiştir.

Gelecekte, geliştirmeye yönelik yapılacak çalışmalarda, satırda kullanılan bit sayısını arttırmak, kimlik belirleyici işlemcisine hata düzeltici eklemek, eş zamanlı değişen güvenlik anahtarları eklemek, güvenlik kamerasının

algılayıcısına doğrudan arayüz oluşturmak düşünülmektedir.



Şekil-5: Video güvenlik kartının görüntüsü.

KAYNAKLAR

- [1] C. Rey, J. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication", EURASIP Journal on Applied Signal Processing, 2002:6, 613-621, June 2002.
- [2] W. Stallings, "Cryptography and Network Security Principles and Practices", ISBN 0-13-609704-9.
- [3] Federal Information Processing Standards Publication, "Announcing the Secure Hash Standard", FIPS PUB 180-2 (Change Notice to include SHA-224), 2002.
- [4] R. Ward, T. Molteno, "Table of Linear Feedback Shift Registers", Dept. of Physics, University of Otago, New Zealand, October 26, 2007.
- [5] Federal Information Processing Standards Publication, "The Keyed Hash Message Authentication Code (HMAC)", FIPS PUB 198, 2002.
- [6] EBU UER "High Definition (HD) Image Formats for Television Production", EBU TECH 3299, Geneva Jan. 2010.

ETSI Gelişmiş Elektronik İmza Formatlarının Kullanımı ve Merkezi Bir Elektronik İmza Servisi Önerisi

Serkan Doğan

Abstract - In our country, basic electronic signature format (CADES-BES) developed by The European Telecommunication Standards Institute (ETSI) is widely used in institutional electronic signature applications. However, this format is not sufficient in terms of providing long term electronic signature validity. In order to achieve longer term validity, advanced electronic signature formats defined by ETSI need to be utilized. In this study, benefits of improved electronic signature formats by ETSI and using options of these formats in different situations will be elaborated. This will be followed by a recommendation regarding a central electronic signature service which will enable transforming data with basic electronic signature into advanced electronic signature formats and which will also meet signature validation needs from one point.

Keywords – Electronic Signature, advanced electronic signature formats, long term validity, electronic signature service

Özet – Ülkemizde, kurumsal elektronik imza uygulamalarında yaygın olarak Avrupa Telekomünikasyon Standartları Enstitüsü'nün (ETSI) tanımlamış olduğu basit elektronik imza formatı (CADES-BES) kullanılmaktadır. Fakat bu format, elektronik imzanın uzun süre geçerliliğinin sağlanmasında yeterli değildir. Uzun süre geçerlilik için yine ETSI'nin tanımlamış olduğu gelişmiş elektronik imza formatlarının kullanımına ihtiyaç duyulmaktadır. Bu çalışmada, ETSI gelişmiş elektronik imza formatlarının sağladıkları ve bu formatlardan hangilerinin ne durumda kullanılmalarının uygun olacağı üzerinde durulacak, basit elektronik imzalı verileri gelişmiş elektronik imza formatlarına dönüştürme işlemlerini ve imza doğrulama ihtiyaçlarını tek bir noktadan karşılayacak merkezi bir elektronik imza servisi önerisi yapılacaktır.

Anahtar Kelimeler - Elektronik imza, gelişmiş elektronik imza formatları, uzun süre geçerlilik, elektronik imza servisi

I. GİRİŞ

Elektronik imzanın geçerliliği, imzayı oluşturan sertifikanın geçerliliği ve imza oluşturma aşamasında kullanılan kriptografik algoritmaların güvenilirliği ile doğrudan ilişkilidir.

Serdar Doğan, TÜBİTAK Bilişim Müdürlüğü, Kavaklıdere Ankara, serdar.dogan@tubitak.gov.tr

İmzayı oluşturmada kullanılan sertifikanın imzanın oluşturulduğu andaki geçerliliğinin kontrol edilebilmesi için gerekli doğrulama verilerine imza oluşturulduktan yıllar sonra erişilemeyebilir. Elektronik sertifika hizmet sağlayıcılar (ESHS) sertifika iptal bilgilerini sadece sertifikanın geçerlilik süresince yayınlamakla yükümlüdür [2]. Dolayısıyla sertifikanın geçerlilik süresi dolduktan sonra da imzayı doğrulayabilmek için bu iptal bilgilerinin elektronik imzanın kullanıcıları olan kurum veya kuruluşlar tarafından saklanması gereksinimi doğmaktadır.

Ayrıca, imza oluşturma aşamasında kullanılan kriptografik algoritmalar da zamanla güvenilirliklerini yitirebilmektedir. Bugün için kırılmaz denilen bir algoritma ya da çözülmesi asırlar alacak şifrelenmiş veriler bundan birkaç yıl sonra gelişen teknoloji ve artan işlem gücü ile aynı güvenilirliği sağlamayabilecektir.

Bu durumların önüne geçmek için elektronik imzanın uzun süre geçerliliğini sağlayacak ek verilerin imzaya eklenmesi gerekmektedir. ETSI bu amaçla TS 101 733[4] ve TS 101 903[5] dokümanlarıyla gelişmiş elektronik imza formatlarını tanımlamıştır. Bu formatları kullanarak yukarıda sıralanan sorunların üstesinden gelmek mümkün olmaktadır.

Fakat, mevcut durumda elektronik imza entegrasyonu yapılmış olan birçok kurumsal uygulamada aslında ETSI'nin tanımlamış olduğu basit elektronik imza (CADES-BES) formatının kullanıldığı, imzanın uzun süre geçerliliğinin sağlanması konusunda gerekli çalışmaların yapılmadığı görülmektedir. Uzun süre saklanması gerekmeyen ya da imza geçerliliğinin kısa vadede önemli olduğu durumlarda bu yaklaşım sorun teşkil etmeyebilir; ancak, uzun süreli saklanması gereken belgelerde uzun süre geçerlilik için gerekli çalışmanın yapılması kaçınılmazdır.

Bu çalışmada, ETSI TS 101 733'te tanımlanmış olan imza formatlarından hangilerinin ne durumda kullanılması gerektiğine değinilecek, çok sayıda elektronik imza uygulaması bulunan bir kurumun uygulamalarının tek bir noktadan elektronik imza doğrulama ve gelişmiş elektronik imza formatlarına dönüştürme işlemlerinin yapılabileceği merkezi bir elektronik imza servisi önerisi yapılacaktır.

II. ELEKTRONİK İMZA

Elektronik imza, en basit anlatımı ile imzalanmak istenen verinin özet değerinin alınarak imzalayan kişinin özel anahtarı ile asimetrik şifreleme algoritmasına tabi tutulması ile elde edilir. İmza verisi imzalanan verinin yanına konarak karşı

tarafa iletildiğinden herhangi bir gizlilik söz konusu değildir, imzalanan belgenin içeriği görülebilir durumdadır. Karşı taraf belge üzerindeki imza verisini imzalayan kişinin açık anahtarı ile çözer. Bulduğu değeri, imzalanan verinin özet değerini olarak karşılaştırır. Eğer aynı ise imza geçerlidir.

Elektronik imza;

- Bütünlük (integrity),
- Kimlik doğrulama (authentication),
- İnkâr edilemezlik (non-repudiation),

özelliklerini sağlar.

İmzalanan bir verinin içeriğinin değiştirilmesi durumunda imza doğrulama aşamasında yapılan özet değeri karşılaştırma işleminde eşitlik sağlanamayacak ve imza geçersiz hale gelecektir. Dolayısıyla veri bütünlüğü kullanılan algoritmalar ile sağlanmaktadır.

İmza, imzayı oluşturan kişinin açık anahtarı ile doğrulandığından ve bu imzayı oluşturacak özel anahtarın kime ait olduğu ESHS tarafından verilmiş olan elektronik sertifikadan tespit edilebildiğinden kimlik doğrulamanın yanı sıra inkâr edilemezlik de sağlanmaktadır. İmzayı oluşturan özel anahtar sadece imza sahibinde olduğundan sertifika sahibi elektronik imzanın kendi sertifikası ile oluşturulduğunu inkâr edemez. Ancak bütünlük ve kimlik doğrulamadan farklı olarak inkâr edilemezlik konusunda bazı aykırı durumlar ortaya çıkmaktadır. Örneğin; kişi, özel anahtarının yer aldığı güvenli imza oluşturma aracını kaybettiğini veya çaldığını ve sertifikasını iptal ettirdiğini, bu imzanın da sertifikayı bulan kişi tarafından oluşturulmuş olabileceğini iddia edebilir. Bu durumda açık anahtar altyapısında tanımlı zaman damgası, sertifika iptal listesi (SİL), çevrimiçi sertifika durum protokolü (ÇİSDUP) gibi mekanizmalara duyulan ihtiyaç ön plana çıkar.

Elektronik imzanın geçerliliği imzayı oluşturan sertifikanın geçerliliğine doğrudan bağlı olduğundan imza kontrol edilirken sertifikanın imza tarihinde geçerli olup olmadığının kontrol edilebilmesi büyük önem taşımaktadır. Belgelerin sadece transferi aşamasında imza kontrolünün yeterli olduğu durumlarda imzanın oluşturulduğu tarih verisine ihtiyaç olmayabilir. Örneğin; bir web uygulamasına girişte yetkilendirme amacıyla imza kullanıldığı durumlarda imzalı veri saklanmayacak ise imzanın o an için sertifika iptal durumunun kontrol edilmesi yeterli olabileceken, uzun süre saklanması gereken belgelerin üzerindeki imzaların ne zaman oluşturulduğunun tespit edilebilmesi ileride yaşanabilecek ihtilaf durumlarında inkâr edilemezlik özelliğinin sağlanabilmesi için büyük önem taşır. Bu makalenin ilerleyen kısımlarında, imza zamanının tutulması ve uzun süre geçerlilik konularına daha ayrıntılı olarak değinilecektir.

III. ETSİ GENİŞLETİLMİŞ İMZA FORMATLARI

Elektronik imzalı verilerin saklanması ve iletilmesi için günümüzde yaygın olarak kullanılan standartlar RSA Laboratories[8] tarafından 1991 yılında yayınlanmış PKCS (Public Key Cryptography Standards) standartlarının

geliştirilmesi ve genişletilmesiyle oluşturulmuştur. PKCS #7 standardı kriptografik mesaj söz dizimini ASN.1 (Abstract Syntax Nonation One) formatında tanımlamıştır. Bu standart daha sonra The Internet Engineering Task Force (IETF)[9] tarafından yayınlanan RFC (Request For Comment) dokümanları ile (RFC2315-PKCS7, RFC2630-CMS, RFC3369-CMS, RFC3852-CMS, RFC5652-CMS) [3] geliştirilmiştir.

CMS standardı şifreli, imzalı vb. kriptografik işleme tabi tutulmuş verilerin saklanması ve iletilmesi için esnek bir yapı sunar. Bu standartta kullanıcıların ihtiyaçlarına göre kullanabilecekleri eklenti alanları tanımlanmış ve ihtiyaca göre özelleştirilmesine olanak verilmiştir. Verinin hangi formatta ve yapıda tutulacağını tanımlarken imzalı bir verinin uzun süre geçerliliğinin sağlanması gibi konularda yapılması gerekenler bu standardın konusu olmayıp, bu standardı genişleten başka standartların konusu olmuştur.

Avrupa Telekomünikasyon Standartları Enstitüsü (The European Telecommunications Standards Institute-ETSI) [10] elektronik imza özelinde CMS standardını genişten TS 101 733[4] standardını yayınlamıştır. Türkiye’de de e-devlet uygulamalarında yaygın olarak kullanılan bu standartta elektronik imzanın kullanıldığı yerlere ve gereksinimlere göre gelişmiş elektronik imza formatları tanımlanmıştır.

ETSI’nin elektronik imzalı verilerin ASN.1 yerine XML tabanlı olarak tutulmasını sağlayan ve TS 101 733’deki imza formlarının aynı şekilde yer aldığı TS 101 903[5] standardı da uzun süre geçerlilik konularındaki sorunlara aynı şekilde çözümler getirmektedir. Bu makalede TS 101 903 standardına değinilmeyecektir.

Aşağıda ETSI TS 101 733 v.1.7.4 Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CADES) standardında tanımlanmış elektronik imza formatları ve ne sağladıkları kısaca açıklanmıştır;

CADES-BES (Basit Elektronik İmza)

CMS formatını temel alan bu formatta CMS standardında tanımlanmış olan zorunlu imza eklentilere ek olarak yeni zorunlu ve isteğe bağlı imza eklentileri tanımlanmıştır. Bu imza formatında imzanın uzun süre geçerliliğinin sağlanmasına yönelik eklentiler yoktur. Örneğin bu formatta tanımlanmış olan imza zamanı eklentisi imzalama işlemini yapan yazılım tarafından eklenir ve herhangi bir güvenilirlik sağlamaz. Bu yüzden imza zamanı verisi beyan edilen imza zamanı olarak kabul edilir ve sertifikanın imza tarihinde geçerli olup olmadığı kontrol edilirken bu tarih dikkate alınmaz. Sertifikanın imza tarihindeki geçerliliğinin kontrolü için zaman damgasına ihtiyaç duyulacaktır. Bu yüzden CADES-BES formatının uzun süre geçerliliğinin önemli olmadığı noktalarda kullanımının uygun olacağı düşünülmektedir.

CADES-EPES (Politika Temelli Elektronik İmza)

Bu formatta imzanın doğrulanması için gerekli bir elektronik imza politikası dokümanına referans veren bir eklenti

tanımlanmıştır. Kurumsal bir e-imza politikası tanımlamış kurumlarda CADES-BES'in yerine kullanılabilir.

Doğrulama Verisini İçeren Elektronik İmza Formatları

CADES-T (Zamanlı Elektronik İmza)

Elektronik imzanın doğrulanmasında temel faktörlerden birisinin imzanın oluşturulduğu tarihte imza sertifikasının geçerli olup olmadığının tespiti olduğu düşünüldüğünde güvenilir imza zamanının gerekliliği ortaya çıkmakta bu da zaman damgası ile ya da ETSI'nin alternatif olarak sunduğu zaman işareti kavramı ile sağlanmaktadır. CADES-T formatı CADES-BES veya CADES-EPES'e eklenecek güvenilir zaman verisi ile oluşturulmaktadır.

Zaman işareti kavramında; zaman damgası gibi imzaya eklenen bir veri yoktur. İmza zamanını tutma yükümlülüğü bu hizmeti sağlayan güvenilir hizmet sağlayıcılardır (Trusted Service Provider - TSP). Ülkemizde mevcut durumda zaman işareti kavramının kullanıldığı bir örnekle karşılaşılmamıştır.

Zaman damgası ise, imzaya bir eklenti olarak eklenen ve yine güvenilir hizmet sağlayıcılardan alınan güvenilir bir zaman verisidir. Bu veri imza verisi ile ilişkili olarak oluşturulur ve üzerinde güvenilir hizmet sağlayıcının imzası vardır. Zaman damgası ile imzanın zaman damgası tarihinden önce oluşturulmuş olduğu kesinlik kazanır ve sertifika daha sonra iptal edilmiş olsa da imza, sertifika iptalinden ötürü geçerliliğini yitirmeyecektir.

Ülkemizde zaman damgası hizmeti tüm ESHS'ler tarafından verilmektedir. İmzanın uzun süre geçerliliğinin sağlanması gereken durumlarda zaman damgasının zaruri olduğu düşünülmektedir. Bilgi Teknolojileri ve İletişim Kurumu "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"inde[11] de belirtilen CWA14171[7] dokümanında da bu durum vurgulanmaktadır.

CADES-C (Doğrulama Verisi Referanslı Elektronik İmza)

İmzanın geçerliliğinin kontrolü için gerekli olan imza sertifikaları, ÇİSDUP cevapları ve sertifika iptal listeleri (SİL) gibi verilerin referanslarının tutulduğu eklentilerin CADES-T formatına eklenmesi ile elde edilir. Doğrulama verilerinin kendileri yerine referanslarının tutulması ile gereksiz veri tekrarının önüne geçilir ve imza verisi içerisinde ciddi yer işgal edecek doğrulama verileriyle imzalı verilerin büyümemesi sağlanmış olur. İmza referansları tutulan doğrulama verileri farklı bir depolama ortamında saklanabilir. Uzun süre imza geçerliliğinin önemli olduğu uygulamalar için en etkin çözümü sunan imza formatı olduğu düşünülmektedir.

CADES-X (Doğrulama Verisini İçeren Gelişmiş Elektronik İmza Formatları)

CADES-C formatındaki imzaya tüm doğrulama verilerinin eklenmesi ile oluşturulur. ETSI bu format için ihtiyaca göre kullanılmak üzere CADES-X Long, CADES-X Type 1,

CADES-X Type 2, CADES-X Long Type 1, CADES-X Long Type 2 türlerini tanımlamıştır. Bu format ile imzalı verinin yaşadığı sistemden bağımsız olarak kendi kendini doğrulayabilmesi sağlanır. Fakat SİL gibi görece büyük boyuttaki verilerin imzalı veriye eklenmesi ile imzalı verilerin büyüklükleri artmakta bu da çok sayıda imzalı veri tutulan bir sistem için depolama maliyetini artırmaktadır.

Bu formatın özellikle imzalı belge kurum dışına çıkacağı ya da arşivleneceği zaman kullanılmasının daha etkin bir yaklaşım olacağı düşünülmektedir.

CADES-A (Arşiv Elektronik İmzası)

İmza oluşturulurken kullanılan kriptografik algoritmaların kırılması veya güvenilirliklerini yitirmelerine karşı ya da imza daha önce kullanılan zaman damgaları üzerindeki imzayı oluşturan sertifikaların iptali ya da geçerlilik süresinin dolması gibi durumlar gerçekleşmeden önce arşiv zaman damgası olarak imzanın korunması gerekir. Bu işlemin zamanla tekrar edilmesi de gerekmektedir (CWA14171[7]).

IV. MERKEZİ BİR ELEKTRONİK İMZA SERVİSİ ÖNERİSİ

Ülkemizde elektronik imza kullanmakta olan kurum ve kuruluşlarda farklı ihtiyaçlara yönelik tasarlanmış elektronik imza desteği sunan yazılımlarda tüm ESHS'lerden alınmış nitelikli elektronik sertifikalar kullanılmaktadır. Bu da her uygulamanın imza oluşturma ve doğrulama işlemlerinde sertifika iptal kontrolü, zaman damgası alma gibi işlemleri ESHS'lerin sunucularına ayrı ayrı erişerek yapmalarını gerektirmektedir.

Her imzalama işleminden önce ya da imzalı belge veya belgeler kullanıcıya gösterileceği zaman, belgenin üzerindeki imzalar kontrol edilmekte ve geçerlilik bilgisi kullanıcıya gösterilmektedir.

Üzerinde 4 imza olan bir belge için imzaları oluşturan sertifikalar aşağıdaki gibi varsayımsal olarak farklı otoritelerden alınmış olsun;

İmza	ESHS	Kök Sertifika	ÇİSDUP Hizmeti	SİL Boyutu
1.İmza	A	KOK A	Var	10KB
2.İmza	B	KOK B	Sorunlu	50KB
3.İmza	C	KOK CA	Yok	100KB
4.İmza	C	KOK CB	Yok	500KB

İmzayı kontrol edecek yazılımın eğer sertifika iptal listesi ve ÇİSDUP cevabı depolama gibi bir özelliği yok ise, her imza için varsa ÇİSDUP sunucusundan yoksa sertifika iptal listesini indirerek sertifika iptal durumunu kontrol etmek durumundadır. Sertifika iptal kontrolü yapılırken sertifika iptal listesi, ÇİSDUP cevabı ve kök sertifikalar üzerindeki bütün imzalara ait sertifikaların da iptal durumu kontrol edilmektedir. Yukarıdaki gibi bir örnekte her imza kontrolünde sertifika iptal kontrolü için 1 MB'a yakın bir

verinin ESHS sunucularından indirilmesi gerekebilmektedir. Ayrıca sertifika iptal listelerinin gün geçtikçe büyüdüğü hesaba katıldığında ve yukarıdaki hesaplamanın sadece bir imzalı belge için yapıldığı düşünüldüğünde sertifika iptal kontrolü işlemlerinin zaman içinde oldukça fazla yük getireceği görülebilir.

Ayrıca imzalı belgelerin doğrulanması gereken bazı noktalarda ağ bağlantısı da olmayabilir. Bu gibi durumlarda ya iptal listelerinin lokal sunucularda depolanması ya da ETSI'nin tanımlamış olduğu doğrulama verisini içeren imza formatlarının kullanılmasının önemi ortaya çıkmaktadır.

Mevcut durumda ülkemizdeki kurumsal uygulamalarda en yaygın kullanılan elektronik imza formatı ETSI TS 101 733 standardındaki CAdES-BES formatıdır. Bu format yukarıda CAdES imza formatları ile ilgili bilgiler verilirken de açıklandığı gibi imza doğrulama için gerekli birçok önemli veriyi içermez. Bu verilerden en önemlisi güvenilir zaman verisidir. Sertifika geçerlilik süresi dolduğunda ya da iptal edildiğinde imzanın doğrulanabilmesi ve inkar edilemezlik özelliğini sağlayabilmesi için imzanın ne zaman oluşturulduğunun bilinmesi gerekir. Bu da zaman damgası ile mümkün olabilmektedir. Mevcut uygulamalarda ya bu duruma gereken hassasiyetin gösterilmediği ya da konu hakkında yeterli bilincin oluşmadığı gözlemlenmektedir.

Kurumların bünyesinde geliştirilmekte olan her yazılım projesinden, farklı kişiler, ekipler veya firmalar sorumlu olabilmektedir. Her projede elektronik imza yazılım kütüphaneleri uygulamayı geliştiren ekibin insiyatifi ile kullanılmaktadır. Kurumsal yazılımlarda elektronik imza entegrasyonu yapılan noktalarda herkesin aynı bilgi ve bilinçle hareket etmesi mümkün olmamaktadır. Elektronik imza ve açık anahtar altyapısı konularında yeterli tecrübesi olmayan bir kişinin her bakımdan yeterli bir imza yazılımı kütüphanesi kullanmasına rağmen ciddi eksiklik ve hatalar yapması olasıdır. Kurum bünyesindeki bir elektronik imza yazılımının CWA 14170 ve CWA 14171 dokümanlarına uygun olması ve bu konuda Türkiye'de söz sahibi olan Kamu Sertifikasyon Merkezi'nin "Kamu SM E-İmza Uygulaması Kontrol Listesi"nin kriterlerini sağlaması kurumda kullanılan diğer yazılımların kriterlere uygun olduğu anlamına gelmeyecektir.

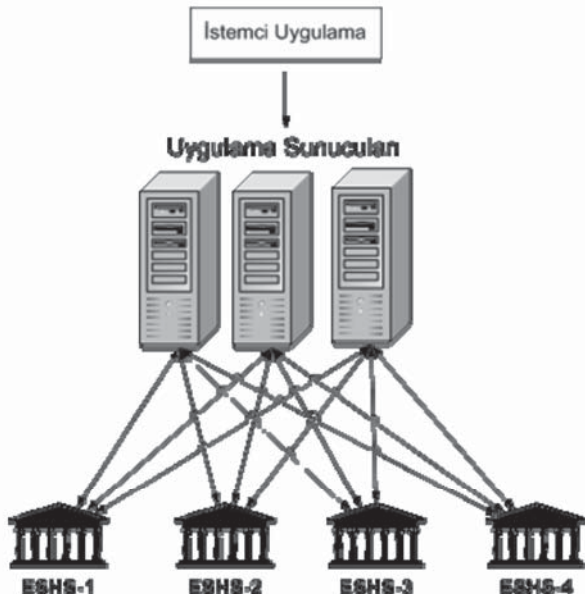
Tüm bu sorun ve gereksinimlerden hareketle, kurum ve kuruluşların bünyelerindeki yazılımların elektronik imza doğrulama, zaman damgası alma, elektronik imzaları ETSI gelişmiş imza formatlarına çevirme ve arşiv imzası oluşturma gereksinimlerinin kurum içerisinde tek bir noktadan sağlanması için merkezi bir elektronik imza servisinin ciddi getirileri olacaktır. Böylece uygulama geliştiricilerin imza işlemlerinin karmaşasından bağımsız olarak çalışabilmeleri sağlanmış olacaktır.

Böyle bir servisin aşağıdaki özellikleri sağlaması ile imza işlemlerinde hem tutarlılık hem güvenlik hem de kolaylık sağlanacağı düşünülmektedir;

1) Yazılım kurum bünyesindeki e-imza kullanılan tüm yazılımlar tarafından kullanılabilir kurum içerisine hizmet verecek bir web servisidir.

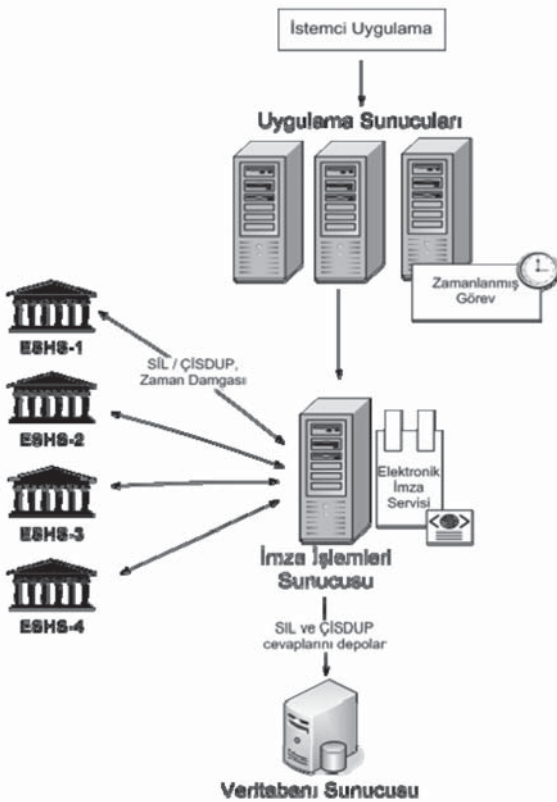
- 2) İmza ile ilgili işlemleri mümkün olduğunca uygulamalardan bağımsız olarak tek bir noktada toplamak, muhtemel hatalı kullanımların önüne geçecek, herkesin konuya hakim olma gereksinimini ortadan kaldıracak ve uygulamaların imza işlemlerinde tutarlı çalışmasını sağlayacaktır.
- 3) Her uygulama sunucusu mükerrer olarak SİL indirmeyecek, ÇİSDUP, LDAP (Lightweight Directory Access Protocol) ve Zaman Damgası sunucularına bağlanmayacak, tüm bu gereksinimler e-imza servisinde karşılanmış olacaktır.
- 4) Zaman damgası alma işlemi istemci uygulamalarda (applet, masaüstü uygulaması vb.) yapılmak yerine web servisinde sağlanacaktır. Böylece her uygulamanın zaman damgası sunucusuna bağlanması, erişim için gerekli kullanıcı adı ve parola bilgilerini istemci uygulama içerisinde barındırmasına da gerek kalmayacaktır. İmza oluşturulurken istemci yazılım, web servisinden imzayı CAdES-T formatına çevirmesini isteyecektir.
- 5) İmzalı verilerden doğrulama referansı verilerini içermeyen formatta olanları sunucu üzerinde belirli aralıklarla çalışan zamanlanmış bir görev sertifika iptal bilgilerinin hazır olmasının ardından (Standart dokümanından tanımlanmış olan "Grace Period" beklenmiş ise.) imzayı web servisi aracılığıyla CAdES-C formatına dönüştürerek kaydedecektir.
- 6) Uygulamalar bir imzalı verinin geçerliliğini kendisi kontrol etmeyecek, bu hizmeti e-imza servisten alacaklardır. Böylece e-imza servisinin çalıştığı sunucuda kullanılacak bir SİL depolama mekanizması ile ESHS sunucularından çekilecek veri minimize edilebilecektir.

İmza işlemlerinin merkezi bir uygulama ile ele alınmadığı durumlardaki yapı Şeki 1'de ifade edilmeye çalışılmıştır.



Şekil 1 Merkezi elektronik imza servisi kullanılmayan yapı

İmza işlemlerinin merkezi bir web servisi tarafından ele alındığı önerilen yapıda ESHS bağlantısı gerektiren işlemler, aşağıdaki şekilde de ifade edildiği gibi sadece elektronik imza servisi tarafından yapılacaktır.



Şekil 2 Merkezi elektronik imza servisi kullanılan yapı

Elektronik İmza Servisi Yetenekleri

A. Sertifika Geçerlilik Kontrolü

Parametre olarak verilen sertifikanın parametre olarak verilen tarihteki geçerliliğini varsa depodaki kayıtlı SİL veya ÇİSDUP cevaplarından, depoda yok ise ÇİSDUP sunucuna bağlanarak veya güncel SİL'i ESHS sunucularından indirerek kontrol eder ve geçerlilik durumunu verir. Sonraki kontrollerde kullanılmak üzere SİL'i ve ÇİSDUP cevaplarını kaydeder.

B. İmzalı Veri Geçerlilik Kontrolü

Verilen imzalı veri üzerindeki imzaların geçerliliğini kontrol eder ve geçerlilik durumunu verir. Sertifika iptal durumu kontrollerini yukarıda sertifika geçerlilik kontrolünde de anlatıldığı şekilde yapar.

C. CAdES BES Formatından CAdES-T Formatına Dönüştürme

Parametre olarak verilen imzalı veri üzerindeki zaman damgası olmayan imzalara zaman damgası alır ve imzaları CADES-T formatına dönüştürüp verir.

D. CAdES-T Formatından CAdES-C Formatına Dönüştürme

Belge üzerindeki imzaların geçerliliğini kontrol eder. İmzalara doğrulama verileri ve ilgili referansları ekleyerek belge üzerindeki imzaları CAdES-C formatına dönüştürüp verir. Referansını imzaya koyduğu ÇİSDUP cevabını veya SİL'i veritabanında saklar.

E. CAdES-C Formatından CAdES-X Long Formatına Dönüştürme

Kurum dışına gidecek bir belgenin tüm doğrulama verilerini (Veritabanında bulunan SİL veya ÇİSDUP cevaplarını) ekleyerek CADES-X Long formatına dönüştürüp verir. Özellikle kurum dışı yazışmalarda ya da belge arşivleneceği zaman kullanılır.

F. CAdES-A Formatına Dönüştürme

Verilen imzalı belge üzerindeki imzalara arşiv zaman damgası alır ve CADES-A formatına dönüştürür. CADES-X Long, CADES-X Long Type 1 veya CADES-X Long Type 2 formatında olmayan imzaları öncelikle CADES-X Long formatına çevirir ve daha sonra arşiv zaman damgası alır.

Daha önce CAdES-A formatına dönüştürülmüş verilere tekrar arşiv zaman damgası alınmak istendiğinde de bu özellik kullanılır.

V. SONUÇ

Ülkemizde elektronik imza 2004 yılında yayımlanan Elektronik İmza Kanunu[1] ile resmîyet kazanmış ve bugüne dek birçok kurumda ıslak imza gerektiren bazı süreçler elektronik ortama taşınmıştır. Elektronik imza kanununda da belirtildiği gibi elle atılan imza ile aynı hukuki sonucu doğurmaktadır. Fakat elle atılan imza herhangi bir ek çaba göstermeksizin uzun süre geçerliliğini korur iken elektronik imzanın uzun süre geçerli kalmasının sağlanması için kullanılmakta olan uygulamalarda ek önlemler alınması gerekmektedir. Mevcut durumda yaygın olarak kullanılmakta olan ETSI CAdES-BES formatındaki elektronik imzalı

verilere öncelikle zaman damgası alınarak güvenli zaman verisinin eklenmesi ve ardından ihtiyaca uygun olarak ETSI'nin tanımlamış olduğu gelişmiş imza formatlarına dönüştürme işlemlerinin yapılması önem taşımaktadır.

Uzun süre geçerli imzaya geçişte; standart kullanımı sağlamak, veri tekrarını önlemek, imza oluşturma ve doğrulama aşamalarındaki gereksiz ağ trafiğinin önüne geçmek için kurum bünyesinde merkezi bir elektronik imza servisinin kullanımı ciddi getiriler sağlayacak bir çözüm olabilir.

TEŞEKKÜR

Bu çalışmanın şekillenmesindeki katkılarından dolayı Sayın Doç. Dr. Ramazan Acun ve Sayın Gonca Hülya Doğan'a teşekkür ederim.

KAYNAKLAR

- [1] 5070 sayılı Elektronik İmza Kanunu:
<http://www.mevzuat.adalet.gov.tr/html/1328.html>
- [2] Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik
<http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/e-imza-yonetmelik.pdf>
- [3] IETF RFC 5652 (2009): "Cryptographic Message Syntax".
- [4] ETSI TS 101 733 V1.7.4 (2008-07) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)
- [5] TS 101 903 - V1.4.1 (2009-06) - XML Advanced Electronic Signatures (XAdES)
- [6] CWA 14170 CEN. Workshop Agreements: " Security requirements for signature creation applications".
- [7] CWA 14171 CEN. Workshop Agreements: "Procedures for electronic signature verification".
- [8] <http://www.rsa.com/rsalabs/node.asp?id=2124>
- [9] <http://www.ietf.org/>
- [10] <http://www.etsi.org/WebSite/Technologies/ElectronicSignature.aspx>
- [11] Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ
<http://www.tk.gov.tr/Duzenlemeler/Hukuki/tebligler/e-imza-teblig.pdf>

Avrupa Birliği Bilişim Sistemleri Güvenliği Yönelimleri ve Türkiye'nin Durumu

Mehmet Kara

Özet —Son yıllarda internet, e-posta, web servisleri, e-devlet, e-sağlık, e-eğitim, e-ticaret gibi hayatımızı kolaylaştıran pek çok alanda yaygın olarak kullanılmaya başlanmıştır. Bu uygulama alanlarına her geçen gün yenileri eklenmektedir. Diğer taraftan internetin yaygın olarak kullanılmaya başlanması ile bilinçsiz kullanıcılar farkında olmadan, kötü niyetli kişileri ise bilinçli olarak bilgisayar sistemlerine zarar vermeye başlamıştır. Son yıllarda bu zararların boyutu ekonomik ve prestij kayıplarının yanında siber savaş olarak adlandırılan bir ülkedeki saldırganların diğer bir ülke sistemlerine topluca saldırması şeklinde büyük çaplı saldırıları da kapsayacak şekilde genişlemiştir. Bu tehditlerin ortadan kaldırılması ya da risklerinin azaltılması için birçok ürün ve çözüm geliştirilmiş ve hala geliştirilmektedir.

Avrupa Birliği ülkeleri bilişim teknolojilerinin kullanılmaya başlandığı ilk yıllardan beri bilişim teknolojileri güvenliği konularında da önemli çözümler sunmuşlardır. Bu makalede Avrupa Birliği'nin özellikle Çerçeve Programlar (Frameworks Programme) aracılığı ile bilişim teknolojileri güvenliği konularında yaptığı araştırmalara ve desteklediği proje başlıklarına yer verilmesi yanında son yıllarda bilişim sistemlerin alanında birçok projeyi destekleyen Türkiye'de yapılan çalışmalar ele alınmış ve yapılaması gerekenler irdelenmiştir.

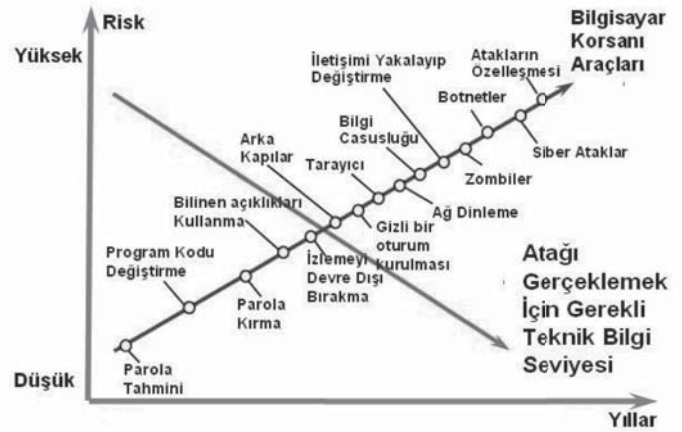
Index Terms—Bilgi iletişim teknolojileri, bilişim teknolojileri güvenliği, çerçeve programlar

I. GİRİŞ

İnternetin yaygın olarak kullanılmaya başlaması, e-posta, web servisleri, e-devlet, e-sağlık, e-eğitim, e-ticaret gibi insan hayatını kolaylaştıran pek çok uygulamayı da beraberinde getirmiştir. Aynı zamanda internetin yaygın olarak kullanılmaya başlanması bilgisayar güvenlik problemlerini de artırmıştır. Bilgisayar olaylarının bir kısmına bilinçsiz kullanıcılar bir kısmına da bilerek sisteme zarar vermek isteyen kötü niyetli kişiler neden olmaktadır.

1980'li yıllarda bilgisayar haberleşmelerinde TCP/IP protokol ailesi büyük kabul görmüş ve internet bu protokol aracılığı ile dünya çapında yaygınlaşmıştır. İnternetin yaygınlaşması ile bilgisayar haberleşmelerindeki atakların sayısı ve çeşidi de artmıştır [1]. Bu ataklar karşısında şifreleme, bütünlük kontrolü, kimlik doğrulama, yetkilendirme, antivirüs programları gibi güvenlik çözümleri geliştirilmeye çalışılmıştır. İlk çıkan ataklar daha çok basit kod yürütme, parola tahminleri gibi etkisi ve olasılığı düşük ataklar olmasının karşın süreç içerisinde atakların karmaşıklığı

ve etkileri artmıştır. Buna karşın bu atakları kullanabilmek için gereken bilgi düzeyi düşmüştür. Çünkü bu bilgiler çoğunlukla internet üzerinden kontrolsüz olarak yayılmıştır. Şekil 1'de atakların zamana göre değişimleri, etkileri ve onları kullanabilmek için gerekli bilgi düzeyi görülmektedir [2].



Şekil 1 Atakların gelişimi

Bilgisayar zararlı yazılım ve ataklarına karşı proaktif önlemler alınması ve bu sistemlerde güvenliğin sağlanması için birçok kuruluş ve ülke tarafından çok sayıda araştırma geliştirme projesi yapılmış ve hala yapılmaktadır. Bu araştırmalar sonucunda bilgisayar sistemlerinde kullanılan antivirüs yazılımları, güvenlik duvarları, VPN yazılım/donanımları, saldırı tespit ve önleme sistemleri, içerik kontrolcüler, merkezi yönetim yazılımları gibi teknik çözümler üretilmiştir. Teknik çözümler yanında iletişim sistemlerinin güvenli olarak tasarlanmasını, test edilmesini ve yönetilmesini sağlayacak TCSEC (Trusted Computer System Evaluation Criteria), ITSEC (Information Technology Security Evaluation Criteria), Ortak Kriterler, BS 7799, BS 17799, ISO/IEC 27001 gibi standartları geliştirmişlerdir [3,4]. AB (Avrupa Birliği) ülkeleri bu güvenlik ürünleri ve standartlarının geliştirilmesinde etkin rol almışlardır. Bugün dünyada 26 ülke tarafından kabul edilen Ortak Kriterler standardının geliştirmesine öncülük etmişlerdir.

Hala da AB veya üye ülkeler bazında BT (Bilişim Teknolojileri) güvenliği konularında ürünler, çözümler, politikalar ve standartlar üretmek için çalışmalar yapmaktadırlar.

2007 yılında EDA (European Defence Agency) yönetim kurulu toplantısında güvenlik bütçelerinin %2'sinin güvenlik

konularında araştırma geliştirme yapılması için ayrılmasının tavsiye edilmesi, güvenliğe verilen önemi göstermektedir. [11].

Günümüzde ülkeler BT güvenliği araştırma geliştirme projelerine hem çok büyük bütçeler hem de büyük iş güçleri ayrılmaktadır. Çok büyük bütçe ve insan kaynağı ayrılmasının başlıca nedenleri internetin insan hayatında vazgeçilmez bir araç olması, e-devlet, e-ticaret, e-sağlık, e-egitim, askeri, iletişim, araştırma, eğlence gibi birçok uygulama için çok etkin ve ekonomik çözümler sunmasıdır. Ülkeler ve şirketler bilgisayar güvenliği alanlarındaki uygulamaları kendi ülkelerinde kullanmanın yanında diğer ülkelere satarak hem teknolojik hem de ekonomik olarak pazarda öne geçmek istemektedirler. Örneğin 11 Eylül 2001 olaylarından sonra ABD’de Yurt Güvenliği Departmanını kurulmuştur (Department of Homeland Security). 2004 yılında bu departmana 34 M\$ doğrudan bütçe ayrılmış ve yıllar içerisinde de bu bütçenin değerini arttırmıştır. Bu durum ABD’nin bu alanlarda lider rol oynamasına ve teknolojiyi yönetmesine neden olmuştur [5]. AB ülkeleri de yeni teknolojilerdeki başarısını sürdürmek ve liderliği ele geçirmek için başta Çerçeve Programları (Framework Programme) olmak üzere birçok proje ve çalışma yapmaktadır. Bu makalede AB’nin BT güvenliği konularında yaptığı çalışmaları ve desteklediği projeleri inceleyerek gelecekte hangi konularda araştırma geliştirme çalışmalarının yapılabileceğine ışık tutmaya çalışma yanında Türkiye’deki durumu irdeleyeceğiz.

Bu makale altı bölümden oluşmaktadır. Giriş bölümünde bilgi güvenliğinin gelişimi AB ülkelerinde bu konularda yapılan temel çalışmalar ele alınmıştır.

İkinci bölümde çerçeve programların gelişimi, 7. Çerçeve Programı’nın tematik alanları ve bütçe dağılımı hakkında bilgi verilmiştir.

Üçüncü bölümde çerçeve programları içinde yapılacak çağrılarda ele alınacak konuların tespit edilmesinde kullanılan projeler ve kurumların yapısı ele alınmıştır.

Dördüncü bölümde 7. Çerçeve Programı içerisinde yer alan çağrılarda BT güvenliği alanlarında istenilen projelerden bahsedilmiştir.

Beşinci bölümde Türkiye’de yapılan çalışmalar ele alınmıştır.

Altıncı ve son bölümde BT güvenliği konularında gelecekte yapılabilecek çalışmalar irdelenmiştir.

II. AB ÇERÇEVE PROGRAMLARI

AB projeleri ilk olarak 1984 yılında başlatılmıştır. Temel amacı Avrupa’daki dağıntık ulusal bilim, teknoloji, politika ve uygulamalarının birbirine yaklaştırılması ve AB’nin rekabet gücünü artırmak olarak tanımlanmıştır. Bu amaç doğrultusunda pazarda var olan gücünü geliştirmek ve lider olmak hedeflenmektedir. Çerçeve programların bütçeleri Çerçeve Program 1’den itibaren artarak devam etmiştir. Hali hazırda 2007-2013 yılları arasında devam edecek olan 7. Çerçeve Programı yürütülmektedir. Bu programın toplam

bütçesi 50.521 Milyar Euro’dur. Türkiye bu programlara aday ülke statüsünde katılma olup üye ülkelerle aynı statüdedir. Güvenlik başlığı bu projeler içinde önemli bir yer tutmaktadır.

7. Çerçeve Programı’nın ana yapısı “İş Birliği” (Cooperation), “Marie Curie Etkinlikler” (Marie Curie Actions), “Fikirler” (Ideas) ve “Kapasiteler Özel Programı” (Capacities) olmak üzere dört programdan oluşmaktadır [6].

A. İş Birliği (Cooperation)

10 başlık altında AB üye ve aday ülkelerin ihtiyaçları doğrultusunda, Avrupa Komisyonu tarafından belirlenen başlıklarda açılan çağrılara yönelik hazırlanan projeler arasında çeşitli kriterlere göre seçim yapılmakta ve uygun görülenler desteklenmektedir. Avrupa komisyonu hangi araştırmalara ve teknolojilere ihtiyaç duyduğunu tanımlamakta ve bu ihtiyaçları karşılayacak projeleri desteklemektedir.

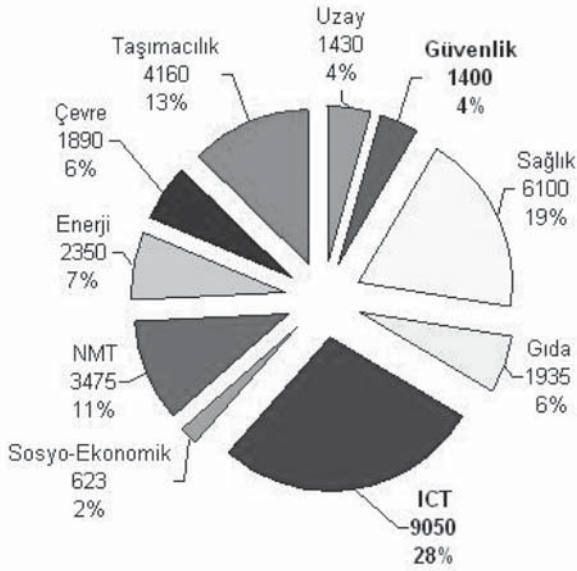
İş birliği programı için 2007-2013 yılları için ayrılan bütçe 32.4 Milyar Euro’dur. Bu program çerçevesinde desteklenecek başlıklar aşağıda verilmiştir:

- Sağlık
- Gıda, Tarım ve Biyoteknoloji
- **Bilgi ve İletişim Teknolojileri**
- Nanobilimler, Nanoteknolojiler, Malzemeler ve Yeni Üretim Teknolojileri (NMT- Nanosciences, Nanotechnologies, Materials and new Production Technologies)
- Enerji
- Çevre (İklim değişikliği dahil)
- Ulaştırma
- Sosyo-Ekonomik ve Beşeri Bilimler
- **Güvenlik**
- Uzay

Bu alanların her biri için ayrılan bütçe (Milyar Euro olarak) ve toplam bütçe içindeki yüzdesi Şekil 2’de verilmiştir. Buna göre Bilgi ve İletişim Teknolojileri (ICT Information and Communication Technologies) konusunda ayrılan bütçe 9.1 Milyar Euro, Güvenlik konusunda ayrılan bütçe ise 1.4 Milyar Euro’dur. Bu iki alan %32’lik bütçe oranı ile bu program içinde en büyük paya sahiptir [7]. Bu alanın tamamı BT güvenliği değildir. Sınır güvenliği, kıyı güvenliği, nükleer, kimyasal, biyolojik ataklara karşı güvenlik gibi birçok alanı da içermektedir. Fakat bu makalede sadece BT güvenliği alanlarındaki proje başlıkları ele alınacaktır.

Türkiye çerçeve programlarına 2002-2006 yıllarında arasında yapılan FP6 ile birlikte katılmaya başlamış ve hali hazırda FP7 programlarından AB üye ülkeleri ile eşit koşullarda yararlanabilmektedir.

AB projeleri yanında uluslar kendi içlerinde ve diğer uluslarla ikili programlarla BT güvenliği alanında ürün ve proje geliştirilmesini desteklemektedirler.



Şekil 2 FP7 bütçesinin alanlara göre dağılımı

III. AB BİLİŞİM TEKNOLOJİLERİ GÜVENLİK POLİTİKASINI OLUŞTURAN PROJELER VE KURUMLAR

AB Çerçeve Programlarında bilgi iletişim teknolojileri ve güvenlikle ilgili desteklenecek alanları belirlemek için 2000 yılından bu tarafa birçok kurul, kurum oluşturmuş (Group of Personalities, ESRAB, ESRIF, JRC, EDA, ENISA) ve projeler yapılmıştır. Bu çalışmalar yanında çeşitli bilimsel toplantılar düzenleyerek geleceğe yönelik ihtiyaçları belirlemeye çalışmış ve çerçeve programlarında desteklenecek proje alanlarını belirlemiştir.

A. ESRIF

ESRIF (European Security Research and Innovation Forum) 2007 yılı Eylül ayında 31 ülkeden 64 üyenin katılımı ile kurulmuştur. Özel sektör, kamu kurumları, araştırma enstitüleri, üniversiteler ve sivil toplum örgütlerinden gelen katılımcılardan oluşmaktadır. ESRIF'in görevleri orta ve uzun dönemde AB'nin güvenlik politikasını oluşturmak, 2004-2007 yılları arasında politikaları oluşturmuş olan GoP (Group of Personalities) ve ESRAB'ın güvenlik politikalarının üzerine politika geliştirmek, güvenlik alanında araştırma yapan kurumlar arasındaki iş birliğini artırmak, AB'de güvenlik araştırması yapan kurumlara rehberlik etmek olarak belirlenmiştir [8].

ESRIF Avrupa Birliğinin güvenlik konularındaki kısa, orta ve uzun vadedeki araştırma ve yenilikçilik ajandasını belirlemek için ESRIA (European Security Research and Innovation Agenda) dokümanını oluşturmuştur. ESRIA beş ana hedef tanımlamaktadır:

Birincisi hedef önleme, koruma, hazırlama, cevap verme ve düzeltme adımlarından oluşan klasik güvenlik çevrimidir. Bu hedef insanların güvenliği, sivil hazırlıklar ve kriz yönetimine odaklanmaktadır.

İkinci hedef değişik tipteki ataklara karşı konulması, bilinen projelendirilmiş risklerin yanında bilinmeyen ataklar ve doğal

olayların etkilerinin azaltılması, yeni gelen teknolojilerin potansiyel risklerinin azaltılması konularını içermektedir.

Üçüncü hedef, enerji, taşımacılık, iletişim gibi kritik altyapıların güvenliğini hedeflemektedir. Sınırlı kaynaklara erişim güvenliği sağlama yanında anahtar üretim yeteneklerinin ve kapasitelerinin korunmasına yönelik güvenlik önlemlerini hedeflemektedir.

Dördüncü hedef, insan ve eşyaların kimlik, erişim, hareketlerinin güvenliğini sağlamaya çalışmakta olup sınır güvenliği ve güvenli kimlik yönetimine odaklanmaktadır.

Son hedef ise değişik alanların güvenli entegrasyonu ve öncelikli politik, stratejik kararlarla ilgilenmektedir. Örneğin uzay ve ICT gibi farklı alanlardaki teknolojilerin güvenli olarak entegre edilmesini hedeflemektedir.

B. JRC (Joint Research Center)

JRC'nin misyonu, AB politikalarının oluşmasına, gelişmesine, uygulanmasına ve izlenmesine bilimsel araştırmacılar aracılığıyla destek sağlamak olarak tanımlanmıştır. Temel yaklaşımı ise Avrupa Araştırma Alanı (European Research Area, ERA) ve 7. Çerçeve Programı kapsamında aday ülkelere bilgi transferini kolaylaştırmaktır. JRC, AB müktesebatı uyumu için, AB'ye katılım sürecindeki ülkeler ile birlikte çalışarak bu ülkelere bilimsel ve teknik destek sağlayarak ERA'nın oluşumuna katkı sağlamaktadır. JRC bu görevleri, çeşitli ülkelerde bulunan altı tane güvenlik enstitüsü aracılığı ile yapmaktadır. Güvenlik alanında birçok araştırma, proje yapmakta ve AB çerçeve programı çağrılarının oluşturulmasına önemli katkılar sağlamaktadır. JRC enstitülerinde Türk araştırmacının çalışması için JRC ve TÜBİTAK arasında protokol da imzalanmıştır.

IV. AB 7. ÇERÇEVE PROGRAMINDA BT GÜVENLİĞİ TEMALARI

AB 7. Çerçeve Programı Güvenlik (Security) [9] ve Bilgi İletişim Teknolojileri (ICT- Information Communication Technologies) [10] çağrılarında birçok alanda bilişim teknolojileri güvenlik projesi çağrısı yapılmaktadır. Güvenlik ve Bilgi İletişim Teknolojileri alanlarında yapılan çağrılarda doğrudan Bilişim Sistemleri Güvenliği ile ilgili olan başlıklar bu bölümde incelenmiştir.

A. Bilgi İletişim Teknolojileri (ICT)

1) Yaygın, Güvenilir Ağlar ve Servislerin Altyapısı

Geleceğin bilgi altyapıları milyarlarca insanı, sayısız organizasyonu, trilyonlarca aracı (kişisel bilgisayar, cep telefonu, sunucu, sensor, eşya vb.) kapsayacaktır. Bu altyapı ekonomik gelişmeye destek olacak ve ekonomideki yeni servis ve iş fırsatlarının merkezinde bulunacaktır. Üretim ve sağlık hizmetleri gibi çeşitli alanlarda bilgi ve iletişim teknolojilerinden en iyi şekilde yararlanabilmek için bu altyapının oluşturulmasına önderlik etmek özellikle önemlidir. Söz konusu olan, bu ağ ve servis altyapılarını daha sağlam, esnek ve güvenli yapabilmek için gerekli Ar-Ge çalışmaları bu

alan kapsamında desteklenmektedir.

Bu başlık altında aşağıdaki konularda projeler desteklenmektedir:

- Geleceğin ağları,
- Servislerin, yazılımların ve sanallaştırmanın interneti
- Büyük ortamların ve eşyaların interneti
- ICT güvenliği
- Ağ ortamı ve 3D internet
- Geleceğin interneti deneysel araçları ve deneysel araştırma

2) Bağımsız Yaşam ve Dahil Olma için ICT

Bağımsız yaşam, dahil olma ve katılım gibi sosyal konulardaki eğilimler geleceğin ICT'i marketini derinden etkileyecektir. Öncelikle yaşlılık, iş gücü marketini ve uzun yaşamın getirdiği bakım ihtiyaçlarını değiştirmektedir. 65 yaş üzerindeki bilişim okur yazarı sayısı gelecek on yılda önemli ölçüde artacaktır. Bu da hacmi 300 milyar Euro olması beklenen yeni servisleri kullanıma açacaktır. İkinci olarak vatandaşların yaşam kalitesinin, ekonomik durumunun ve sosyal topluma katılım oranının artması beklenmektedir. Üretkenlik artışı sonucu yeni mesleklerin oluşması, yeni servislerin ortaya çıkması ve yeni ICT marketlerinin oluşması beklenmektedir.

Üçüncü olarak bu alandaki politika ve ticari ilginin artması, dağınık durumda bulunan potansiyel ICT'lerin birleşerek bir değer oluşturması e-dahil (e-inclusion) olma araştırma ve geliştirmelerini artıracaktır.

Sonuç olarak e-dahi olma ile ilgili büyük teknolojik değişiklikler daha uyumlu, az zorlayıcı, akıllı ve kişiye özgü özellikler taşıyacaktır.

Bu başlık altında aşağıdaki konularda projeler desteklenmektedir:

- ICT ve yaşlılık
- Erişilebilir ve yardımcı ICT
- Yönetişim ve politika modelleme için ICT

3) Yeni ve Gelişen Teknolojiler

Bu başlık altında kuantum haberleşme, kuantum kriptoloji, bio cihazlar, sıfır güçle çalışan cihazlar gibi ileri, düzey yenilikçi projeler desteklenmektedir.

B. Güvenlik (Security)

1) Vatandaşların Güvenliğini Artırma

Bu aktivitenin amacı uyuşturucu, silah kaçakçılığı, kara para aklama, çocuk pornografisi trafik akışı, bireysel ve sektörel suçlar, eşya, bilgi ve teknoloji kaçakçılığı suçlarına karşı, bilgi güvenliği adli analiz araçları ve izleme araçlarıyla katkıda bulunmaktır.

Bu başlık altında aşağıdaki konularda projeler desteklenmektedir:

- Lojistik ve destek zinciri güvenliği
- Organize suçlar ve terörist aktivitelerden korunmak için bilgi yönetimi
- İleri adli analiz araç kutusu

2) Araçların ve altyapıların güvenliğinin artırılması

Bu aktivitenin amacı yönetim binaları (sembolik değeri de olabilir), tren ve metro istasyonları, havaalanları, barajlar, hassas üretim fabrikaları, enerji üretimi, dağıtım ve saklama tesisleri, nükleer atık saklama yerleri, bilgi ve iletişim ağları gibi kritik yapıları terörist saldırılara, sabotaja, doğal felaketlere, ihmale, kazaya, bilgisayar saldırılarına (hacking), kötü niyetli davranışlara karşı korumaktır. Bu saldırıların amacı çoğu zaman zincirleme bir etki yaratmaktır (Örneğin enerji ya da haberleşmedeki bir kesintinin birçok şeyi etkilemesi gibi). Etkili teknolojiksel çözümlerin üretilmesi beklenmektedir. Etkili çözümlerin olmadığı durumlarda düşük maliyetli çözümler önerilmelidir. Eğer teknoloji var ve pahalıysa düşük maliyetli yapılmaya çalışılmalı ve aşağıdaki konularda etkili çözümler üretilmelidir:

- Akıllı izleme ve genişletilmiş sınır güvenliği
- İletişim hat güvenliğinde süreklilik, kapsam ve performans

3) Kriz durumunda güvenlik ve güvenin sağlanması

Bu aktivitenin birinci amacı, hükümetlere, ilk yardım ekiplerine, toplumlara beklenmeyen yıkıcı olaylar karşısında daha yenilikçi ve uygulanabilir çözümler sağlamaktır. İkincil amacı ise olay anında ve olaydan sonra cevap vermek ve durumu düzeltmek için gerekli olan araçlar, altyapı, prosedür ve organizasyonları iyileştirmektir.

4) Sistem bütünleştirilmesi, bağlanması ve uyumlulaştırılması esnasında güvenliğin iyileştirilmesi

Güvenlik ve Bilgi İletişim Teknolojileri çağrılarında ele alınan tüm başlıklarda güvenliğin artırılması ve sistemlerin uyumlulaştırılmasını öngören projeler desteklenmektedir.

5) Güvenlik ve toplum

Avrupa topluluklarında potansiyel güvenlik tehditlerini önlemek, cevaplamak ve yönetmek için teknoloji önemli bir araçtır. Fakat o sadece etkin cevabın bir parçasıdır. Kültürel taban, sosyal ve güvenlik olayları bu yönetimi dengelemekte önemli bir rol oynamaktadır. Bunun sonucu olarak teknik araştırmaları tamamlamak için politik, sosyal ve insanla ilgili konularda araştırma gerekmektedir. Bu alanda aşağıdaki konularda projeler desteklenmektedir:

- Vatandaşlar ve toplum
- Halk kullanıcılarının kültürel ve organizasyonel yapılarının anlaşılması
- Güvenlik yatırımları ve diğer toplumsal hedefler arasındaki farklılıkları değerlendirmek için metodolojiler üzerine araştırma
- Güvenlik ekonomisi

6) Güvenlik araştırması, koordinasyon ve yapılandırması

Güvenlik teması Avrupa insanın güvenliğini artırma yanında sınırlı kaynakları etkin kullanarak Avrupa endüstrisinin global pazardaki başarısını artırmayı hedeflemektedir. Bu hedefler için Avrupa seviyesinde, üye veya aday ülkelerde çeşitli araştırma projeleri yürütülmektedir.

Bu aktivitenin amacı Avrupa'da münferit yapılan çalışmaları ortak bir sinerjiye dönüştürerek aynı çalışmaların iki defa yapılmasını önlemektir. Bu aktivite ilgili yasal ve prosedürel aktivitelerin ilerletilmesine odaklanmalıdır. Bu başlıkta desteklenen projelerle Avrupa'da güvenlikle ilgili yapılan araştırmalar konusunda bir koordinasyon sağlanması hedeflenmektedir.

V. TÜRKİYE'DEKİ ÇALIŞMALAR

Türkiye'de 2003 yılına kadar bilgi iletişim teknolojileri ve bilişim teknolojileri güvenliği konularında yapılan çalışmalar şirket ya da kurum bazlı olarak yapılmış ve da daha çok kurumun ihtiyaçlarını karşılamaya yönelik altyapı ve uygulama projeleri şeklinde olmuştur. Bu uygulama ve projeler genellikle birbirinden bağımsız, ülkenin öncelik ve ihtiyaçları yerine, kurumsal öncelik ve ihtiyaçlara dayalı olarak ön plana çıkmış projeler yapılmış, onlar da etkin olarak uygulanamamıştır. 2003 yılında hükümet tarafından hazırlanan Acil Eylem Planında e-Dönüşüm Türkiye (eDTR) Projesi'ne yer verilmiş, söz konusu projenin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile ilgili olarak Devlet Planlama Teşkilatı (DPT) Müsteşarlığı görevlendirilmiştir [12].

eDTR Projesinin başlangıcında ortaya konan amaç ve hedefleri, ülkemizin bilgi toplumu alanında mevcut durumunun güncel, bilimsel ve ayrıntılı tespitlerini, iç dinamiklerini ortaya koyan çalışmalar yapılmadan, kısa vadeli bir yaklaşımla belirlenmiş; daha çok AB'nin hazırladığı metinlerin ülkemize uyarlanması şeklinde olmuştur. Öte yandan, belirlenen hedefler yıllık ve somut ara hedeflere dönüştürülmemiştir [13].

Daha sonra yayınlanan Bilgi Toplumu Stratejisinde; toplumun temel öğelerini oluşturan vatandaşlar, kamu sektörü ve işletmeler ile bilişim teknolojileri sektörünün mevcut durumları ve Türkiye'nin 2010 yılında bilgi toplumuna dönüşüm potansiyeli değerlendirilmiş, belirlenen stratejik öncelikler çerçevesinde 2010 yılı için hedefler ve bu hedeflere ulaşmak için atılması gereken adımlar tespit edilmiştir. Bu strateji dokümanının eki Eylem Planı, Bilgi Toplumu Stratejisi kapsamında belirlenen stratejik amaç ve hedeflere ulaşılmasını sağlamak üzere, stratejinin uygulanması döneminde hayata geçirilecek faaliyet ve projeleri içermektedir. Bu planda 111 eylem, bu eylemlerden sorumlu kurum ve ilgili kuruluşlar da belirtilmiştir [14]. Sorumlu kurumlar ilgili kurumlarla iş birliği içinde DPT desteği ile projelere başlamıştır.

Bu eylem maddeleri DPT tarafından incelenmekte ve düzenli olarak eylem maddelerinin durumu yayınlanmaktadır. Eylem Planının 2009 yılı sonu itibarıyla uygulama sonuçlarına göre; eylemlerden 22 adedinin (% 20) tamamlandığı, 62 eylemin (% 56) çalışmalarında önemli aşama kaydedildiği ve 19 eylem (% 17) ile ilgili çalışmaların ise henüz başlangıç aşamasında olduğu görülmektedir [15].

TÜBİTAK kamu, sanayi ve akademisyenler için araştırma destekleri vermektedir. Özellikle ARDEB (Araştırma Destek Birimi), TEYDEB (TÜBİTAK Yenilik ve Destek Programlığı

Başkanlığı) ve BİDEB (Bilim İnsanı Destekleme Daire Başkanlığı) birimleri aracılığı ile araştırma projelerini desteklemektedir. ARDEB'de bu destekler temel bilimlerden çevre, elektronik sağlık, sosyal, tarım, kamu araştırmaları, savunma teknolojileri araştırma grupları gibi birçok alanı hi:ap etmektedir. Bu programlar içerisinde sadece Savunma Teknolojileri Grubu (SAVTAG) ve Kamu Araştırmaları Grubu (KAMAG) grubu bilişim teknolojilerini ve güvenlik içeriği olan ve bir kamu kurumu veya Milli Savunma Bakanlığının ortak olduğu projeleri desteklemektedir. Bunlar da daha çok hali hazırda bir kurumun ihtiyacına çözüm sunan projelerdir. Diğer destek programları da bilgi iletişim teknolojileri veya güvenlik alanındaki projeleri desteklemektedir. Fakat bu projelerde önceden belirlenmiş alanlara yönelim yapılmamakta sadece sunulan projenin araştırma niteliği, maliyeti, iş gücü, ülkeye katkısı vb. kriterlere göre değerlendirilmektedir.

Bunlar dışında bilgi iletişim teknolojileri ve bilgi iletişim güvenliği alanında yapılan çalışmalar genel bir politikayı içermeyen kişisel ya da kurumsal öngörülere göre yapılmaktadır.

TÜBİTAK destekleri dışında üniversiteler, kamu kuruluşları, sanayi kuruluşları kendi misyon ve vizyonları doğrultusunda araştırma projeleri yapmaktadır. Bu çalışmalar arasındaki eş güdümü veya üst düzey yönlendirmeyi yapan etkili politika veya kılavuz bulunmamaktadır.

VI. SONUÇ VE YORUMLAR

E-devlet, e-sağlık, e-ticaret, e-öğrenme gibi günlük hayatta yaptığımız işlerin internet üzerinden kısa ve etkin olarak gerçekleştirilmesini sağlayacak çözümler, interneti hayatımızın ayrılmaz bir parçası haline getirmektedir. Bu çözümlerin uygulanmasında gizliliğe, bütünlüğe ve sürekliliğe yönelik tehditleri ortadan kaldırmak için de birçok ürün, çözüm ve standartlar geliştirilmektedir. Ülkeler veya toplumlar bu alanlarda çözümler veya yeni teknolojiler geliştirerek hem bilişim sistemlerinde güvenliği sağlamayı hem de dünya BT pazarındaki öncülüğün ele geçirmeyi hedeflemektedirler.

AB, ürün ve sistemlerin güvenliğinin değerlendirilmesi için ITSEC'le başlayarak bugün dünyada 26 ülke tarafından kabul edilen Ortak Kriterler standardının geliştirmesine öncülük etmiştir. Aynı şekilde BS 7799 ile başlayıp ISO tarafından da yayınlanan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardının oluşturulması ve güncellenmesinde öncü rol oynamıştır.

AB, Avrupa'daki dağıtık ulusal bilim, teknoloji, politika ve uygulamaları birbirine yaklaştırmak, AB'nin rekabet gücünü artırmak, var olan gücünü geliştirmek ve lider olmak için geliştirdiği çerçeve programlarda bilgi iletişim teknolojileri ve güvenlik alanına büyük önem vermiş ve bu konularda birçok projeyi desteklemiş ve hala desteklemektedir.

2007-2013 yılları arasında geçerli olacak 7. Çerçeve Programı içerisinde bilişim teknolojileri alanında özellikle BT güvenliği içeren yaygın ve güvenilir ağlar ve servisler,

bağımsız yaşam ve dahil olmak için ICT ana başlıkları altında birçok BT güvenliği projesini desteklemektedir. Yine 7. Çerçeve Program içerisinde güvenlik alanında aşağıdaki konularda projeler desteklenmektedir.

- Vatandaşların güvenliğini artırma,
- Araçların ve altyapıların güvenliğinin artırılması,
- Kriz durumunda güvenlik ve güvenin sağlanması,
- Sistem bütünleştirilmesi bağlantısı ve uyumluluğunda güvenliğin sağlanması,
- Güvenlik ve toplum

Bu alanlarda desteklenen projelerin çoğu iş birliği projeleri olup hem AB içindeki sinerjiyi artırmak hem de internet sanal ortamında ulusların birlikte hareket etmesini sağlamaktadır. AB'nin gelecekte destekleyeceği güvenlik projelerinin belirlenmesi için hali hazırda çalışmalara devam edilmektedir.

Türkiye eDTR ile başladığı ve 2006-2010 Bilgi Toplumu Stratejik Eylem Planı ile devam ettirdiği bilgi iletişim teknolojilerinin ülkede yaygın olarak kullanılması, güvenlik faktörlerini de göz önüne alarak, sağlayacak çok değerli birçok projeyi ve eylemi başlatmıştır. Bunlardan bir kısmı başarılı olarak yürütülmesine karşın bir kısmı için Sayıştay'ın denetim raporunda da belirttiği gibi etkin proje yönetim mekanizmalarının geliştirilmesi gerekmektedir.

TÜBİTAK tarafından desteklenen bilişim teknolojileri ve güvenlik projeleri bilime, ülkeye, projeyi sunan kuruma katkıları, bütçesi, süresi iş gücü yönünden değerlendirilmektedir. Projeyi sunan tarafın gerekçeleri değerlendirilerek karar verilmektedir. Ülkenin bu günü ve geleceği için gerekli ve önemli konular üst düzey politikalar ile tanımlanıp o doğrultuda projeler istenmemektedir. Bu da bilgi iletişim teknolojileri ve güvenlik alanlarında önemli bazı konuların gözden kaçabileceği ve bu konularda geri kalma riskini doğurmaktadır. Desteklenecek projelerin belli bir politika ile tespit edilip o yöndeki projelerin desteklenmesi belli konularda uzmanlaşmayı ve ülke içindeki iş birliklerini artıracaktır. Bu iş birlikleri dış dünya ile olan rekabeti güçlendirecek ve daha etkin ürünlerin pazara sürülmesini sağlayacaktır.

Türkiye olarak BT sistemlerinin güvenliğinin artırılması ve AB projeleri içinde daha fazla yer alınması için ulusal yol haritasının belirlenmesi ve bu yol haritasının hedefleri doğrultusunda projelerin desteklenmesi faydalı olacaktır. Bu yol haritasında mevcut ihtiyaçların karşılanması yanında geleceğe yönelik çalışılacak Ar-Ge konuları belirlenmeli ve bu konuda üniversite, sanayi ve araştırma kurumlarını içeren büyük projelerin desteklenmesi sağlanmalıdır. Türkiye içindeki BT sistemleri güvenliği Ar-Ge çalışmalarının ve iş birliklerinin artırılması için iletişim ağları oluşturulmalı, proje pazarları yapılmalıdır. .

VII. KAYNAKLAR

- [1] L. DeNardis, "The History of Information Security: A Comprehensive handbook", Elsevier, 2007, pp.681-704
- [2] Cisco Systems, "IP Next Generation Networks for Service Providers", Ulaşılabılır: http://www.cisco.com/en/US/solutions/collateral/ns341/ns52/4/ns562/ns583/net_implementation_white_paper0900aecd803fcbbe.pdf

- [3] Common Criteria for Information Technology Security Evaluation, Part I, Part II, Part III, July 2009, Ulaşılabılır: <http://www.commoncriteriaportal.org/thecc.html>
- [4] Information Technology -- Security techniques -- Information security management systems -- Requirements, ISO Standard 27001:2005, 2005
- [5] Group of Personalities "Research For a Secure Europe", 2004
- [6] O. Hangül, "Avrupa Birliği Çerçeve Programları", Akademik Bilişim 2008, Çanakkale, 2008
- [7] G. Ambroziewicz., P. Ortiz de la Torre, "CALL:FP7-Sec-2010-I", Security Research Info day, September 2009, Brussels
- [8] ESRI, European Security Research and Innovation Form Final Report, Eylül 2009
- [9] European Commission, "Security Research Call 3", July 2009, Ulaşılabılır: <http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.FP7CallsPage#Security>
- [10] European Commission, "ICT Call 5", July 2009, Ulaşılabılır: http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=232
- [11] Council of European Union, "Declaration of Strengthening Capabilities", Brussels, 2008
- [12] Devlet Planlama Teşkilatı, Bilgi Toplumu Dairesi Başkanlığı Web Sitesi (<http://www.bilgitoplumu.gov.tr/edtr.asp>)
- [13] Sayıştay Raporu "e-Dönüşüm Türkiye Projesi Çerçevesinde Yürütülen Faaliyetler", 2006, Ulaşılabılır: <http://www.sayistay.gov.tr/rapor/perdenrap/2006/2006-3eDTR/2006-eDTR.pdf>
- [14] Devlet Planlama Teşkilatı, Bilgi Toplumu Stratejisi 2006-2010 Eylem Planı, 2006, ulaşılabilir: http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060700_EylemPlanı.pdf
- [15] Devlet Planlama Teşkilatı, Bilgi Toplumu Stratejisi 2006-2010 Eylem Planı Değerlendirme Raporu V, 2010, ulaşılabilir: http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/20100323_BT_S_Değerlendirme_V.pdf

Birinci, K. Mehmet, 1993 yılında Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliğinden mezun oldu. 1996 yılında yüksek lisansını 2001 yılında da doktorasını Kocaeli Üniversitesi Elektronik ve Haberleşme Anabilim Dalı'nda tamamladı. 1994-2000 yılları arasında Kocaeli Üniversitesi Bilgisayar Mühendisliğinde Araştırma Görevlisi olarak çalıştı. 2000-2001 yılında Armada Bilgisayarda A.Ş.'de Sistem Mühendisi olarak çalıştı. 2001 yılından beri TÜBİTAK UEKAE'de Bilişim Sistemleri Güvenliği bölümünde çalışmaktadır.

Mehmet Kara bilgisayar ağlarında çok yönlü yönlendirme, güvenli ağ tasarımı, gerçekleştirme ve ağ güvenlik testleri konularında çalışmaktadır. Özellikle sınır güvenliği elemanları olan güvenlik duvarı, yönlendirici, saldırı tespit/önleme sistemleri ve içerik kontrolcüler konularında çalışmaktadır.

Uzaktan Eğitim Sisteminde E-Öğrenim Süreci Ve Bilgi Güvenliği

Akin Marsap^a, Gizem Akalp^b, Ebru Yıldırım^b

Özet—21 nci yüzyılda e-öğrenim uzaktan eğitim sistemi yönetimin sürecinde akademik değerlendirme ve sürekli gelişim ilkeleri giderek artan bir öneme sahiptir. Bu anlamda yapılan gayretler uzaktan eğitim ve güvenli bilgi yönetim sistemlerinin bütünlüğü içinde yenilenen özgün bir yapıda ele alınarak değerlendirmelidir. Uzaktan eğitim (UE) uygulamaları bilişim ve iletişim teknolojilerini etkin bir şekilde kullanarak büyük oranda bir değişim içindedir. Organizasyonlar e-öğrenim politikaları alanında birçok yenilikleri başarı ile yapıyor olsa da, bu sistemi kullananlar tarafından zaman zaman farklı biçimde algılanabilirler. Bu açıdan e-öğrenim entegrasyonu/uygulamaları araştırma ve gözden geçirmeler ışığında karşılaşılan engellerin zamanla aşılabacağı açıktır. Buna karşın, e-öğrenim sürecinde tam potansiyelinin anlaşılabilir olarak geliştirilmesi oldukça önemlidir. UE geleceğin e-öğrenim sürecinde yaşamsal bir öneme sahiptir. Bu bildirinin amacı uzaktan eğitim yönetiminde e-öğrenim sürecinde akademik değerlendirme konularının ve güvenli bilgi yönetim sistemlerinin gelişim dinamizmi ve önemi üzerinde durulmaktadır.

Bu çalışma bilimsel araştırma projesinin bir parçasıdır. “Bilgi Güvenliği, Dijital İmza ve E-Ticaret’in Teknik ve Yasal Boyutunun İncelenmesi” (Proje Numarası: TBMYO-2008/75).

Anahtar kelimeler: E-öğrenim, uzaktan eğitim, akademik değerlendirme, akreditasyon, güvenli bilgi yönetimi

I. GİRİŞ

E-öğrenim süreçlerinde, bilişim teknolojileri yeni gelişimler ışığında, daha fazla etkinlik kazanmıştır. Özellikle internet üzerinden uzaktan eğitim sistemleri eğitimin her alanında olduğu kadar, iş dünyasında insan kaynağının eğitim/öğretimini, bulunduğu yerden erişimle zaman/mekan sınırlılıklarını ortadan kaldırarak yüksek bir başarı ile sağlar. İnternet üzerinden uzaktan eğitim kalite ve standartının gelişimi, katılımcıların memnuniyeti, danışmanların uzmanlığı, teknik uzmanların desteği, uzaktan eğitim sistem yönetiminde karşılaşılan sorunların anında çözümü çok önemlidir. Yönetim; işletmenin yada organizasyonun, elindeki kaynak planı, organizasyonu, işletimi ve denetimini etkili ve verimli bir şekilde amaçları gerçekleştirme sürecidir [1]. Bu

anlamda yönetim; yönetim, etkileşim ve iletişim işlevlerinin etkin bir biçimde bütünler. Kurumsal yönetim, işletmenin stratejik yönetimi ve yönlendirilmesi ile görevli sorumlu üst yönetimin, bu görev ve sorumluluklarını yerine getirirken, işletme üzerinde kendilerini belirli nedenlerle hak sahibi gören; pay sahipleri, çalışanları, tedarikçi, müşteri ve diğer toplumsal kurumlarla olan ilişkilerini kapsar.

Kurumsal yönetim, işletmenin üst yönetiminin yönetilmesidir. Kurumsal yönetim etkinliği; yapılandırma, performans ve uygunluğu işlevleri ile sağlanabilir [2]. Bilişim toplumu çağdaş yönetim süreci; e-öğrenim alanında açıklık, şeffaflık, paylaşım, güvenlik ve hesap verilebilirlik ilkelerini ön plana çıkarır. Yeniden dönüşen dijital dünyaya öncülük edecek öncül nitelikteki ciddi adımlar UE içinde e-öğrenim sürecinden geçmektedir. Bilişim teknolojilerinin sağladığı yeni olanaklar e-öğrenim yönetiminde UE’de e-öğrenim için olduğu kadar, e-devlet, e-ticaret ve dijital işletmeler sistemlerinin sürekli işlerliğini hızlandırır. Bilişim ve teknolojik gelişmeler bilişim kavrama yeteneğinin değişik alanlarda başarılı uygulamaları e-öğrenim alanındaki gelişimi hızlandırmıştır. Bu açıdan değerlendirildiğinde, insan kaynağı yönetimi/denetimi konusu daha stratejik bir rol almıştır. E-öğrenimin temel amacı, genel eğitim sistemi organizasyonu açısından gerçek durumuna ilişkin tam/doğru ve zamanında yapılan açıklamalar, yönetimin özellikle tüm ilgili birimlerin çıkarlarını gözeterek şekilde çalışmasını dijital sistemlerin güvenli desteğinde kaliteli/verimli ve etkin bir biçimde sağlamaktır.

^a Ahmet Yesevi Üniversitesi, Uzaktan Eğitim Programları, Ankara, 06490, Turkey, (e-mail:akinmarsap@yahoo.com)

^bUludağ Üniversitesi, Teknik Bilimler MYO, Bursa, 16059, Turkey, (e-mail:gizema@uludag.edu.tr; yeniman@uludag.edu.tr)

Yenileşen yaklaşım içinde, e-öğrenim için sağlanan esneklik, birey-organizasyon-danışman/eğitici ve idari yönetim arasındaki işleyiş akışına; yaratıcılık, gelişim ve

sürekli yenilikçi açılımlar sağlayabilir. UE içinde, ara sınavlar, ödevler ve final sınavlarını kapsayan akademik değerlendirme süreçlerinin bilgi güvenliğinin sağlanması en temel faktördür. Bu açıdan günümüzde e-öğrenim yönetiminde UE'in yenilik, kalite ve standartların daha üst noktalara erişimi için strateji, akademik standart, akademik gözetim ve etkileşim; entegrasyon ve senkronizasyon odaklı anlayış daha da ön plana çıkar. Bu süreçte, e-öğrenim tele öğrenim eğitim sisteminde

UE'de yatay akademik yaklaşımların, bilimsel, akademik ve dinamik süreçleri kapsayacak biçimde yeniden tasarımıyla gelişimi önemlidir. Bu açıdan, UE sürecinin yüz yüze eğitim sistemleri ile gelişimi sağlık UE mimarisinin güvenli bilgi yönetim sistemlerine dayalı çalışmalarında önemlidir. E-öğrenimde UE yönetim ve organizasyonu, insan kaynakları, akademik danışmanlık, yüz yüze eğitim ve sonuçların değerlendirilmesini de içeren e-öğrenim/dönüşüm süreçlerini kapsar. Yüksek kalite, katılım ve verimlilik yeni e-öğrenim modellerinin temelinde yer almaktadır. E-eğitimin öğrenim hedefleri doğrultusunda değişen süreçlerini e-ortama taşıyarak etkinlik, verimlilik ve maliyet tasarrufu ile çağdaş eğitim modellerine istenilen düzeyde erişilebilir.

II. İNTERNET ÜZERİNDEN UZAKTAN EĞİTİM

Topluma eğitim hizmeti sunan bir kurum olarak eğitim işletmeleri gerek meslek dalı, gerekse uzmanlık alanları yönünden çeşitlenerek; uzaktan eğitimde, e-kayıt, e-kitap, e-laboratuvar ve diğer uzaktan eğitim sistemlerini de kullanmaktadır. Bu nedenle uzaktan eğitim veren okul ve merkezler; eğitim ve öğretim fonksiyonlarının yanı sıra, eğitim kurumu, bir araştırma birimi, ekonomik bir işletme, birçok meslek gruplarından kişilerin çalıştığı, sosyal bir kurum ve çoğunluğu kamu kuruluşu niteliğinde olan hizmet işletmeleridir. UE işletmeleri, bir açıdan diğer işletmeler gibi çevresinden farklı girdiler alıp bunları bir süreçten geçirip nihai olarak bir hayati öneme haiz bir hizmet sunarlar. UE işletmelerinde dış çevre ve ürün yelpazesi karmaşıktır. Süreç açısından işlevler değişiktir. Nihai ürünün geri bildirim mekanizması tam organize edilememiştir. UE sağlayan hizmetlerinin temel özelliği itibarıyla eğitim/öğretim başta olmak üzere işlevsel süreçlerin her evresinde yüksek bir güven faktörünün ön planda olduğu yapılardır. Modern e-öğrenim hizmetleri katılımcılara anında, çabuk, tam ve doğru yanıtlar verebilmelidir. Çünkü tüm eğitim hizmetinin sunumunda katılımcıların etkin paylaşımcı öğrenim süreci söz konusudur. Bunun yanında e-öğrenim hizmetlerinde katılımcıların ihtiyaç ve farklı beklentileri her geçen gün değişir. E-öğrenim gelişen yeni buluşlar ve çözümlerin yanında bütün bunların danışman/katılımcı sağlıklı iletişim ve evrensel eğitimde etik ilkelerinin ışığında birleştirilmesi gereklidir. Bunun için UES işletmesinin faaliyetine başladıktan sonrada yenilikleri çok yakından izlemesi gerekir. Bunun için, UE merkezlerinin tüm bu hızlı değişimleri anında takip edip cevap verebilmesi büyük bir önem taşımaktadır. Eğitim/öğretime olan talep diğer alanlara kıyasla farklı talep nitelikleri içerir. E-öğrenim

yapısal itibarıyla gösterdiği çeşitli özellikler eğitim sektöründe talep analizi yapmayı engeller. Çünkü öğrencilerin/katılımcıların eğitime ne kadar istekli ve hazır olduğunu tespiti güçtür. UE hizmetlerin özelliği, kesintisiz öğrenim, danışmanların uzmanlığı, derslerin kalitesi, iletişim ve değerlendirici süreç, sistemin teknik ve karmaşık yapısı, açık ve dinamik sistem özelliklerini taşır. Bu temel ilkelerin yanı sıra, bilişim teknolojilerinin sunduğu yeni olanakları kendi bünyesinde değişim sürecine uyumlu geçişler sağlayan modeller UE kalitesi, etkin zaman kullanımı ve gelişimi de beraberinde getirmektedir. E-öğrenim potansiyelinin gerçekleştirmesini engelleyen riskli noktalar oluşabilir. Örneğin, işletmelerin Zeus Botnet ve InfoStealing Truva atlarından bilişim sistemindeki bilgilerin gizliliği ve muhafazası önem kazanıyor. Bu alandaki bütün tehditler kötü amaçlı yazılımlardan kaynaklanmıyor. UE sistemi dışındaki e-öğrenim kaynaklarına erişimi sağlayan yazılımların birbiriyle iletişimini sağlayan API'ler de güvenlik riski oluşturuyor. Sosyal ağlar geliştikçe daha çok sayıda site uygulama programcılığı arayüzlerini (API'ler) kullanıyor. API'ler değişik kaynaklardan alınan verilerden yeni veriler ve bilgiler türetirken farklı yazılımlar arasında etkileşim sağlıyor. Bir e-öğrenim sisteminde birden çok API kullanılabiliyor ve bu API'lerden yalnızca birinde güvenlik açığı olması bile bütün sistemin risk düzeyini yükseltebilir.

III. E-ÖĞRENİMDE AKADEMİK DEĞERLEME

Genel anlamı ile eğitim bireylerdeki öğrenim eğilimlerini toplumun beklentileri doğrultusunda karşılayıcı davranışlar kazandırma süreci olarak düşünülebilir [3]. Ağ tabanlı öğretimde seslendirilen kalite ile ilgili sorunlar, sistemin işleyişi gereği ortadan kalkar. Katılımcılar sınıf geçmek için değil öğrenerek öğrendiklerini bir işe dönüştürmek için çalışır. Sınıf geçmek için çalışan öğrencilerde görülen bir zaman baskısı, sınıfta küçük düşürülme, diğer arkadaşlarıyla kıyaslanmadığından kendine uygun zamanlarda öğrencinin öğrenim için çalışması kaliteyi beraberinde getirir [4]. E-öğrenim yönetiminde bilişim teknolojilerinde tasarruf, ya da gelirleri artırmak amacı internet çağının hız faktörü kurumsal planların çok yönlü kullanımına avantajlar sağlayabilir. E-öğrenim UE'nin yenileşiminde aktif katılımlı akademik etkileşim süreçlerinin zenginliği yaşam boyu eğitim sürecinde öncül rolü olan gerekli bir öğedir.

UE'de internete dayalı etkileşimli e-öğrenim süreci, yönetsel, idari, teknik ve destek birimlerde dengeli bir senkronizasyon gerektirir. Eğitsel başarı kriterleri üst yönetimin e-dönüşüm projelerindeki yaratıcı liderlik başarısındadır. Üst yönetimin iyi fikirleri yanında iş birimlerinin yönetici ve tüm çalışanların projeye özverili ve istekli katkısı oldukça önemlidir. Kurumlar, iş ortamları, iş arkadaşları, mesleki başarı ya da başarısızlıklar bireyin kendisi hakkındaki fikrini oluşturmaya katkıda bulunur. Her bireyin çalıştığı iş ya da kurumdaki durumuna ilişkin bir fikri vardır. Kurum ve yöneticilerin çalışanlara sürekli geribildirim,

farkındalık düzeyi açısından gerçekçi bir zemin sağlar. Aslında olumsuz geribildirim alımı, olumlu geribildirim almaktan daha zordur. Dolayısıyla yapıcı olumsuz geribildirim değeri bilerek ondan yararlanmak gerekir [5]. Bilgi, ilgi, duyarlılık ve deneyim öyle şeylerdir ki, pek çok işte yalnızca kişinin kendi yaşantısıyla değil geçmişe dayalı alışkanlıklarla, görgü ile kendine miras kalan yaşantılarla da beslenerek kazanılır [6]. E-öğrenim, öğrenenin bireysel öğrenim etkinlikleri ile kendi başına bireyselleştirilmiş bir öğrenim pratiği yanında eş zamanlı ya da eş zamansız diğer öğrenen ve öğretmenler ile birlikte bilgisayar ağları üzerinden kurulan bir etkileşim ortamının paylaşılır. Web'in eğitim ortamlarında kullanımında biricik özelliklerden bir tanesi katılımcılar arasında etkileşimdir [7].

Dünyanın her coğrafyasından ağ tabanlı öğretim ortamlarında iletişimin bir otoriteye bağlı olmaksızın, hızla kurgusu öğrencilerin insiyatif alıp kendini gerçekleyen yetkin özelliklerine önemli bir katkı sağlar. Ağ tabanlı öğretim ortamlarında akademik danışmanlık bir kişiye atfedilen bir görevin ötesinde öğrenci ve öğretmenin birlikte kurguladığı etkileşimli bir olgudur. UE kalite ve standart gelişimi için vizyonel girişim ve senaryolara gereksinim vardır. UE çalışanları tarafından e-eğitim portalı oluşturup bütünleşik portala e-eğitim ve bilişim teknolojileri ile ilgili önemli ve güncel gördüğü bilgi, belge, doküman, yazı, görüş ve yorumlarıyla katılarak gelecekte bu yönde daha derin bir donanımına sahip araştırmacı bilgilerini sürekli olarak güncelleyebilir. UES konusunda uzman ve profesyonel bir yönetim, uzman çalışan kadrosu, konularında çok iyi yetişmiş danışmanlardan oluşan bir eğitim ekibi başarı sürekliliğinin garantisidir. Tasarlanan bu sistem ile uzman bilgileri sisteme dinamik aktarımı ve bilgisayarın anlamlı değerlendirmeleri sağlanabilir. İleri çalışma olarak yapay zekanın diğer teknolojileri de sisteme uyumu sonucu daha hassas sonuçlar sağlanabilir [8]. Entegrasyonun yarattığı değişimin aşamaları, değişim benimseme, alıştırma, kabullenme ve kullanma olarak dört evreden geçmektedir [9]. Şüphesiz bu evrelerde izlenebilirlik yönetimi bilgi güvenliği için önemlidir. İzlenebilirlik yönetimi, bir ürünün üretildiği, dağıtıldığı ve bulunduğu yerler, geçmiş olduğu işlem ve uygulamaların saptanarak raporlanmasını sağlayan yazılım bileşenlerini kapsar [10]. İnternet üzerinden iletişimi gerçekleştiren bilgilerin güvenilirliği, açık anahtar kriptografi olarak adlandırılan bir teknik (şifreleme ve şifre çözme, kurcalama/sezme, kimlik doğrulama, inkar edememe) içeriğinde sağlanabilir [11]. Güvenlik sürecinde kullanılan sayısal sertifikalar, bir kişi, sunucu ya da bir organizasyonun kimliğinin tanımlanarak bir açık anahtarın bu kimlikle ilişkilendirilmesinde kullanılan elektronik belgelerdir [12]. E-öğrenim UE yeni bir ortamında ağ tabanlı eğitim kavramı, dijitalleşen eğitim merkezlerine yönelik değişim sürecinde eğitimde yaşanan bu dönüşüme paralel öğretim ortamlarına ait kavramı temelden değiştirmiştir. Gerçek anlamda eğitimde evrimsel bir dönüşüm niteliği taşıyan bu değişimler öğrenci, danışman, yönetici, eğitim programcı ve rehberlik uzmanları, kısaca tüm

eğitimciler için geleneksel bakış açılarının derinden sorgulandığı yepyeni bir oluşumdur.

Gelişen sanal ortamda öğretimde fırsat eşitliği, öğretim yöntem ve teknikleri, sınıf içi etkileşim ve öğretim materyalinin niteliğinde klasik öğretimden farklı yeni kavram ve teoriler ağ üzerinde sürekli yeniden tanımlanan bir nitelik taşır. Ağ tabanlı eğitim, bireyin gereksinimi ile iş imkânları arasında dengeye özenlidir, endüstriyel sorunların çözümünde katkı sağlar. UE'de, eğitim yönetici, çalışan, danışman ve öğrencilerin yıllık sosyal ve kültürel faaliyetlere etkin katılım izlemeyi kolaylaştırır. E-öğrenim UE alanında akademik değerlendirme kurulları arasında iletişimin artırılarak eşgüdümün kazanımında yararlıdır. E-öğrenim alanında UE'de kalite odaklı çalışmaların çeşitli bakımlardan geliştirilmesinin uygun olacağı değerlendirilmektedir;

1. E-öğrenimde kaliteli yönetim, gözetim ve denetim
2. E-öğrenim sürecinde inter aktif geribildirimler
3. E-öğrenimde matematiksel etkinlikler ve yeni katkılar
3. E-öğrenimde akademik kalite gelişimine yönelik yeni araştırmalar
4. E-öğrenimde yönetsel, eğitsel ve teknik destek unsurları entegrasyonu
5. UE sürecinde artan oranda yüz yüze eğitim katkısı

E-öğrenim alanında yeni gelişimler UE' de kullanılan teknolojilerin, iletişim-ortam-etkileşim ve teknoloji ilişkilerinin entegrasyonu daha güvenli bir bilişim modeli boyutunda tasarımı ortaya çıkarabilir. Etkileşim iki ya da daha fazla taraf arasındaki iletişimdir. Ancak UE'de etkileşim sadece bu genel anlamı ile kullanılmamaktadır. Etkileşim denildiğinde uzaktan yürütülen eğitimin kalitesi üzerinde de doğrudan etkisi olan üç farklı etkileşim düzeyi akla gelmelidir [13]. UE etkileşim yaklaşımları, öğrenci ve öğrenim materyali arasındaki etkileşim, öğrenci ve eğitmen arasındaki etkileşim, öğrencinin diğer öğrencilerle olan etkileşimidir. Etkileşimde göz önünde bulundurulması gereken diğer bir unsur da zamandır. UE'de öğrenci ile etkileşimde genellikle bir zaman gecikmesi yaşanabilir. Örneğin basılı materyallerle etkileşimde posta ya da telefon gibi iletişim araçları yoluyla katılımcı-öğretim elemanı etkileşimi de sağlanabilir. Buradaki etkileşim gecikmeli sağlanmakta, katılımcıdan geri bildirim, gecikmeli alınarak katılımcıya iletilmektedir. Senkron, gerçek zamanlı etkileşimin sağlandığı teknolojilerdir. Bu bağlamda yüz yüze iletişime yakın etkileşim sağlayan video-konferans, etkileşimli TV gibi teknolojiler ile etkileşimin üç düzeyi de eş zamanlı gerçekleştirilebilir [14]. Geliştirilen programların iletildiği kitle olan öğrenenlerin demografik, ekonomik, coğrafi konum, akademik alt yapı özellikleri, etkinlik üzerinde oldukça etkilidir. Etkinlikte merkez unsur, öğrenenlerdir. Bütün çabalar onlara uygun, onların gereksinimlerini karşılayıcı esneklikle gelişen kurumsal yapının kurgusundadır. Program bu eğitimi alabilecek nitelikteki kişilere sunumu, söz konusu hedef kitlenin bu yöndeki ihtiyaç ve beklentilerine göre geliştirilişi; öğrenci tatmini ve başarısını, bağlı olarak da etkinliği sağlayacaktır. Etkinliğe etki eden bir diğer faktör de eğitimdeki diğer taraf olan, danışman öğretmenlerdir.

Eğitimcilerin etkin seçilip eğitimi, program başarısında çok önemli bir faktör olabilir. Bu nedenle eğitimcilerin program ve öğrencilerin ihtiyaçlarına göre eşleştirilmeleri önemlidir [15]. Uzaktaki öğrenciyle öğretmen arasında doğrudan etkileşime izin veren, iki yönlü iletişim öğrenciler ya bireysel ya da grup olarak eğitime katıldığında hem bireysel ortam hem de iletişim sistemleriyle zenginleşmiş ortamlar söz konusudur. Bu oluşumdaki teknolojiler, öğretmen-öğrenci ve öğrencilerin kendileri arasında, diğer kuşaklarda yaşanandan çok daha eşit bir iletişim ağı sağlanabilir [16].

IV. E-ÖĞRENİM BİLGİ GÜVENLİĞİ

Uzaktan eğitim e-öğrenim sürecinde sistem güvenliğinin sağlanması önemlidir. Hem kurumun bilgi güvenliği açısından hem de kullanıcı memnuniyeti açısından çok önem taşır.

Sunucu Güvenliği: Sunucular, istekler doğrultusunda gerekli uygulama hizmetlerini karşılayan cihazlar olması nedeniyle ağlar içerisinde en fazla göz önünde olma özelliğine sahiptirler. Sunucular, hem içerdikleri uygulamalar ve hem de üzerlerindeki diğer donanımsal parça çeşitliliği ile çok fazla üreticinin ürünlerini kendi bünyesinde toplarlar. Bu karmaşık yapı saldırılar karşısında doğabilecek hata veya açık olasılığını artırır. Bu nedenlerle sunucu üzerindeki uygulama ve işletim sistemleri, çıkan yeni yazılım sürümleri, 'fix'ler ve 'patch'lerle desteklenmelidir. Bunun yanı sıra sunucu ve uygulama güvenliğini hedef alan saldırılar karşısında, sunucu ve ağ temelli saldırı saptama sistemleri ile bu saldırıların saptanarak durdurulması gibi etkinlikler gerçekleştirilebilir. Böylelikle doğabilecek saldırılar anında engellenebilir.

İstemci Erişim Kontrolü: Cihazlara ve uygulamalara erişim kontrolü sayesinde istenmeyen kişilerin erişimini engellemek ve kısıtlamak mümkündür. Bu amaçla kullanılan kimlik kontrol ve yetkilendirme sunucuları, erişim kısıtlama veya sınırlandırma gibi etkinliklerini gerçekleştirir. Erişim kontrolü, gerekli kayıtları toplar ve bunun sonucunda ayrıntılı raporlar üreterek sistemlere ulaşan ve ulaşmakta başarısız kalan girişimleri, kullanım süresi gibi kritik bilgileri sistem sorumlularının dikkatine sunar.

Sistemin Saldırlara Karşı Korunması: Saldırlara karşı sistemleri korumak bilgisayar ağına, tek bir sistemin veya cihazın eklenmesi olarak düşünülmemelidir. Ağ içerisinde bulunan her sistem ve cihaz üzerinde gerekli tedbirler alınarak, kurumun iş modeline ve ihtiyaçlarına uygun bir güvenlik politikası oluşturulmalıdır. Politika, kurumla birlikte yaşayıp sürekli güncellenerek, kurum gereksinimlerini karşılayacak şekilde yenilenmelidir. En güvenli sistem kurulsadahi ağ sürekli gözlem altında tutulmalı ve gözlemler doğrultusunda doğabilecek sakıncalar ilk aşamada önlenmelidir [17].

E-öğrenim alanında özellikle "UE Kayıtları", "Bitirme Projeleri" e-öğrenim ve UE uygulamaları ile ilgili yasal düzenlemeler, internet üzerinde UE programı'nın en önemli bileşenleridir. E-öğrenimde en iyi bilinen sorunlar uzaktan eğitim uzman/danışmanları, teknik altyapı, artan maliyetler, kaynak ve bilgi yönetiminde yaşanan çeşitli sıkıntılardır. Bu

açıdan internet üzerinden uzaktan eğitim e-öğrenim stratejisinin temelinde e-öğrenim-net omurgasını, standartları, veri elemanları, tanımlamalar ve kodları oluşturan veri sözlüğü, e-kütüphaneler, bilgi-bankaları veri paylaşımı", "çevrimiçi eğitim hizmetleri, UE temelini oluşturur. UE yaşam boyu eğitim kayıtlarında öğrenim süreci kayıtları içeren bilgilerinin gizlilik, güvenlik ve mahremiyet ilkeleri doğrultusunda korunmasını sağlamak için sayısal güvenlik önemlidir. Özellikle sanal ders sürecinde çekilen görüntüler, uluslararası standartlara uygun bir şekilde sayısal görüntü haline çevrilir. İnternet üzerinden UE bilgi sistemi ile tam entegre sayısal görüntüleme sistemleri; yeni gelişen bilişim ve telekonferans, servislerini de kapsamı içene alır. Çok çeşitli e-öğrenim süreçlerinin anında izlenerek evden/ofisten eğitim teknolojileri, kuşkusuz eğitim bilgileri, özelliği nedeniyle, gizlilik, güvenlik ve mahremiyet ilkeleri doğrultusunda büyük bir titizlikle korunan bilgilerdir. E-öğrenimde uzaktan eğitim sürecinde en önemli konulardan olan enformasyon güvenliği, tam bir güvenlik ortamında sağlanabilir. Bu süreçte taraflar güvenli olarak e-öğrenim sürecinde başlayabilir. Bu güvende çeşitli şifreleme yöntemleri, algoritmalar, sayısal imzalar ve sertifikalar gibi birçok temel öğeler sisteme entegre edilmelidir. Bilginin güvenli tutulması, bilgi güvenliği politikaları ve teknik altyapı olmak üzere iki önemli safhayı içerir. İnternet üzerinden e-öğrenimde UE organizasyonunda güvenlik stratejisi bu ölçütler doğrultusunda değerlendirilerek, ortaya çıkacak yeni gereksinimlere göre güvenlik ölçütleri değişik düzeylerde yeniden incelenmelidir. Bu anlamda e-öğrenim kayıt/katılım bilgileri güvenliğinin en üst düzeyde sağlanarak, kişilerin e-öğrenim kayıtlarına öğrenci/danışman izni doğrultusunda erişim yetkisi ile mümkündür. Bu karakteristiklere göre kimlik denetim sistemi tarafından karşılanması gereken ihtiyaçlar; sağlamlık, alan-kesiştirici kimlik denetimi, ölçülebilirlik ve performans olarak sıralanabilir [18]. İşlemcili kartlara akıllı kart denir. Akıllı kartlar e-imza gibi uygulamalar için en güvenli ve kullanımı kolay araçlardır. Akıllı kartlar, sağladığı kolaylıkların yanında her geçen gün üzerine eklenen yeni yetkinlikler sayesinde hayatın her alanında kullanılır bir konumdadır. Akıllı kartların, verimliliği arttırdığı ve maliyetleri düşürdüğü için hem özel sektör, hem de kamu projelerinde kullanımı bir zorunluluk haline gelmiştir [19]. E-öğrenim kapsamında kayıtlarına erişim denetimi ve gizlilik ilkelerine yönelik etik ve yasal düzenlemeler önemlidir. Kişisel eğitim bilgilerinin dijital ortamlarda korunması, gerektiğinde kişinin izniyle istendiği yerden ulaşılabilmesi ve kişilerin tanınmasını önleyecek şekilde toplumsal bilgilerin istatistiki sonuçlarının yaygın kullanımı eğitim alanında verimlilik ve etkinliğini önemli ölçüde artırabilir. Bilgilerin gerektiğinde kolaylıkla paylaşımında ortak standartlara, bilgilerin gizliliğinin korunabilmesi için de güvenilir denetim ve gözetim sistemlerine ihtiyaç vardır. Teknolojilerinin yapı taşı olarak, kimlik denetim sistemi kullanıcıların kimliklerini doğrularken servislere yetkisiz girişleri engellemek için önemli bir rol üstlenir. E-öğrenim sisteminin güvenliği kontrol alanları;

- 1- UE bilgi güvenlik politikası,
- 2- E-öğrenimde bilgi güvenliği organizasyonu
- 3- Öğretim sistemi bilgi yönetim sistemi
- 4- UE insan kaynağı güvenliği
- 5- UE fiziksel ve çevresel güvenlik işlemleri
- 6- İletişim ve güvenli işletim yönetimi
- 7- Çoklu erişim denetimi ve güvenliği
- 8- E-öğrenim bilgi sistemleri gelişim ve bakımı
- 9- E-öğrenim bilgi güvenliği ihlalleri yönetimi
- 10-E- öğrenim sürekliliği yönetimi
- 11-E-öğrenimde entegrasyon ve uyum

V. SONUÇ VE DEĞERLEMELER

Bu açıdan, e-öğrenim sürecinde uzaktan eğitim uygulamaları oldukça farklı sistemlerin bütünsel ve hassas bir entegrasyonunu gerektirir. UE ile e-öğrenim olanakları kurumsal çapta eğitim teknoloji işletmeleri öncülüğünde, kendi çalışanlarına yönelik eğitimler güvenlik kültürünü de kapsayan bir yaklaşım içinde sağlanır. E-öğrenim süreçlerinde ortaya çıkan zayıf yönlerin zamanında yüz yüze eğitim süreci ile desteklenerek giderilmiştir. Sistemin olgunluğa erişimi, tasarım ve sistematigi, belli standartların kullanılışı, hazırlanan içeriklerin sürekli güncellenerek çekiciliğinin artırılması, çalışabilirliği, kalitesi, birbirleriyle uyumlu hale gelen internet alt yapısında, öğrencilerin derse katılımının artışında çekici bir model yapısına erişim esastır. UE bütünsel yapısında kişinin en kısa sürede davranış değişikliğine yol açan, kendine ve iş sonuçlarına pozitif etkili eğitsel aktivitelerin uyumlu birliğidir. Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini hedefleyen tehditlere karşı yazılımlarda bilgi güvenliğinin sağlanmış olması gerekir. Bilgi güvenliği hedefleri, tehditlerin farkında olmak, işlerin devamlılığını sağlama, Kayıpları en aza indirme, kuruluşların varlıklarının her koşulda gizliliği, erişilebilirliği ve bütünlüğü koruma evrelerinden oluşur. E-öğrenim sisteminde Bilgi Güvenliği Yönetim Sistemi (BGYS) bu amaçları gerçekleştirmek için ortaya çıkan ve sürekli geliştirilen bir sistemdir. Yazılım geliştirme sürecinde BGYS sağlanmış olması; Yazılımdaki bilgilerin kullanıma hazır olması, Sadece yetkisi olanların erişebilmesi, Bilginin doğru ve güncel olması önemlidir. Yazılımın her aşamasında güvenliğe ilişkin ortaya çıkabilecek problemleri gözetin etkin bir geliştirme süreci sonuç ürünün daha güvenilir olmasına önemli katkı sağlayacaktır. E-öğrenim yazılım döngüsünü analiz, tasarım, kodlama, test, bakım, düzeltim ve yeniden gelişim evrelerinde hazırlanabilir. BGYS, bilgi güvenliğini kurmak, işletmek, izlemek ve geliştirmek için iş riski yaklaşımına dayalı, doküman

edilmiş, işlerliği ve sürekliliği garanti altına alınmış bir yönetim sistemidir. Bu süreçler Planla, Uygula, Kontrol et, Önlem al (PUKÖ) döngüsünden oluşan bir model olarak da ortaya konmuştur. Diğer yandan, UE içinde internet üzerinden, sanal sınıflarda yapılan derslerin yanı sıra, yüz yüze eğitim olanaklarının birleşimi karma eğitim modeli yapısında, etkinlik olumlu yönde artabilir. UE, modelinin işletiminde, sistemin kullanıcılar ile etkileşimi, tepkileri, eleştirileri ile karşılaştıkları sorunlar yakından izlenerek kişilerin kendisini sistemle baş başa ve yalnızlığı yerine, sistemin sürekli desteklediği duygusunun yaşanırılığı sağlanabilir. Katılımcıların performans izlenimi ile düzenli raporların sonuçları katılımcılarla paylaşılarak kurumsal kültür kazanımı hızlanır. UE'lerinin daha net anlaşılabilirliği için, kavramlar, standart ve akreditasyonun çoklu katılımlarla, ulusal/uluslararası düzeyde sürekli gelişimi gerekir. Katılımcılar e-posta, telefon ve faks aracılığıyla ilgili ders danışman ve eğiticilerine erişebilir. İletişim sürecinde etkileşim, eşzamanlılık (senkron veri akışı), zaman ve mekan sınırını ortadan kaldırışı, iletişim dönencesi gibi geleneksel kitle iletişimin ötesinde yeni medyalara özgü avantajlarının kitle iletişim araçları kullanılarak gerçekleştirilen UE gelişimini hızlandırır. E-öğrenim alanında derslik, televizyon ve kitabın yanında internet üzerindeki "sanal sınıflar" da eğitim gelişim dinamizmini arttırmaktadır. E-öğrenim sürecinde son gelişmeler ışığında öğrenim mimarisi ve öğrenim standartları konusunda öğretim yönetim sistemleri kullanılarak etkin işletimi sağlanabilir. Uluslararası akademik etkileşimde; dil eğitimi, uluslararası konferanslara geniş bir katılım, potansiyel ortak üniversitelerin gelişimi, akademik etkileşimin cesaretlendirilerek ödüllendirilebilir. Katılımcılar e-eğitim merkezi ile iletişimlerini direkt e-posta, telefon, faks aracılığıyla gerçekler. Kendi iş çevrelerine ve genel hayata özgü kritik beceri ve yetkinlikler kazanır. Bu yetenekler grup ve takım içerisindeki işbirliği becerileri, yazım yeteneği, araştırı yeteneği, iletişim becerisi, çoklu ortam paylaşım yeteneği ve on line öğrenim topluluğundaki kaynaklara erişim yeteneğidir. Günümüz öğrenim gereksinimini yanıtlayan e-öğrenimde; asenkron (kendisel); kişinin kendi kendine internet ve CD-ROM vasıtasıyla kurslar, videoya çekilen sınıflar, işitsel-görsel olarak web sunumları, online müzakere, senkron (Eş zamanlı öğrenci-öğretmenin sanal sınıfta canlı buluşması); sanal sınıflar, işitsel ve görsel konferanslar, internet üzerinden telefon bağlantısı, çift taraflı (interaktif) ve canlı udu yayınlardır. UE programı yüz yüze eğitim ile birleştirilebilir. Sistemin, esnek, kullanıcı dostu ve kişisel nitelikte uyumlu tasarımı gerekir. Eğitimlerden istenen eğitimi parçalar halinde verilmesi, katılımcıların geçmiş bilgi ve deneyimle ilişkiler, kişilerin kendi bilgi, deneyim ya da çalışma ortamları ile ilgili örneklerle karşılaştırmalar, değişken sunumlar, geri bildirim desteğinde öğrenim ödüllendirilir. UE yönetimi, klasik anlamda eğitim yönetiminden farklı düşünsel ve yönetsel beceri ve modelleri gerektirir.

Bilişim olanaklarının giderek arttığı dijital ortamda yaşayacak bireylere gerekli genel yetenekleri kazandırabilen

teknolojik ortamın gerektirdiği niteliklere sahip insan gücünü yetiştirip teknolojik olanaklardan yararlanan, eğitilen öğrencilerin yapısal değişimi, e-öğrenimde beklentilerin değişimi, bilginin üretimi ile yaygınlaşan teknolojinin açık ve baskın etkisi, eğitim-öğretimde etkin eğitsel yaklaşımların gelişimidir. Bilgi toplumu hizmetlerinin gelişiminde bilgi güvenliği, korunma, uluslar arası standartlar, gerekli düzenlemeler, kullanıcı ve servis sağlayıcıların görev tanımlamaları, kullanıcıların bilgilendirilerek bilinçlendirilmesi, bilgi güvenliği için hukuki, teknik ve idari tedbirlerin alınması oldukça büyük önem taşır. Uzaktan eğitim sürecinde kurumsal güvenlik politikası geliştirilmesi, bilgi güvenliği konusunda oluşturulan standartların kullanımına itina gösterilmelidir. Kişisel verilerin mahremiyetinin korunması, istek dışı haberleşmenin önlenmesi, iletişim ağı güvenliği, işletim sistemi güvenliği, veri tabanı, internet erişim, terminal cihazı ve sistem güvenliği, özetle, toplam sistem güvenliği içinde sağlanmalıdır [20]. E-öğrenim sürecinde güvenli yazılım geliştirme sürecinde ele alınması gereken temel olarak ana güvenlik konuları öne çıkar. Girdi geçeri, kimlik doğrulama, yetkilendirme, konfigürasyon yönetimi, hassas bilgi, kriptografi, parametre manipülasyonu, hata yönetimi, kayıt tutma ve denetimdir. Sonuçta, tüm bilim dallarının katkısı yanında, matematik alanındaki yeni gelişmelerin desteğinde, e-öğrenimde internet üzerinden uzaktan eğitimin akademik gelişim düzeyi daha da gelişmiş bir konuma gelmiş bulunmaktadır. Bu açıdan yaklaşımlar eşliğinde, e-öğrenimin akademik değerlendirilmesi oluşturulacak kalite ve standartların artan oranda bir güven, katılım ve geleceğe doğru sürekli gelişen yeni ve yüksek güvenilirliği olan etkin ve kaliteli bir model oluşturabilecektir.

VI. KAYNAKLAR

- [1] Daft, R., Management, Dryden, 2000, s. 7.
- [2] Ülgen, H. ve Mirze, S.K., İşletmelerde Stratejik Yönetim, Arıkan, İstanbul, 2007, s. 423.
- [3] Kuzgun, Y., Rehberlik ve Psikolojik Danışma, (5. Basım), Ankara, ÖSYM Yayını, (1997).
- [4] Langford, P. David ve Barbara A. Cleary. Eğitimde Toplam Kalite, 1999.
- [5] Yöney, H., Profesyonel Zeka, Remzi Kitabevi, İstanbul, 2007, s. 83.
- [6] Onat, E., Mimarlığa Yolculuk, Yem Yayın, İstanbul, 2006, s. 54.
- [7] Davidson-Shivers, G. and K.L. Rasmussen, Web-based Learning, USA: Merrill-Prentice Hall, 2006.
- [8] Öncü, A., ve Varol, S., "Uzman Sistem Teknolojisi ile Web Tabanlı Sınav Değerlendirme Modeli Geliştirilmesi", IETC, 6th International Education Technology Conference", North Cyprus., 19-21 April, 2006, s.1327-1331.
- [9] Ahire, S.L., Ravichandran, T., "An Innovation Diffusion Model of TQM Implementation" IEE, Transactions on Emerging Management, November 2001, Vol.48, No.4.
- [10] Cebeci, Z., ve diğ., "Karma Yem Sanayinde Ağ Tabanlı İzlenebilirlik Sistemi Tasarımı ve Uygulaması", Bilişim 08, Bildiriler Kitabı, Ankara, 2008, s.82-89.
- [11] Tanenbaum, A., Computer Networks, New Jersey:Prentice Hall, 1988.
- [12] Laudon, K.C., "E-Commerce", Prentice Hall, 2006.
- [13] Trentin, G., The Quality-Interactivity Relationship in Distance Education, Educational Technology 40, January-February, 2000, 1: 17-27.
- [14] Girginer, N., Uzaktan Eğitim Kararlarında Teknoloji, Maliyet, Etkinlik boyutları ve Uzaktan Eğitime Geçiş İçin Kavramsal Bir Model Önerisi. Doktora Tezi, Eskişehir, 2001.

- [15] Moore, M.G. and Thompson, M.M., The Effects of Distance Learning. Pennsylvania: The Pennsylvania State University, 1997.
- [16] Bates, A.W., Technology, Open Learning and Distance Education. London: Routledge, 1995.
- [17] Türkiye Bilişim Vakfı, "E-Öğrenme Klavuzu", 2003.
- [18] <http://www.tbv.org.tr/TBV/Documents/EgitimveBilisim/UzaktanEgitimKlavuzu.pdf>.E.T. 2009.
- [19] Zrelli, S., Medeni, T., Shinoda, Y., Medeni İhsan Tolga, Kurumlar Arasındaki Alan-Kesitirici İşbirliği İlişkisi İçin Kerberos Güvenlik Sistemini Geliştirme: Gelişen Doğrulanabilir E-Toplum İçin Yenilikçi Bir Bilgi Teknolojisi Örneği, Ulusal E-İmza Sempozyumu, Ankara, 2006, s.105-115.
- [20] Özbey, R. S., Akıllı Kart Teknolojileri, Ulusal E-İmza Sempozyumu, Ankara, 2006, s.208-211.

Yüz Çehresi Ebatları ve Yapay Sinir Ağları Kullanılarak Yüz Tanıma

Birol Tilki¹ ve Bekir Karlık²

¹İstanbul Meslek Yüksekokulu
Fatih Üniversitesi, İstanbul
birolt@fatih.edu.tr

²Bilgisayar Mühendisliği Bölümü
Mevlana Üniversitesi, Konya
bkarlik@mevlana.edu.tr

Özetçe—Biyometrik tanıma ve kimliklendirme yakın zamanlarda güvenlik ve teknoloji alanlarında önem kazanmış ve önemli bir örüntü tanıma sistemlerinden biri haline gelmiştir. Bu çalışmada farklı bir yöntem kullanıldı. Bu yöntemde, yüzdeki organların ebatları ve bu organlar arasındaki mesafe ölçülerek bir veri dosyası elde edildi. Ölçümlerde PhotoShop programı kullanıldı. Ölçülen bu organ ebatları yapay sinir ağları ile eğitilerek yüz tanıma işlemi gerçekleştirildi.

I. GİRİŞ

İsteğe bağlı (arbitrary) sahnelerinde nesne algılama bilgisayar görme de önemli ve zor bir araştırma konusudur. Aydınlatma şartları, boyutları, pozları ve başaşağı nesneleri algılama gibi faktörler sonucu etkileyebilir. Bir nesne algılama sisteminde genellikle iki temel bileşen, özellik çıkarma ve sınıflandırmanın olması gerekir.

İnsanın biyolojik yapısını modellemenin giderek öne çıktığı son yıllarda, yüz tanıma sistemlerinin önemi de giderek artmaktadır. Yüz tanıma sistemlerinin çalışma mantığı diğer biyometrik tanıma sistemleriyle bire bir aynıdır. Yüz tanıma sisteminin temelinde her insanın farklı ve benzersiz bir yaratılışa sahip olması yatmaktadır. Yüz tanıma, havaalanı gibi güvenlik kontrolü istenen yerlere girişte, bankacılıkta ve finans sektöründe kimlik onaylamada, insan-makine etkileşiminde ve aranan suçlu kişilerin tanınmasında kullanılan özel bir örüntü tanıma (pattern recognition) konusudur[1-2]. Yeni öznelik vektörü çıkarma ve sınıflandırma tekniklerinin gelişmesiyle son yıllarda yüz tanıma alanında önemli gelişmeler kaydedilmiştir.

Gelişmiş optik teknolojileri ve yüz model çıkarma algoritmaları kullanılarak, farklı açılardan birçok yüz görüntüsünü elde edilir. Farklı görüntülerden kişinin 3D görüntüsü elde edilir. Elde edilen görüntüler bir yüze ait bir veritabanında saklanır. Daha sonra tanıma sırasında kişinin yeni görüntüleri optik teknolojilerle elde edilir. Yeni görüntüler veritabanında kayıtlı olan eski görüntüyle karşılaştırılır. Görüntüler aynıysa kişinin yüzü tanınmış olur.

Yüz tanıma kullanılan çok çeşitli teknikler olmasına rağmen, aslında bu tekniklerin büyük çoğunluğu ya sınıflandırıcı ya da öznelik vektörü çıkarımında ki farklılıklardan geliştirilmiş tekniklerdir. Kullanılan öznelik vektörlerinden bazıları; Dalgacık dönüşümü [3], Gabor Filtresi [4], Temel Bileşen Analizi (PCA) , Doğrusal Discriminant Analizi (PDL), Özdeğer ve özvektörleri (Eigen Faces ve Fisher Faces) [5-6], 2B-HFD Tabanlı Özneliklerin Ortak Matris Yaklaşımı [7] vb sayılabilir. Kullanılan sınıflandırıcılar ise En yakın komşuluk, Şablon eşleme, Bulanık Sınıflandırıcı ve Yapay Sinir Ağlarıdır [2, 8]. Yapay sinir ağları; ses tanıma, karakter tanıma, robot görme ve görme tabanlı kontrollerde, görüntü ve yüz tanıma sistemlerinde çok sık olarak kullanılmaktadır. Yüz tanıma kullanılan YSA algoritmalarının bazıları; Geriye Yayılım (Back-Propagation) [9], Radyal Temel Fonksiyon (Radial Basis Function-RBF) [10], Kendini Düzenleyen Harita (Self Organizing Map-SOM) [11], Destek Vektör Makinaları (support vector machines-SVM) [4].

Yüz tanıma da Yapay Sinir Ağları çok etkin olmasına rağmen, farklı ayarlar (sınıflar) ve örtüşen değerler ile zaman ayırt edici olan ikizler suratlarında YSA eğitim süresi sınırlıdır [Aleksievs M, Glazs A].

Klasik yüz tanıma işleminde, PCA, PDL, Dalgacık, Ayrık Kosinüs vb gibi değişik dönüştürme yöntemleri kullanılarak resim nümerik değerlere dönüştürülür. Bu çalışmada makalede farklı ve basit bir yöntem kullanarak yüz çehresindeki organların ebatlarını ve bu organlar arasındaki mesafeyi ölçerek bu değerleri YSA ile eğitilmesi ile yüz tanıma işlemi gerçekleştirdik. Çehreye ait ebatların ölçümlerinde PhotoShop programı kullanılmıştır.

II. YÖNTEM VE SONUÇLAR

Genellikle yüz tanıma sisteminde, Şekil 1'de [13] görüldüğü üzere yüksek çözünürlüklü optik kameralarla insan yüzü taranır. Bu tarama sonucunda insan yüzündeki belli noktalar ve bu noktaların birbirine mesafesi belirlenir ve bunlar referans alınarak insan yüzünün bimetric bir haritası çıkarılır.



Şekil 1: Yüzün bimetrik haritasının çıkartılması

Çıkarılan bu Biyometrik harita daha sonra ki yüz okutmalarda referans olarak alınır ve yüz tanıma için eşleştirilmeden kullanılır.

Yüz tanıma teknolojisinin avantajları şunlardır:

- İnsan yüzlerini tanınır ve kimlik tespiti yapılır
- O anda veritabanı sorgusu yapılır
- Hareket Algılama Özelliği ile yüz bulunamasa bile tüm hareketleri kayıt altına alınır
- Kişilerin fotoğraf veya video görüntüleri kayıt edilebilir

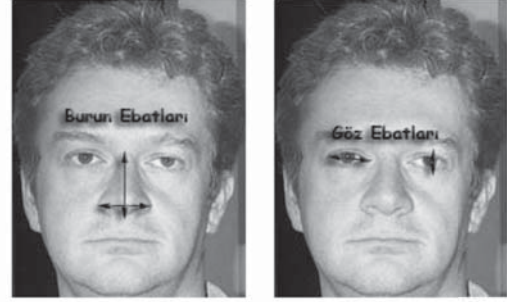
Yüz Tanıma Sistemlerinde kişilerin kamera görüntüleri kullanılarak gerçek zamanlı veritabanı sorgusu ve tehlikeli/şüpheli olarak belirlenmiş şahısların tespiti durumunda alarm vererek anında müdahale olanağı mümkündür. Sistem kullanılarak banka şubeleri, ATM'ler güvence altına alınabilir.

Yüz tanıma sisteminde işlem adımları şu şekildedir:

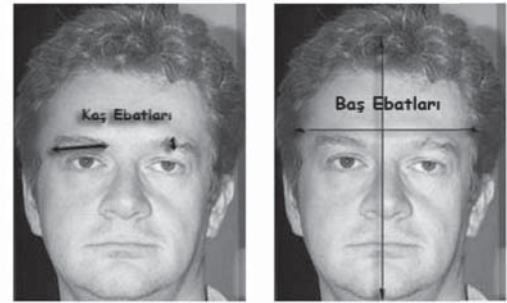
- 1) İnsan yüzleri otomatik olarak tespit edilir.
- 2) Özel görüntü veri tabanından otomatik veya manuel olarak sorgu başlatılır.
- 3) Tespit edilen yüz hangi kişiye ait ise tespit edilir.
- 4) Kişi daha önce şüpheli veya tehlikeli olarak kaydedilmiş ise, konfigüre edilebilen sesli ve görsel alarmlar üretilir.
- 5) Yalnızca yüz görüntü eşleşmeleri değil, algılanan tüm hareketler hareket tablosunda saklanır ve incelenebilir.
- 6) Kaydedilmiş video dosyalarından kayıt gerçekleştirilebilir.
- 7) Bu fonksiyon ile özellikle geçmişe yönelik kişi kayıt ve sorguları gerçekleştirmek mümkündür.
- 8) Kaydedilmiş resim dosyalarından da kayıt etme işlemi gerçekleştirilmektedir.
- 9) Bu fonksiyon ile özellikle personelin veya şüpheli şahısların mevcut resimleri ile sisteme kişi tanıtmak ve sorgu gerçekleştirebilmek mümkün olmaktadır.
- 10) Her kayıt işlemi sırasında kaydı yapılan kişiye ait demografik bilgiler de sisteme kaydedilmektedir.
- 11) Sistemde gerçekleşen tüm eşleşmeler tarih ve saat sırasına göre hareket tablosundan da takip edilebilir.
- 12) Bu tablodan çeşitli parametreler ile sorgu yapmak mümkündür.
- 13) Aynı zamanda yüz olarak algılanmayan, çeşitli anlık hareketlerin resimleri de bu tablodan takip edilebilir.

A. Yüz Çehresinin Özelliklerini Belirleme

Yüze ait 19 özellik belirlendi. Bazı özellikler yüzdeki organların ebatları ve bazıları organlar arasındaki uzaklıktır. Bu özellikler aşağıda Şekil 2, Şekil 3, Şekil 4 ve Şekil 5'de görülmektedir.



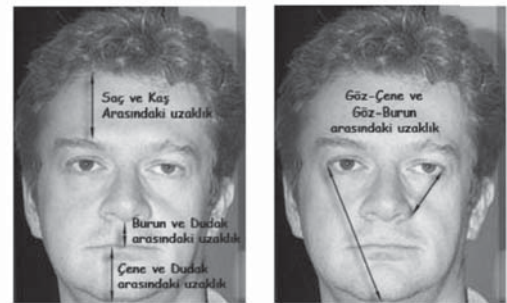
Şekil 2: Burun ve göz ebatları



Şekil 3: Kaş ve baş ebatları



Şekil 4: Yatay uzaklıklar



Şekil 5: Dikey ve çapraz uzaklıklar

B. Kopyalama, Resimlerin Ebatlarını Ayarlamak ve Ölçümleri Yapmak

Yüze ait özellikler belirlendikten sonra 10 kişinin 2'şer resmi bir görüntü galerisinden seçildi. Bu resimlerden birisi sınıflandırma ve diğeri test amaçlı kullanıldı.

Her bir resmin sadece baş bölümünü gösteren kısımları alındı ve bu resimlerin çözünürlükleri eşitlendi. Sonuçların sağlıklı olması için çözünürlüğün eşitlenmesi gerekir. Farklı çözünürlükte yanlış sonuçlar alınabilir.

C. Kaynak Veriler

PhotoShop Measurement aracı kullanılarak her bir resmin yüzüne ait 19 özelliği piksel cinsinden ölçüldü. Bu veriler aşağıdaki Tablo 1 ve Tablo 2'ye kayıt edildi.

TABLO 1
RESİM 1-5 YÜZ ÖLÇÜMLERİ

Yüze ait organların ölçümleri	Resim 1-1	Resim 1-2	Resim 2-1	Resim 2-2	Resim 3-1	Resim 3-2	Resim 4-1	Resim 4-2	Resim 5-1	Resim 5-2
Baş genişliği	147	148	149	151	144	143	140	141	147	148
Baş yüksekliği	210	209	244	243	230	230	205	207	229	228
Burun genişliği	40	41	37	37	41	40	36	36	36	37
Burun yüksekliği	50	52	59	58	58	59	52	54	52	53
Göz genişliği	30	29	30	29	27	26	24	24	29	29
Göze yüksekliği	8	8	10	10	9	8	10	10	12	12
Kaş genişliği	40	42	44	44	52	53	43	44	49	50
Kaş yüksekliği	7	7	10	10	10	10	6	6	5	5
Dudak ve çene arasındaki uzaklık	39	39	46	47	36	37	41	42	26	27
Dudak ve burun arasındaki uzaklık	19	19	23	23	12	11	15	15	19	19
Saç ve kaş arasındaki uzaklık	51	52	57	58	47	49	60	59	55	56
Dudak genişliği	53	54	55	56	52	51	49	52	56	55
Alın genişliği	125	124	124	126	126	127	118	120	127	127
Kaşlar arasındaki uzaklık	27	27	26	26	9	9	21	21	30	30
Kulak ve burun arasındaki uzaklık	51	49	52	53	42	45	42	45	56	56
Dudak ve çene arasındaki uzaklık	31	30	36	35	31	33	30	30	28	29
Burun delikleri arasındaki uzaklık	28	29	26	27	33	32	27	28	25	25
Burun ve göz arasındaki uzaklık	45	44	52	52	50	48	42	42	54	54
Çene ve göz arasındaki uzaklık	112	112	140	141	127	126	124	125	118	119

TABLO 2
RESİM 6-10 YÜZ ÖLÇÜMLERİ

Yüze ait organların ölçümleri	Resim 6-1	Resim 6-2	Resim 7-1	Resim 7-2	Resim 8-1	Resim 8-2	Resim 9-1	Resim 9-2	Resim 10-1	Resim 10-2
Baş genişliği	153	155	148	146	153	154	144	143	136	136
Baş yüksekliği	247	250	226	227	220	218	210	208	237	237
Burun genişliği	42	42	41	41	37	37	41	41	34	34
Burun yüksekliği	50	51	57	58	63	64	58	58	57	57
Göz genişliği	35	35	28	28	31	31	30	30	32	32
Göze yüksekliği	14	14	15	15	14	14	13	13	13	13
Kaş genişliği	62	63	49	50	52	53	38	38	55	56
Kaş yüksekliği	15	15	10	10	6	6	4	4	9	9
Dudak ve çene arasındaki uzaklık	49	50	50	48	42	40	37	36	40	39
Dudak ve burun arasındaki uzaklık	23	24	20	19	19	19	13	12	22	21
Saç ve kaş arasındaki uzaklık	75	77	41	41	45	46	44	42	52	51
Dudak genişliği	56	57	62	60	46	46	50	50	54	55
Alın genişliği	148	148	125	124	119	119	130	131	91	93
Kaşlar arasındaki uzaklık	16	16	23	23	16	16	30	30	22	22
Kulak ve burun arasındaki uzaklık	52	55	46	45	53	54	53	54	47	47
Dudak ve çene arasındaki uzaklık	38	40	32	30	40	40	35	34	33	32
Burun delikleri arasındaki uzaklık	27	27	30	30	29	29	28	28	25	26
Burun ve göz arasındaki uzaklık	47	47	43	44	52	52	52	52	49	50
Çene ve göz arasındaki uzaklık	139	140	140	138	134	132	123	122	134	135

Resimler ölçüldükten sonra, kaynak ve test resimleri birbirinden ayrıldı. Giriş ve Test verilerinin ölçüm sonuçları 100'e bölünerek verilerin normalizasyonu yapıldı.

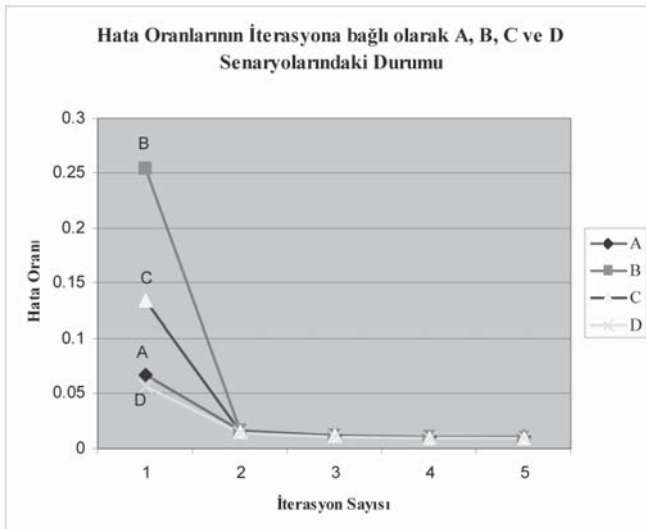
D. YSA ile Eğitim ve Test

Bu çalışmada, sınıflandırıcı olarak bilinen çok katmanlı idrak (multi layered perceptron-MLP) yapısı seçildi. Yüz çehresine ait 19 veri giriş katmanına, gizli katmanlarında her bir senaryoda aynı oranda nöron sayısı kullanılmış olup çıkış bir tanedir. YSA eğitim algoritması Geriye Yayılım (Back-propagation) olarak kullanıldı. Aşağıdaki Tablo 3'de yer aldığı gibi farklı MLP yapıları (A, B, C ve D) ve onlara ait yine farklı uygun sabitler kullanarak ağ eğitildi ve tablonun son sütunundaki hata oranları (MSE) bulundu.

TABLO 3
Farklı MLP yapısına göre bulunan hata oranları

	İterasyon	Öğrenme oranı	Momentum	Nöron sayısı	Hata Oranı
A	1000	0,95	0,1	20	0,067
	2000	0,95	0,1	20	0,016
	3000	0,95	0,1	20	0,012
	4000	0,95	0,1	20	0,011
	5000	0,95	0,1	20	0,011
B	1000	0,95	0,01	20	0,254
	2000	0,95	0,01	20	0,016
	3000	0,95	0,01	20	0,012
	4000	0,95	0,01	20	0,011
	5000	0,95	0,01	20	0,01
C	1000	0,95	0,01	8	0,134
	2000	0,95	0,01	8	0,015
	3000	0,95	0,01	8	0,012
	4000	0,95	0,01	8	0,01
	5000	0,95	0,01	8	0,01
D	1000	0,95	0,01	30	0,057
	2000	0,95	0,01	30	0,014
	3000	0,95	0,01	30	0,011
	4000	0,95	0,01	30	0,01
	5000	0,95	0,01	30	0,01

Tablo 3’den de görüleceği gibi, tüm ağ yapılarında aynı öğrenme oranı (0,95), momentum sabiti A tipi ağda 0,1 ve B, C ve D tipi ağlarda 0,01, A ve B de gizli katmandaki nöron sayısı 20, C de 8, D yapısında ise 30 olarak kullanıldı. İterasyon sayısına bağlı olarak hata oranlarına bakıldığında en iyi sonucu D tipi ağ [0,057-0,01] vermiştir. Tüm ağ yapıları için iterasyona bağlı hata grafiği Şekil 6’da verilmiştir.



Şekil 6: İterasyona bağlı hata grafiği

III. TARTIŞMA

Bu çalışmada çehreye ait ebatlar yapay sinir ağlarına giriş yapılarak basit ama kullanışlı bir Yüz Tanıma algoritması sunulmuştur. Sunulan yüz tanıma algoritması ile için elde edilen yüz resimleri %99 doğruluk oranıyla tanındı. YSA dışında eşleşme algoritmalarının eşleştirmelerin de belki basit matematiksel çıkarımlarla sonuca ulaşmaktadırlar. Fakat eşleme algoritmasında elde edilen sonuçların kesinliği kullanıcı tarafından kontrol edilmektedir. YSA kullanıldığında ise kullanıcı ve sistem için böyle bir denetlemeye ihtiyaç yoktur. Bu kullanıcıya ve sisteme büyük bir kolaylık sağlar. Zira, bir polis sisteminde aranan kişinin resmi veri tabanındakilerle karşılaştırıldığında 10 binlerce resim bulunan veri tabanında belki de onlarca çok yakın olan eşleşme arasında seçimi zor olabilir. Bu nedenledir ki yapay sinir ağlarının yüz tanıma sistemlerinde önemini artırmaktadır. Ayrıca önerilen özellik çıkarma yönteminde daha az veri kullandığından Dalgacık dönüşümüne göre daha iyi performans elde edilebilir.

IV. KAYNAKÇA

- [1] Anil K. Jain, Robert P.W. Duin, and Jianchang Mao, Statistical Pattern Recognition: A Review, IEEE Transactions On Pattern Analysis and Machine Intelligence, Vol. 22, No. 1, January 2000.
- [2] Brunelli R and Poggio T. Face recognition: Features versus templates, IEEE Transaction on Pattern Analysis and Machine Intelligence, 15, 1042-1052, 1993.
- [3] Khalid Saeed, Jerzy Pejaś and Romuald Mosdorf, Wavelet Transform in Face Recognition, book chapter of Biometrics, Computer Security Systems and Artificial Intelligence Applications, January 11, 2007
- [4] Amin MA, Yan H, An Empirical Study on the Characteristics of Gabor Representations for Face Recognition, Int. Journal of Pattern Recognition and Artificial Intelligence, 23, (3), 401-431, 2009
- [5] Sahoolizadeh H, Ghassabeh Y.A. Face Recognition using Eigen-faces, Fisher-faces and Neural Networks, Proceeding of 7th IEEE International Conference on Cybernetic Intelligent Systems, Leicestershire, England, 287-292, 2008
- [6] Swets D. L. and Weng J. Using Discriminant Eigenfeatures for Image Retrieval. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(8):831–836, August 1996.
- [7] Ergin S., M. Yılmaz, S. Çakır ve E. Seke, “Yüz Tanımda 2B-HFD Tabanlı Özneliklerin Ortak Matris Yaklaşımı’nda Kullanılması,” Bildiri Kitapçığı, Akıllı Sistemlerde Yenilikler ve Uygulamaları Sempozyumu (ASYU’08), Isparta, 2008
- [8] Juang C.F, Sun W.K, Chen G.C. Object detection by color histogram-based fuzzy classifier with support vector learning, *Neurocomputing*, 72 (10-12), 2464-2476, 2009
- [9] Khashman A. Application of an emotional neural network to facial recognition, *Neural Computing & Applications*, 18 (4), 309-320, 2009
- [10] Wang W.H. Face Recognition Based On Radial Basis Function Neural Networks, Proceeding of Inter. Seminar

- on Future Information Technology and Management Engineering, Leicestershire, England, 41-44, 2008
- [11] Monteiro I.Q., Queiroz S.D., Carneiro A.T., et al. Face Recognition Independent of Facial Expression Through SOM-based Classifiers, Proceedings of International Telecommunications Symposium (ITS), Fortaleza, Brazil, 1-2, 263-268, 2006
- [12] Alekseichevs M and Glazs A. Face Recognition Using Ensemble of Neural Networks, Proceeding of 1st International Conference on Agents and Artificial Intelligence, Porto, Portugal, 144-149, 2009
- [13] http://www.meyer.com.tr/bio_face_d.htm

Kurumsal Risk Değerlendirmesi

Emine UÇAR, Baha ŞEN

Milli Eğitim Bakanlığı, Eğitim Teknolojileri Genel Müdürlüğü, Bilişim Hizmetleri Dairesi Başkanlığı, Yönetim Bilgi Sistemleri Şubesi,
Zemin Kat, B.Blok ANKARA, e-mail: emine_shn@meb.gov.tr
Karabük Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Balıklar Kayası Mevkii 78050, KARABÜK,
e-mail: baha.sen@karabuk.edu.tr

Özet—Günümüzde kurumların sahip olduğu bilgilerin gizliliği, bütünlüğü ve ulaşılabilirliğine ilişkin güven ortamının oluşturulması, stratejik bir önem taşımaktadır. Bu nedenle kurumlar bu bilgilerin güvenliğini sağlamak için tüm kurum çalışanlarını kapsayan bir kurumsal risk yönetim prosesine ihtiyaç duymaktadır.

Risk yönetim stratejisi; kurumun risk yönetim anlayışını, temel prensiplerini, genel risk alma isteğini ve profilini, temel görev ve sorumlulukları gibi konulara açıklık getirmelidir.

Kurumsal Risk Yönetimi; kurumu etkileyebilecek potansiyel olayları tanımlamak, riskleri kurumsal risk alma profiline uygun olarak yönetmek ve kurumun hedeflerine ulaşması ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; kurumun üst yönetimi ve tüm diğer çalışanları tarafından etkilenen ve stratejilerin belirlenmesinde kullanılan, kurumun tümünde uygulanan sistematik bir süreçtir.

Bu çalışmada kurumsal risk değerlendirme süreci risk analizi ve yönetimi sırasında yapılması gereken işlemler detaylı olarak anlatılmaktadır.

Anahtar Kelimeler—Risk, Risk Analizi, Risk Yönetimi.

I. GİRİŞ

Korunması gereken ve bir değere sahip olan her şey varlıktır. En temel varlık olan bilgi, bir kurumun en önemli değerlerinden biridir ve birçok formda bulunabilir. Örneğin, kâğıda basılabilir, elektronik olarak depolanabilir, posta veya elektronik yollarla gönderilebilir, filmler üzerinde gösterilebilir ya da sohbetlerde konuşulabilir. Bilgi hangi şekilde olursa olsun, her zaman uygun olarak korunmalıdır[1].

Açıklık, bir varlığı tehditlere karşı korumasız hale getiren kusurlardır. Bir bilgi sistemi varlığı için açıklık, varlığın programlamasındaki hatalar olabileceği gibi, doğal etkenlere (toz, nem, güneş ışığı, yangın, vb) karşı korumasız durumda olması da olabilir. Tehditler, açıklıkları kullanarak varlığa zarar verirler. Bu nedenle, açıklıklar, riskin en önemli nedenidir [2].

Tehdit ise, bir bilgi varlığındaki açıklıkları kullanarak varlığa kısmen ya da tamamen zarar veren etkenlerdir. Bilgi sistemlerine zarar verebilecek üç tip tehdit vardır. Bunlar, doğal tehditler, kasıtsız tehditler ve kasıtlı tehditlerdir [3].

Riskin yukarıda değinilen varlık, açıklık ve tehdit kavramları bağlamındaki tanımı “*bir varlıktaki bir açıklığın bir tehdit tarafından kullanılma ihtimalidir*” şeklindedir[3],[4].

Başka bir tanıma göre ise; risk, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayba ya da zarara uğrama olasılığıdır [5].

Bir varlıkta bulunan açıklıkları kullanan tehditlerin verdiği zararı sıfırlamak ya da azaltmak amacıyla alınan tedbirlere karşı önlem denir. Karşı önlemler riski azaltan faktörlerdir. Bunlar; varlığın değerini düşürücü(kriptoloji), açıklığın değerini düşürücü(yazılım yamaları) ve tehdidin olma ihtimalini düşürücü(eğitim) gibi önlemler olabilir [2].

Kamu kurumlarında sıklıkla karşılaşılan riskler şunlardır[6]:

- Risk analizi yapılmaması
- Kurum içinde bilgi güvenliği konusunda eğitim ve bilinçlendirme faaliyetleri yapılmaması
- İş sürekliliği ve bilgisayar güvenlik olaylarına müdahale faaliyetlerinin yerine getirilmemesi
- Yazılımlar için uygulama geliştirme ve test ortamlarının ayrı olarak bulunmaması, canlı sistemle birlikte olması
- Bilgi güvenliği sorumluluklarının atanmamış olması
- Varlık envanteri eksiklikleri
- Güvenlik olaylarını, zayıflıklarını ve yazılım arızalarını raporlama süreçlerinin olmaması
- Personel eksikliği
- Personel eksikliğine bağlı olarak görevlerin ayrılığı prensibinin uygulanamaması
- Yazılı politika ve prosedür eksikliği

Bu çalışmanın amacı; bilgi güvenliği yönetim sistemi aşamalarından biri olan risk değerlendirmesi, analizi ve yönetimi konusunun detaylı bir şekilde incelenerek kurumlara risk analizi ve yönetimi konusunda yapacağı çalışmalarda katkı sağlamaktır.

II. RİSK DEĞERLENDİRME

Bir kurumun risk altında bulunan bilgi ve diğer varlıkların iş sahasındaki değerini dikkate alarak kendi güvenlik risklerini değerlendirilmesi gerekmektedir. Kurumun kendi iş özelliği ve ortamıyla ilişkili olan ve kurum tarafından seçilen denetim hedefleri ve denetimleri; bir risk değerlendirme prosesi kullanılarak güvenlik risklerinin tanımlanması ve değerlendirilmesi prosesiyle belirlenmesi şeklinde olmalıdır.

Risk değerlendirmesi aşağıdaki faktörlere bağlıdır [3]:

- Varlıkların tanımlanması ve değer atanması
- Tehditler, açıklıklar, yasal ve iş gereksinimleri gibi tüm güvenlik gereksinimlerinin tanımlanması
- Olması muhtemel tehditler ve açıklıklar ile yasal ve iş gereksinimlerinin öneminin değerlendirilmesi

- Yukarıda sayılan faktörlerden çıkarılan riskin hesaplanması
- Uygun risk giderme biçiminin seçimi
- Riskleri kabul edilebilir bir seviyeye indirmek için kontrollerin seçimi.



Şekil I. Risk değerlendirme süreci

A. Risk Analizi

Risk analizi, sonucu itibariyle güvenlik ihlallerine neden olan risklerin ortaya konması ve yorumlanması işlemidir. Risk analizi kendi içerisinde uzun ve ayrıntılı bir prosestir [3].

Risk analizinde ilk olarak bilgi sisteminde var olabilecek tüm varlıklar, bu varlıklardaki açıklıklar ve bu varlıkları etkileyebilecek tüm tehditler ortaya konur. Ayrıca, hâlihazırda mevcut olan karşı önlemler incelenir. Daha sonraki aşamada ortaya konulmuş olan varlık, açıklık, tehdit ve karşı önlemlerinin değerlendirilmesi işlemi yapılır. Son olarak değerlendirilmiş varlık, açıklık, tehdit ve karşı önlem değerleri girdi olarak alınıp, çeşitli metotlar kullanılarak risk değeri bulunur. Nitel ve nicel olmak üzere iki temel risk analizi yöntemi mevcuttur [7].

Nicel risk analizi, riski hesaplarken sayısal yöntemlere başvurur. Nicel risk analizinde, varlık, açıklık, tehdidin olma ihtimali, tehdidin etkisi gibi değerlere sayısal değerler verilir ve bu değerler matematiksel ve mantıksal metotlar ile proses edilip risk değeri bulunur [7].

$$\text{Risk} = \text{Tehdidin olma ihtimali} * \text{Tehdidin etkisi} \quad (1)$$

Nitel risk analizi, riski hesaplarken ve ifade ederken nümerik değerler yerine yüksek, çok yüksek gibi tanımlayıcı değerler kullanır. Nitel risk analizi tehdidin olma ihtimalini kullanmaz, riskin sadece etki değerini dikkate alır [7].

$$\text{Risk} = F(\text{Varlığın değeri}, \text{Tehdidin Etkisi}, \text{Açıklığın seviyesi}) \quad (2)$$

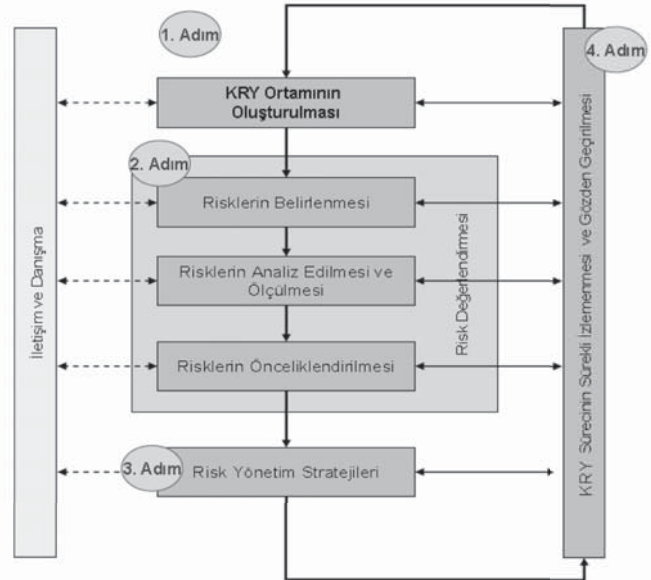
Risk analizi metotlarının avantaj ve dezavantajlarına ait bilgiler Tablo I'de gösterilmektedir [2].

TABLE I
RİSK ANALİZİ METOTLARI AVANTAJ VE
DEZAVANTAJLARI

Risk Analizi Metotları	Avantaj	Dezavantaj
Nitel	Geniş katılıma imkân verir. Süreç tabanlı yaklaşımlar için uygundur.	Sübjektif sonuç verebilir.
Nicel	Eğer basit matematiksel işlemler kullanılırsa uygulaması kolaydır.	Karmaşıktır.

B. Risk Yönetimi

Risk yönetimi, risk analizi sonucunda ortaya konan ve yorumlanan risklerin önüne geçmek ve/veya azaltmak amacıyla uygun, maliyet etkin karşı önlemlerin alınması işlemidir. Karşı önlem maliyetleri ve risk analizi sonucunda çıkan varlık-risk eşleşmesi risk yönetimi prosesi için en önemli girdilerdir. Şekil II'de kamu için kurumsal risk yönetimi risk yönetimi evreleri görülmektedir [6].



Şekil 2. Kurumsal risk yönetimi(KRY) evreleri

Risk analizi sonuçlarına göre, risk yönetimi dört farklı işten birini yapabilir [3].

- Risk yüksektir, karşı önlemler yoktur ya da çok pahalıdır. Varlık kullanılmaz.
- Uygun karşı önlemler alınarak risk düşürülebilir.
- Karşı önlemlerin alınmasının maliyeti, riskin açacağı zarardan çok daha fazla olduğu için risk önemsenmeyebilir.
- Varlıklar sigortalanarak risk transfer edilebilir.

C. Örnek Risk Değerlendirmesi

Risk değerlendirme sürecinde;

1. Adım: Varlıklar tanımlanır. Varlıklar; bilgi varlıkları, yazılım varlıkları, fiziksel varlıklar, insanlar, hizmetler vb. şeklinde sınıflandırılabilirler. Tablo II'de örnek bir varlık envanteri görülmektedir.

TABLE II
VARLIK ENVANTERİ ÖRNEĞİ

SUNUCULAR		
Tipi	Adet	Donanım Özellikleri
E-posta Sunucusu	1	PII 800, 128Mbyte hafıza
DNS Sunucusu	1	PIII 600, 128Mbyte hafıza
Web Sunucusu	2	PIII 600, 128Mbyte hafıza

2. Adım: Varlıklara değer atanır. Varlığın gizliliğine, bütünlüğüne veya elverişliliğine zarar gelme ihtimali varsa; varlıkların her biri için değer biçilmelidir. Bu türden bir değer ölçütüne örnek skala Tablo III'de gösterilmektedir.

TABLE III
ÖRNEK SKALA

Önemsiz(0)	Varlığın zarar görmesi bilgi sistemini hiç etkilemez. Zarar görmesi, kurumun ismini etkilemez.
Çok Önemli Değil(1)	Varlığın zarar görmesi bilgi sistemini çok az etkiler. Bilgi sistemi işlemeye devam eder. Zarar görmesi, kurumun ismini etkilemez.
Orta(2)	Varlığın zarar görmesi bilgi sistemini etkiler. Bilgi sistemi işlemeye devam eder fakat varlığın yerine konması gerekir. Zarar görmesi, kurumun ismini kötü yönde çok az etkiler.
Önemli(3)	Varlığın zarar görmesi bilgi sistemini oldukça etkiler. Bilgi sistemi yarı yarıya kullanılabilir. Varlığın yerine konması gerekir. Zarar görmesi, kurumun ismini kötü yönde etkiler.
Çok Önemli(4)	Varlığın bilgi sisteminin işleminde önemli rolü vardır ve zarar görmesi bilgi sisteminin işlerliğini büyük ölçüde etkiler. Bilgi sisteminin çok az bir kısmı kullanılabilir. Zarar görmesi, kurumun ismini kötü yönde oldukça etkiler.
Son derece Önemli(5)	Varlık bilgi sisteminin işlemesi için gereklidir. Varlığın zarar görmesi, bilgi sistemini doğrudan etkiler. Bilgi sistemi kullanılamaz. Zarar görmesi, kurumun ismini çok kötü yönde etkiler.

Varlıklara değer atanması ile ilgili örnek Tablo IV'de görülmektedir.

TABLE IV
VARLIKLARA DEĞER ATANMASI ÖRNEĞİ

SUNUCULAR	
Tipi	Değeri
E-posta Sunucusu	4
DNS Sunucusu	4

Web Sunucusu	5
--------------	---

3. Adım: Güvenlik açıklıkları ve tehditler tanımlanır. Güvenlik açıklıkları, kuruluş varlıklarıyla ilişkili zayıf noktalar. Bu zayıf noktalar, varlıklarda kayba, hasara veya zarara yol açabilecek istenmeyen olağan dışı olaylara neden olan bir tehditle istismar edilebilir. Açıklığın kendisi bir zarara neden olmaz. Tablo V'te varlıklarda bulunabilecek açıklıklar, Tablo VI'da ise bu açıklıklardan doğan tehditler gösterilmektedir.

TABLE V
GÜVENLİK AÇIKLIKLARI

YAZILIM AÇIKLIKLARI	
Açıklık	Açıklığın bulunduğu varlıklar
İşletim sistemleri varsayılan ayardadır. Üzerlerinde herhangi bir güvenlik sıkılaştırması yapılmamıştır.	Tüm kullanıcı bilgisayarları DMZ'de bulunan sunucu bilgisayarlar
FTP servisi açıktır.	Web sunucusu
İçerik güvenliği yazılımının olmaması	E-posta sunucusu ve güvenlik duvarı
DONANIM AÇIKLIKLARI	
Açıklık	Açıklığın bulunduğu varlıklar
BIOS şifresi yoktur.	Tüm kullanıcı bilgisayarları DMZ'de bulunan sunucu bilgisayarlar
Düşük donanım özellikleri	E-posta sunucu, Hub
Özel bir sistem odası yoktur.	DMZ'de bulunan sunucu bilgisayarlar, güvenlik duvarı, yönlendirici

TABLE VI
GÜVENLİK AÇIKLIKLARINDAN DOĞAN TEHDİTLER

YAZILIM AÇIKLIKLARINDAN DOĞAN TEHDİTLER		
Tehdit	Kullandığı Açıklık	Etkilenen varlık(lar)
Virüsler	İçerik güvenliği ve anti-virüs yazılımının olmaması	Kurumun prestiji, Kullanıcı ve kurum verileri, e-posta sunucusunun işletim sistemi ve üzerinde çalışan yazılım
İnternette yapılan hacker saldırılarından erken haberdar olamamak	Saldırı tespit sisteminin olmaması	Kurumun prestiji, Web sunucularının işletim sistemleri ve üzerinde çalışan yazılımlar
DONANIM AÇIKLIKLARINDAN DOĞAN TEHDİTLER		
Tehdit	Kullandığı Açıklık	Etkilenen varlık(lar)
Toz, nem, güneş ışığı gibi çevresel faktörler	Özel bir sistem odasının olmaması	DMZ bölgesindeki sunucu bilgisayarlar, güvenlik duvarı, yönlendirici, hub

4. Adım: Belirlenen tehditlere olasılık ve etki değerleri atanır. Tehdidin olma ihtimali için örnek bir skala Tablo VII’de gösterilmektedir.

TABLO VII
TEHDİDİN OLMA İHTİMALİ İÇİN ÖRNEK SKALA

İhmal Edilebilir(0)	Olması imkân dahilinde değil
Çok Düşük(1)	Beş senelik bir sürede iki veya üç kere olabilir
Düşük(2)	Senede veya daha kısa bir sürede bir kere olabilir
Orta(3)	Altı ayda veya daha kısa bir sürede bir kere olabilir
Yüksek(4)	Ayda veya daha kısa bir sürede bir kere olabilir
Çok Yüksek(5)	Ayda veya daha kısa bir sürede birçok kere olabilir
Son derece Yüksek(6)	Günde birçok kere olabilir.

TABLO VIII
TEHDİDİN OLMA İHTİMALİ DEĞER ATAMASI ÖRNEĞİ

Tehdit	Olma İhtimali
Virüsler	5
İnternette yapılan hacker saldırıları	3
Bilgisayarlara yetkisiz erişim	5
Dinleme(sniffing) yapılması	2

Belirlenen tehditlerin mutlak etki değerlerinin belirlenmesi için örnek bir skala Tablo IX’da gösterilmektedir.

TABLO IX
TEHDİDİN MUTLAK ETKİSİ İÇİN ÖRNEK SKALA

Önemsiz(0)	Tehdidin varlık üzerinde hiç etkisi yoktur.
Küçük(1)	Tehdidin varlık üzerinde küçük etkisi olur. Varlığı tamir etmeye veya yeniden konfigüre etmeye gerek yoktur.
Önemli(2)	Tehdidin etkisi küçük olmasına rağmen somut bir zararı olabilir. Hasarın giderilmesi ve önlem alınması için bir takım harcamalar olabilir.
Zarar verici(3)	Varlığın ya da sistemin sahiplerine ve yöneticilerine kötü ün kazandırabilir ve kaynakta önemli zararlar olur. Hasarın giderilmesi ve önlem alınması için önemli harcamalar gerekebilir.
Ciddi(4)	Varlığa büyük ölçüde zarar verir ve kurumun kendisi zarardan etkilenebilir. Zarar gören sistemde büyük ölçüde yeniden yapılandırma gerekmektedir.
Çok ciddi(5)	Varlığın süresiz olarak işlem yapamamasına yol açar. Sistemin tamamen baştan dizayn edilmesini ve yapılandırmasını gerektirir.

TABLO X
TEHDİDİN MUTLAK ETKİSİ DEĞER ATAMASI ÖRNEĞİ

Tehdit	Mutlak Etki Değeri
Virüsler	5
İnternette yapılan hacker saldırıları	5
Bilgisayarlara yetkisiz erişim	3
Dinleme(sniffing) yapılması	4

5. Adım: Risk hesaplama işlemi yapılır. Burada dikkat edilmesi gereken nokta; risklerin hesaplanmasında kullanılan usullerde “yanlış” veya “doğru” usul bulunmadığıdır. Örnek bir risk puanlaması Tablo XI’de gösterilmektedir.

TABLO XI
RİSK PUANLAMASI

Tehdidin olma olasılığı* mutlak etkisi	Önemsiz (0)	Küçük (1)	Önemli (2)	Zarar verici (3)	Ciddi (4)	Çok Ciddi (5)
İhmal edilebilir (0)	Yok	Yok	Yok	Yok	Yok	Yok
Çok Düşük(1)	Yok	Düşük	Düşük	Düşük	Orta	Orta
Düşük(2)	Yok	Düşük	Orta	Orta	Yüksek	Yüksek
Orta(3)	Yok	Düşük	Orta	Yüksek	Yüksek	Kritik
Yüksek(4)	Yok	Orta	Yüksek	Yüksek	Kritik	Çok Yüksek
Çok Yüksek(5)	Yok	Orta	Yüksek	Kritik	Çok Yüksek	Çok Yüksek
Son Derece Yüksek(6)	Yok	Orta	Yüksek	Kritik	Çok Yüksek	Çok Yüksek

Mutlak Risk = Tehdidin Olma İhtimali * Tehdidin Mutlak Etkisi
Gerçek Risk Değeri = Yeni Mutlak Risk Puanı * Varlık Değeri

TABLO XII
RİSK HESAPLAMA TABLOSU

Tehdit	Olma İhtimali	Mutlak Etkisi	Mutlak Risk	Etkilediği Varlık Değeri	Gerçek Risk Değeri
Virüsler	5	5	25	4	100
İnternette yapılan hacker saldırıları	3	5	15	5	75
Yetkisiz erişim	5	3	15	3	45

6. Adım: Risk yönetimi yapılır. Risk yönetiminde ilk olarak, sistemde var olan riskler, en kritik riskten en düşük riske doğru sıralanmalıdır. Daha sonra, bulunmuş olan taban risk değerinin yanına taşınabilir risk değeri eklenmelidir.

Taşınabilir (istenen) risk değeri, kurumun belli bir varlık için, öngördüğü ve kabul ettiği risk miktarıdır. Taşınabilir risk seviyesine, kurum çalışanları ve yönetimi ile konuşulduktan sonra karar verilmelidir.

Taşınabilir risk seviyesinin belirlenmesi, risk yönetiminin çekirdeğini oluşturur. Çünkü gerçek risk seviyesinden, taşınabilir risk seviyesinin çıkarılması ile bulunan değer, karşı önlemin alınma önceliğini belirler.(Tablo XIII)

TABLO XIII
KARŞI ÖNLEM ALINMA ÖNCELİKLERİ

Tehdit	Gerçek Risk Değeri	İstenen Risk Değeri	Karşı önlem alınma önceliği
İnternette yapılan hacker saldırıları	75	30	45
Virüsler	100	60	40

Karşı önlemler tablosu oluşturulur.(Tablo XIV)

TABLO XIV
KARŞI ÖNLEMLER TABLOSU

No	Tehdit	Karşı Önlem Öncelik	Kullandığı Açıklık	Etkilenen Varlık	Karşı Önlem
1	İnternet ten yapılan hacker saldırısı	45	Varsayılan işletim sistemi ayarları	Kurumun prestiji, Web sunucularının işletim sistemleri ve üzerinde çalışan yazılımlar	Güvenlik duvarı için ayrı bir işletmen
2	Virüsler	40	İçerik güvenliği yazılımının olmaması, anti-virüs yazılımının olmaması	Kurumun prestiji, Kullanıcı ve kurum verileri, e-posta sunucusunun işletim sistemi ve üzerinde çalışan yazılım	Anti-virüs, içerik güvenliği yazılımlarının kullanılması

Bu risk yönetimi sürecinin sonunda karşı önlemler ve maliyetleri tablosu oluşturulur.(Tablo XV)

TABLO XV
KARŞI ÖNLEMLER VE MALİYETLERİ

Tehdit No	Karşı Önlem	Maliyet
1	Yeni işletmen alınması	30000\$ (yıllık)
1	İşletmen eğitimleri	2000\$ (yıllık)
2	Anti-virüs yazılımı	1000\$
2	İçerik güvenliği yazılımı	1500\$

7. Adım: Tekrar risk analizi ve yönetimi yapılır. Karşı önlemler alındıktan sonra ikinci bir risk analizi yapılmalıdır. Böylece, alınan güvenlik önlemleri sonucunda, sistemde kalan risk miktarı (residual risk) bulunmalıdır. Kalan risk miktarının, taşınabilir risk miktarı ile aynı ya da taşınabilir risk miktarından düşük olması gerekmektedir.

III. SONUÇLAR VE DEĞERLENDİRME

Bilişim sistemlerinin ve bu sistemler tarafından işlenen bilgilerin güvenliğinin sağlanması ancak tüm kurum çalışanlarının kolektif çabası ile mümkündür. Kurumsal güvenlik politikasının belirlenmesi ve bu doğrultuda yönetsel ve teknik denetimlerin yerleştirilmesi ve tüm kurum çalışanlarının düzenli ve kesintisiz eğitiminin sağlanması bilişim güvenliğinin sağlanması için en iyi yaklaşım olacaktır.

Bu çalışmada bilişim güvenliğinin sağlanması için kurumun koruması gereken bilgiler üzerindeki risklerin analizi bu risklerin giderilmesi veya azaltılması için önerilen risk yönetimi metotları özetlenmiştir. Unutulmamalıdır ki, bilişim güvenliği hiç bitmeyen bir süreçtir ve bu güvenliğin sağlanmasına yönelik çabalar sürekli iyileştirmelerle güncel tutulması gereken faaliyetlerdir.

KAYNAKLAR

- [1] International Standart, ISO/IEC 17799-2005, "Information Technology-Security techniques-Code of Practice for Information Security Management.
- [2] B., Karabacak, I., Soğukpınar, "ISRAM:Information Security Risk Analysis Method", Computers and Securitiy, 2005, s. 147-159.
- [3] Türk Standartları Enstitüsü (TSE)"Bilgi Güvenliği Yönetim Sistemi" Sunumu,2007.

- [4] TS ISO/IEC 27001, "Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler", 2006.
- [5] V., UCAL, "Risk Değerlendirmesi ", http://www.kocaeli.abigem.org/egitim/makale/risk_deger_vehbi_ucal.doc, 2009.
- [6] TÜBİTAK-UEKAE, Kamu Kurumları Bilgi Sistem Güvenliği Analizi Raporu
- [7] DURMUŞ, G., "Risk Analizi",<http://www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh275.pdf>
- [8] SAKA, T., "Kurumsal risk yönetimi", <http://www.tusiad.org/FileArchive/TamerSaka.pdf>, 2008.



Emine UÇAR, 1982 yılında Ankara'da doğdu. İlk ve ortaöğrenimini aynı şehirde tamamladı. Ankara Gazi Anadolu Teknik, Teknik ve Endüstri Meslek Lisesi'nden mezun olduktan sonra 2000 yılında Gazi Üniversitesi Teknik Eğitim Fakültesi Elektronik Bilgisayar Eğitimi Bölümü'ne girdi. 2004 yılında lisans öğrenimini tamamladı ve aynı yıl Gazi Üniversitesi Fen Bilimleri Enstitüsü Elektronik Bilgisayar Eğitimi Bölümü'nde yüksek lisans eğitimine başladı.

Halen 2008 yılında girdiği Karabük Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda doktora programını sürdürmektedir. 2004 yılında Kastamonu ili Tosya ilçesi Atabinen Kız Meslek Lisesi'nde bilgisayar öğretmeni olarak göreve başladı. 2006 yılında M.E.B. Eğitim Teknolojileri Genel Müdürlüğü'nde yazılım geliştirme uzmanı olarak göreve başladı ve halen bu göreve devam etmektedir.



Baha ŞEN, 1974 yılında Mersin' de doğdu. İlk, orta ve lise eğitimini aynı ilde tamamladı. 1996 yılında Gazi Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi bölümünden mezun oldu. 1999 yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Sistemleri Abd.'da yüksek lisans eğitimini tamamladı. 2006 yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Sistemleri Abd'da doktora derecesini aldı.

Gazi Üniversitesi'nde araştırma görevlisi, MSB 'da proje subayı, LBS ve Havelsan'da yazılım mühendisi, Ankara Üniversitesi' nde öğretim görevlisi olarak çalıştı. Halen Karabük Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünde öğretim üyesi olarak çalışmaktadır.

Modeling and Software Implementation of NN-Based AES Cryptosystem

Siddeeq. Y. Ameen, and Ali H. Mahdi

Abstract— The paper presents the design of Neural Network NN based encryption and decryption processes that adopts symmetric key cipher as a target. The target from the network has been selected to match the output of the Advanced Encryption Standard AES that adopts the Rijndael algorithm. Levenberg–Marquardt algorithm has been used to train the network because of its low cost and high speed. The final weights of the neural network represent the final key that can be used for encryption and decryption processes.

The proposed NN design has been simulated using Matlab ver.7. Simulation results show the closeness of the results achieved by the proposed NN-based AES cryptosystem with that of the normal AES.

Index Terms—Advanced Encryption Standard, Neural Networks Cryptosystem, Levenberg–Marquardt algorithm, Symmetric Block Ciphers.

I. INTRODUCTION

AS electronic communications spread to every area of modern life, cryptography has become an essential component to control the authenticity, integrity, confidentiality and non-repudiability of private data that flows through public networks. With increasing performance, requirements and improvements in technology, better-adapted ciphers are making their apparition to replace aging algorithms that have proven to be too weak or too slow for the current applications [1]. Block ciphers are mostly based on the idea by Shannon, that sequential application of confusion and diffusion that obscure redundancies in the plaintext. Confusion involves substitutions to conceal redundancies, and statistical patterns in the plaintext, and diffusion involves transformations (or permutations), to dissipate the redundancy of the plaintext, by spreading it out over the ciphertext. DES and Rijndael are examples of algorithms based on this idea [2].

AES (Advanced Encryption Standard) is an iterated block cipher which was selected by NIST as an international standard, and replaced DES. It is now the most widely

deployed block cipher in both software and hardware applications. Rijndael is an iterated block cipher, the encryption or decryption of a block of data is accomplished by the iteration of a specific transformation which is called (a round function). The number of round N_r depends on the block length and key length. If the key length is 256 bits, there are 14 rounds, if key length is 192 bits, there are 12 rounds, and in another case there are 10 rounds. The algorithm consists of an initial round (Add Round Key), and N_r standard rounds. The first N_r-1 rounds are similar and they consist of four transformations, called: Byte Sub (Substitution Bytes), Shift Row (Shift Rows), Mix Column (Multiply Columns) and Add Round Key (XORed by key). The last round has only the transformations Byte Sub, Shift Row and Add Round Key. Further details about these rounds and operation were found elsewhere [1].

The three standardized versions of AES are called AES-128, AES-192, and AES-256 differ from each other in the key length (128, 192, and 256 bits) and the number of rounds (10, 12, and 14). Their data encryption rounds are all the same, but the details of the key schedule (which turns the given key into a sequence of subkeys for the various encryption rounds) are slightly different since different amounts of key material are available and required in the three variants [3]. Their security was thoroughly analyzed by the NSA [4]. However, recently, there are some sorts of attacks that have been proven to be effective on the AES [5]. Thus the paper attempts to do some modification to stand against such sort of attacks by employing nonlinear neural network in the design and implementation of the AES.

Artificial neural networks (ANNs) are models of intelligent systems that consist of large numbers of simple processing units that collectively are able to perform very complex pattern matching tasks. These mathematical neural networks are designed to simulate biological neural networks that exist in the human brain. Neural networks are used for classification and function approximation/mapping problems which are tolerant of some imprecision, which have lots of training data available, but to which hard and fast rules cannot easily be applied [6]. The idea of Artificial Neural Network (ANN) came from the desire to produce a system that are capable to sophisticated computations in the same way that the human brain performs so that it can give that same understanding of problem as human brain.

The modification proposed by the paper is to achieve the

Manuscript received 1st April, 2010. This work was part Master thesis submitted to the University of Technology, Baghdad, Iraq.

S. Y. Ameen, Professor with the Gulf University, Kingdom of Bahrain, Dean of College of Engineering (phone: 973-39304338; fax: 973-17622230; e-mail: prof-siddeeqr@ieee.org).

A. H. Mahdi, He is now with the Department of Information Engineering, Baghdad University, Bagdad, Iraq (e-mail: aliinfo1980@yahoo.com).

AES (implementation of Rijndael algorithm) cryptosystem using ANN. This approach is less complex in design than the normal AES more nonlinear in operation. The nonlinear neural network must be reversible that can make encryption/decryption process on plaintext/ciphertext with high performance and very low error rate. This will consider the architectural design of the ANN, the modification of ANN on software, testing the results of simulation, in order to provide NN-based AES. Further investigations are on the points of the significant effect on the implementation of NN, by keeping the internal structure of the NN components in mind, while making the design.

II. LEVENBERG-MARQUARDT ALGORITHM (LMA)

Levenberg-Marquardt Algorithm (LMA) is an advanced non-linear optimization algorithm. It can be used to train the weights in a neural network just as Back Propagation Algorithm would be. It is reputedly the fastest algorithm available for such training. LMA had been introduced to feed-forward networks for a number of years. The primary objective of this learning algorithm of multi-layer feedforward networks is based on gradient descent which is usually slow and the convergence is of linear order. In addition, the speed usually depends on some parameters, for example, the step size. Alternatively, various second order learning methods had been proposed. Among these second order methods, LMA method, a modification to the Gauss-Newton method, is one of the popular and the effective methods. One characteristic of this method is that it incorporates an extra term to stabilize the system and to deal with the small residual problems in the learning [7].

LMA is based on nonlinear optimization technique by minimizing the sum of squares of errors (SSE). The LMA represents a simplified version of Newton's method applied to the problem of training Multi Layer Perceptron NNs. The LMA is often superior to other training algorithms in off-line application. This motivates the proposal of using the algorithm to train the NN. Furthermore, LMA represents a simple heuristic strategy to increase the convergence speed of the back propagation algorithm with a batch update [7].

Consider the numerical optimization algorithm problem of finding a vector that minimizes a given energy function $E(w): R^{N \times 1} \rightarrow R^+$

According to Newton's method, an iterative procedure that will accomplish this minimization task can be formulated as follows [7]:

- 1) Initialize the components of the vector $w \in R^{N \times 1}$ to some random values.
- 2) Update the vector w according to

$$w(k+1) = w(k) - H_k^{-1} g_k \quad (1)$$

where matrix $H_k^{-1} \in R^{N \times N}$ represents the inverse of the

Hessian matrix. The vector $g_k \in R^{N \times 1}$ represents the gradient of the energy function, computed as [7]

$$g = \begin{bmatrix} \frac{\partial E(w)}{\partial w_1} & \frac{\partial E(w)}{\partial w_2} & \dots & \frac{\partial E(w)}{\partial w_N} \end{bmatrix}^T \quad (2)$$

and evaluated at the point $w = w(k)$. If the number of patterns is finite, the energy function can be written as [7]

$$E(w) = \frac{1}{2} \sum_{q=1}^Q (d_q - x_{out,q}^{(3)})^T (d_q - x_{out,q}^{(3)}) \quad (3)$$

where Q is the total number of training patterns, w represents the vector containing all the weights in the network, d_q is the desired output, and $x_{out,q}^{(3)}$ is the actual network output due to the q th training pattern. The energy function can be found by [7];

$$w(k+1) = w(k) - H_k^{-1} g_k \quad (4)$$

where

$$H_k = \nabla^2 E(w) \big|_{w=w(k)} \quad (5)$$

and

$$g_k = \nabla E(w) \big|_{w=w(k)} \quad (6)$$

By defining $P = n_3 Q$, the energy function will be;

$$E(w) = \frac{1}{2} \sum_{p=1}^P (d_p - x_{out,p}^{(3)})^2 = \frac{1}{2} \sum_{p=1}^P e_p^2 \quad (7)$$

The gradient of the energy function in (6) can be computed as [7]

$$g = J^T e_p \quad (8)$$

where $J \in R^{P \times N}$ is the Jacobian matrix.

In the computation of the Hessian matrix, k_j element of the Hessian matrix can be expressed as [7]

$$\nabla^2 E(w) \big|_{k,j} = \frac{\partial^2 E(w)}{\partial w_k \partial w_j} = \sum_{p=1}^P \left(\frac{\partial e_p}{\partial w_k} \frac{\partial e_p}{\partial w_j} + e_p \frac{\partial^2 e_p}{\partial w_k \partial w_j} \right) \quad (9)$$

Using the expression for the Jacobian matrix, the Hessian can be expressed as [7]

$$\nabla^2 E(w) = J^T J + S \quad (10)$$

where the matrix $S \in R^{N \times N}$ is the matrix of second-order derivatives given by [7]

$$S = \sum_{p=1}^P e_p \nabla^2 e_p \quad (11)$$

When approaching the minimum of the energy function, the elements of the matrix S become small, and the Hessian can be closely approximated by [7]

$$H \approx J^T J \quad (12)$$

Substituting (8) and (12) into the expression for Newton's method given in (5), we obtain [7];

$$w(k+1) = w(k) - [J_k^T J_k]^{-1} J_k^T e_k \quad (13)$$

where the subscript k indicates the evaluation of the appropriate matrices at $w = w(k)$. One problem with the iterative update given in (13) is that it requires the inversion of the matrix $H = J^T J$, which may be ill conditioned or even

singular. This problem can be easily resolved by the following modification to (13) [7]

$$H \approx J^T J + \mu I \quad (14)$$

where μ is a small number and $I \in R^{N \times N}$ is the identity matrix. Substituting (14) into (13) results in the Levenberg-Marquardt algorithm for updating the network weights.

$$\begin{aligned} w(k+1) &= (w(k) - [J_k^T J_k]^{-1} J_k^T e_k) \\ &= w(k) - [\mu_k I]^{-1} J_k^T e_k = w(k) - \frac{1}{\mu_k} J_k^T e_k \end{aligned} \quad (15)$$

For a small value of μ in (15), Levenberg-Marquardt algorithm approaches Newton's algorithm. However, when the value of μ_k is increased, the second term inside the square brackets in (15) becomes dominant. Defining $\alpha_k = 1/\mu_k$ and using (7), the update equation becomes [7]

$$w(k+1) = w(k) - \alpha_k g_k \quad (16)$$

This is the steepest decent gradient method. The magnitude of learning rate must be changed according to the error produced.

The algorithm can be summarized as follows [7]:

1. If the error function over the entire training set has decreased, increase the learning rate (η) by multiplying it by a number $\eta_{\text{increment}}$.
2. If the error function has increased more than previous error, decrease the learning rate (η) by multiplying it by a number $\eta_{\text{decrement}}$.

III. DESIGN OF NONLINEAR NN-BASED AES CRYPTOSYSTEM

The idea in this section is to design a non-linear reversible NN that can make encryption/decryption process on plaintext/ciphertext with high performance and very low error rate. The cryptographic algorithm which must be implemented by the neural network is the Rijndael algorithm. ANN provides a useful way of controlling non-linear systems. The purpose of nonlinearity is to reduce the cracking ability on the system by using nonlinear activation function, and also nonlinear approximation property of the network makes it more useful for practical applications.

Multi Layer Perceptron (MLP) MLP is the most the most popular type of feed-forward NN, and the interesting property of it is its ability to emulate any input/output relationship [8]. The MLP designed here as a Batch training (Block – Adaptive) is a frequency update because it updates the weights after the entire block of training data is presented [8]. The block adaptation is more robust since the training step is averaged over all the training patterns. The MLP takes the following parameters:-

For the encryption process, the following settings can be used:-

1. The input vector is the plaintext.
2. The target (desired output) from the neural network will be the ciphertext of the AES.
3. The initial weights will be the key of the encryption process.
4. The non-linear activation function of each neuron

will be (log sigmoid) that gives an output between (0-1).

For the decryption process, the following settings can be used:-

- 1) The input vector is the ciphertext.
- 2) The target (desired output) from the neural network will be the plaintext.
- 3) The initial weights will be the key of the decryption process.
- 4) The non-linear function of each neuron will be (sigmoid) that gives an output between (0-1).

The input and output can be scaled by a factor to as to be compatible with the activation function. For creating a successful NN, there are few tips to increase the likelihood of succeeding [9]:-

- 1) When the network design is too large for system that it implements, the network will “memorize” the training data, rather than “learn” from it. This will lead to a poor data performance for the testing data.
- 2) When initial weights are assigned to the network before training, randomize them with values between -1 and 1. This will usually result in faster convergence of the network.
- 3) A perfect error is ideal, it is not practical. In practical situations, strive for an acceptable error.

The designed NN-based cryptosystem must work for both encryption and decryption processes so as to achieve a symmetric system. Fig. 1 shows the proposed encryption process. The parameters used in the process are:

- 1) The plaintext (the original text) represents the input vector to the NN.
- 2) The ciphertext which represents the target vector (desired output) of the NN.
- 3) The cipher key which represents initial weights of the NN.

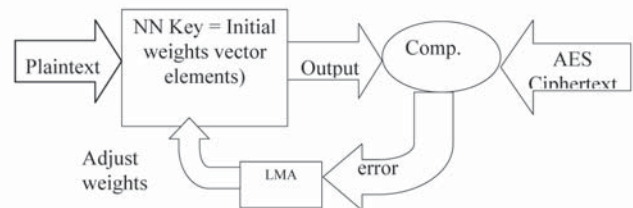


Fig. 1. Training operation for encryption process.

The decryption process is as shown in Fig. 2. The parameters used in the process are:

1. The ciphertext which represents the input vector to the NN.
2. The plaintext which represents the target of the NN.
3. The cipher key which represents the initial weights of the NN.

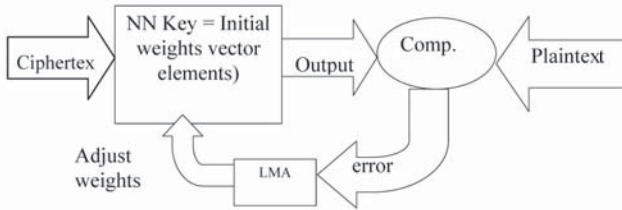


Fig. 2. Training operation for decryption process.

For the NN based cryptosystem to pass, two phases need to be verified, training and operation phases, as follows;

In the training phase, the plant (Rijndael algorithm) produces a ciphertext from specific input plaintext. The NN takes the input text as an input and the output text of the plant as the target output, and trains itself with the target output. After 5 to 10 iterations (according to the key used) with a group of plaintexts, but with the same initial weights (the key). The neural model structure is called “series-parallel model” where the plant (Rijndael algorithm) affects the dynamic behavior of the neural model [9].

The operation phase will be the feed-forward multi-layer NN with the final weights used to produce the output of encryption/ decryption processes. This phase will continue produces plaintext/ ciphertext until new key will be used in the system, where NN will need to train it-self with the new key.

In the encryption and decryption processes, nonlinear activation function was used for each neuron which is the hyperbolic tangent (*tanh*). The property of Sigmoid produces an output in range of (-1 to 1). The data that are used in the AES are in range of (0-255). So, to make the NN working properly with the AES data (plaintext, ciphertext, cipher key) in presence of the Sigmoid activation function, there is a need to make the data in range of (0-1). This is achieved by using scaling factor (1/256) so as to be compatible with the output of activation function. The scaling factor can be used at the output of each neuron to re-change the output range back in (0-255).

IV. SYSTEM IMPLEMENTATION AND EVALUATION

In this paper and for simplicity only a 128-bit key length version of AES was considered for investigation. The AES uses a data block of length 128 bits for both of encryption/decryption process. Thus, the NN will use the data in bytes form, so each of the input and the output will be 16-bytes. The NN must have at least one hidden layer of 16 neurons so to achieve the input key length of 16 bytes.

The NN used in the training processes has a topology of [16-16-16-1]. It takes a vector of 16 bytes as an input and produces 16 bytes vector as a trained text. The weights of each layer are the key (16 bytes) vector. In this NN, the encryption process will not produce the desired text, because the minimum gradient will be reached without reaching the goal performance. Figs. 3 and 4 show the training with each of

encryption and decryption processes with 16 bytes input NN.

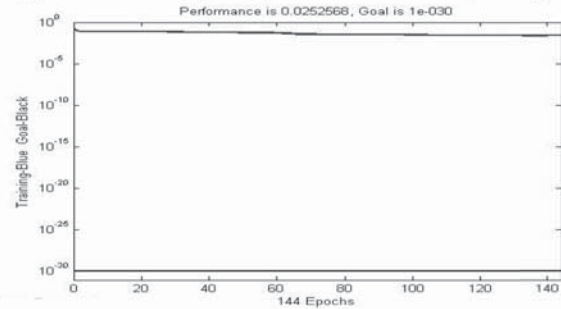


Fig. 4. Training of encryption process with 16 bytes input

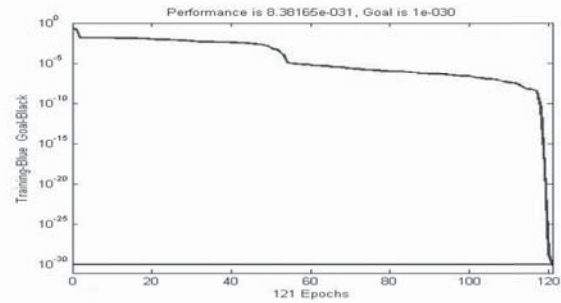


Fig. 5. Training of decryption process with 16 bytes input

Operation phase test shows that the output text on NN-Based AES in both encryption and decryption processes were not identical to that of the of encryption and decryption process of the normal AES.

One of the main solutions to this problem is to reduce the input and target vectors of the NN. This solution will tend to reduce the training time and to meet the goal performance. The idea of reduction is to make more than one NN operate in parallel. Each NN will operate with part of input and target vectors, but with all of weight vector to achieve the normal AES operation.

The NN-based AES has been tested by building three NNs, each one has input and output vectors from the following:

- 1) 16 bytes input and output vectors.
- 2) 8 bytes input and output vectors.
- 3) 4 bytes input and output vectors.

Each of these NNs had been tested with three plaintext vectors, three ciphertext vectors, and three key vectors. Each of these had length of 16 bytes. Figs. 5 and 6 show differences between the encryption and decryption processes for the three NNs. The idea of training NN for more than one data block (one block of data per iteration) is to train the weights of the NN for all (plaintext block/ ciphertext block) pairs so as to reduce the output bit error. This attempt will ensure that the NN will be trained with all the possibilities of input/target patterns which tend to train the weights with all these possibilities to get the final weights that represent the final keys for encryption and decryption processes. The increasing of iterations for each NN shows a reduction in bit error for all NNs. Fig. 5. shows the error bits at encryption process. The error bits range of 16 inputs NN are (33 - 40),

and (22 – 28) for 8 inputs NN, these because the minimum gradient has been reached without meet the goal performance (which is 10^{-30} between the input and the desired output). The minimum reduction in the error bit is in the 4 input NN (6 – 10).

The decryption process shown in Fig. 6 has lower error bits rate than that in encryption process, for the three NNs, because the ciphertext produced by the NN in the encryption process will pass through the same NN topology with the same initial weights (key). Thus the NN will be trained without reaching the minimum or maximum gradient.

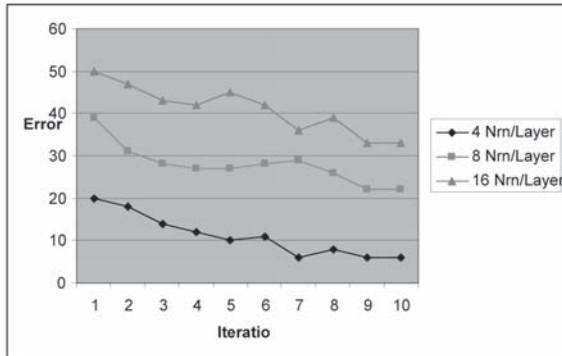


Fig. 5. Error bits/iteration for the three NN in the encryption process.

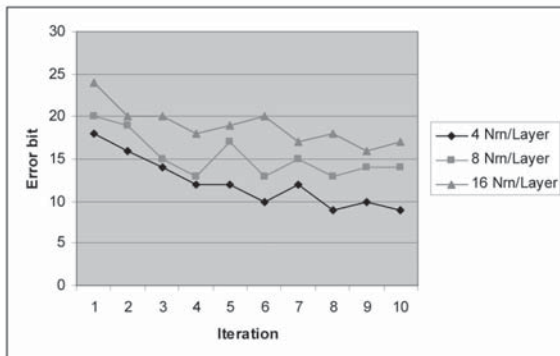


Fig. 6. Error bits/iteration for the three NN in the decryption process.

Several NN topologies have been tried and it has been found that the NN with topology [4-16-16-1] is the best one of these NNs. Each of encryption and decryption processes must have 4 NNs, from the chosen NNs; operated in parallel to achieve the AES with 16 bytes plaintext, ciphertext cryptosystem. The NN cryptosystem consists of 4 NN layers work in parallel. Each of the NN layer takes input vector of 4 bytes. The topology of the desired NN in the encryption/decryption process is as follows:-

- 1) Layer 1 with 4 neurons, where each neuron receives 1 byte from the input vector (plaintext/ciphertext).
- 2) Layer 2 with 16 neurons that each neuron is a weighted sum of all the 8 neurons in the 1st layer.
- 3) Layer 3 with 16 neurons that each neuron is a weighted sum of all the 8 neurons in the 2nd layer.
- 4) Layer 4 (output layer) with 1 neuron that is a

weighted sum of all the 8 neurons in the 3rd layer.

The initial weights of the NN are the key for the encryption/decryption process. Thus the 16 bytes key in the NN were taken in the following way:

- 1) 4x1 matrix (represents the 4 bytes from the key according to the 4 bytes positions of input vector) to be the initial weights from input to layer 1.
- 2) 16x4 matrix (represents 16 bytes from the key and repeated 4 times) to be the initial weights from layer 1 to layer 2.
- 3) 16x16 matrix (represents the same 16 bytes in the layer 1, but repeated 16 times) to be the initial weights from layer2 to 3.
- 4) 1x16 matrix (represents the same in layer 1 from input, but transposed) to be initial weights from layer 3 to output layer.

The equation of the output of this NN is as follows:

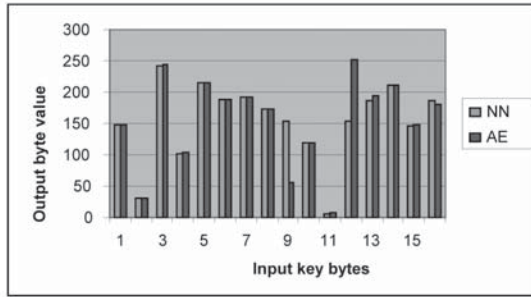
$$output = \tanh\left(\sum_{k=1}^{16} w_{1k} \cdot \tanh\left(\sum_{k=1}^{16} \sum_{j=1}^{16} w_{kj} \cdot \tanh\left(\sum_{j=1}^{16} \sum_{i=1}^4 w_{ji} \cdot \tanh\left(\sum_{i=1}^4 w_{il} \cdot input\right)\right)\right)\right) \quad (17)$$

where; output: plaintext/ciphertext (according to the process), w is the symmetric key. The tangent sigmoid transfer functions in the hidden layers compress an infinite input range into a finite output range. Sigmoid functions are characterized by the fact that their slope must approach zero as the input gets large. This causes a problem when using steepest descent to train a multilayer network with sigmoid functions, since the gradient can have a very small magnitude; and therefore, cause small changes in the weights and biases, even though the weights and biases are far from their optimal [8]. The learning algorithm suitable in this design is the LMA. This algorithm was designed to approach second-order training speed without having to compute the Hessian matrix.

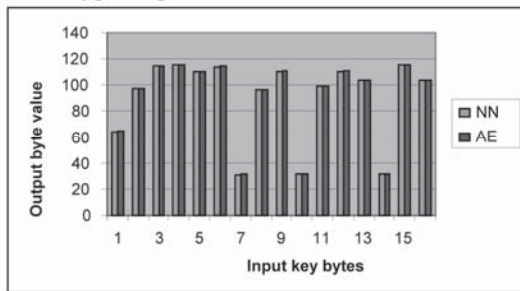
The training parameters for LMA are η -inc, η -dec. The η is multiplied by η - dec whenever the performance function is reduced by a step. It is multiplied by $-\eta$ inc whenever a step would increase the performance function. If η becomes larger than $-\eta$ max, the algorithm is stopped. The parameter mem_reduc is used to control the amount of memory used by the algorithm [10].

The chosen NN has been trained with different initial weights (keys) to check the validity of the proposed cryptosystem. The same evaluation was carried out through the comparison of the proposed NN-AES with the AES as shown in Fig. 7. In Fig. 7., the x axis represents the input 16 bytes whereas the y axis represents the output byte value (0-255) in the encryption or decryption process.

From the results of the execution, it's shown that some of the differences in the bits between the AES and NN cryptosystem. These error bits are reduced after a number of iterations, where the NN has been trained on all of the data that can be used in this cryptosystem.



a - encryption process



b- decryption process

Fig. 7. Normal AES and NN-AES comparison (encryption and decryption) with different key.

V. CONCLUSIONS

The design NN-based cryptosystem is a good idea of building very complicated cryptosystem, where the crypto analyst or the cracker not just need the topology of the NN and the key to crack the system, but also need to know the number of adaptive iterations and the final weights for the encryption and decryption systems. Applying higher numbers of plaintext/ ciphertext to the NN-based cryptosystem so as to make the error rate as minimum as possible (which must be match 0 error).

The paper has shown that it is possible to implement such powerful security algorithm such as AES with the use of NN. This will ensure that the required confusion and diffusion have been achieved in the ciphertext of the NN-based AES cryptosystem.

Finally, extra works now under investigation to implement the system with the FPGA devices with more investigation the confusion and diffusion achieved by NN-based AES.

REFERENCES

- [1] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, 3rd Edition, 2007.
- [2] S. Sagioglu, N. Özkaya, "Neural Solutions for Information Security", Journal of Polytechnic, Vol: 10 No: 1 pp.21-25, 2007
- [3] J. Daemen, V. Rijmen, "The Block Cipher Rijndael", NIST's AES home page 2001. <http://www.nist.gov/aes>.
- [4] A. Samih, A. Aziz and N. Ikram, "An Efficient Software Implementation of AES-CCM for IEEE 802.11i Wireless St" 31st Annual International Computer Software and Applications Conference, Beijing, China, 2007.
- [5] A. Biryukov, D. Khovratovich, and I. Nikoli, "Distinguisher and related-key attack on the full AES-256", CRYPTO'09, LNCS. Springer, 2009.

- [6] B. Chandra, and P. Paul Varghese, "Application of Cascade Correlation Neural Networks for Cipher System Identification", World Academy of Science, Engineering and Technology 26 2007.
- [7] C. Kanzow, N. Yamashita and M. Fukushima, "Levenberg-Marquardt Methods for Constrained Nonlinear Equations with Strong Local Convergence Properties", Journal of Computational and Applied Mathematics 172, 2004, pp. 375-397.
- [8] J. Principe, N. Euliano, and W. Lefebvre, "Neural and Adaptive Systems: Fundamentals through Simulations", John Wiley & Sons, Inc., 2000.
- [9] W. Sun, Y. Yuan, "Optimization Theory and Methods: Nonlinear Programming, Springer Optimization and Its Applications", Springer, New York, 2006.
- [10] K. Madsen, H.B. Nielsen, O. Tingleff, "Methods for Nonlinear Least Squares Problems, Informatics and Mathematical Modeling", Technical University of Denmark, 2nd Edition, April 2004

Siddeeq Y. Ameen (M'05) born in 1960 in Mousol, Iraq. He awarded BSc in Electrical and Electronic Engineering from the University of Technology, Baghdad, Iraq in 1983. Next, he awarded the MSc and PhD from Loughborough University, UK. in 1986 and 1990, respectively in the field of digital communication systems and data communication. From 1990-2006, Professor Siddeeq worked with the University of Technology in Baghdad with participation in most of Baghdad's universities. From 2006-present, he acts as a dean of college of Engineering at the Gulf University in Bahrain. Through his academic life he published over 70 papers in field of data communication and information security.

Hash-based Authentication Key Generation for Smart Card Technology

Görkem Saygılı

Öznur Özkasap

Abstract—Smart Card technology, as a commonly used mechanism in a wide range of applications, inevitably becomes the target of attackers. Usually the aim of the attackers is to break the unique password of a smart card, as well as breaking the master key used to generate the keys of each individual smart card. The effect of a broken master key is catastrophic, because the authentication password (session key) generation algorithm is based on ciphers such as DES and with the enough knowledge on algorithm of the cipher, Initial Vector (IV) and card ID, the attacker can break any of the smart card's authentication passwords generated with this broken master key. The lengths of these master keys do not exceed 8 bytes which seems insecure with today's high computational power. In this study, we introduce a new method to generate authentication password based on SHA-1 that can be used in many kinds of smart cards applications. In this method, there is no limit for the length of the master key (the hash coded data) which causes the attempts to break it down infeasible. Besides, this method allows us to generate different authentication passwords for every data sector of the smart card.

Index Terms—smart card, authentication password, key generation, SHA-1.

I. INTRODUCTION

The smart card technology has been widely used in a wide range of applications in daily life such as credit cards, highway contactless smart card toll collection System (ETC), mobile phone SIM cards and even ID cards in some countries, which makes the security of these systems crucial [7]. The wide range of usage causes smart cards to store different kinds of information, ranging from bank account information to telephone numbers and addresses. The common usage of smart cards comes with a price of being at the target of attackers. Therefore, the data of the smart card should be protected with utmost security.

Görkem Saygılı (M.Sc) is a research assistant at College of Engineering, Koç University, Istanbul. e-mail: gsaygili@ku.edu.tr

Öznur Özkasap is an associate professor at Department of Computer Engineering, Koç University, Istanbul. e-mail: oozkasap@ku.edu.tr

A smart card has an authentication password and this password secures the read/write permissions of the data stored in the memory. Commonly used memory is an EEPROM consisting of rows (sectors) and columns of data chunks that store different kinds of data [1]. Each card has an Arithmetic Logic Unit (ALU) for simple operations such as incrementing or decrementing a data in one of those chunks or copying it to another chunk. The physical structure of the card will be discussed in the next section.

The authentication password generation is based on DES algorithm in many applications such as ID cards that are used in companies and some countries [2]. Additionally 3DES is also used for applications such as credit cards where more security is needed. If we consider ID cards that have DES/3DES generated authentication passwords, every sector would have the same password as others. Therefore, the card has only one password that protects different kinds of information in different sectors. Thus, breakdown of the password causes all the information of the owner to be captured by the attacker. Besides DES/3DES are cryptographic ciphers which give attacker the chance of decrypting the master key with the proper assumption of IV, authentication key (A Key) and enough knowledge about the cipher algorithm. DES is vulnerable to brute force attacks with today's computer technology and 3DES will probably be vulnerable to such attacks in the near future considering the increase of the processing power of the computers. Since 3DES is an extension of DES for greater security, our discussion will be based on DES.

In this study, we present a SHA-1 based authentication password algorithm that supports the ability of assigning a different authentication password to each and every sector of a smart card. Additionally, this algorithm gives flexibility for the length of the master key which makes the attacks to break it infeasible and it is efficient in terms of using less memory and taking less time [3]. Furthermore SHA-1, as a result of being a hash function, is not reversible so it increases the security of the master key.

This paper is organized as follows. In the next section, we describe the structure of smart card we have used. In Section III, we describe DES algorithm, followed by SHA-1 description, our approach of key generation for smart cards, and discussion in Section IV. Finally, we conclude the paper in Section V.

II. SMART CARD INFRASTRUCTURE

A. Infrastructure of the Card

In this study, we preferred to utilize one of the most common cards, namely MIFARE MF1ICS50 IC [1]. It can be used in many different applications such as public transportation, access control and event ticketing. It has an operating frequency of 13.56 MHz which is suitable for RFID applications and has an EEPROM memory of 1 Kbytes. This memory has 16 sectors and 4 blocks which has the storage of 16 bytes each. Figure 1 shows the general structure of the MIFARE card. The wire that circulates around the card is the antenna and the chip of the card can be visualized also. The antenna is necessary for contact less functioning. Figure 2 shows the block diagram of the infrastructure of the chip. Digital Control Unit (DCU) and EEPROM are the key units of the chip [4]. DCU lets all memory operations to be encrypted after secure authentication.



Fig. 1. Mifare Card Structure

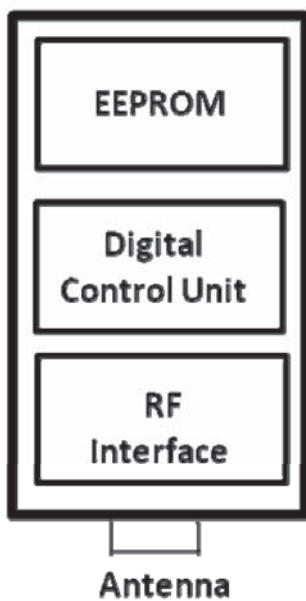


Fig. 2. Block Diagram of the chip

B. Infrastructure of the EEPROM

Figure 3 represents the logical structure of the EEPROM unit that can be described as follows:

- The only readable chunk is the one located at sector 0 and column 0 (chunk(0,0)). This chunk contains the 4 digit ID of the card and information of the producer.
- The chunk located at the end of each sector (column 3) contains authentication key for authentication permissions. All permissions (both read and write) are granted to the users that know this key. Therefore, we only need to focus on authentication key which is the first 6 bytes of the chunk.
- The rest of the chunks are the data storage memories that can store any information about the owner. For example, if we consider the ID cards that are used in some countries, chunk (0,1) may contain the name and surname and chunk(1,1) may contain the driving license number.

All the data stored in the EEPROM is protected with the authentication password of the smart card. Therefore, without the knowledge of key A, it is not feasible to read and write data. On the other hand, with today's technology such as electron microscope, professionals find a way to read the data directly from the hardware of EEPROM and this type of attack is out of the scope of this paper [4-5].

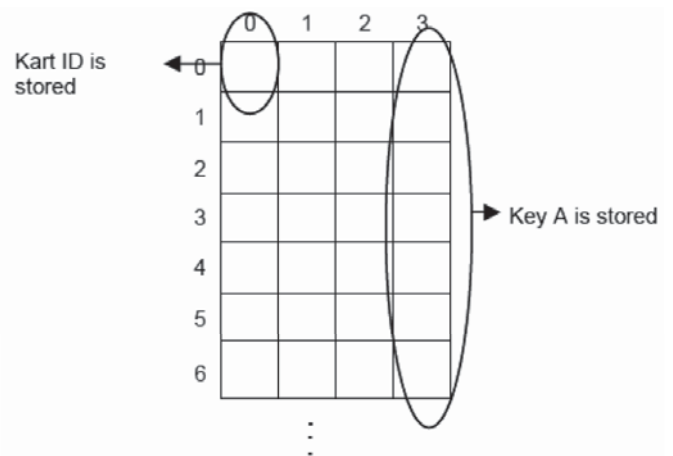


Fig. 3. EEPROM logical structure

III. DES ALGORITHM

Data Encryption Standard (DES) is a block cipher based on symmetric-key algorithm which uses 56-bit key. It is well known that DES with 56-bit key is insecure since it can be broken with the help of high computational power and knowledge of the general structure of DES algorithm [6].

The main focus here is on the vulnerability of DES on smart card authentication password generation. It is important to mention the importance of the authentication password for the smart cards. Data on the EEPROM of the smart card cannot be read or modified by any software or hardware (except using physical methods) without the knowledge of this authentication password. Therefore, generation of authentication password has a significant importance in smart card technology.

There are two stages in the authentication password generation with DES algorithm, as illustrated in Figure 4.

1. In the first stage, the plaintext, that is the unique ID of the card and some part of the manufacturer information is input to the DES algorithm with the master key of the corporation. The output is 8 byte long cipher text which cannot be used as authentication key since authentication key length must be 6 bytes.
2. In the second stage, the first and the last bytes of the cipher text is discarded (most commonly), and as a result key A is obtained with a length of 6 bytes. Since the plaintext is unique, all cards are not expected to have the same authentication password. However, since there is a discarding operation, there should be a number of cards that have the same authentication keys with each other.

It is important to note that, there is only one authentication key for every sector, which means if an attacker somehow breaks the key A, all of the data that are stored in different sectors can be easily observed. This is one of the most significant weaknesses of this password generation scheme.

IV. SHA-1 AND OUR APPROACH

A- Secure Hash Algorithm

SHA-1 is a commonly used and well established hash function in SHA hash function family. When we consider the significance of SHA-1 for the smart card technology, the SHA-1 function takes a plaintext as input rather than a fixed length master key to generate the hash code. This plaintext corresponds to the master key with various lengths in our algorithm. The output length of the hash function does not vary with the length of the plaintext. It is fixed to 20 bytes.

The hash code changes totally even a single bit of the plaintext changes, which results with different authentication keys for different smart cards if IDs of the cards are included in the procedure of generating plaintext. Additionally, this property would also let us to generate different passwords for each sector of the smart card as the sector numbers are included in the plaintext. However, there is still a problem which is very similar to the problem with DES algorithm. The cipher text is 20 bytes long but the authentication key needs to be 6 bytes long. This problem can be solved by taking any 6 bytes from hash code and discarding the rest.

One of the most crucial weaknesses of SHA-1 algorithm is the possible collisions [8] that may be found which means there can be two plaintexts, M1, M2 such that:

$$\text{Hash}(M1) = \text{Hash}(M2)$$

Moreover, this can be successfully done for all n-bit iterated hash functions with less than 2^n amount of work [9]. However, the main goal of our algorithm is to secure the original plaintext (master key). Hash functions are one way (irreversible) so it is not possible to find the original plaintext (M1) via any methodology. Finding another text (M2) that has an identical hash code with M1 would not let the attacker to generate the authentication key of any other card secured with the hash code of M1.

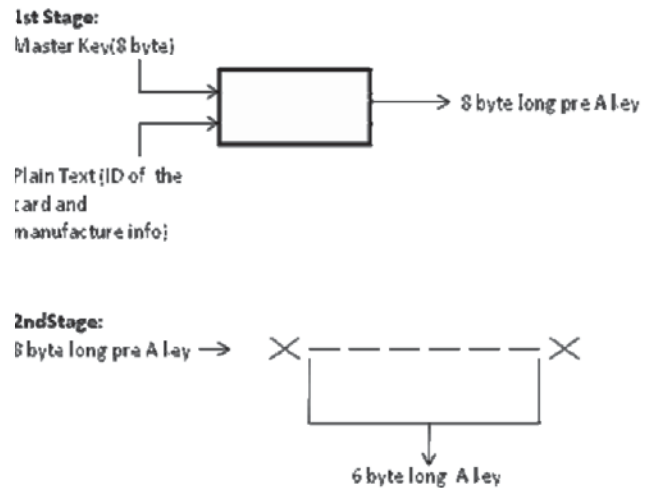


Fig. 4. DES Methodology

B- Our methodology

This study proposes a new authentication key generation method by using SHA-1 hash function. The method consists of the following steps:

- Generate plaintext utilizing sector ID and unique ID of the smart card. Master key is the same for all cards but

unique ID varies, therefore plaintext is different for each and every card. Also, sector ID causes the passwords of each sector to be different for each smart card.

- Input the plaintext into SHA-1 hash function algorithm.
- Choose 0th, 2nd, 6th, 4th, 10th, 8th bytes of the hash code with the given order to generate the authentication password. Likewise, the order can be generated by using the characteristics of the plaintext.

Figure 5 represents the block diagram of the proposed algorithm. We have implemented this method on a MIFARE smart card, and evaluated its performance through test cases that efficiently assigned all the sectors of the smart card with different authentication passwords. The user interface of our hash-based authentication key generation approach and each field's description are given in Figure 6. In general, our demonstration provides four techniques that can be used to format the smart card as follows:

1. format the card with only one authentication key (mono key SHA) so that all sectors would have the same password, and do not use the unique ID of the card.
2. format the card with mono key but at this time using the ID of the card as the plaintext.
3. use different keys for every sector (multi key SHA) and do not use the ID of the card in the plaintext.
4. the most secure case where both multi key is used and card ID is included in the plaintext.

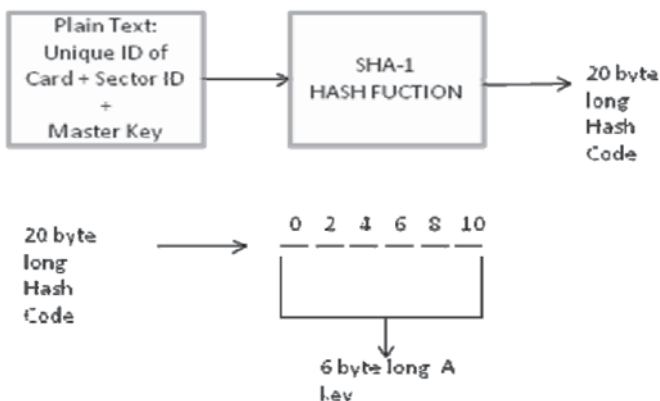


Fig.5. Algorithm with SHA-1(Key A corresponds to authentication key)

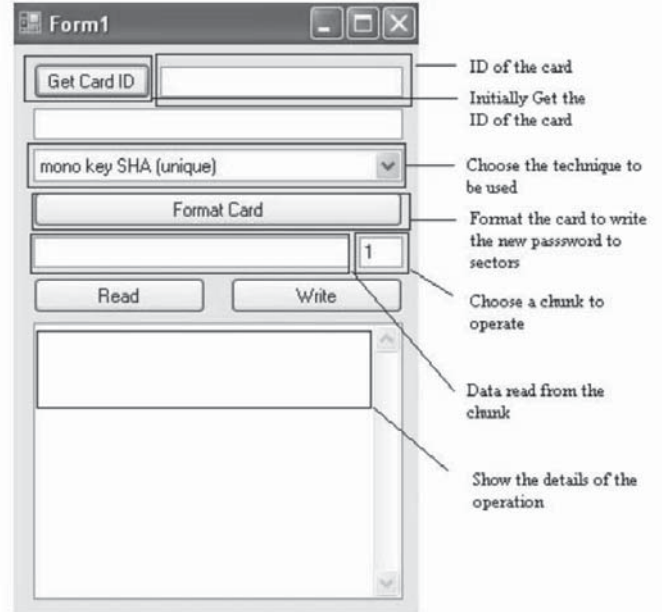


Fig.6. User interface of our implementation

C- Discussion

Advantages of our approach can be summarized as follows.

- All the sectors would have its own (unique) authentication key with SHA-1 algorithm, since it is a known fact that different information is stored in different sectors, this provides extra security against attackers.
- The master key can be initialized to a much larger size than the master key size of DES. Besides, SHA-1 is computationally more efficient than DES.
- It is infeasible to use the hash code to find the plaintext because SHA-1 is not reversible unlike DES.
- The authentication procedure is applicable for contactless (RFID) functioning of the card.

The only disadvantage is choosing 6 bytes out of 20 bytes of the hash code to generate authentication key. This may increase the matching rates of different plaintext with the same authentication key.

V. CONCLUSION

Since the smart card technology has vital importance in today's daily life, security of these cards is a very crucial issue. In this study, we have introduced a new method to generate authentication password for smart cards. The method is based on SHA-1, and it allows generating different authentication passwords for every data sector of the smart card. When SHA-1 and DES are compared, using SHA-1 for authentication password generation has advantages over DES. The proposed method was implemented on a MIFARE smart card, and successfully worked through all test cases, in which all the sectors are assigned with different authentication passwords.

REFERENCES

- [1] MIFARE1ICS50 Contactless Multi Application IC Product Data Sheet.
- [2] L. Dang, W. Kou, and Y. Xiao, "An Improved Mutual Authentication Scheme for Smart Card Secure Messaging", *IEEE International Conference on E-Commerce Tech for Dynamic E-Business*, 2004.
- [3] G. Keating, "Performance Analysis of AES Candidates," *AES Round 1 public comment*, April 15, 1999.
- [4] S. C. C. Chan, "An Overview of Smart Card Security," 1997 August.
<http://home.hkstar.com/~alachan/papers/smartCardSecurity/>
- [5] B. Schneier, A. Shostack, "Breaking up is hard to do: Modeling Security Threads for Smart Cards," *USENIX Symposium on Smart Cards*, 1999.
- [6] E. Biham, A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems" in *Proceedings of Advances in Cryptology – CRYPTO*, Springer Verlag, 1997, pp. 513-525.
- [7] W. Rankl, *Smart Card Applications: Design models for using and programming smart cards*, John Wiley & Sons, 2007.
- [8] B. Schneier, "Cryptanalysis of SHA-1," available at:
http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html
- [9] J. Kelsey and B. Schneier, "Second Preimages on n-bit Hash Functions for Much Less than 2^n Work," *Advances in Cryptography – EUROCRYPT 2005*, volume 3494, *Lecture Notes in Computer Science*, pages 474-490, 2005.

Kayıtlı Elektronik Posta Sistemi ve Hizmetleri

Mustafa ÜNVER, Demet KABASAKAL, Yüksel GÜNAYDIN

Özet— Bilgi ve iletişim teknolojilerindeki gelişim, her geçen gün elektronik ortama olan bağımlılığı arttırmaktadır. Kamu kurum ve kuruluşları, şirketler ve vatandaşlar arasındaki iş ve işlemler büyük oranda elektronik ortamda gerçekleşmeye başlamıştır. Bu gelişme beraberinde güven ve güvenlik problemlerini getirmiştir. Bu sorunların çözülmesi için farklı yöntemler geliştirilmektedir. Özellikle elektronik ortamda önemli bir araç olarak kullanılan elektronik postanın güvenli ve hukuki değere sahip bir hizmet olarak kullanıcılara sunulmasının bu problemlerin çözümüne büyük katkı sağlayacağı düşünülmektedir. Bu hizmetlerden biri de Kayıtlı Elektronik Posta'dır.

Anahtar Kelimeler — Kayıtlı Elektronik Posta, Kayıtlı Elektronik Posta Hizmet Sağlayıcı

I. GİRİŞ

KURUMLAR, şirketler ve bireyler arasındaki ilişkilerin elektronik ortamda gerçekleşme oranı her geçen gün artmaktadır. Bu ilişkiler için çok önemli bir ihtiyaç hatta bir zorunluluk haline gelmeye başlayan unsur olarak güven ön plana çıkmaktadır. 15.01.2004 tarihinde kabul edilen 5070 sayılı Elektronik İmza Kanunu ile güvenli elektronik imza tanımlanmış elle atılan imza ile aynı hukuki geçerliliğe sahip kılınmıştır. Böylece ülkemizde güvenli elektronik imza ile imzalanan elektronik ortamdaki bilgi ve belgelere hukuki geçerlilik kazandırılmıştır. Ancak bu bilgi ve belgelerin, taraflar arasında güvenli ve hukuki geçerliliğe sahip bir şekilde paylaşımı sağlanamamıştır. Bu sorunun çözülebilmesi için; elektronik hizmetleri kullanan ya da elektronik ortamdaki bilgi ve belgelerini paylaşan tarafların, elektronik ortamda işlemleri güvenli bir şekilde gerçekleştirmek ve muhataplarıyla karşılıklı güveni sağlamak için uygun güvenlik kontrollerine ve mekanizmalarına sahip olmasının sağlanması gereklidir.

Kriptoloji, internet ortamındaki elektronik mesajlaşmalarda ve bu mesajlaşmanın bir türü olan elektronik posta hizmetinde; işlemlerin güvenliğini, göndericinin kimliğinin doğrulanmasını, mesajın bütünlüğünü, gizliliğini ve kaynağın inkar edilemezliğini sağlamayı garanti etmek için kullanılabilir. Bu hedefleri gerçekleştirmek için kriptolojiyi de içeren uçtan uca çözüm sağlayan çeşitli metotlar bulunmaktadır. Ancak uçtan uca kriptoloji yüksek seviyede bir güvenlik sağlasa da bazı dezavantajları da mevcuttur. Herşeyden önce kullanılacak olan bu teknolojinin kullanıcılar arasında yaygın olarak kullanılıyor olması gerekmektedir. Bu durum, her kullanıcının bir çift simetrik anahtara ve bir

sertifika otoritesi tarafından onaylanmış ve o kullanıcının açık anahtarıyla ilişkilendirilmiş bir sertifikaya sahip olması ihtiyacını doğurmaktadır. Ayrıca kullanıcıların bu teknolojiyi kullanabilmek için yeteri kadar teknik bilgiye sahip olmaları da gerekmektedir [1].

Oysa uçtan uca çözümlerin getirdiği karmaşıklıktan uzak ve doğrudan sunucular üzerinde çalışan uygulamalar aracılığıyla elektronik mesajları sayısal olarak imzalayan, mesajların kullanıcılar arasındaki iletimini güvenli bağlantılar üzerinden gerçekleştiren başka bir teknoloji de Kayıtlı Elektronik Posta (KEP) sistemidir. KEP sistemi ve bileşenleri Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) tarafından 20 Kasım 2008 tarihinde yayımlanan "ETSI TS 102 640" numaralı standart ile resmi olarak bir telekomünikasyon standardı olarak düzenlenmiştir. KEP'de güveni sağlayan en önemli iki bileşen güvenli elektronik imza ve zaman damgasıdır. KEP sistemini kullanan kullanıcılar, sadece etkileşimde bulunacağı elektronik posta istemci programına ihtiyaç duymaktadır. Uygulama oldukça basittir ve özel kullanıcı becerilerine gereksinim duyulmamaktadır. Bu da uygulamanın kullanıcılar arasında yaygınlaşmasını kolaylaştıran en önemli etkidir [2].

II. KEP NEDİR?

KEP hizmeti Kayıtlı Elektronik Posta Hizmet Sağlayıcılar (KEPHS) vasıtasıyla verilen bir hizmettir. Bu hizmeti vermek isteyen bir kurum, kuruluş ya da şirketin yasal olarak işlevsel kabul edilebilmesi için belirli düzenlemelere uyması, birçok uyumluluk ve birlikte çalışabilirlik testinden geçmesi gereklidir. KEPHs'lerin sahip olmaları gereken niteliklerin belirlenmesi, yetkilendirilmeleri, denetlenmeleri çoğunlukla bilgi teknolojileri alanındaki düzenleyici kuruluşlarca yerine getirilmektedir.

KEP kullanıcılarına, bilinen elektronik posta hizmetine ilave olarak elektronik ortamda yapılan gönderilerin;

- ✓ Kim tarafından gönderildiği,
- ✓ Gönderimin ne zaman yapıldığı,
- ✓ Mesajın karşı tarafa ulaşmış olup olmadığı, ulaşılmışsa ne zaman ulaştığı,
- ✓ Mesajın alıcısı tarafından okunup okunmadığı, okunmuşsa ne zaman okunduğu,

gibi konularda hukuksal geçerliliğe sahip kesin delil seti oluşturan bir sistemdir[3].

Sistemin kullanıcısı olan gönderici, elektronik postanın kendisi tarafından gönderilmediğini, alıcı ise kendisine

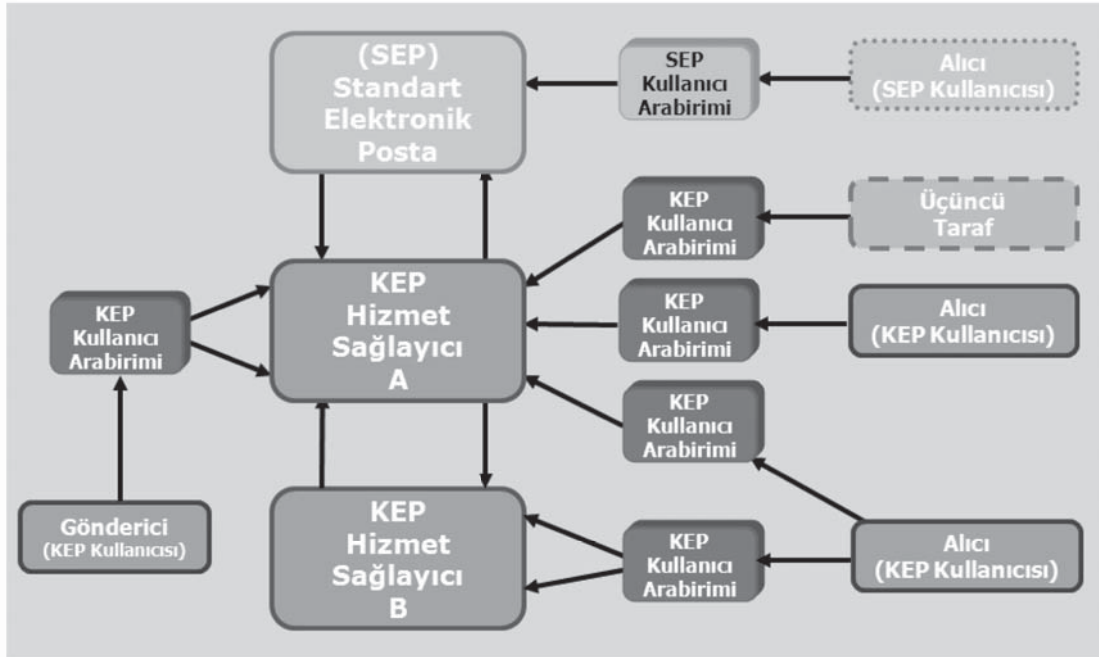
ulaşmadığını iddia edememektedir. KEP sistemin de meydana gelen bütün işlemlere ilişkin tutulan olay kayıtları, elektronik imza ile imzalandıkları için hukuki geçerliliğe sahiptirler. Bu nedenle de herhangi bir anlaşmazlık durumunda kesin delil niteliğindedirler. Ayrıca ihtiyaç duyulması halinde elektronik postalara sistem aracılığı ile yeniden erişebilme imkânı da vardır.

III. KEP SİSTEMİNİN MANTIKSAL MODELİ

KEP sisteminin en önemli iki bileşeni güvenli elektronik imza ve zaman damgasıdır. Sistemde gönderimi yapılan bütün mesajlar ilgili kullanıcının güvenli elektronik imzasıyla imzalanmaktadır. KEPHS'nin ürettiği delil niteliğindeki her olay kaydı KEPHS'nin elektronik imzasıyla imzalandıktan sonra zaman damgası da eklenerek sistemde

saklanmaktadır. Sistemdeki mesajların ve olay kayıtlarının güvenli elektronik imza ile imzalanması bir zorunluluktur. Çünkü normal bir elektronik imza ile imzalanmış bir belgenin hukuki geçerliliğe sahip olmayacağı bilinen bir husustur[4].

Şekil 1’de mantıksal modeli gösterilen KEP sisteminin kullanıcıları olan gönderici ve alıcılar KEP sistemi ile KEP kullanıcı arabirimi üzerinden, Standart Elektronik Posta (SEP) kullanıcıları ise SEP kullanıcı arabirimi üzerinden haberleşmektedir. KEP kullanıcı arabirimi, kullanıcının bilgisayarında kullandığı elektronik posta istemci uygulamasına (Microsoft Outlook, Mozilla Thunderbird vs.) eklenmiş bir yazılım parçası olabileceği gibi KEPHS’nin sisteminde çalışan ve kullanıcının uzaktan eriştiği bir uygulama da olabilmektedir[5].

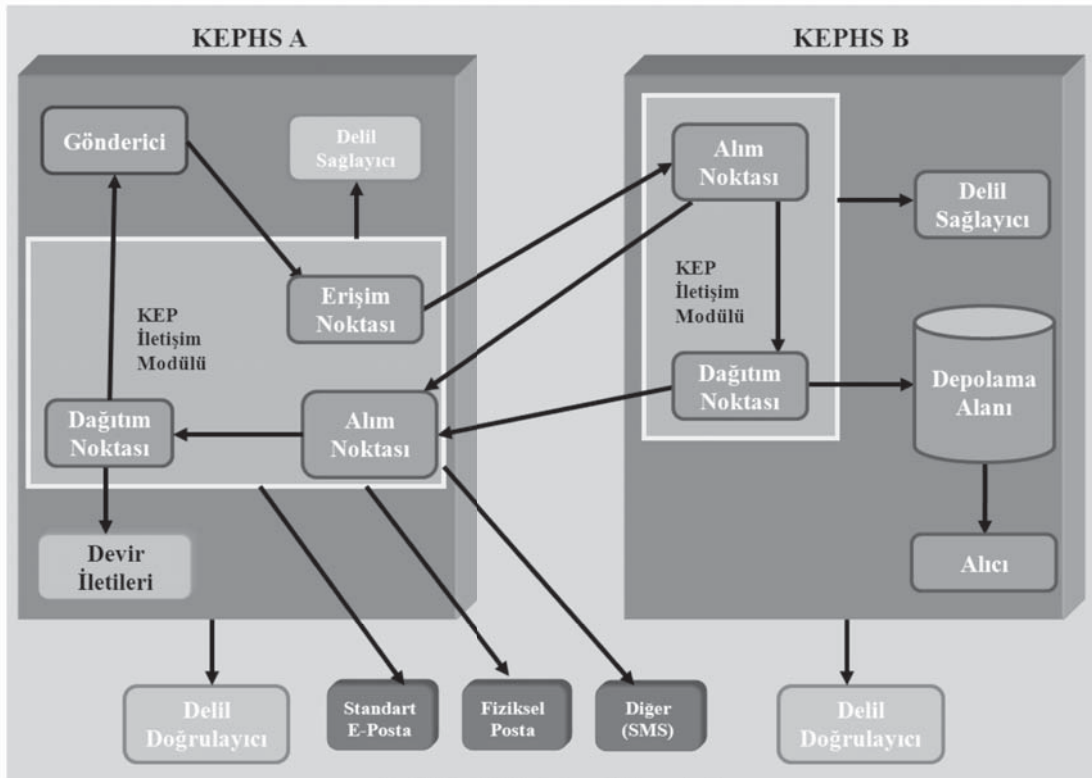


Şekil 1 : KEP sisteminin mantıksal modeli

KEP sistemini kullanmak isteyen kullanıcılar yetkilendirilmiş olarak hizmet verecek olan KEPHS'lerden herhangi birini tercih ederek kendileri adına bir hesap açtırmak zorundadırlar. Bu işlemten sonra kullanıcılar KEP Kullanıcı Arabirimi vasıtasıyla KEP sistemine güvenli bir oturum üzerinden bağlanabilirler. Bu adımdan sonraki her elektronik posta gönderimi ve alımı KEPHS ile kurulan bu güvenli oturum üzerinden gerçekleşmektedir. Sistem SEP ile entegre bir şekilde de çalışabilmektedir. Ancak SEP'in kullanılması halinde, sadece mesaj gönderme / alma hizmeti verilirken, KEP hizmetinde olduğu gibi belgeleri güvenli elektronik imza ile imzalama, mesajın gönderildiğine ve alındığına dair olay kayıtlarına ilişkin delilleri oluşturma gibi hizmetler sunulamamaktadır. KEP sisteminin tuttuğu delil niteliğindeki kayıtlara ihtiyaç duyulması halinde

üçüncü taraflarca (mahkemeler, emniyet birimleri) erişilebilme mümkündür.

KEP sistem mimarisi için genel olarak benimsenen yaklaşıma göre KEP hizmetinin sunumunda birlikte çalışabilirliğin sağlanabilmesi için yetkilendirilmiş birden fazla KEPHS'nin bir denetleyici gözetiminde hizmet vermesi gerekmektedir (Şekil 2). Bu durumda kullanıcıların, herhangi bir KEPHS'ye hesap açtırdıktan sonra bir kimlik doğrulama mekanizması ile sisteme erişimi sağlanabilmektedir. Ayrıca, gereken durumlarda KEP sisteminden, KEP dışında SEP, fiziksel posta ve Kısa Mesaj Hizmeti (Short Message Service - SMS) gibi diğer iletişim ortamlarına da bir ara yüz sunulabilmektedir [6].



Şekil 2 : KEP sistem bileşenleri

IV. KEP İLE İLGİLİ DİĞER ÜLKELERDEKİ ÇALIŞMALAR

KEP'in, kullanıcılara bir hizmet olarak sunulabilmesi için bu konudaki yasal düzenlemelerin de yapılmış olması gerekir. Ülkemizde KEP konusunda yapılmış yasal bir düzenleme hali hazırda bulunmamaktadır. Ancak Avrupa Birliği üye ülkelerinde bu hizmeti tanımlayan çeşitli mevzuat çalışmaları yapılmaktadır. ETSI tarafından yapılan çalışmalardan önce İtalya, Belçika, Fransa, İsveç, İspanya gibi değişik ülkelerde elektronik tebligatı da içerecek şekilde ülkeden ülkeye farklılık gösteren, belirli bir standart çerçevesinde geliştirilmemiş, KEP ile ilgili değişik projeler hayata geçirilmiştir. İtalya, Belçika, Fransa gibi ülkelerde KEPHS'lerin işleyişlerine ilişkin yasal düzenleme yapılırken, İsveç ve İspanya gibi ülkelerde ise herhangi bir yasal düzenlemeye gerek duyulmamış KEPHS hizmeti kamu idareleri tarafından, noterlik fonksiyonunu da içerecek şekilde sunulmaya başlanmıştır [7].

İtalya'da 28 Ocak 2005 tarihinde KEP hizmetini düzenleyen Kanun bakanlar kurulu tarafından kabul edilmiştir. Konu ile ilgili ikincil düzenlemeler de yapılarak hizmet verilebilir ortam oluşturulmuştur. 17 (Onyed) maddeden oluşan KEP Kanunuyla KEP Sisteminin çerçevesi çizilmiş, hizmeti vermek isteyen sağlayıcıların sağlaması gereken şartlar ve uyması gereken kurallar düzenlenmiş, sistemin detaylarına ilişkin düzenlemelerin ise ikincil mevzuatla belirleneceği belirtilmiştir. İtalya'da

ikincil düzenlemeler CNIPA (the National Centre for the Informatics in the Public Administration- Kamu Yönetimi Ulusal Bilişim Merkezi) tarafından yapılmıştır. İkincil düzenlemeyle sistemin mimarisi, KEPHS'lerin teknik olarak karşılaması gereken kriterler, sistemin güvenliğinin sağlanmasına yönelik yapılması gereken çalışmalar, hizmeti almak isteyen kullanıcıların yapması gerekenler gibi başlıca konular detaylı bir şekilde düzenlenmiştir. Şu an için İtalya'da hizmet veren 22 adet KEPHS vardır. İtalya'nın KEP konusundaki çalışmaları aynı zamanda taslak bir RFC (Request For Command) standardı haline getirilmiştir. İtalya'da konuyla ilgili çalışmaların devam ettiği bilinmektedir[8].

Fransa'da 2000/31/AB sayılı e-Ticaret Direktifinin[9] iç hukuka uyarlanabilmesi amacıyla 17 Haziran 2005 tarihli bir yasal düzenleme ile KEPHS'ler için özel bir yasa yapılmıştır [10]. Ülkede KEP hizmeti, kamu yararına bir kuruluş olarak standardizasyon misyonu yürüten ve standardizasyon, belgelendirme ve faaliyet alanları ile ilgili yayın, eğitim sağlayan uluslararası bir kuruluş olarak faaliyet gösteren AFNOR tarafından verilmektedir.

Fransa'da oluşturulan modelde göze çarpan temel özellik delil sağlayıcının KEPHS'den ayrı bir birim olması ve aynı zamanda delil doğrulayıcı olarak da görev yapmasıdır. Oluşturulan yapı SEP'ya bir ara yüz sağlamamaktadır. Bu modelde hizmetin sunulması sırasında oluşturulan mesajlar veya deliller sadece doğrulanması talep edildiğinde sunulmak üzere oluşturulmaktadır. Ayrıca Fransa'daki mevzuata göre KEP kullanılarak oluşturulan bu

delil ve mesajlar, yasal olarak bir mahkemeye sunulurken değerlendirilebildikleri halde tek başına hukuki geçerlilik ifade etmemektedirler [11].

İspanya'da KEP hizmetlerini iki ayrı kurum vermektedir. Bunlardan birincisi Güvenli Bilişim Tebligat Hizmetleri Sistemi, diğeri ise adalet alanında kullanılan Lexnet isimli sistemi işletmektedir[12]. Her iki altyapı için özel yasal düzenlemeler yapılmış olup, yasal düzenlemelerde, iletinin gönderilmesi, tebliğ edilen zaman ve tarihi ve aynı zamanda elektronik ortamda gönderilen tebligatın delillendirilmesi hususları yer almaktadır[13].

Chamber Sign İsveç, İsveç Ticaret Odaları Birliğine bağlı, kar amacı gütmeyen, İsveç'te elektronik ortamda KEP hizmeti veren bir kuruluş olarak faaliyet göstermektedir. Burada öncekilerden farklı olarak KEP hizmeti, diğer hizmetlerin yanı sıra, onlarla birlikte bir alt hizmet olarak verilmektedir. Bu sistemde KEP'e ilişkin yasal düzenlemelerin Kamu İhale Kanunu içinde düzenlendiği belirtilmektedir. Sistem daha çok deniz aşırı yapılan ihalelerde kullanılmakta ve Chamber Sign İsveç, güvenilir üçüncü taraf olarak e-postalara ilişkin delilleri toplamakta ve saklamaktadır [14].

Almanya'da Federal Bakanlar Kurulu tarafından, "Vatandaş Portalı Kanun Tasarısı" onaylanmış ve böylece elektronik ortamda tebligat hizmetlerine ve kamu kurumları arasında doküman değişimine imkân sağlanmıştır. Tasarıya göre Almanya'da vatandaşların kimliklerini belgeleyerek, elektronik tebligat amacıyla kullanmak üzere, akredite olmuş servis sağlayıcılardan, "De-Mail" isimli KEP hesabı almaları gerekmektedir. Vatandaşlar bu e-posta aracılığı ile güvenli ve şifreli olarak e-posta gönderebilecek ve kabul edebileceklerdir. Gönderici De-Mail sistemi ile hukuken geçerli gönderi onaylama kaydı alacaktır. KEPHS bu gönderi onay kaydını elektronik imza ile imzalamak zorundadır. Böylece resmi kurumlarda iş emirlerinin ve yazışmaların elektronik ortamda emniyetli, güvenilir ve bağlayıcı bir şekilde gönderilmesi sağlanmış olacaktır. İşişlerinin hesaplamalarına göre De-Mail Sistemi işleme alındığında senelik 1 Milyar ile 1,5 Milyar Avro arasında tasarruf sağlanacaktır[15].

V. KEP ALTYAPISI ÜZERİNDEN VERİLEBİLECEK HİZMETLER

KEP sistemi kullanılarak çeşitli katma değerli hizmetlerin verilmesi mümkündür. Ülkemizde de bu altyapının oluşturulması ve gerekli düzenlemelerin tamamlanması ile;

- Tarafların inkâr edemeyeceği bir şekilde güvenli olarak elektronik belgelerin gönderilmesi ve alınması,
- İletişimin gizliliği prensibine uygun bir şekilde elektronik ortamda güvenli haberleşmenin sağlanması,
- Elektronik belgelerin güvenli bir ortamda saklanması,

- Kamu kurumlarının elektronik ortamda resmi yazışma yapmaları,
- Tacirlerin ihtar, ihbar ve benzeri beyanları birbirlerine yöneltmeleri,
- Elektronik faturaların muhataba gönderilmesi,
- Ortaklar ve şirketler arasında güvenli iletişimin sağlanması,
- Elektronik ortamda tebligat hizmeti verilmesi (İdari, mali ve adli),
- Tüketici şikâyet ve taleplerinin ucuz, hızlı ve kolay bir şekilde muhataba iletilmesi,
- Bilgi Toplumu Stratejisi Eylem Planında yer alan; karşılıklı etkileşimle elektronik belge ve başvuru gönderilmesi, alınması ve yanıt verilmesini gerektiren her türlü işlemde kullanılması,
- Vatandaşlar arasında güvenli elektronik posta haberleşmesinde kullanılması,
- Ticari sır, bankacılık sırrı ve vergi mahremiyeti gerektiren konularda güvenli bir alt yapı olarak kullanılması,
- Elektronik ortamda oluşturulan ve elektronik ortamda muhafaza edilen değerlerin (Fikir ve Sanat Eserleri Kanunu kapsamındaki eserlerin) güvenli bir şekilde saklanması

gibi bir çok hizmetin KEP sistemi kullanılarak gerçekleştirilmesi mümkün olacaktır.

SONUÇ

Bilgi ve iletişim teknolojilerindeki hızlı gelişim sonucunda gerek kamu kurum ve kuruluşları gerek şirketler gerekse de vatandaşlar arasındaki ilişkiler büyük oranda elektronik ortamda gerçekleşmeye başlamıştır. Bu gelişmeye paralel bir şekilde daha dinamik bir kamu hizmeti sağlamak, bürokratik engelleri azaltmak, kurumlar arası veri paylaşımına imkân sunmak ve kamusal hizmetlerin etkileşimli biçimde yürütülmesini sağlayan bir hizmet ortamı oluşturmak gibi amaçlarla çeşitli kurum ve kuruluşlar tarafından, kısa vadede kurum içi, uzun vadede ise kurumlar arası veri paylaşımını hayata geçirmeyi de içeren projeler yürütülmektedir. Bu projelerin çoğunun sadece kurum içerisindeki bilgi ve belge paylaşımını gerçekleştirebilmek amacıyla oluşturulduğu, bilgi ve belge paylaşımı konusunda tek yönlü bir iş akışına sahip olduğu görülmekle birlikte yaygın olarak asıl hedeflenen bilgi ve belgelerin farklı taraflar arasında elektronik ortamda hukuksal geçerliliğe sahip ve güvenli bir şekilde paylaşımının sağlanması olduğu bilinmektedir. Bu güvenli ortamın sağlanabilmesi için bilişim sistemlerinin çeşitli güvenlik kontrolleri ve mekanizmaları ile desteklenmesi gerekmektedir. Bu kapsamdaki hizmetlerden biri olan KEP, eksikliği duyulan güvenilirlik ve güvenlik ihtiyacını karşılamak üzere ETSI tarafından geliştirilmiş bir standart olup elektronik ortamda bilgi ve belgelerin gönderimine, iletilmesine ve alıcılara ulaştırılmasına ilişkin deliller sunmaktadır. Ülkemizde de elektronik ortamdaki işlemlerin güvenli ve hukuki değere sahip bir şekilde paylaşımının sağlanabilmesi için KEP'in gerekli mevzuat altyapısının

oluşturularak ülkemizin bilgi toplumuna dönüşüm yolundaki ivmesini arttırılması gereklidir.

KAYNAKÇA

- [1] Günaydın Yüksel, Kayıtlı Elektronik Posta Sistemi, HABTEKUS'09, Aralık 2009
- [2] GÜNAYDIN Yüksel, Kayıtlı Elektronik Posta Sistemi, HABTEKUS'09, Aralık 2009
- [3] ETSI TS 102 640-1, “Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 1: Architecture”, s. 10
- [4] ETSI TS 102 640-1, “Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 1: Architecture”, s. 4
- [5] ETSI TS 102 640-1, “Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 1: Architecture”, s.4
- [6] KAMAG 108G131 nolu : “Kayıtlı Elektronik Posta Sistemi Konusunda Araştırma, Geliştirme Ve Uygulamalar” proje, s. 29.
- [7] GÜNAYDIN Yüksel, Kayıtlı Elektronik Posta Sistemi, HABTEKUS'09, Aralık 2009
- [8] ETSI TR 102 605 V1.1.1, “Electronic Signatures and Infrastructures (ESI); Registered e-Mail”, 2007–9, s. 20, 57
- [9] (Erişim) http://www.e-ticaret.gov.tr/hukuk/ABdirekt_tic.htm, 30 Mart 2010
- [10] ETSI TR 102 605 V1.1.1, “Electronic Signatures and Infrastructures (ESI); Registered e-Mail”, 2007–9, s. 21
- [11] ETSI TR 102 605 V1.1.1, “Electronic Signatures and Infrastructures (ESI); Registered e-Mail”, 2007–9, s.34
- [12] Tanrıkulu Cengiz, Türk ve Avusturya Hukukunda Elektronik Tebligat, , Barolar Birliği Dergisi, Ankara, Kasım-Aralık 2009, sayı 85, s.315
- [13] ETSI TR 102 605 V1.1.1, “Electronic Signatures and Infrastructures (ESI); Registered e-Mail”, 2007–9, s. 22
- [14] ETSI TR 102 605 V1.1.1 “Electronic Signatures and Infrastructures (ESI); Registered e-Mail”, 2007–9, s. 22
- [15] Tanrıkulu Cengiz, Türk ve Avusturya Hukukunda Elektronik Tebligat, , Barolar Birliği Dergisi, Ankara, Kasım-Aralık 2009, sayı 85, s.315

Protection of Electronic Environment in Arab Countries: Strategy and Approach

Mohamed Soltan.

Abstract— The current research paper handles the issue of protecting the electronic environment in Arab countries and illustrates the risks and threats that surround the electronic environment in the Arab nation. It also illustrates the serious risk facing the electronic environment represented in crime and terrorism. It highlights the Arabic strategy set for insuring the electronic environment in Arab countries.

I. INTRODUCTION

The great advancement achieved in the field of Information technology and communication has an unprecedented effect on our daily life and communities. A large percentage of our daily activities depends mainly on information technology. Such dependence is very obvious in the public sector as well as the private sector evenly.

All the vital utilities used in our daily life such as air, land and marine transportation, railways, traffic, energy, electricity and gas, wire and wireless communications, cellular phones, police, SOS, hospitals, governmental authorities and many other public services are being controlled and organized via the usage of computers and communication networks.

The private sector is no exception, many of the transactions and commercial deals are executed via computers, for example, e-selling, e-purchase, shares and banks, and many other institutions that invest billions of dollars through the electronic environment.

Such great reliance on information technology created a new form of weakness facing the society, public and private lives and facilitated the achievement of terrorists' illegal objectives. Many crimes which target the electronic environment arouse through passage of time. Such crimes are the fastest growing ever when compared with other crimes as they comprise a wide range of illegal activities including financial fraud, hacking, downloading infamous images, viruses, service cutoffs, racism. These activities led to a decline in the legal provided by national laws to combat these crimes.

The current world war is to fight terrorism. The mechanisms of confrontation are changing; however, the reasons behind it remain the same. The world is now facing uncommon terrorist

weapons, from which is the electronic terrorism which targets computers either by damage or destruction. In this context, pressing a key in the keyboard is only what is needed to unless there are safeguards to protect such objectives.

Information technology is considered of the cheapest means in terrorist attacks. Although information technology and network operations and protection is extremely costly, the required means to attack them is very cheap, all what is needed in this concern is a computer and a modem.

A period of time ago, many experts anticipated, with a relatively low percentage, that computers systems and internet would never be a target for terrorist attacks either from an individual, group or a country. But after some time later, and specifically after September 11th attacks, everyone became certain that electronic terrorism is a serious danger that threatens the whole international community.

The current research is based on an essential hypothesis which is:

- Electronic Terrorism is a serious threat for information systems and security.
- Terrorist threats are still existing, and do face the international community.
- The infrastructure of information technology is subject to terrorist attacks and electronic crime.
- It is simple to attack the basic and vital structures of countries, and therefore, blocking lots of services.
- The extreme ability of computers to carry out the illegal objectives of terrorists.

Therefore, we can say that our nation is subject to electronic terrorism and attacks at any time.

By searching in the history of terrorist internet crimes we find out that there are many reasons indicating the need for more protection.

From this point, we can say that the problem of the study could be defined as:

"The method of providing the required protection of electronic environment in the Arab nation against crime and terrorism, on both national and international levels".

This problem can be solved via the theoretical framework of the study which is as follows;

II. THE ELECTRONIC ENVIRONMENT: A BORDERLESS WORLD

The current age is described as the technological age, where a vast technological advancement has been taken place in the

PhD student, University of Assiut, and researcher in the security and strategic affairs, and Executive Director - Center for Law and human rights to peace, Egypt, phone: 0020108683084; fax: 0020882324926; e-mail: Mohamed.s.soltan@gmail.com.

past three decades. The electronic revolution started with the production and then the gradual upgrading of computers through software manufacture. The technological advancement was widely spread through connecting computers all around the world via internet which contributed in providing many services such as electronic mail which is the most used internet service, World Wide Web (www) that facilitated navigating internet using browsers and internet gates.

The following section handles the origin of internet and how it reached such universal state, the basic characteristics of the electronic environment in the Arab nation and how this electronic environment facilitated crimes. Also it handles the internet as a perfect environment for terrorists.

A. Internet: From Privacy to Universality:

The origin of the word internet goes back to the English word (INTERNET). It is divided into two parts: Inter; which means (between) and NET; which means network, and therefore the word internet means inter network.

There are many different definitions for the word internet and other synonymous terms such as web network and spider network.

The internet appeared firstly at the end of the sixties when the U.S. Department of Defense formed an expert committee, its main duty was to establish a network to connect computers with each other. This committee was formed in 1957 and was titled as "Advanced Research Base Agency". The committee succeeded in its achieving its objective and therefore, the first internet network was founded and it was called "ARBANET", standing for "Advanced Research Base Agency Network". Its purpose was to assist the military intelligence [1].

The network started to gradually move out of its private use to the global use. In 1983, the network was divided into two networks, the first one ARBANET, which retained its name and the second network, MILNET, with its purpose is to satisfy the civil needs.

In 1986, the Americans were able to connect the networks of five famous centers with one network called "NSFNET", which was later considered the basic structure to the growth and advancement of internet not only in America but also in other countries.

B. The Basic Characteristics of Electronic Environment in the Arab Nation"

The Arabic electronic environment was not different from other environments. And we will not be wrong if we argued that it does not enjoy the same safety and technical levels as other electronic environments. The Arabic electronic environment as not away of electronic terrorism and crime but we could say that it is within reach of terrorists.

To conclude, we can say that the Arabic electronic environment did not reach a high secure state and this problem will get much more complicated especially with the growth of

terrorist thought in the Arab nation.

C. Facilitation of Crime through Electronic Environment

After the advancement of the electronic environment, one can not manage without computers, however, computers are considered as double-edged weapons. Whereas keyboards could be used to type our future development it could also be used to type the end of such future. The fulcrum between crime and electronic environment is the keyboard. The main problem is restricted to the person using the keyboard. The flexibility of information technology, computers and internet helped terrorists to spread violence and crime and plan and attack. Information technology is useful to terrorists in the following aspects [2]:

- It could be used to enhance the traditional terrorist activity, such as using internet in conscription training, and exchange of information between terrorist groups.
- The infrastructure of information is an attractive goal for terrorism as it easily influences public opinion.

Computers also are no exception due to the following [3]:

- Computers are cheaper than traditional terrorist means, all what is needed is a computer and a modem. Electronic terrorist attacks do not need weapons or bombs to carry out their tasks, they can only create a destructive virus through telephone line or cable or wireless communication.
- The executor of electronic terrorism is completely unknown when compared to the traditional terrorist. Many web users have nick names which make it difficult to trace the terrorist, I.D., also, the cyber has no physical barriers which control the crossing of borders.
- Diversity of computer goals that could be targeted by terrorists.
- The distant dealing with computers, which is a major advantage to terrorists.
- The use of computers requires less training than the training required to carry out traditional terrorism.

And if this was the case with information technology and computers, then we can say that internet is more flexible because of the following reasons [4]:

- Easily reached.
- The absence of organization and control as well as governmental control over internet.
- Widely spread.
- The easy use of internet and the availability of a good multi-media environment. It is very simple to illustrate texts and images as well as sound files and videos. Also it facilitates the download of movies, songs, books and other files.
- The ability to influence public opinion via media coverage.

D. Internet: A scene for terrorists

Internet became an open scene to commit terrorist crimes due to its flexible use and easy access to the web and absence of a lot of other internet negatives.

The following are some forms and methods of using by terrorists [5].

1st scene: - Circulating the terrorist thought:

Terrorism may cause the death of terrorists themselves, or internationally chasing them. Due to this, no one can undertake the risk of terrorist crime except those who believe in extreme principles which do not accept moderate solutions and reject the others, and sometimes, abolish their moral and physical existence. This explains the need for communication media by terrorists to circulate their thought and also the need for a wide base to adopt this thought.

The circulation of this thought via internet is reached through constructing websites representing terrorists groups. Such websites are in continuous growth. It publishes articles and reports which convey threats of carrying out terrorist attacks or to announce its responsibility for one of these attacks. It also publishes denial reports or comments on news from other groups or international authorities.

2nd scene:-Conscription and training:

Terrorists groups may use internet to conscript new members (mainly youth) to help in carrying out their goals. They announce their need to new members as if they were announcing job vacancies, using the religious aspect. These groups always depict their targets as disbelievers. They call youth for jihad to win paradise.

Terrorist groups train their members via internet by demonstrating videos and images illustrating how to make bombs and how to attack the target. In the Al-Azhar attack in Egypt, April 7th, 2005, carried out by Hassan Bashandy, a student at Faculty of Engineering, investigations showed that the executor got information from internet on how to make bombs.

3rd scene: Using Internet in Planning and Carrying out terrorist Attacks:

Planning for terrorist attacks takes place after gathering the required information about the target. They can easily obtain information about departures and arrivals of planes, trucks and trains. They can also obtain maps and photos taken by satellites.

The execution of terrorist attacks has two types:

Type I: Targets physical object and adopts traditional terrorism, for example, altering departure and arrival time of planes which lead to collision of planes which leads to collision of planes.

Type II: Terrorist attacks target internet itself. They are diverse, such as information attacks and destruction of information infrastructure.

of internet. The dramatic effects of electronic terrorism are not yet manifested, but risk indicators are arising. Internet is used in all vital fields; atomic reactors, electricity and water, marine, ground and air navigation lines medical fields, banks, stock markets...etc [6].

Any breakdowns in any of the above fields lead to serious negative results. Nowadays, we have to claim not only the fight of mass destruction weapons but also mass breakdown weapons. Breakdown of internet service lead to mass breakdown of many vital activities.

The following are some examples of scenarios on electronic threats that may target information contents, military or political targets, financial or economic targets. Such threats are extremely dangerous.

A. Attacking information content and infrastructure

This attack targets internet itself, so that it breaks down for some hours causing material negative effects. The attack starts by directing a large amount of information to an internet modem. The modem capacities usually do not assimilate all such information leading to breakdowns in the modem. An example on this, the attack which continued to one hour and directed a large amount of data about 40 times the capacity of the modems. Such attack leads to a breakdown of nine modems out of a total of 13 modems all around the world. Terrorists could destroy information infrastructure by targeting communication cables either by cut or damage.

B. Attacking military and political objectives

This type targets military and political objectives. As for military objectives, it rarely happens for some reasons, mainly, that countries usually separate between military and default reality, and they do not connect computers containing information with internet. Terrorist attacks which target political sites are numerous and happened a lot. An example on these attacks, the success of "Nicolas Anderson", an English citizen, in entering the website of U.S. Navy, stealing passwords and codes used in nuclear attacks. Also, "haes Lander", a German citizen succeeded in penetrating Pentagon database and was able to get 29 documents related to nuclear weapons. An American teenager, 16 years old, stole some software belonging to NASA, amounting to 1.7 million dollars. These software include information about constructing an international space station. NASA paid 41000 million dollars in order to re-design the system. The teenager was arrested while he was trying to enter the site of the pentagon. The American citizen "Ariel Prince" was able to enter the official website of the White House. He was later arrested and prosecuted in November 1999.

C. Attacks on Economic and Financial Objectives

Internet is almost an open free market, where transactions of high values take place, a matter which made the internet an attractive target for terrorists. The reasons for this are [7]:

III. SCENARIOS OF ELECTRONIC THREATS:-

Electronic threats are increasing, especially after the wide use

- Because they are in need for money.
- Attacks targeting economic information centers highly influence public opinion.

Examples:

In 1997, a group of youth, called "Mess club", was able to make a program that enabled them to trick the "Quicken" program of money transfer. The group was able to steal money from "Quicken users' balances.

IV. MECHANISMS OF FIGHTING ELECTRONIC TERRORISM AND CRIME: STRATEGY AND APPROACH

On the international level, the mechanisms and methods of fighting electronic terrorism and crime are diversified and different from one organization to another. In this section, we will shed some light on international mechanisms stated in the international law. After that we will handle International cooperation. The last part deals with a proposal to set an Arabic strategy to secure the electronic environment against terrorism and crime.

A. The international mechanisms of fighting electronic terrorism and crime:

The sole international convention in this regard was the European Convention of Electronic Crimes. And since the reliance on information technology, wire and wireless communication is growing, and since this technology may include many new crimes, therefore we have to discuss the international legal framework and also we have to get acquainted with the international mechanisms adopted to fight electronic terrorism.

United Nations:

There are many international conventions that are approved by the United Nations and which handled different terrorist activities such as crimes committed on board of planes, illegal take over of planes, crimes against civil aviation safety, taking hostages, illegal use of nuclear materials, illegal acts against marine navigation safety and nuclear terrorism. Additionally, United Nations issued a strategy to fight terrorism and which works on assisting member countries and developing their potentials to fight terrorism.

As for electronic terrorism, the United Nations General Assembly decided in 2000, to discuss the means of fighting information technology misuse. This resolution took into consideration the recommendation of countries which is to take the necessary procedures, including [8]:

- Member countries are to state in their laws not to provide any protection of any kind for anyone who might criminally use information technology.
- To state in the legal systems the protection of confidentiality, safety and availability of data and computer systems against any unauthorized block and to guarantee the criminal punishment of the

executor.

In 2000, the United Nations 10th conference of crime prohibition and criminal's penalization was held in Vienna-Austria, where an agreement was reached to emphasize the importance of making every effort on the international level, as regards prohibiting threats against security of information systems and internet. The conference recommended the exchange of technical experiences among the national authorities [9].

The European Council:

The European council endeavored to fight electronic terrorism and information crime. Foreign ministers of member countries signed in November 15th, 2001 the International convention of electronic crime, which is considered the first international convention in this concern. It was the outcome of a 4-year work. Experts from 45 member countries and also experts from non-member countries such as Japan, U.S.A. and Canada participated in its preparation. The convention was the result of the European Council report; it was approved in October 2nd, 2000-Strasbourg. It gained the acceptance of the Eight Nations in their meeting held in Berlin in October 24th, 2000. On the international level, this convention is considered the most effective outcome on the global level to fight terrorism.

Interpol:

Interpol has great endeavors in the field of fighting information crimes and terrorism. According to this organization, 178 countries cooperate together in order to fight crimes. It provides assistance to member countries.

The following are some of the steps taken by the international community to fight crime and terrorism:

- In 1968, the First International Conference of Human Rights was held in Tehran. It concerned with influence of technological advancements on human rights. United Nations General Assembly adopted recommendations of the conference.
- In 1996, the United Nations approved the Ancestral standard act concerning electronic commerce. The act is considered from the major international efforts in the field of fighting electronic crime.
- In the meeting of the Eight Nations held in Washington in 1997, ten principles were approved concerning crime and terrorism.
- In May 2002, the ministers of the Eight Nations held a meeting in Tromblin –Canada, to issue a set of recommendations concerning wiring international calls in order to have control over terrorist attacks.
- In May 11th 2004, the Eight Nations issued a joint announcement entitled "The continuous enhancement of local laws". The announcement recommended all countries to resume the upgrading of laws which criminate the misuse of electronic networks and laws

which permit the international cooperation during investigations.

- In November 17th 2004, the ministerial meeting of IPEC organization was held in Chile. A joint announcement was issued to enhance the economies of member countries in order to fight electronic crime by legislating local laws that conform with international legal rules, including the convention of electronic crimes.
- In April 28th 2004, the fifth meeting of ministers of justice was held in Washington. They issued recommendations to the general assembly of American Countries Organization in order to execute the principle listed in the European Convention concerned with electronic crime and to decide upon joining that convention.
- In 2005, the ASIAN organization set a plan for the exchange of information about safety of computers.

B. International Cooperation as a Tool of Fighting Electronic Crime:

Cooperation between all countries is a major element in fighting terrorism, although the electronic environment does not have an international cooperation plan to protect it against risks of crime and terrorism. The reasons behind this are:

First: These crimes took place recently in some countries.

Second: Many countries do not know about counteraction mechanisms.

Third: These crimes involve critical issues such as economic competition, privacy up to the national security.

The sensitivity of national security and privacy is considered of the main reasons that prevents countries from cooperating together in order to protect the electronic environment, especially, because this cooperation may lead to the announcement of some weaknesses in one country or another. Due to technological advancement, the increase of financial and banking systems, wire and wireless communication networks, aviation systems, aviation traffic control, all of which depend mostly on computers and information technology.

Despite the benefits gained by many countries, there is no single country which have control over such technology. Therefore, it is very reasonable to for countries to cooperate with each other in order to serve the whole international community. Dual and multi cooperation proved to be the most reliable mean of fighting electronic terrorism for two main reasons:

- Some countries did not experience electronic terrorism till now, while other countries experienced many electronic terrorism attacks.
- Some countries have local laws which criminate electronic terrorism, while other countries do not have any of these laws.

The following are some examples on dual cooperation [10]:

- In February 2000, national U.S. Center received a

report informing that C.N.N, yahoo, Amazon and other websites were attacked after service cutoffs. Investigation showed that attacks came from Canada. The National U.S. Center and the Canadian Police Center cooperated together and succeeded in arresting the executors who were a group called "Mafia Boys".

- In May 2000, All companies and individuals all over the world were attacked by a virus called "I Love You", which caused gross losses, the American National Center conducted an investigation, the executors were arrested. Cooperation took place between the Federal Bureau of Investigations (FBI) and the Philippine National Investigation Office.

C. The Arabic Strategy of Electronic Environment Security.

It is highly recommended to discuss the issue of the Arabic strategy of electronic environment security due to the increasing terrorist attacks globally. For many reasons, Information infrastructure in many Arab countries lacks the required protection, mainly, the absence of an electronic crime legislation. Therefore there is an insisting need for setting an Arabic strategy, in order to protect our Arab Nation from terrorist threats that causes major losses amounting to billions of dollars. The strategy is to be set under the sponsorship of United Arab Nations Organization. All Arab countries are to participate in setting such strategy and accordingly they are to cooperate in effecting it.

The researcher's vision for this strategy depends on three main axes:

- Awareness and education.
- Coordination to provide protection against electronic terrorism and crime.
- Exchange of Information among Arab Countries.

D. Illustration of Strategy Framework

1. Awareness and Education:

We have to focus on increasing the awareness of the Arab citizen of the risks of electronic terrorism and crime either through education, media channels or through Internet itself. We have to concentrate on youth as they are the target of terrorists and also acquainting them with kinds of electronic crimes. They are to learn the optimum and limited use of the internet and not to enter terrorist and suspicious websites. We knew that the one who executed Al-Azhar attacks learned how to make a bomb via internet sites.

2. Coordination to provide protection against electronic terrorism and crime.

All Arab countries are to coordinate together in order to protect the electronic environment. This could be achieved by an Arabic convention to confront electronic terrorism and crimes or conducting dual or multi- party convention to facilitate investigation and gathering evidences between the concerned agencies. Also, strategic coordination is to take

place to fight terrorist groups existing inside Arab countries.

3. Exchange of Information

Exchange of Information is considered the most important strategic axis. All international statistics showed that the majority of terrorist crimes carried out in any country were financed, armed, trained or provoked by another country. Terrorist groups cooperate with each other effectively than do the countries and international organizations themselves. They use information technology to provide other groups with required data and information. Therefore, Arab countries are to interchange information to avoid terrorist attacks. The Participants of the 29th conference of Arab security and police chiefs held in Amman in the period between 13, 14-11-2005, emphasized the Arabic coordination. The closure statement recommended the importance of Arabic cooperation to face terrorist crimes. In the previous sections we noticed that international helped in decreasing the number of electronic terrorist attacks and proved to be an effective tool in fighting electronic terrorism and crime.

V. SUMMARY

There is no doubt that electronic terrorism a serious threat, however, it did not yet reach a high risk degree. It is not a negligible. Problems related to information technology represent an international threat. All countries are to face these problems to overcome their risks.

In the mean time, there are no 100% safety methods that provide protection for electronic systems. Also, there is no completely secure computer systems that prevent terrorists from penetrating it. This fact made many governments to follow the policy of isolation. For example, most armies do not keep their highly classified and confidential information on internet- connected computers; however, they keep it on computers that are not connected to the cyber world.

The isolation policy being considered as avoidance means against electronic terrorism and crime does not conform to the reality imposed by the electronic environment on our daily life. Away from the isolation policy, we can use codification, fire walls. Such methods and many other technical protection means can not provide the required protection without the involvement of the governmental protection. Most Arab countries lack the presence of national legislations which protect the electronic environment against electronic attacks. The nature of this environment makes it difficult to describe, follow and arrest the executor of the crime. This environment is of changing, widely-spread nature. Therefore, a powerful legislation to protect such environment against terrorism and crime is a must.

To conclude, Arab governments are to reconsider and amend their national laws to conform to recent crimes. They have to cooperate with each other via an Arabia strategy to protect the electronic environment against terrorism and crime and to reconsider the concepts of national security.

REFERENCES

- [1] Ballard, J.D, Tlomik, J. G, & mekenzie D. 2000, "Technological facilitation of terrorism: Definitional, legal and policy issues "American Behavioral scientist, 45, (6), 989- 1016.
- [2] Weimann.G, (2004 may) Cyber terrorism, How Real Is the Threat? <http://www.usip.org/resources/cyberterrorism-how-real-threat>.
- [3] Collegium Civitas" Foreign Policy of the United States of America how to prevent and fight international and domestic CYBERTERRORISM AND CYBERHOOLIGANISM prepared by Lukasz Jachowicz Warsaw", January 2003, honey.7thguard.net/essays/cyberterrorism-policy.pdf.
- [4] Weimann .G. (2004, march) www.terror.net:How 5-modern terrorism uses the Internet.
- [5] Kraft, D. (2000, October 26). Islamic groups 'attack' Israeli web sites. Retrieved November 10, 2003, from <http://www.landfield.com/isn/mail-archive/2000/Oct/0137.html>
- [6] Mohamed sultan ,
- [7] Vatis, M. (2002, June). Cyber attacks: Protecting America's security against digital threats. Discussion paper, ESDP-2002-04, John F. Kennedy School of Government, Harvard University.
- [8] McWethy, J. & Starr, B. (2001, April 26). Hacker alert: Pentagon braces for Chinese computer attacks. Retrieved November 2, 2003, from, http://abcnews.go.com/sections/world/DailyNews/chinahackers_010426.html.
- [9] Nagpal, Rohas. Defining Cyber Terrorism. 2004. Asian School of Cyber Laws. 04 June 2006. http://www.asianlaws.org/cyberlaw/library/cc/def_ct.htm.
- [10] Responses to Cyber Terrorism, Center, IOS Press, 2008, p74.

Power Analysis On Rfid Smartcard Algorithms Using Simulation

Rohalah Heshmati, Advisor: Dr. Mohamad Ali Doustari

Email: rooh2000_heshmati@yahoo.com, doustari@sgi.ir

Department of Electrical and Computer Engineering, University of Shahed

Estimated Graduation Date: Fall 2010

Abstract—this paper presents the results from a power analysis of the AES algorithms by simulation using the PROTEUS software. Our simulation is capable of simulating the power consumption of assembler programs implemented in, amongst others, microcontroller 8051 assembler. Using the simulation, the Vulnerability for power analysis attacks of straightforward AES implementations is examined. In case countermeasures are added to the implementation that attempt to counter power analysis attacks. After these modifications the analysis is performed again and the new results are compared to the original results.

Index Terms— smartcards- AES- Power analysis attacks- cryptographic algorithm

1. INTRODUCTION

In modern times, smartcards are a widely occurring phenomenon. They are used for electronic money, security, the subway, digital signatures and in numerous other places. Because of the wide use of the smartcard, they also become very interesting for attackers. It is therefore of importance that a smartcard itself is well secured. Up until recently the use of safe and secure encryption algorithms was enough to accomplish this. The introduction of a new type of attack changed all that. Power analysis attacks use the Power signals produced by the smartcard to retrieve information from it that was considered Secure. No longer is a mathematical secure smartcard enough. The information leaked by the Hardware of the smartcard must also be minimal and of no use to an attacker. This can be accomplished by modifying the hardware itself or by modifying the implementation of the Algorithm to include various forms of

countermeasures against power analysis attacks. This paper reports the results we obtained by using the tool created in the PROTEUS software, project to analyze the security of the implementation of common encryption algorithms for smartcards. These are the AES algorithms. First the theory behind power analysis is presented along with an introduction to the simulation. Next we will discuss the AES algorithm. This will include the theory behind the algorithm, our implementation of the algorithm and the results we obtained from the power analysis.

2. POWER ANALYSIS

2.1 general

When cryptographic algorithms are designed and analyzed, a lot of effort is put into securing them against all forms of mathematical attacks. In practice it is often a lot easier to attack the algorithm by using side-channel information generated by an implementation of the algorithm on certain hardware. In this paper we will be concentrating on smartcard hardware. Sources of side-channel information when running algorithms on smartcards are: power consumption, timing information, electromagnetic emissions and introducing faults into the hardware. In Our research we will focus on power consumption. It is not complicated to measure the power consumption of a smartcard; because the smartcard has no power source of itself it has to rely on an external power source that can be easily Monitored, for example, by using a digital oscilloscope as described in [1]. Power analysis uses the fact that the power consumption of a smartcard is based on the hamming weight of the value it is currently processing.

2.2 simple power analysis

Simple Power Analysis or SPA is power analysis based on a single power trace generated by an algorithm run on a smartcard. By observing the trace

one can, for example, gain information about the hamming weight of a certain byte of the key when the location in the power trace where it is being used is known. One can also use visible characteristics of the Power trace to gain information on the key.

2. 3differential power analysis

Differential Power Analysis or DPA was discovered by Kocher, see [2]. DPA is a technique where power traces are combined in a statistical manner to obtain information about the algorithm running on the smartcard. DPA works as follows:

- Generate a (large) number of power traces
- Establish an attack point, as described below
- For all key guesses k run a function D_k (called a condition) that gives a value 0 or 1, to divide the traces in two sets S_0 and S_1 for each trace.
- For all positions i in the power trace, calculate the average power usage (A_{i0} and A_{i1}) for both sets at this position.- Calculate the difference E_i between (A_{i0} and A_{i1}) for all positions i . Attacks are possible at points, where the outcome of a calculation can be predicted, by using known information (for example input and output) and information for which all possibilities can be checked (for example a small part of the key). D is a function that calculates the predicted value at the attack point and divides the traces according to this output. DPA is based on the fact that E_i will be small at positions i , where the power usage is Independent of the outcome of the function D (i.e. places where the key is not being used or where the key was guessed incorrectly). At positions i where the power usage is dependant on D , E_i will be bigger. This technique can be used to identify the location in the power trace where the key is used and to find the key that has been used.

3. PROTEUS SIMULATION SOFTWARE

The project's goal is to develop an integrated support environment for countering side channel attacks (focusing on power analysis), selecting the most suitable type of smartcard and to determine the sensitivity of an implementation to power analysis. By describing an implementation of a cryptographic algorithm in a suitable programming language with Dedicated data types, constructions to counter power analysis and by compiling it into generic assembly code the project has the following advantages:

- Power analysis can be performed at the software level.

- Attack scenarios based on the algorithm can be developed and automatically executed
- Implementation more secure against power attacks. It Calculates a power trace based on this simulation. The tool can also perform DPA and SPA analysis on the generated traces, or export these traces to allow another program to perform the analysis.

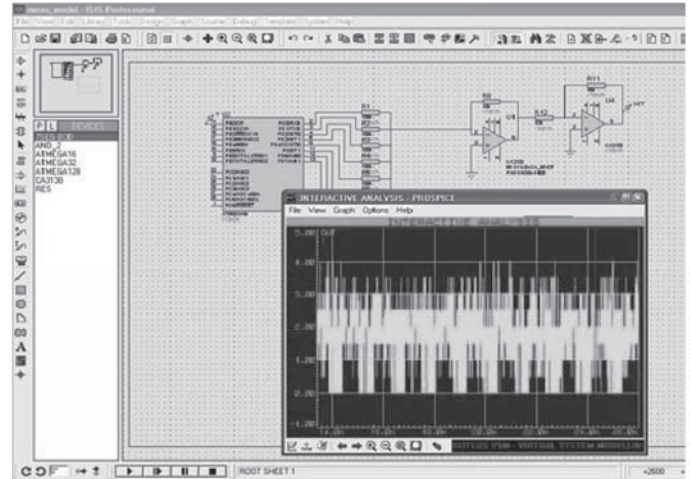


Figure 1: The project showing a power trace of the AES algorithm.

4. AES

4.1.1 Global

The current AES is the cipher Rijndael with the added constraint that the key size is limited to 128, 192 or 256 bits and the block size is limited to 128 bits. Rijndael was developed by Joan Daemen and Vincent Rijmen and is fully documented in [3]. In many ways, AES is a simple cipher. It takes an input of 128 bits (which equals 16 bytes) and orders this as a 4x4 matrix. The key, in our environment always 128 bits, is ordered in a similar fashion.

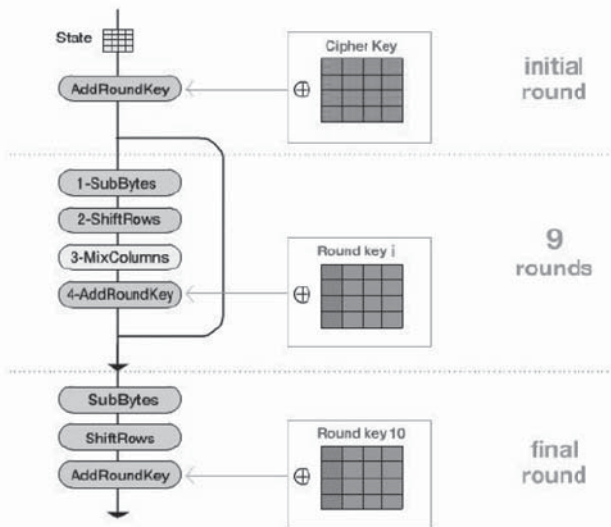


Figure 2: A global overview of the AES algorithm

The algorithm consists of a single AddRoundKey, using the cipher key, followed by 9 regular rounds each consisting of 4 steps and a final round. The steps of the regular rounds are Sub Bytes , Shift Rows, Mix Column and AddRoundKey. The final round skips the Mix Column step. Every round requires its own round key. These keys can be generated in advance or one per round by adding an extra round step. We will now discuss what calculations are performed in each of the 4 steps mentioned.

4.1.1 SUBBYTE

In the Sub Bytes step, every byte from the current state block is replaced by the matching byte from the S-Box. The S-Box is a simple invertible lookup table consisting of 256 values. The specification of AES [3] contains an explanation about how the S-Box can be Calculated. We will not discuss that any further here.

4.1.3 SHIFT ROW

In the Shift Rows step, the bytes from the current state block, still ordered as the 4x4 column major matrix are shifted as follows:

From:	To:
01 05 09 13	01 05 09 13
02 06 10 14	06 10 14 02
03 07 11 15	11 15 03 07
04 08 12 16	16 04 08 12

In our situation, where we limit ourselves to 128bit keys and 128bit input blocks, this equals shifting row i , i places left. Note that for other key / block size combinations the algorithm using different shifting that may not have this property.

4.1.4 MIXCOLUMN

In the Mix Column step, the columns of the current state block are considered as polynomials over $GF(2^8)$ and multiplied modulo the polynomial $x^4 + 1$ with a fixed polynomial given by: $'3' x^3 + '1' x^2 + '1' x + '2'$. This can be written as multiplying each column with the following matrix:

```

2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2

```

4.1.5 ADD ROUNDKEY

The last step of a regular round is AddRoundKey. In this round the algorithm performs a simple XOR on the current state block and the current round key.

4.1.5.1 KEY SCHEDULE

In the Key Schedule process all the round keys that are needed are calculated. The initial setup step of the algorithm uses the cipher key. The 10 regular rounds each need their own round key. The key for round i is generated by performing a series of calculations on the previous key. This includes several XOR operations using the previous key or a round constant, S-Box lookups and permutations. See [3] for a detailed description. The round keys can all be generated in advance and stored in a buffer large enough to hold all 10 round keys and the cipher key, or the key for round i can be generated in round i somewhere before the AddRoundKey step (which is the only step that uses the round key). The latter approach only requires a buffer large enough to hold a single key.

4.1.6 Encryption

Encryption is done with the algorithm described above. The decryption algorithm is the inverse of the encryption algorithm. This means the order of the round transformations are reversed and the transformations

Themselves are replaced by their inverse transformations. Note that the inverse of AddRoundKey is AddRoundKey itself. This means the reverse of a round is given by:

AddRoundKey (State, Round Key);

InvMixColumn (State);

InvShiftRow (State);

InvSubByte (State);

The decryption algorithm omits the InvMixColumn step in the initial round and performs an AddRoundKey using the cipher key after completing all regular rounds.

4.2 IMPLEMENTATION

4.2.1 TARGET PLATFORM

For use in the PROTEUS software an implementation of the algorithm for the 8051 processor needed to be created. The assembler version of the algorithm was created by compiling a C implementation of the algorithm.

4.2.2 IMPLEMENTATION GOALS

Before implementation of the algorithm in C was started a number of implementation goals were set. A readable and simple version of the algorithm was preferred, but not at all costs. The resulting compiled assembler version needed to be efficient enough for use in the PROTEUS simulation software. All round constants and the S-Box table are stored entirely in memory during program execution and are thus not generated on the fly. To not put any further pressure on the memory usage (the memory size is usually very limited on smart cards) only a single round key at a time is stored and a new round key is calculated every round, overwriting the previous round key. Because if all Round Keys were stored on the card, they would all have to be stored in secured memory locations. Because the round constants and S-Box table are publicly known, they can be stored in less secure ROM memory and they do not have to be recalculated for every card as these are constants for the AES algorithm.

4.2.3 C IMPLEMENTATION

Implementing the AES algorithm is pretty straightforward. The resulting implementation can be found in appendix A.

4.2.4 OPTIMIZING THE C IMPLEMENTATION

Compiling the initial implementation of the AES algorithm to assembler, results in an unnecessary inefficient program. The number of steps performed is just too high. Because a large number of power traces need to be generated by PROTEUS simulation software for the Differential Power Analysis an inefficient program can quickly lengthen the calculation time to unacceptable proportions. An inefficient program is also not realistic for smartcards. Therefore a number of steps are taken to optimize the C version in such a way that the resulting assembler program is usable. These steps include, but are not limited to, removing all local variables (thus accessing only global memory), rewriting all functions not to include parameters, rewriting all functions not to include return values and replacing all loops (for,

while) by their equivalent code that only uses labels and go to statements. Finally we profiled the version to see which functions took the most steps and actions were taken to optimize these functions (for example, by writing out an entire loop).

4.2.5 FINAL ASSEMBLER IMPLEMENTATION

All steps taken to optimize the C implementation significantly reduce the number of steps the assembler version takes. Our final assembler version has a constant running time, except for the MixColumn step, and takes approximately 13500 steps. This proved to be more than efficient enough for use in the PROTEUS simulation software. All our attack points lie before the first regular round (which includes the first MixColumn step), so the part of the program that we evaluate in the PROTEUS simulation software has a constant running time.

4.3 DIFFERENTIAL POWER ANALYSIS

4.3.1 IPER-BYTE ATTACK

4.3.1.1 SETUP

4.3.1.1.1 ATTACK POINT

The first step is to identify a place in which the algorithm can be easily attacked. The goal of our attack is to retrieve the cipher key. In AES an obvious place for such an attack is in the initial AddRoundKey, which takes place before the first regular round. In this step the input state block is XOR-ed with the cipher key (which we are looking for). The C implementation is given below (The 8051 assembler version is a direct descendant of this version):

```
01: void AddRoundKey()
02: {
03:   for (i = 0; i < 16; i++)
04:   {
05:     inputdata[ i ] = inputdata[ i ] ^ key[ i ];
06:   }
07: }
```

Note line number 5. This is the line in which our DPA attack is possible. The right hand side of the expression on that line equals a single assembler instruction in which a byte of the input data is XOR-ed with a byte of the cipher key. Since the values of the input are known and there are only 256 possibilities for the value of that particular byte of the key a DPA attack is possible. Attacking at this point was made slightly more convenient by modifying the assembler version as follows. First the execution of the algorithm is halted after the first

AddRoundKey. We can do this, since we're attacking before this point and everything that happens after this point is of no interest to us nor relevant to the attack. We've also configured PROTEUS simulation software to only record power signals concerning to the XOR operation on the input data and cipher key (line number 5 of the C implementation). This limits the number of steps that PROTEUS simulation software has to calculate for a single execution of the program severely and results in a power trace length of 16 (since there are 16 bytes in the cipher key). If an actual physical DPA is performed one also only needs to inspect those 16 values. Note that the AddRoundKey is not the only place where such an attack is possible, also the SubBytes round is vulnerable to a similar attack. When securing Rijndael against DPA one has to consider the other rounds as well.

4.3.1.1.2 CONDITION

For an attack using PROTEUS simulation software a DPA condition is required, which we've called the Rijndael Condition. This condition is given below (only relevant code is shown):

```
01: public Boolean select
02: throws Unsortable Exception
03: {
04: int attackedbyte;
05:
06: Word inputs = t.getInputs();
07:
08: if ( mode % 2 == 1 )
09: attackedbyte = inputs[ (mode-1)/2 ].getByte(0);
10: else
11: attackedbyte = inputs[ (mode)/2 ].getByte(1);
12:
13: // XOR the byte with the key.
14: attackedbyte ^= key;
15:
16: // Calculate the hamming weight.
17: int wgt = Util.hammingWgt( attackedbyte, 8 );
18:
19: // Return true or false depending on the hamming weight.
20: if ( wgt > 4 ) return true;
21: if ( wgt < 4 ) return false;
22:
23: throw new UnsortableException();
24: }
```

This condition will divide traces into two groups, by calculating the predicted hamming weight for the result of the XOR operation used in the add Round Key step. It does this by using the known input and trying all 256 possible values for the current byte of the key.

4.3.1.1.3 INPUT

The test is performed three times, each time with different input sets of different sizes. PROTEUS simulation software was fed with 400, 2000 and 4000 random input values. This results in 50, 250 and 500 power traces respectively.

4.3.1.2 INITIAL RESULT

The table below shows the results of the initial Differential Power Analysis on the straightforward AES implementation:

Byte	DPA Result (50 traces)	DPA Result (250 traces)	DPA Result (500 traces)	Correct value
0	182 (10110110)	59 (00111011)	43 (00101011)	43 (00101011)
1	84 (01010100)	126 (01111110)	126 (01111110)	126 (01111110)
2	149 (10010101)	21 (00010101)	21 (00010101)	21 (00010101)
3	48 (00110000)	86 (01010110)	22 (00010110)	22 (00010110)
4	146 (10010010)	40 (00101000)	40 (00101000)	40 (00101000)
5	175 (10101111)	174 (10101110)	174 (10101110)	174 (10101110)
6	199 (11000111)	210 (11010010)	210 (11010010)	210 (11010010)
7	160 (10100000)	166 (10100110)	166 (10100110)	166 (10100110)
8	82 (01010010)	171 (10101011)	171 (10101011)	171 (10101011)
9	243 (11110011)	241 (11110001)	247 (11110111)	247 (11110111)
10	52 (00110100)	21 (00010101)	21 (00010101)	21 (00010101)
11	136 (10001000)	136 (10001000)	136 (10001000)	136 (10001000)
12	9 (00001001)	9 (00001001)	9 (00001001)	9 (00001001)
13	139 (10001011)	207 (11001111)	207 (11001111)	207 (11001111)
14	236 (11101100)	79 (01001111)	79 (00111100)	79 (01001111)
15	56 (00111000)	60 (00111100)	60 (00111100)	60 (00111100)

It is clear from the table that 50 power traces aren't sufficient to correctly retrieve the key. The results with 250 power traces have improved vastly, but three bytes of the key are still guessed incorrect, although the errors are only marginal (1 and 2 bits). A DPA with 500 traces retrieves all bytes of the key correctly. However, experiments show that this is not necessarily always the case. A different set of 500 traces provided us with a situation in which 15 of the 16 bytes of the key were guessed correctly and 1 byte was guessed wrong, with a 1 bit error.

4.3.1.3 COUNTER MEASURE

The – relatively simple – DPA attack performed above is possible because the implementation contains absolutely no countermeasures against such an attack. The program performs the same calculation (using the cipher key) at exactly the same place during each execution of the program. As a countermeasure against this situation a technique called *randomization* has been used to strengthen the implementation. This technique randomizes the execution order of a series of instructions. This helps to protect against DPA attacks as a DPA attack relies on the same instruction being executed at the same time in each run of the

program. The *randomization* countermeasure was implemented in the AddRoundKey step as follows:

```
01: void AddRoundKey()
02: {
03: // Create random permutation from 0..15.
04: for (tmp = 0; tmp < 16; tmp++)
05: {
06: // Get two random indices in the range 0..15
07: i = rand( 16 );
08: j = rand( 16 );
09:
10: // Store value at first index.
11: tmp2 = order[ i ];
12:
13: // Overwrite value at first index with value from second index.
14: order[ i ] = order[ j ];
15:
16: // Write temporary stored value from 1st index to 2nd index.
17: order[ j ] = order[ i ];
18: }
19:
20: // Execute XOR in the above calculated order.
21: for (i = 0; i < 16; i++)
22: {
23: inputdata[ order[ i ] ] ^= key[ order[ i ] ];
24: }
25: }
```

As one can see above, this countermeasure is not hard to add to the implementation, yet it should prove efficient enough to make simple DPA attacks, like in section 4.3.1.2, impossible. We will explore that in the next subsection. Another advantage of this countermeasure is that it doesn't make the execution time of the algorithm significantly larger. It only increases the number of steps required a little and the program maintains its constant runtime. This technique, however, does require that a random number generator is present on the smart card.

4.3.1.4 FINAL RESULT

After implementing the countermeasures a DPA was performed again. This time, off course, we hoped that the correct key would not be found. DPA was performed again with trace sets of three different sizes, as in the previous test. The results are shown in the table below.

	(50 traces)		(250 traces)		(500 traces)		
0	39 (00100111)	2	(00000010)	2	(00000010)	43	(00101011)
1	41 (00101001)	94	(01011110)	138	(10001010)	126	(01111110)
2	235 (11101011)	119	(01110111)	32	(00100000)	21	(00010101)
3	239 (11101111)	91	(01011011)	6	(00000110)	22	(00010110)
4	178 (10110010)	138	(10001010)	21	(00010101)	40	(00101000)
5	28 (00011100)	200	(11001000)	50	(00110010)	174	(10101110)
6	70 (01000110)	222	(11011110)	97	(01100001)	210	(11010010)
7	116 (01110100)	119	(01110111)	220	(11011100)	166	(10100110)
8	205 (11001101)	147	(10010011)	14	(00001110)	171	(10101011)
9	219 (11011011)	1	(00000001)	140	(10001100)	247	(11110111)
10	58 (00111010)	140	(10001100)	85	(01010101)	21	(00010101)
11	178 (10110010)	70	(01000110)	100	(01100100)	136	(10001000)
12	179 (10110011)	37	(00100101)	112	(01110000)	9	(00001001)
13	105 (01101001)	105	(01101001)	223	(11011111)	207	(11001111)
14	190 (10111110)	2	(00000010)	67	(01000011)	79	(01001111)
15	93 (01011101)	38	(00100110)	140	(10001100)	60	(00111100)

As expected the correct key is not found. Even in the situation with 500 traces, which guessed all bytes of the key correct in the straightforward implementation without any countermeasures, none of the bytes of the key are found. Three bytes are differing by only one bit, one by two bits and two by three bits. All others differ by 4 bits or more.

As a stress test PROTEUS simulation software was used again on a set of 8000 traces. This is 16 times the of traces that was needed to retrieve the correct key for the implementation without countermeasures. Even in this situation the correct key is not found as can be seen in the table below. It should be noted that the average number of wrong bits is reduced. However, the number of wrong bits is still too significant to make any assumptions or reasonable guesses about the cipher key.

Byte	DPA Result (8000 traces)		Correct value	
0	40	(00101000)	43	(00101011)
1	94	(01011110)	126	(01111110)
2	17	(00010001)	21	(00010101)
3	3	(00000011)	22	(00010110)
4	32	(00100000)	40	(00101000)
5	130	(10000010)	174	(10101110)
6	234	(11101010)	210	(11010010)
7	2	(00000010)	166	(10100110)

8	134	(10000110)	171	(10101011)
9	150	(10010110)	247	(11110111)
10	20	(00010100)	21	(00010101)
11	12	(00001100)	136	(10001000)
12	18	(00010010)	9	(00001001)
13	183	(10110111)	207	(11001111)
14	5	(00000101)	79	(01001111)
15	9	(00001001)	60	(00111100)

4.3.2 PERBIT ATTACK

4.3.2.1 SETUP

4.3.2.1.1 ATTACK POINT

Although the per-byte attack described above already successfully retrieves the key of the AES implementation, we also present a per-bit attack on AES below. This can be considered a proof of concept that per-bit attacks are also possible to simulate using PROTEUS simulation software. This is useful because certain algorithms or cards might be safe from per-byte attacks, but vulnerable to per-bit attacks.

4.3.2.1.2 CONDITION

The relevant part of the condition file for the per-bit AES attack is given below:

```
01: public boolean select
02: throws UnsortableException
03: { int attackedbyte;
04: Word inputs = t.getInput();
05:
06: // Extract the required byte from the input
07: int modebit = (mode % 8);
08: int modebyte = (mode - modebit)/8;
09:
10: if (modebyte % 2 == 1) {
11: attackedbyte = inputs[(modebyte-1)/2].getBytes(0);
12: } else {
13: attackedbyte = inputs[(modebyte)/2].getBytes(1);
14: }
15:
16: // Return true if the input bit xor keybit != 0
17: return (((attackedbyte >> modebit) & 1) ^ key != 0);
18: }
```

4.3.2.1.3 INPUT

Although the key list is now much smaller, the list of input needs to be much bigger: a per-bit attack requires significantly more traces. We've performed the test three times, once with 4000 inputs, once with 8000 inputs and once with 100000 inputs. This results in 500, 1000 and 12500 traces respectively.

4.3.2.2 RESULT

Since we're attacking per-bit it's not much use to show a table with the byte-wise results that contains the number of erroneous bits, so we simply present the outcome of the test of whether the key was actually found or not:

Number of traces	Key found
500	No
1000	Yes
12500	Yes

A number of 500 traces was enough to retrieve the key in a per-byte attack, but as expected isn't enough to retrieve the key in a per-bit attack. Since a per-bit DPA attack is much faster (only 2 keys to test) we were able to perform an attack using 12500 traces, which successfully retrieved the key. However, a final test showed that 1000 traces were already enough to discover the key.

5. CONCLUSION

When AES is implemented in the way described in [3], it is very likely that the implementation is vulnerable to a DPA attack, because in the reference implementation the key is XOR-ed directly with the input in the first execution of AddRoundKey. This is almost the ideal case for a DPA attack based on Hamming weights. This problem can be resolved, for example, by using the randomization countermeasure described in section 4.3.1.3. If this measure is implemented, DPA in AddRoundKey will be a lot more difficult but in theory not impossible, as the randomization should be canceled out if enough samples are used. We have, however, not been able to successfully use the attack above on the improved version using the PROTEUS simulation software. More advanced countermeasures are described in [4] and could be used to protect the algorithm against other attacks (such as timing attacks in Mix Columns).

REFERENCES

- [1] Investigations of Power Analysis Attacks on Smartcards, T. S. Messerges, E. A. Dabbish, R. H. Sloan
http://www.eecs.uic.edu/~tmesserg/usenix99/paper_n.ps
- [2] Differential Power Analysis, P. Kocher, J. Jaffe, B. Jun, Advances in Cryptology - Crypto 99 Proceedings
<http://www.cryptography.com/resources/whitepapers/DPA.pdf>

[3]

The Rijndael Block Cipher, J. Daemen, V. Rijmen
<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndaeldocV2.zip>

[4]

Multiplicative Masking and Power Analysis of AES, J. Dj. Golic, C. Tymen
http://www.gemplus.com/smart/r_d/publications/pdf/GT03perm.pdf

Source Code Vulnerability Detection: Techniques and Tools

Sarah Berenji, Reyhaneh Eslami, Mohammad Akbari

Abstract— Vulnerability in software is one of the most important security issues in computerized systems. There are two main approaches for analyzing source code and detecting its vulnerabilities: the static and the dynamic approaches. In static method, there is no need to run source code to detect its vulnerabilities but in dynamic method the vulnerabilities are detected during the execution of the program and prevented from. Both, static and dynamic approaches utilize different methods for detecting vulnerabilities. Here we review several tools that use different techniques have been presented.

Index Terms— static and dynamic vulnerability detection, source code analyzing and assessment, software security

I. INTRODUCTION

VULNERABILITY in software is one of the most important security issues in computerized systems. These vulnerabilities show the weakness in program or errors in their execution. When the programmers pay attention to security features, they pay attention to security features like encoding, password and access mechanisms most. According to Michael Howard, the programming manager of Microsoft security engineering team, security features are different from the security of features [1]. To have a secure program, all parts should be supplied with enough security not just those parts that are related to security directly. In many cases security failures are not related to the security features at all. Most of the security problems are as a result of weaknesses and defects of non-security features. For example, vulnerabilities in LibPNG source caused denial of service attacks in the system of Firefox, Opera, Safari and many other software users [2]. Many other similar cases have been detected that in all of them, image processing codes have some vulnerabilities, not the security parts. Not only these vulnerabilities can cause denial of service but they can also put whole system in danger too. Many of the software vulnerabilities are because of

programming defects, especially incorrect use of insecure methods of C language. The invader can utilize this vulnerability and run its commands on the system and put away all the access limits. Buffer overflow and format string are the common vulnerabilities.

Although software vulnerability is a common problem and there is a lot of information about it, yet lots of problems are being reported. Figure 1 shows the number of detected vulnerabilities by CERT/CC center during 2000-2006.

As figure 1 illustrates, the number of reported vulnerabilities has been increased. One reason for this increment is the complexity of current software. Another reason is the increase in the size of software.

There are two main approaches for detecting and omitting vulnerabilities: static and dynamic. In this paper we first review the methods and current tools of detecting vulnerabilities in source code. Then we will categorize different methods of source code static analysis and explain about their operation in part 2. In part 3 we will discuss about dynamic techniques of detecting vulnerability and in part 4 we will have conclusion.

II. STATIC TOOLS

Static analysis of code is a way for analyzing and checking the program without executing it. Each tool that analyzes the code without executing it is called static code analyzer tool. A static tool acts like a spell checker. Even a good typist uses a spell checker although the spell checker won't recognize all

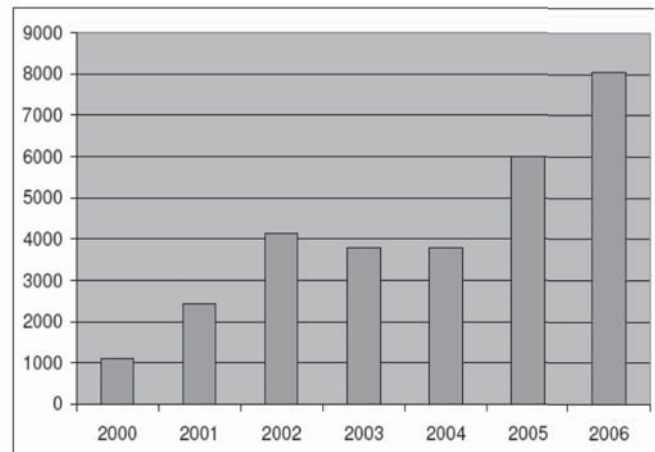


Fig. 1. Vulnerability report by CERT/CC Years: 2000-2006

Manuscript received March 31, 2010.

F. S. Berenji was with Kish University, Kish Island, Iran, (e-mail: Sarah.Berenji@gmail.com).

S. R. Eslami is with Iran Argham Co. Tehran, Iran. (e-mail: Reyhaneh@Akbari.asia)

T. M. Akbari, is with Computer engineering Department, Islamic Azad University, Shahr-e-Ghods branch, Iran. (Corresponding author to provide phone: +989126966690; e-mail: Mohammad@Akbari.asia).

mistakes as there is no guarantee for a piece of writing to be free of errors. For example if we use moot instead of mute, the spell checker won't recognize the mistake. Static tools are like spell checkers. There is no guarantee that the code won't have any vulnerability after it has been analyzed because they only recognize common mistakes. Both professional and ordinary writers use the spell checker but it doesn't transform an ordinary writer to a professional one. The same is true for static tools. Utilizing these tools has a positive effect in a professional programmer's code but a weak programmer may still generate invalid codes [3].

Small mistakes like faults in spelling can cause security problems. Carelessness, tiredness or being in hurry can cause security problems too. They even may occur because of not having enough knowledge about secure programming. It is quite normal for a programmer not to be aware of all methods of hacking and invasion. As a result static tools will be very useful in detecting security problems.

The goal of static tools is to extract some parts of code and judge them. Static tools have been used in code picturing recently [4]. For example more than one hundred hidden bugs in Linux core have been detected by utilizing these tools [5].

Some researches and investigations have been done to detect vulnerabilities of source code statically. These researches led to introduction of some vulnerability detection tools. Classifying tools according to their approach will be very useful in understanding current methods of detecting vulnerabilities. In the following we will categorize current tools according to their approach and will introduce some of the most popular tools.

A. Syntax Oriented Tools

This category includes those tools that use pattern matching and lexical analysis. Pattern matching is one of the easiest ways of static analysis. This method acts like Grep and finds vulnerable functions like gets (), sprint () and strcpy () and decides whether they are safe or not. The number of false positive in tools that utilize this simple method is great. One example of these tools is Flawfinder [6]. This tool examines the source code to find buffer overflow or format string vulnerabilities. Because of not having a C parser this tool can't distinguish code comments from source code and in case of empty spaces or unexpected macros it produces incorrect result [7].

Another group of tools convert the source code into tokens by using a lexical analyzer. They omit unimportant features like white spaces and comments. This approach is called source code lexical analysis. Lexical analysis tools act better than pattern matching tools. To produce more useful reports, tokens usually carry information like the location of vulnerable code (row and column number). Tools like ITS4 [8] and RATS [9] are included in this category.

ITS4 has been introduced by Cigital group in 2000 to detect security vulnerabilities of C and C++ languages [10]. This tool has a database of current vulnerabilities in C functions and like Grep checks the security of source code. For example if

the second parameter of strcpy () function is a static string, it won't be an insecure call function.

RATS is a lexical analysis tool that has been presented in 2001 [11]. This tool can check the code of C, C++, Perl, PHP and Python languages. Like Flawfinder and ITS4 it has a data base of vulnerable functions and the level of their security risk.

B. Compiler Based Tools

Alexander Sotirov has introduced some of static analysis code tools as type qualifiers [7]. These types of tools have been developed according to Type qualifier frame work.[12, 13] Introduces type qualifiers as features that can describe current standards of C, C++ and Java languages. In fact Type qualifiers are a kind of light type-oriented mechanisms that improve the quality of soft wares [14]. These languages usually have some type qualifiers (for example key words like *const* and *register* in C language). Foustier has presented a general purpose system for adding user-defined type qualifiers by means of annotating on source code. Type qualifiers are actually light annotations for specifying attributes of program. Type qualifiers technique is being used in a language to compare the code with valid annotated qualifiers and check whether it contradicts the qualifiers condition or not. By using qualifiers, programmer will be able to remove bugs from source code. In this system, user-defined type qualifiers are added to the system through source code annotation. Type contradictions will be recognized through inference on type qualifiers.

This technique is used in CQual [15] to add user-defined type qualifiers to C language. It is also used for detecting buffer overflow and format string vulnerabilities. CQual utilizes type qualifiers to run a taint analysis and detect format string vulnerabilities in C language.

The programmer should annotate on source code, declare some variables as taint or untainted and use type-inference rules for qualifiers propagation. After qualifiers propagation, system will be able to recognize format string vulnerabilities.

Type qualifier technique has been used in BOON [16] to detect buffer overflow vulnerabilities. In fact, BOON is a special-purpose tool for detecting buffer overflow in source code. At first, it examines string variables and then examines the variables according to their allocated memory and the amount of memory they're using. It also examines the boundary of integer variables to see whether a C program can index an array out of its boundary or not.

BOON presents a list of detected vulnerabilities, their run-time duration and the correct run-time duration. Although this tool recognizes many ignored mistakes by lexical analysis tools, it's not an exact tool yet. BOON doesn't care about the order of program sentences and can't model the inner procedural dependencies. It also ignores aliasing pointers [17].

C. Theory Based Tools

Theory-based tools get their concept from common theories in computer science. These tools are divided into two groups:

finite automaton and program verification [18].

1) *Finite Automaton*

A finite automaton is a mathematical model with finite states. It takes a group of tokens as input and transfers between a series of states according to a transition function.

According to the final state (state that the machine will stop) the input string will be accepted or not. The language of finite automaton is all set of words that are being accepted by the finite automaton. The finite automaton has a finite set of states that some of them are considered as vulnerability bugs. The machine will take source code of the program or a set of semantic information that are being extracted from the program as input and then detects its vulnerabilities.

2) *XGCC*

This tool utilizes finite automaton to specify the validity of the condition [19, 20]. At first the control flow graph will be build from source code and then it searches the graph. If the status of checked nodes adjusts with one transition of the automaton, its status will be updated. If a branch is being visited (for example an if statement) in the graph, the whole automaton that is being affected by the branch will be duplicated again.

3) *¹MOPS*

MOPS uses model oriented approach for detecting vulnerabilities in C language [21]. Developers can model their security features and utilize MOPS to detect errors of privilege management, change-root jail, file access race condition and temp files misunderstanding. A ²FSA will be built for every under survey case and the program will be compiled by a ³PDA.

MOPS utilizes a similar method like XGCC for detecting vulnerabilities. It is a tool for confirming the correspondence of C programs to the security rules (identified as temporary security features). MOPS represents these features as final states and utilizes the procedure of studying model to find insecure states of the program.

4) *Confirm Program Validation*

In software development the programmer knows the meaning of every code segment. But a static analysis tool should extract this meaning or even conjecture the meaning (according to the evidences). If the programmer specifies some of this information in the code, the tool can use them in source code analysis. Code annotations are extra syntax structures that specify the semantic features of source code. Tools that support annotation help the programmer in detecting vulnerabilities [22]. In some resources, these tools are being categorized as annotation-dependent tools.

Annotation is in fact information about some parts of the document. In fact annotation is comments that the programmer puts them in the source code so that static analysis tools can use them. For example:

```
Strep (char *s1, char *s2)
```

```
Annotation /*maxSet (s1) >= maxRead (s2)*/
```

This annotation is for being sure that s1 is big enough to include all s2 characters. This approach is being used for detecting format string buffer and buffer overflow

vulnerabilities. Splint has implemented this method. A static analysis will be done in syntactic level by means of semantic comments that are specified by user and pars tree of program. This tool is being used to find problems like unused variables, null pointer dereferences, memory leak and buffer overrun [14].

Splint uses pre-condition and post-condition to detect buffer overflow [23]. Without annotation, this tool acts like Lint and checks the code. By using annotation, developers can find abstract vulnerabilities and time of check – time of use TOC-TOU. This tool can also limit the use of buffers by using pre-conditions and post-conditions. Therefore programmer should add pre-conditions, post-conditions and annotation to the code.

III. DYNAMIC TOOLS

In this section, we will discuss about dynamic tools and their categories. Prevention of infusion is done by making changes in run-time environment or system performance. This makes the program less vulnerable. It means in a normal environment the program is still vulnerable (there are some security problems). But in a more secure environment the vulnerabilities can't act like before [18]. If an attack is done, the dynamic method terminates the program.

A. *Dynamic Tools for Detecting Vulnerabilities*

¹STOBO is a dynamic tool that acts according to test technique [24]. It implements source code by adding small wrapper functions to supervise buffers and check the security of library functions. It keeps size of all buffers in a global table. For each variable declaring a buffer a special function is called. All buffers and constructors that use buffer memory are wrapped by special functions. Library functions have some pre-conditions. For example in strepy (), memory allocated to the destination buffer should be bigger than the source buffer otherwise buffer overflow occurs and a warning is logged in a log file.

STOBO gets a source file as input and adds some extra code to it. During run-time the program proceeds its normal routines, but some information is logged in a file according to test codes. STOBO replaces `_STOBO_libraryfunc ()` as wrapper instead of insecure library functions. It checks pre-conditions before calling main function and logs buffer overflows.

B. *Dynamic tools for Preventing Vulnerabilities*

Tools that are presented to prevent vulnerabilities in source code can be categorized in two groups. First group include tools that protect buffer stacks against buffer overflow attacks. StackGuard, Stack Shield and ProPolice are three common tools of this category. Second group include tools that protect all memory regions from buffer overflow attacks. This group of tools is called Bounds checker. In continue, CRED will be described as a sample of this group.

1) *StackGuard*

StackGuard compiler that is planned and implemented by

Crispin Cowan and others [25] is one of the most popular dynamic methods. This method is planned for detecting and preventing overflow of stack buffers. StackGuard uses return address.

The main idea of StackGuard is that all important values for the target are rewritten when a buffer overflow occurs. We can detect and prevent attacks with setting a special value between the return address and top of the stack. Then we check whether this special value has been rewritten or not before using the return address. This special value is called Canary value.

Some attackers can access to return address and change it with their desirable value without changing the Canary value. It can be done through rewriting the Canary value with its previous value (as a result, the Canary value seems unchanged) or through using a pointer that rejects the Canary value. For solving the first problem two versions of Canary value have been introduced. First Canary version is a 32-bit random value that is being calculated during run-time. The second Canary version is a terminator that includes all four string terminators: Null, Carriage Return, -1 and Line Feed. In Random Canary method, invader should guess or retrieve Canary value during run-time. In Terminator Canary method, the invader should enter a string of terminators so that the canary value remains unchanged when overflow occurs, although it is impossible because string function considers each terminator as the end of string.

We should note that these techniques only can prevent from overflow attacks that rewrite everything in stack, not those attacks that are related to return address. The invader still can put a new address in this memory location through a pointer that points to the return address. To solve this problem, the StackGuard team has suggested that in addition of keeping the canary value its value should be XOR with the correct return address and the result should be saved. As a result, the attack could be detected even if the Canary value remains unchanged because the XOR value of Canary value and return address has changed. In the case of using XOR technique the Canary value should be of random type, because if Terminator Canary is used its XOR result with return address is not a terminator string any more.

2) Stack Shield

Stack Shield is a patch for GCC compiler that has been introduced by *Vendicator* [26]. Three type of protection have been presented in its seventh version. Two types are for preventing from writing on return address (that can be used simultaneously) and one type is for preventing from function pointers rewriting.

Global Return Stack

Default preventing method of Stack Shield is preventing according to global return stack. Global return stack is a separate stack for keeping return address of different function calls during run-time. This stack is a general array with 32-bit inputs. Whenever a function is called its return address is kept in system stack and global return stack simultaneously. When the function returns, the return address in system stack is

replaced with the address in global return stack. If an invader rewrites the return address, the attack will be stopped without terminating the program. As there is no comparison between the value of return address in system stack and global return stack, the occurrence of attack can't be detected and only prevention is being done.

Return Range Check

Another easier and faster version of Stack Shield for protecting return address is checking the return range. Return range checking uses a global variable for keeping return address of current function. Before returning, value of stack return address will be compared with the current value of global variable and if they were different, the program terminates. In spite of global return stack, return range check can detect intrusions

Protecting Function Pointers

The main idea of this approach is that function pointers should point to the text segment of procedure memory. If the procedure gives this certainty that all function pointers only can point to text segment, it will be impossible for the invader to change function pointer so that it will point to the injected code. Because code injection is only possible through data segment, BSS segment, heap and stack.

Stack Shield adds checking code before all function calls that use function pointers. Then a global variable is declared in data segment and its address is used as border value. Checking function gives this certainty that each function pointer points to the memory under global variable address. If it points to upper memory unit, the procedure terminates. If the programmer wants to use dynamic function pointer allocation, prevention may face with false positive.

3) ProPolice

ProPolice is one of the most complicated compiler patches for preventing source code vulnerabilities [27]. GCC patch has borrowed its main idea from StackGuard and uses Canary value for detecting stack attacks. The new point is that for protecting stack variables, local variables are rearranged so that char buffers are always located at the lower parts of stack beside the old base pointer. As a result local variables don't get damaged.

4) ¹CRED

Some dynamic tools for detecting buffer overflow don't prevent buffer overflow attacks completely. Tools like StackGuard, Stack shield and ProPolice that are mentioned before, protect program only from stack smashing. Scope checkers detects all parts that are invaded during the run-time and prevent all buffer overflow attacks. Some of the scope checkers change representation of C pointers [29, 30, 31]. These tools replace each program pointers with a structure that keeps necessary information for checking scopes, like base address and buffer extent. This change not only increase use of memory but also is inconsistent with inheritance.

As CRED checks the scope of memory accesses directly, it can detect all buffer overflow attacks [32]. It uses a global table to keep memory scopes. For each memory reference during run-time, an entry is made in table. Each entry consists

of allocated memory scope and a base address. Whenever a pointer refers to memory, the table is being used to check if accessing to memory is legal or not. Pointers that are out of scope are legal unless they have no reference.

This way all memory scopes are protected against overflow attacks except those are allocated by external libraries.

IV. CONCLUSION

Because of software development and source code complexity, vulnerabilities of source code have increased. Although lots of efforts have been done to prevent buffer overflow vulnerabilities by different groups, still there are demands for new solutions. Some tools are introduced in recent years that were successful in detecting vulnerabilities of software. Using these tools, improves the security of softwares. In this paper, we have introduced current methods and categorizations of detecting vulnerabilities and some tools in summary.

REFERENCES

- [1] Howard and LeBlanc, *Security Features != Secure Features*, 2002
- [2] <http://www.securityfocus.com/bid/6431>, August, 2004
- [3] Brian Chess, Jacob West, *Secure Programming with Static Analysis* Addison-Wesley, 2007, ISBN-10: 0321424778
- [4] GrammaTech. CodeSurfer. <http://www.grammatech.com/products/codesurfer/>.
- [5] Engler, D., B. Chelf, A. Chou, and S. Hallem. 2000. Checking system rules using system-specific, programmer-written compiler extensions. In *Proceedings of the fourth symposium on operating systems design and implementation*. San Diego, CA, USA.
- [6] FlawFinder Home Page. <http://www.dwheeler.com/flawfinder/>.
- [7] Alexander Ivanov Sotirov, Automatic Vulnerability detection using static source code analysis, MSc Thesis, University of Alabama, 2005
- [8] John Viega, J. T. Bloch, Tadayoshi Kohno, Gary McGraw, ITS4: A Static Vulnerability Scanner for C and C++ Code, Reliable Software Technologies
- [9] <http://www.fortify.com/security-resources/rats.jsp>
- [10] Viega, J., Bloch, J. T., Kohno, T. and McGraw, G. ITS4: A Static VulnerabilityScanner for C and C++ Code. In *Proc. 16th Computer Security Applications Conferences* pp. 257- 266, New Orleans, LA, 2000.
- [11] RATS: Rough Auditing Tool for Security. <http://www.securesoftware.com/resources/tools.html>
- [12] Foster, Jeffrey. 2002. Type qualifiers: Lightweight specifications to improve software quality. Ph.D. thesis, University of California, Berkeley
- [13] Wagner, D., Foster, J. S., Brewer, E. A. and Aiken, A. A First Step Towards Automated Detection of Buffer Overflow Vulnerabilities. In *Network and Distributed System Security Symposium*, pp. 3-17, San Diego, CA, 2000
- [14] Kamran Zafar Asad Ali, Static Techniques for Vulnerability Detection, Linkopings University Sweden
- [15] CQual Home Pages: <http://www.cs.umd.edu/~jfoster/cqual/>
- [16] Wagner, D. BOON: Buffer Overrun Detection. <http://www.cs.berkeley.edu/daw/boon/>.
- [17] J. Wilander, M. Kamkar. A comparative study of publicly available tools for static intrusion prevention. In *Proceedings of the 7th Nordic Workshop on Secure IT Systems*, Karlstad, Sweden, November 2002
- [18] Martin Johns, Preventing Buffer Overflows, University of Hamburg, 2006
- [19] Seth Hallem, Benjamin Chelf, Yichen Xie, and Dawson Engler. A system and language for building system-specific static analyses. In *ACM Conference on Programming Language Design and Implementation*, pages 69--82, Berlin, Germany, June 2002
- [20] <http://www.stanford.edu/~engler/p27hallem.ps>
- [21] Chen, H. and Wagner, D. MOPS: Model Checking Programs for Security Properties. <http://www.cs.berkeley.edu/daw/mops/>.
- [22] Martin Johns, A practical guide to vulnerability checkers, University of Hamburg, 2006
- [23] Evans, David. SPLINT. <http://www.splint.org/>
- [24] Eric Haugh and Matt Bishop. Testing C Programs for Buffer Overflow Vulnerabilities. In *Proceedings of the 10th Network and Distributed System Security Symposium (NDSS03)*, San Diego, California, U.S.A., February 2003. Internet Society
- [25] C. Cowan, C. Pu, D. Maier, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang, and H. Hinton. Stack-Guard: Automatic adaptive detection and prevention of buffer-overflow attacks. In *Proceedings of the 7th USENIX*
- [26] Vindicator. Stack Shield technical info file v0.7. <http://www.angelfire.com/sk/stackshield/>, January 2001.
- [27] H. Etoh. GCC extension for protecting applications from stack-smashing attacks. <http://www.trl.ibm.com/projects/security/sp/>, June 2000
- [28] John Wilander and Mariam Kamkar, A Comparison of Publicly Available Tools for Dynamic Buffer Overflow Prevention, Dept. of Computer and Information Science, Linköping universitet
- [29] J. Condit, M. Harren, S. McPeak, G. C. Necula, and W. Weimer. CCured in the real world. In *Proceedings of the ACM SIGPLAN 2003 Conference on Programming Language Design and Implementation*, June 2003.
- [30] T. Jim, G. Morriset, D. Grossman, M. Hicks, J. Cheney, and Y. Wang. Cyclone: A safe dialect of C. In *Proceedings of the USENIX Annual Technical Conference*, pages 275 –288, June 2002.
- [31] ¹ S. C. Kendall. Bcc: Run-time checking for C programs. In *Proceedings of the USENIX Summer Conference*, pages 5–16, 1983.
- [32] O. Ruwase and M. S. Lam. A Practical Dynamic Buffer Overflow Detector. In *Proceedings of the Network and Distributed System Security (NDSS) Symposium*, pages 159--169, February 2004. <http://suif.stanford.edu/papers/tunji04.pdf>

Sarah Berenji received the B.Sc. degree in Software Engineering from Kish University, Kish Island, Iran, in 2005. She worked at AICTC Center of Sharif University of Science and Technology, Tehran, Iran, from 2005 to 2007. Her research interests include Reverse Engineering and Secure Operating System. S. Berenji is a member of Computer Society of Iran (CSI).

Reyhaneh Eslami received the B.Sc. degree in Software Engineering from Ferdowsi University, Mashad, Iran, in 2007. Her research interests include Secure Operating System.

Mohammad Akbari received the B.Sc. degree in Computer Engineering from Teacher Training University, Tehran, Iran, in 2004, and the M.Sc. degree in Computer Science and intelligent system from Amirkabir University, Tehran, Iran, in 2006. He is a lecturer in the department of engineering, Islamic Azad

University, Shahr-e-ghods branch from September 2007. He is now the head of the Computer Engineering department of Islamic Azad University, Shahr-e-ghods branch. His research interests include document image processing, pattern recognition and Secure Operating System.

Mr. Akbari is a member of International Association of Computer Science and Information Technology (IACSIT).

The application of RBF Neural Network for Trust and Reputation Management in P2P Overlay Network

Reza Azmi, Mahdiah Hakimi

College of Engineering, Alzahra University, Tehran, Iran

Email: azmi@alzahra.ac.ir, mahdiah_hakimi@yahoo.com

Abstract—Peer-to-Peer overlay networks employ scalable mechanisms that allow anyone to offer content and services to other system users. However, the open accessibility of these systems makes them vulnerable to malicious users wishing to poison the system. Because of this danger, users must be wary of the quality or validity of the resources they access. To mitigate the adverse behavior of unreliable or malicious peers in a network, researchers have suggested using reputation systems. In this paper we proposed a novel trust and

reputation system, using RBF artificial neural network to determine trust level. Inputs of this neural network are recommendations from other peers about a file provider. After each interaction, the neural network could be trained by requester's experiment and tuned network's weights. Output of the neural network addresses the trust level of the file provider.

Index Terms— Peer-to-Peer Overlay Networks , RBFⁱ Artificial Neural Network , Reputation , Trust.

I. INTRODUCTION

What distinguishes P2P systems from other distributed systems is their focus on full user autonomy. Typically, distributed systems consist of computers managed by a single organization or hierarchy. Devising an efficient architecture that spans many networked machines is much simpler when all machines can be monitored and controlled by a single operator. However, in pure P2P architectures there are no centralized services or control mechanisms dictating the actions of other nodes. Each user decides what computing resources he will contribute, as well as when and for how long. The architecture is designed to handle large numbers of nodes joining and abruptly leaving the network. In addition, these systems emphasize equality and balancing the load across nodes. This flexibility, self-determination and low participation cost encourages a much larger number of participants, which, in turn, greatly increases the number and value of the services provided by the system to all [11]. The most important contribution of peer-to-peer system research is providing an architecture that allows a group of users spread throughout the Internet to cheaply and efficiently connect their commodity computing resources into one massive system, useable by all. In previous researches p2p systems have been experienced in network computation, storage and digital memories. But recently these systems are usually applied to file sharing and social networks. The open environments are dynamic and agents are heterogeneous and anonymous also there is no central authentication system, so accessing to data,

information and shared services are related to trust and reputation of peers. Now trust and reputation systems or recommended trust models are applied broadly as one kind of decision support systems that help peers to download from reliable peers. They differ in selections of recommenders and in aggregations of recommendations. To design a trust and reputation system we have to take two problems into consideration: how to design a trust computation model that provides more accurate trust value for decision procedure; and how to design an efficient and scalable information collection strategy.

II. RELATED WORK

Various techniques have been proposed to secure P2P networks over the last decade. Abdul-Rahman and Hailes [1] captured the most important characteristics of trust and reputation and proposed the general structure for developing trust and reputation in a distributed system. Most of the later works in this area followed their ideas, but in different application domain, such as [2, 3, 4, 5]. Sabater and Sierra [6] extended the notion of trust and reputation into social and ontological dimensions. Social dimension means that the reputation of the group that an individual belongs to also influences the reputation of the individual. Ontological dimension means that the reputation of a peer is compositional. The overall reputation is obtained as a result of the combination of the peer's reputation in each aspect. Cornelli and Damiani [4] also worked in the area of file sharing in peer-to-peer networks. However, it concentrated on how to prevent attacks on the reputation system and

did not discuss how peers could model and compute trust and reputation. EigenTrust model of Kamvar et al. [7] is built on the notion of transitive trust. A major issue of applying this model is to find pre-trusted peers that guarantee convergence of the algorithm and avoid malicious collectives. Wang and Vassileva [10] applied Naive Bayesian network to recommendation trust. The model can be used to solve the problem of

III. TRUST AND REPUTATION

In this paper, we adopt the following working definitions:

Trust – a peer's belief in another peer's capabilities, honesty and reliability based on its own direct experiences;

Reputation – a peer's belief in another peer's capabilities, honesty and reliability based on recommendations received from other peers.

Reputation can be centralized, computed by a trusted third party, like a Better Business Bureau; or it can be decentralized, computed independently by each peer after asking other peers for recommendations. Although trust and reputation are different in how they are developed, they are closely related. They are both used to evaluate a peer's trustworthiness, so they also share some common characteristics.

- Context specific

Trust and reputation both depend on some context. For example, Mike trusts John as his doctor, but he does not trust John as a mechanic who can fix his car. So in the context of seeing a doctor, John is trustworthy. But in the context of fixing a car, John is untrustworthy.

- Multi-faceted

Even in the same context, there is a need to develop differentiated trust in different aspects of the capability of a given peer. The same applies for reputation. For instance, a customer might evaluate a restaurant from several aspects, for example, the quality of food, the price, and the service. For each aspect, she develops a kind of trust. The overall trust depends on the combination of the trusts in each aspect. While the context-specificity of trust accentuates that trust in an identical peer can be different in different situations, the characteristic, multi-faceted, emphasizes that trust has multiple aspects, which can play a role in deciding whether a peer is trustworthy to interact with.

- Dynamic

Trust and reputation increase or decrease with further experience (direct interaction). They also decay with time.

different estimation process of the same online service. Song and Phoha [8] and Zong, Feng and Jun [9] proposed the trust and reputation system based on artificial neural network. [8,9] are built on back-propagation algorithm to train the MLPs neural network. In proposed paper we used RBF neural network since these networks tend to learn much faster and require fewer training samples than MLPs.

IV. DETERMINATION OF TRUST AND REPUTATION LEVEL BY NEURAL NETWORK

In this paper we focus on pure P2P networks for file exchange and, more precisely, on the Gnutellaⁱⁱ architecture. The reason for focusing on a pure P2P network is that it is closest to the ideal structure of the peer-to-peer networks, where all participants have a uniform role. Therefore, first we define the working of the Gnutella protocol and then sketch the basic idea of our approach about using RBF neural networks in p2p overlay networks.

A. Overview of Gnutella protocol

Gnutella offers a fully peer-to-peer decentralized infrastructure for information sharing. Each peer is associated with a self-appointed ID, which can be communicated to others when interacting, as established by the P2P communication protocol used. The id of each peer in Gnutella can change at any instantiation or remain persistent.

The topology of a Gnutella network graph is meshed, and all peers act both as clients and servers and as routers propagating incoming messages to neighbors. While the total number of nodes of a network is virtually unlimited, each node is linked dynamically to a small number of neighbors, usually between 2 and 12. To reduce network congestion, all the packets exchanged on the network are characterized by a given Time-To-Live (TTL). On passing through a node, the TTL of a forwarded message is decreased by one; when the TTL reaches zero, the message is dropped. The limit of the TTL creates a horizon of visibility for each node on the network. The horizon is defined as the set of nodes residing on the network graph at a path length equal to the TTL and reduces the scope of searches, which are therefore forced to work on only a portion of the resources globally offered. Peers in Gnutella can gain a complete vision of the network within the horizon by broadcasting Ping messages. Peers within the horizon reply with a Pong message containing the number and size of the files they share.

B. Basic idea of proposed system

In a peer-to-peer overlay network like Gnutella, exchanging a file is containing two

phases:1)Searching a file 2)Downloading it(see Figure 1 and 2). But some other researches like [4,10,12] complete this protocol by adding two other phases into it: pooling and evaluating the votes. In this way before a requester decides about downloading the file from a provider, first it asks other peers about reputation of the provider.

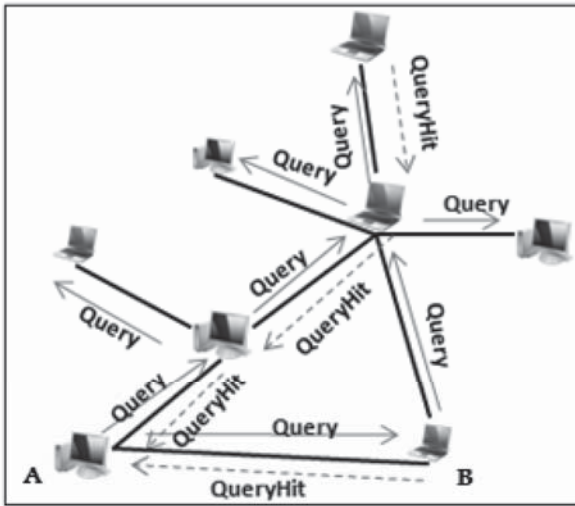


Fig 1. Research process by peer A in Gnutella

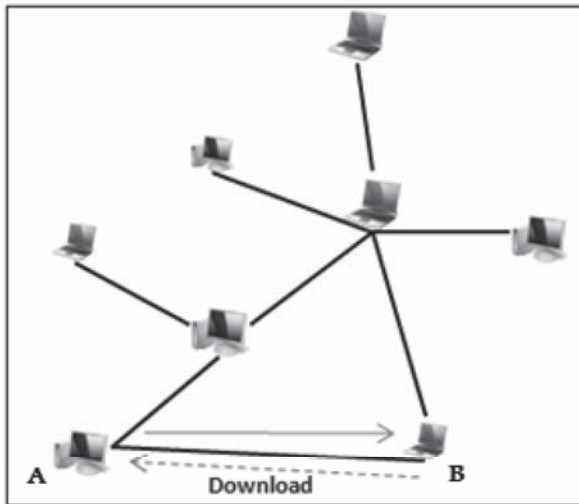


Fig 2. Download from peer B in Gnutella

In this paper we decide to study about influence of layering concept on evaluating trust for the first time and for this reason we use artificial neural network to achieve higher reliable trust and reputation about provider. In the other word, as it's showed by literature review about trust and reputation systems, all the collected votes about reputation of a file provider from other peers, are in the same level. Whereas being more hops between responses to the requester causes more malicious responses and spoofing. In this paper we assume that there is one

hope between peers who are in the first layer and the requester, and there are two hopes for peers in the second layer and so on. As it mentioned before about concept of TTL, we can conclude that TTL is equals to the maximum number of layers.

TABLE I
DIFFERENT LEVEL OF TRUST

Meaning	Trust level
Very Trustworthy	vt
Trustworthy	t
Untrustworthy	u
Very Untrustworthy	vu

Since peers are heterogeneous, they may have different preferences and judge issues by different criteria. For example, some peers may consider a movie provider good because it provides movies with high quality, while others may consider the movie provider bad because the speed of download from it is very slow. If two peers A and B are similar in their evaluation criteria, peer A can trust peer B's recommendations, if it knows that peer B is truthful. On the other hand in this paper same as [1] we consider different level of trust like Very Trustworthy, Trustworthy, Untrustworthy, Very Untrustworthy (see Table 1). We use these levels of trust to determine the output of neural network.

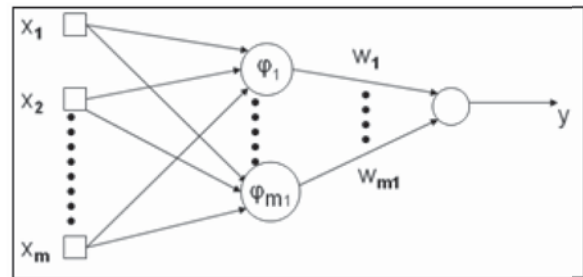


Fig 3. RBF artificial neural network

It is a difficult problem to predict the character of a client. Furthermore, because the open environments are dynamic, it is much more complicated to predict the distribution of clients with different characters on specific time. Therefore we use RBF neural network to evaluate other peer's recommendation as it's showed in Figure 3. Artificial neural networks are robust to noise data and support incremental training. So our proposed trust model tries to overcome some disadvantages of previous trust systems by training the RBF neural network and tuning its weights by similarity matching to find the index of best center.

Before describing more details about application of neural network in our model, we need to explain about Gnutella phases as they presented in [12].

C. Phase 1: Resource searching

At first peer **A** who is a peer that looking for a resource, broadcasts a Query indicating the resource it is looking for. Every other peers which receiving the query and willing to offer the requested resource for download, sends back a QueryHit message stating how it satisfies the query and providing its id and its pair(IP, port), which peer **A** can use for downloading.

D. Phase 2: Polling

Upon reception of the QueryHit messages, peer **A** selects a top list of favorite peers **T** and polls its peers about the reputations of them. In the poll request, peer **A** includes the set **T** of peers IDs about which it is enquiring and a public key PKpoll generated on the fly for the poll request, with which responses to the poll will need to be encrypted. The poll request is sent through the P2P network and therefore peer **A** does not need to disclose its ID or its IP to be able to receive back the response. Peers receiving the poll request and wishing to express an opinion on any of the peers in the list, send back a PollReply expressing their votes and declaring their (IP, port) pair. Peer **A** hash of the votes and pair (IP, port) is also added in order to allow peer **A** to check the integrity of the message. The PollReply is then encrypted with PKpoll to ensure its confidentiality (of both the vote and the voters) when in transit.

E. Phase 3: Vote evaluation

As a result of the previous phase, peer **A** receives a set of votes, where, for each peer in **T**, some votes can express a good opinion while some others can express a bad opinion. To base its decision on the votes received, peer **A** needs to trust the reliability of the votes. Thus, peer **A** first uses the hash to detect tampered-with votes and discard them. Second, peer **A** detects votes that appear suspicious, for example since they are coming from IPs suspected of representing a clique. Third, peer **A** selects a set of voters that it directly contacts (by using the (IP, port) pair they provided) to check whether they actually expressed that vote. For each selected voter, peer **A** directly sends a TrueVote request reporting the votes it has received, and expects back a confirmation message TrueVoteReply. This forces potential malicious peers to pay the cost of using real IPs as false witnesses.

F. Application of RBF neural network in proposed trust model

After evaluating received recommendations or votes, finally peer **A** has to select the provider who seems to be the best on the list, in different aspects like download speed, file type and file quality. In this point we use RBF artificial neural network to solve the problem (see Figure 4). RBF networks provide a powerful alternative to MLPsⁱⁱⁱ for function approximation or classification. They train faster and require fewer training samples than MLPs. There are several techniques for training these networks. RBF networks are nonlinear hybrid networks typically containing a single hidden layer of processing elements. This layer uses Gaussian transfer functions, rather than the standard sigmoid functions employed by MLPs. In other word the RBF is a single-hidden-layer feed forward network with linear output transfer functions and nonlinear transfer functions, on the hidden layer nodes. The primary adjustable parameters (see Figure 4) are the final layer weights, $\{\lambda_{jk}\}$, connecting the j th hidden node to the k th output node. There are also weights $\{\mu_{ij}\}$ connecting the i th input node with the j th hidden node [13].

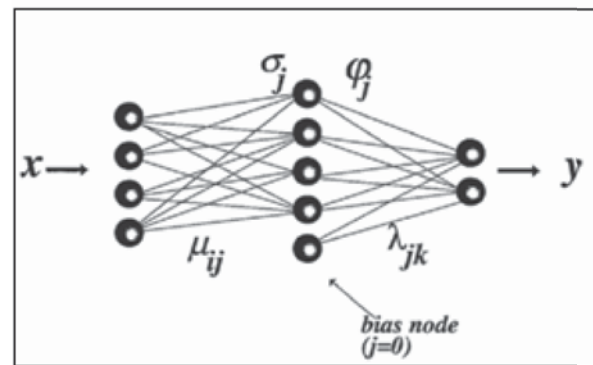


Fig 4. The basic radial basis function structure[13]

The mathematical embodiment of the RBF takes the following form. The k th component of the output vector y_p corresponding to the p th input pattern x_p is expressed as:

$$[y(x_p)]_k = \sum_{j=0}^n \lambda_{jk} \phi_j \left(\|x_p - \mu_j\|; \sum_j \right) \quad (1)$$

Where $\Phi_j(\dots)$ denotes the nonlinear transfer function of hidden node j . In the RBF neural network there are three basic parameters like 1- centers, 2- spreads, 3- weights. We use K-means clustering algorithm for determining centers:

1. Initialization: random $\mu_j(t=0)$

2. Sampling: draw $x_p(t)$ from input space
3. Similarity matching: find index of best center

$$k = \arg \min_j \square xp(t) - \mu_j(t) \square \quad (2)$$

4. Updating: adjust centers

$$\mu_k(t+1) = \mu_k(t) + \eta * [xp(t) - \mu_k(t)] \quad (3)$$

5. Continuation: increment t by 1, go to 2 and continue until no noticeable changes of centers occurred.

Next we use normalizing method to find spreads:

$$\sigma = \frac{\text{Maximum distance between any 2 centers}}{\sqrt{\text{number of centers}}} = \frac{d_{\max}}{\sqrt{m_1}} \quad (4)$$

$$\varphi_i(\|x - t_i\|^2) = \exp\left(-\frac{m_1}{d_{\max}^2} \|x - t_i\|^2\right)$$

$$i \in [1, m_1] \quad (5)$$

At last using LMS method for tuning weights:

$$\lambda_{jk} = \lambda_{jk} + \eta * [y(k) - y'(k)] \quad (6)$$

$$0 < \eta < 1,$$

y' is predicted output of network and y is actual output of network.

$$y'(k) = \begin{cases} 1 & \text{if confidence condition is true} \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

$$y(k) = \text{output of function } \varphi \text{ from } [0, 1] \quad (8)$$

Generally inputs of this RBF neural network are other peer's recommendations about a file provider based on their assigned layer. As mentioned before these recommendations are in vt, t, u, vu format. Thus total number of input neurons of this neural network will be equals to product of network TTL in these 4 trust levels. In order to normalization of inputs of trust levels, we divide number of received recommendations from each trust level into the all number of them. In RBF network hidden layer's neurons do the similarity matching and find index of best center. As previous terms express weights of

hidden layer's neurons calculate by K-means clustering algorithm. Finally neuron's weights of output layer are difference between predicted output of network and actual output by assessment of different aspect of providers like response time, download speed, file quality and file type. A requester keeps the last trained neural network in its memory. After each interaction, the neural network could be trained by requester's experiment and tuned network's weights. If the neural network was built beyond a certain period of time or some recommenders have changed their trust models, or the requester changes his trust estimation accuracy requirement, the requester collects up-to-date trust data and retrains the neural network. After a while the network is well trained and it would help peers to find reliable file providers.

G. Phase 4: Resource downloading

At this point, before actually initiating the download, peer **A** challenges the selected peer **B** to assess whether it corresponds to the declared peer-id. Peer **B** will need to respond with a message containing its public key PK_B and the challenge signed with its private key SK_B . If the challenge-response exchange succeeds and the PK_B 's digest corresponds to the peer-id that peer **B** has declared, then peer **A** will know that it is actually talking to **B**. Note that the challenge-response exchange is done, like the download, via direct communication on a secure connection, to prevent impersonation by which peers can offer resources using the peer-id of other peers. With the authenticity of the counterpart established, peer **A** can finally download the resource and, depending on its satisfaction for the download, update its reputation information for peer **B**.

V. CONCLUSIONS

In this paper we decide to use the neural-network based recommendation trust model since experiments in this area have discovered these facts that hidden variables capture by hidden layers of the model, and these networks are robust to noise in the training data, also they have fast speed with high accuracy. In addition adaptability and non-linear aggregation of heterogeneous agent's recommendations are other properties of neural-network based trust systems. Inputs of proposed neural network are recommendations from other peers about a file provider. After each interaction, the neural network could be trained by requester's experiment and tuned network's weights. Output of the neural network finds the trust level of the file provider.

For future research we will reduce number of input neurons of the network by using fuzzy modeling.

REFERENCES

- [1] A. Abdul-Rahman, S. Hailes, "Supporting trust in virtual communities", In Proceedings of the Hawai'i International Conference on System Sciences, Maui, Hawaii, Jan 4-7 2000.
- [2] F. Azzedin, M. Maheswaran, "Evolving and Managing Trust in Grid Computing Systems". IEEE Canadian Conference on Electrical & Computer Engineering (CCECE '02), May 2002.
- [3] J. Carter, E. Bitting, A.Ghorbani, "Reputation Formalization for an Information-Sharing Multi-Peer System", 515-534. Computational Intelligence, Volume 18, Number 4, November 2002.
- [4] F. Cornelli, E. Damiani, "Implementing a Reputation-Aware Gnutella Servent". In Proceedings of the International Workshop on Peer-to-Peer Computing, Pisa, Italy, May 24, 2002.
- [5] M. Montaner, B. L'opez, "Opinion based filtering through trust". In Proceedings of the 6th International Workshop on Cooperative Information Peers (CIA'02), Madrid (Spain), September 18-20 2002.
- [6] J. Sabater, C. Sierra, "Regret: a reputation model for gregarious societies". In 4th Workshop on Deception, Fraud and Trust in Peer Societies, 2001.
- [7] S. Kamvar, M. T. Schlosser, and H. Garcia-Molina. "The EigenTrust Algorithm for Reputation Management in P2P Networks". In Proceedings of the 12th International World Wide Web Conference (WWW'03), May, 2003.
- [8] W. Song, V. Phoha, X. Xu, "An Adaptive Recommendation Trust Model in Multiagent System", IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'04).
- [9] B. Zong, F. Xu, J. Jiao, J. Lv, "A Broker-Assisting Trust and Reputation System Based on Artificial Neural Network", In IEEE 978-1-4244-2794-9/09/ 2009.
- [10] Y. Wang, J. Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks", Proceedings of IEEE Conference on P2P Computing, Linköping, Sweden, 2003.
- [11] S. Marti, "Trust and Reputation in Peer-to-Peer Networks", A dissertation of Stanford university, Doctor of Philosophy, May 2005.
- [12] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, "Managing and sharing servants' reputations in p2p systems", IEEE Transactions on Knowledge and Data Engineering, 15(4), 840-854, 2003.
- [13] D. Lowe, "Radial basis function networks and statistics, in Statistics and Neural Networks: Advances at the Interface", New York: Oxford University Press, pp. 65-95, 1999.

ⁱ Radial-Basis Function

ⁱⁱ www.Gnutella.com

ⁱⁱⁱ Multi-Layer Perception

On the Analysis of Dynamic Software Watermarking

S. Jamal H. Zaidi and Hongxia Wang

Abstract—Since birth, the necessity of software becomes more essential not only to deal with scientific tasks but to solve our daily life activities. It takes more value time by time and become not a physical property but an intellectual property. As a member of digital family, software has to face the same threats like, illegal copying, distribution, modification, stealth, misuse and *etc.* Many mechanisms were introduced like, copyright, registration, licensing, intellectual property, information auditing, security dongle and *etc.* to resist from the attacks. To protect software from piracy, watermarking is the one in which the owner embeds some secret information in the code as a mark of identification to ensure and authenticate their ownership rights. During last decade, different algorithms were developed to implement this scenario and to stop different attacks. This paper is an attempt to gives an analysis on a particular branch of watermarking algorithm hierarchy i.e., *dynamic watermarking*. This work focuses on the organization of dynamic watermark, embedding styles and watermarking algorithms.

Keywords—Dynamic software watermarking, watermarking algorithms, software piracy, software security.

I. INTRODUCTION

SOFTWARE watermarking is currently the most demanding technique to prevent the software from piracy. We usually observe watermarks on different daily life products, like; to prevent the use of fake currency, to safe the illegal use of products by pasting a fragile rainbow colored sticker having some logo or information from the brand maker, to avoid the piracy of digital objects by embedding secret information and *etc.* All of these procedures were applied to stop or prevent from the illegal use and to maintain the authority of copyright.

From the last few decades, the threat of piracy and illegal use become a key concern for software industry and many algorithms and approaches were designed to overcome this problem. Moreover, a survey conducted by [1] shows that more than 41% software are being used worldwide without having ownership rights or simply pirated. Software watermarking algorithms [2] and [3] are classified in different classes depending upon their functional goals,

execution, extraction techniques, visibility, statistical behaviors, robustness and sensitivity. Statistical properties or reordering the structure of program statements may be treated as a seed to implement watermarks [4,5].

This paper highlights one of the flavors of algorithms based on implementation. These watermarking algorithms are further classified into (1) static and (2) dynamic techniques. This paper comprises on three main sections. Followed by the introduction (*section 1*), *section 2* describes about the art of dynamic watermarking and its algorithms. Finally, the paper concludes in the last section and presents some future directions..

II. DYNAMIC WATERMARKING

A. Mechanism

As discussed above, the fundamental task of any watermarking algorithm is to embed or implant any known or secret information within the code or data structure of any software application. In particular, dynamic watermarking permits to embed the embedding information during the execution state. Moreover, for recognition [6,7] of watermark the application should be executed by the recognition tool (Fig.1). To keep this feature, we may write the embedding function, $\mathbb{E}(\cdot)$, as follows:

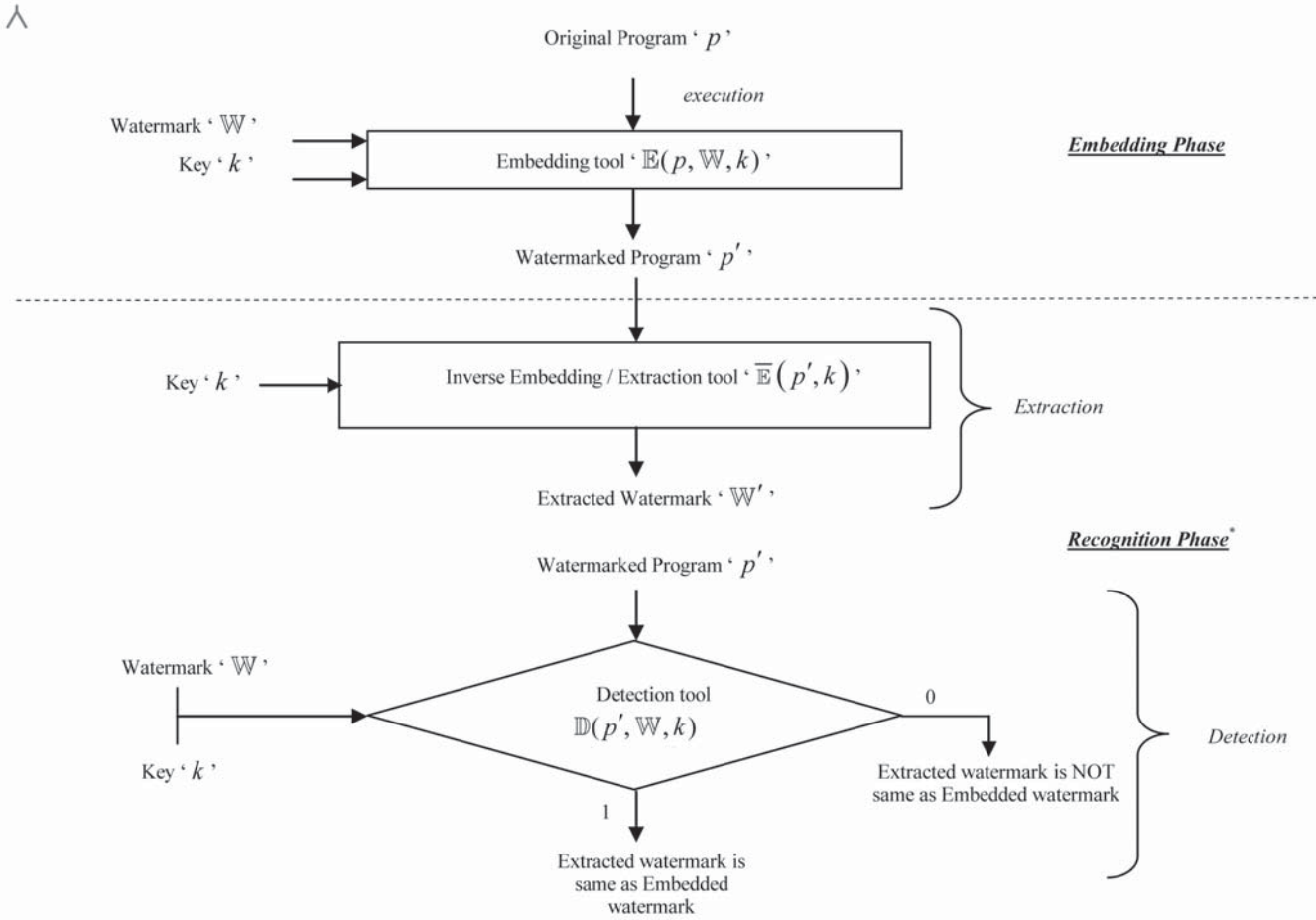
$$p' = \mathbb{E}(p, \mathbb{W}, k). \quad (1)$$

where p' denotes the watermarked program, p represents original program, $\mathbb{W}$ is the watermark, and k is the (secret) key / (valid) input sequence, also regarded as part of embedding process.

The second phase of watermarking mechanism is the process of recognition, which can be treated as two fold activity; the first one is the inverse operation of the embedding function to obtain the embedded watermark, $\mathbb{W}'$, named as '*extraction function*', $\bar{\mathbb{E}}(\cdot)$ (Eq. 2), and the other is to detect the presence of the embedded watermark [8], called '*detection function*', $\mathbb{D}(\cdot)$ (Eq. 3).

S. Jamal H. Zaidi is with the School of Information Science & Technology, Southwest Jiaotong University, Chengdu, Sichuan 610031, P.R. China (e-mail: sjamalzaidi@{mars.swjtu.edu.cn, gmail.com}).

Hongxia Wang, Ph.D., is attached with Southwest Jiaotong University, Chengdu, Sichuan 610031, P.R. China, as Professor and Director of Key Laboratory for Information Security (e-mail: hxwang@home.swjtu.edu.cn).



* p' should be executed by the extraction or detection tools to recognize W

FIGURE 1. FLOWCHART OF A COMPLETE DYNAMIC WATERMARKING MECHANISM

$$W' = \overline{E}(p', k). \quad (2)$$

$$D(p', W, k) = 1 \text{ or } 0. \quad (3)$$

where '1' represents the correct match and '0' denotes incorrect match of the detected watermark. We may also include p during the detection function.

B. Algorithms

Watermarking techniques always shows a tradeoff between stealth, effective cost, resilience, performance and data rate [2,9]. If there is no change in the statistical properties of p after embedding W , such property is named as Stealth. The stealth is said to be static if the static analysis shows no change in p and p' , whereas, the dynamic stealth is the one which shows no variation during execution. If W is placed at a reliable location and can be extracted safely, such embedding is known as Resilient. For high data rate, W should be large enough to resist the decoding attacks.

According to [10], dynamic watermarking algorithms are classified into three flavors (1) Easter Egg (EEW), (2) Data Structure (DSW), and (3) Execution Trace Watermarks (ETW). If W information appears which is immediately noticeable by the user after giving an unusual input(s), the W is said to be EEW. If W is embedded into stack, heap, global or any other kind of data structure and it is extracted by observing the current values hold by p then W is known as DSW. ETW is embedded within the address or instruction trace or both of p while giving a particular sequence of input and can be extracted by performing some statistical analysis.

In 1996, Davidson *et al.* [11] published the first patent for software watermarking of static behavior in which the watermark was embedded by reordering the basic block of the program. Collberg *et al.* [1] implemented the first dynamic graph watermark (CT) in 1999. CT algorithm involves three main steps: (1) selection of suitable graph, (2) partitioning of graph into sub-graphs, and (3) construction of a set of graph generating code for each sub-graph and chose an execution path with the help of a secret key to embed those codes. For embedding [10] used two techniques: (a) Radix-k Encoding

using circular linked list, and (b) Graph Enumeration Encoding. Venkatesan *et al.* [12] introduced the first graph based watermark with a static behavior which was practically implemented by [13] with some necessary changes to the original algorithm.

Qu *et al.* [14] proposed watermarking algorithm as a graph coloring problem and it was first implemented by Myles *et al.* [15] using register allocation technique. Both [14,15] fits into a static watermarking category but these algorithm were further modified into dynamic watermarking. After an implementation of [14] by Zhu *et al.* [16,17,6], it was observed that if two different messages were inserted into the actual graph the resultant watermark will be identical. Lee *et al.* [18,19] gave an idea of color permutation and color change to overcome the weaknesses of [14,15] whether large number of variables or interface graphs are present.

Collberg *et al.* [20] highlights the weakness of [11] and [15], as both the approaches can be damaged by straightforward binary optimizers, whereas, the technique used in [10] will remain stable by obfuscating the code (modification of pointer topology of data structure). Moreover, [20] proposed a new technique of dynamic path-based watermarking having capability of embedding large watermarks and shows resistance against variety of attacks. Thomborson *et al.* [21] introduced a tamper proofing technique for dynamic data structures watermarks using constant encoding. Dynamic graph based fingerprinting was proposed by Collberg *et al.* [22] by using pointer alias which is difficult to analyze and hard to attack.

Luo *et al.* [23] extend the CT algorithm by implementing Asmuth-Bloom threshold scheme (technically based on Chinese Remainder Theorem) with a share connected to the secret key. This algorithm results as an improved version of CT algorithm but due to the sharing mechanism the watermark information will expand gradually and reduce the available space to accommodate. Another extension to the CT was proposed by Zhu *et al.* [24] by introducing 2D and multidimensional intensified planted plane cubic tree to obtain higher data rate along with better temper proofing.

Thread contention technique was first used by Nagra *et al.* [25] to embed robust watermark dynamically. The algorithm depends on the new thread initiated in a single threaded portion of a program and can embed single or multiple bit watermark. Similarly, as [25], Larkin *et al.* [26] also took Java program as a working platform to establish a dither modulation watermark in the dynamic memory traces. Furthermore, [26] generalize the spread-transform algorithm for software watermarking using N-element vector to the total corresponding dynamic memory allocation during N-length time intervals of the program execution.

Myles *et al.* [27,28] introduced a branch-based dynamic watermarking approach which includes features of both obfuscation and tamper proofing. This algorithm takes two secret keys to embed ownership identification mark and consumer fingerprint mark simultaneously.

Integration of chaotic system with an EEW style dynamic watermarking was introduced by Liu *et al.* [29]. By involving chaotic system, the watermark dispersed all over the code and acts as a protection shield for the whole program. Also, the anti-reverse engineering technique was used to resist from various reverse engineering attacks. Ke-Xin *et al.* [30] and Jian-Qi *et al.* [31] introduced the same mechanism to split the watermark into pieces using Shamir's threshold scheme in order to increase resilience. Furthermore, [30] applied single dimensional logistic chaotic encryption to the watermark pieces, whereas, [31] used block cipher and self-isomorphic mapping operations to associate the unrelated pieces of watermark.

Mixed Boolean arithmetic transformation was applied by Zhou *et al.* [32] to hide the secret key and make the watermarking algorithm hard to identify. The constants were created at runtime and will not be visible in the executable file.

Zhang *et al.* [33] proposed a hash based dynamic algorithm to watermark and attempts to distinguish the proposed method from the traditional watermarking techniques. This watermark is not hidden in the code or in the runtime. Whereas, the watermark can be extracted dynamically and resist various forms of transformation attacks. According to Preda *et al.* [34], loops can be the fundamental block for establishing dynamic watermark. Iteration of loops can be taken as traces of execution and can be fold into a single loop body after abstraction of code. Therefore, a single iteration can initiate the computation of watermark correctly [34].

Dynamic program slicing was implemented by Deng *et al.* [35] to watermark distributed and mobile software. Modules of the systems were categorized as visible and hidden using slicing technique. Embedding of watermark was done by modifying the data dependency between the communicating modules and by logging the dependent relation the watermark information can be recognized.

III. CONCLUSION AND FUTURE DIRECTIONS

This paper shows the contrast of different watermarking styles, as well as gives a reasonable bridge between the theoretical ideas to the practical implementation of watermarking algorithms. Also, this work gives detail advancements in dynamic watermarking algorithms.

It is observed that a reasonable work has been discussed about dynamic graph based algorithms but still requires more attention. Similarly, some more work is required to mature the concepts of dynamic watermarking using hash functions, chaotic systems, threading and program slicing. According to [36], we may implement rough set techniques not only to create watermark but to embed it.

ACKNOWLEDGMENT

We thank M. Khalid Anis (Bahria University, Pakistan) and M. Khurram Khan (King Saud University, Saudi Arabia) for their invaluable help and motivation.

REFERENCES

- [1] Business Software Alliance, Sixth Annual BSA and IDC Global Software Piracy Study, (May 2009).
(<http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf>)
- [2] C. Collberg and C. Thomborson, Watermarking, Tamper-Proofing, and Obfuscation-Tools for Software Protection, *IEEE Trans. Soft. Eng.* 28 (8), pp. 735-747 (2002).
- [3] W. Zhu, C. Thomborson, and F. Y. Wang, A Survey of Software Watermarking, *ISI 2005, LNCS 3495*, Springer Verlag, pp. 454-458 (2005).
- [4] V. Yarmolik and S. Partianka, Software IP Protection Based on Watermarking Techniques, *Info. Proce. Secur. Syst.*, 2005, pp. 227-234 (2005).
- [5] M. Shirali-Shahreza and S. Shirali-Shahreza, Software Watermarking by Equation Reordering, *IEEE Conf.*, 2008, 4 Pages (2008).
- [6] W. Zhu and C. Thomborson, Recognition in Software Watermarking, *MCPS 2006, Santa Barbara, ACM Conf.*, pp. 29-36 (2006)
- [7] W. Zhu, Informed Recognition in Software Watermarking, *PAISI 2007, LNCS 4430*, Springer Verlag, pp. 257-261 (2007).
- [8] W. Zhu and C. Thomborson, Extraction in Software Watermarking, in *Proc. MM-Sec'06, Geneva, Switzerland*, pp. 175-181 (September 2006).
- [9] C. Collberg, S. Kobourov, E. Carter, and C. Thomborson, Error-Correcting Graphs for Software Watermarking, *WG 2003, LNCS 2880*, Springer Verlag, pp. 156-167 (2003).
- [10] C. Collberg and C. Thomborson, Software Watermarking Models and Dynamic Embeddings, *POPL 1999, San Antonio, ACM Conf.*, pp. 311-324 (1999).
- [11] R. Davidson and N. Myhrvold, Method and system for generating and auditing a signature for a computer program, *US Patent 5,559,884*, (1996).
- [12] R. Venkatesan, V. Vazirani and S. Sinha, A Graph Theoretic Approach to Software Watermarking, *IH 2001, LNCS 2137*, Springer Verlag, pp. 157-168 (2001).
- [13] C. Collberg, A. Huntwork, E. Carter, and G. Townsend, Graph Theoretic Software Watermarks Implementation, Analysis, and Attacks, *IH 2004, LNCS 3200*, Springer Verlag, pp. 192-207 (2004).
- [14] G. Qu and M. Potkonjak, Analysis of Watermarking Techniques for Graph Coloring Problem, *ICCAD 1998*, pp. 190-193 (1998).
- [15] G. Myles and C. Collberg, Software Watermarking Through Register Allocation Implementation, Analysis, and Attacks, *ICISC 2003, LNCS 2971*, Springer Verlag, pp. 274-293 (2004).
- [16] W. Zhu and C. Thomborson, On the QP Algorithm in Software Watermarking, *ISI 2005, LNCS 3495*, Springer Verlag, pp. 646-647 (2005).
- [17] W. Zhu and C. Thomborson, Algorithms to Watermark Software through Register Allocation, *DRMTICS 2006, LNCS 3919*, Springer Verlag, pp. 180-191 (2006).
- [18] H. Lee and K. Kaneko, New Approaches for Software Watermarking by Register Allocation, *SNPD 2008, IEEE Comp. Socie. Conf.*, pp. 63-68 (2008).
- [19] H. Lee and K. Kaneko, Two New Algorithms for Software Watermarking by Register Allocation and their Empirical Evaluation, in *Proc. ITNG 2009*, pp. 217-222 (2009).
- [20] C. Collberg, E. Carter, S. Debray, A. Huntwork, J. Kececioğlu, C. Linn and M. Stepp, Dynamic Path-Based Software Watermarking, *PLDI 2004, ACM Conf., Washington DC*, pp. 107-118 (2004).
- [21] C. Thomborson, J. Nagra, R. Somaraju and C. He, Tamper-proofing Software Watermarks, *AISW 2004, Australian Computer Society 23*, pp. 27-36 (2004).
- [22] C. Collberg, C. Thomborson and G.M. Townsend, Dynamic Graph-Based Software Fingerprinting, *ACM Trans. Program. Lang. and Syst.*, 29, 6, Article 35, 67 pages (2007).
- [23] Y.X. Luo, J.H. Cheng and D.Y. Fang, Dynamic Graph Watermark Algorithm Based on the Threshold Scheme, in *Proc. ISISE 2008*, pp. 689-693 (2008).
- [24] J. Zhu, Y. Liu and K. Yin, A Novel Dynamic Graph Software Watermark Scheme, in *Proc. ETCS 2009*, pp. 775-780 (2009).
- [25] J. Nagra and C. Thomborson, Threading Software Watermarks, *IH 2004, LNCS 3200*, Springer Verlag, pp. 208-223 (2004).
- [26] A.J. Larkin, F. Balado, N.J. Hurley, and G.C.M. Silvestre, Dither Modulation Watermarking of Dynamic Memory Traces, *IH 2005, LNCS 3727*, Springer Verlag, pp. 372-386 (2005).
- [27] G. Myles and H. Jin, Self-validating Branch-Based Software Watermarking, *IH 2005, LNCS 3727*, Springer Verlag, pp. 342-356 (2005).
- [28] G. Myles, Software Theft Detection Through Program Identification, *Ph.D. Thesis, University of Arizona* (2006)
- [29] F. Liu, B. Lu and X. Luo, A Chaos-Based Robust Software Watermarking, *ISPEC 2006, LNCS 3903*, Springer Verlag, pp. 355-366 (2006).
- [30] Y. Ke-xin, Y. Ke and Z. Jian-qi, A Robust Dynamic Software Watermarking, in *Proc. ITCS 2009*, pp. 15-18 (2009).
- [31] Z. Jian-qi, L. Yan-heng and Y. Ke, A Robust Dynamic Watermarking Scheme based on STBDW, *CSIE 2009, IEEE Conf.*, pp. 602-606 (2009).
- [32] Y. Zhou, A. Main, Y.X. Gu, and H. Johnson, Information Hiding in Software with Mixed Boolean-Arithmetic Transforms, *WISA 2007, LNCS 4867*, Springer Verlag, pp. 61-75 (2007).
- [33] X. Zhang, F. He and W. Zuo, Hash Function Based Software Watermarking, *ASEA 2008, IEEE Comp. Socie. Conf.*, pp.95-98 (2008).
- [34] M.D. Preda, R. Giacobazzi, and E. Visentini, Hiding Software Watermarks in Loop Structures, *SAS 2008, LNCS 5079*, Springer Verlag, pp. 174-188 (2008).
- [35] X. Deng, G. Xu, G. Sun, and J. Man, Software Watermarking Based on Dynamic Program Slicing, in *Proc. IIH-MSP 2008*, pp. 461-464 (2008).
- [36] W. Zhu, Concepts and Techniques in Software Watermarking and Obfuscation, *Ph.D. Thesis, University of Auckland* (August 2007)

Analysis and Implementation of Distinct Steganographic Methods

Ünal TATAR and Tolga MATARACIOĞLU
TÜBİTAK UEKAE, Department of Information Systems Security
06700, Kavaklıdere, Ankara/TURKEY
[tatar,mataracioglu}@uekae.tubitak.gov.tr](mailto:{tatar,mataracioglu}@uekae.tubitak.gov.tr)

Abstract - In this paper, different steganographic methods have been analyzed and implementations of those techniques have been performed. Those methods include hiding in text, hiding in audio file, hiding in file system, and hiding in image files.

Index Terms - Steganography, steganographic methods, implementation, analysis.

I. INTRODUCTION

Steganography is the art of hiding data in data in an undetectable way. The word Steganography is derived from Greek and it means covered or hidden writing. Main concern of steganography is hiding existence of hidden message. Steganography seems related with cryptography but it is different. Main concern in cryptography is hiding the content of the message but in steganography main concern is hiding the existence of hidden message.

Johannes Trithemius (1462-1516) has published a series of books named "Steganography: the art through which writing is hidden requiring recovery by the minds of men". The book I and Book II describe the methods to hide messages in writing. Book III is about secret astrology. Two researchers have discovered that Book III contains some hidden messages. One of those messages was "the quick brown fox jumps over the lazy dog".

Mary Queen of Scots has used the combination of steganography and cryptography so as to hide letters. She has used beer barrels which can easily pass in and out of her prison.

Another use of steganography is shaving a messenger's hair and writing the message on the head. After the messenger's hair grows up, the messenger can go to the intended receiver and the receiver also shaves his hair and retrieves the message. This method has been used by Histaiacus in 5th century BC.

In 480 BC, Demaratus warned Spartans about the risk of the invasion of the Xerxes. Heroclotus has described his method like:

"As the danger of discovery was great, there was only one way in which he could contrive to get the message through: this was by scraping the wax off a pair of wooden folding tables, writing on the wood underneath what Xerxes intended to do, and then covering the message over with the wax again."

In World War II, some steganographic methods have been used by Nazis. The name of the method was microdots. They were actually microfilm chips produced in high magnification. Those chips were the size of a period in a typewriter. However these periods contained very dense information, images, etc. The Nazis has also developed invisible inks as a method in steganography.

A Nazi spy has sent the information below:

"Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils."

When you pick the second letter in each word up, the following sentence occurs:

"Pershing sails from NY June 1."

Cardano Grill, developed by Girolama Cardano, is another method in steganography. The grill is actually a piece of paper consists of holes. When this paper is put on the paper with information, the actual information can be retrieved from that paper by means of that grill.

The last ancient method described in this paper is using eyelids to blink words in Morse code. US Armed Forces prisoners in Vietnam have used this method by means of a five by five matrix. Each element of the matrix consists of a letter in the alphabet, and the Morse code of that letter. The following figure shows this five by five matrix:

	1	2	3	4	5
1	A . .	B . .	C, K . . .	D	E
2	F . .	G . . .	H	I	J
3	L . . .	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Figure 1: The Morse code used by the US Armed Forces prisoners in Vietnam

II. ANALYSIS AND IMPLEMENTATION

There are different types of steganography. Main difference between techniques is using different carriers. In application, a text message, an image file, an executable program file or an audio file can be used as a carrier. In this part of paper, we

will introduce steganography techniques with different types of carriers.

A. Hiding in Text

In this part, text based steganography, as another method in steganography, will be explained briefly.

Figure 2 illustrates the block diagram of text based steganography.

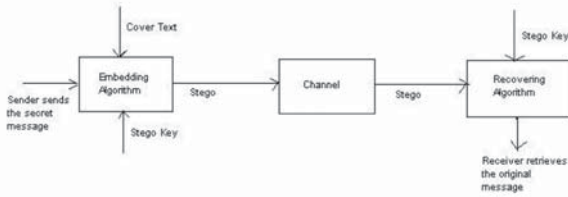


Figure 2: Block diagram of text based steganography

Firstly, sender sends the secret message by using the embedding algorithm, stego key and the cover text which will conceal the original message and the stego text is formed. Then this text is transmitted over the channel and comes to the receiver. The receiver uses the recovering algorithm and the stego key so as to retrieve the original message from the stego text.

Text based steganography can be classified into three main categories: Format-based, Random and statistical generation and linguistic method.

Generally, format-based method modifies existing text so as to hide the steganographic text. Random and statistical generation method is generating cover text according to the statistical properties. This method is based on character sequences and words sequences. Linguistic method specifically considers the linguistic properties of generated and modified text, frequently uses linguistic structure as a place for hidden messages.

One example of text steganography is to turn a short message into a spam mail content, send the mail to the receiver and retrieve the original message. We have given the following message as the input to the program in:

"This is a secret message!"

The program has turned this input into a spam mail content as below:

"Dear Friend; Thank-you for your interest in our publication . If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club ! This mail is being sent in compliance with Senate bill 1816 ; Title 3 ; Section 304 . This is not multi-level marketing . Why work for somebody else when you can become rich within 45 days . Have you ever noticed more people than ever are surfing the web & people love convenience ! Well, now is your chance to capitalize on this . We will help you SELL MORE and use credit cards on your website . You are guaranteed to succeed because we take all the risk ! But don't believe us ! Ms Ames of North Carolina tried us and says "I was skeptical but it worked for me" ! We are licensed to operate in all states . We IMPLORE

you - act now . Sign up a friend and you'll get a discount of 80% ! Cheers . Dear Cybercitizen , You made the right decision when you signed up for our mailing list ! This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1621 , Title 2 ; Section 301 ! THIS IS NOT A GET RICH SCHEME . Why work for somebody else when you can become rich within 74 weeks . Have you ever noticed people love convenience & nobody is getting any younger . Well, now is your chance to capitalize on this . WE will help YOU decrease perceived waiting time by 130% plus increase customer response by 150% ! You can begin at absolutely no cost to you . But don't believe us ! Ms Anderson who resides in Alabama tried us and says "Now I'm rich many more things are possible" ! This offer is 100% legal ! So make yourself rich now by ordering immediately ! Sign up a friend and you'll get a discount of 60% . Best regards !"

B. Hiding in Audio File

Audio steganography and spectral estimation methods will be explained briefly as the subject of this part of the paper.

In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images.

Another aspect of audio steganography that makes it so attractive is its ability to combine with existing cryptography technologies. Users no longer have to rely on one method alone. Not only can information be encrypted, it can be hidden altogether.

In order to estimate the power spectra of the signals in Additive White Gaussian Noise, there exists some estimation methods. Some of those are The Periodogram Method, The Blackman and Tuckey Method, Capon's Method, Yule-Walker Method, and Modified Covariance Method.

To compare, it can be said that the Blackman-Tuckey estimates perform better than the corresponding Periodogram estimates. This means that the variance in Blackman-Tuckey estimate curves is smaller than that of the Periodogram estimate curves.

In our implementation, a real data is concerned to analyse the practical situation. This data is a sound data and it is transmitted to the MATLAB by means of the Standard MATLAB function given below:

```
signal=wavread('sample.wav');
```

After performing this line, the original sound is transmitted to a vector. To give sound to the data vector, the standard MATLAB function given below is necessary:

```
sound(signal);
```


The waveform of the sound used for this paper is given in Figure 3:

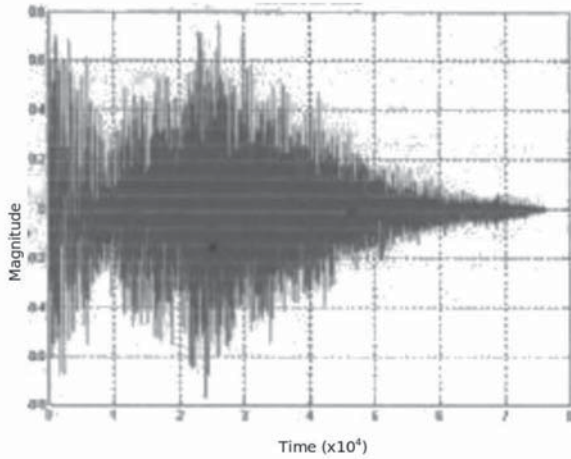


Figure 3: The waveform of the sound

And let our signal be:

$$x(n) = \cos(0.4\pi n) + \text{sound}(n)$$

It can be observed from Figure 4 that, all the methods give worse performance since the noise part of the signal (here, the sound) is correlated and its shape is not Gaussian distributed. However the Modified Covariance Method estimates the frequency.

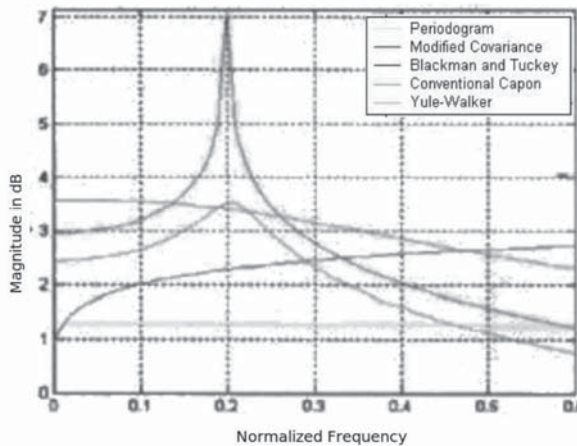


Figure 4: Estimation of the frequencies for the specified signal

By means of this simulation, we can say that we can add our information signal to a real data and send it to the receiver through a channel and the receiver takes the data and applies the best estimator to pull out the information from the real data.

In conclusion, as more emphasis is placed on the areas of copyright protection, privacy protection, and surveillance, we believe that steganography will continue to grow in importance as a protection mechanism. Audio steganography in particular addresses key issues brought about by the MP3 format, P2P software, and the need for a secure broadcasting

scheme that can maintain the secrecy of the transmitted information, even when passing through insecure channels.

C. Hiding in File System

In this section of the paper, file system steganography will be explained. Slack spaces, alternate data streams and merging files in other files are the subsections of this section.

A file system uses fixed size of space to store files in chunks of data which is known as blocks in Unix/Linux systems, and clusters in Windows systems. The smallest process unit is called sector and one sector consists of 512 bytes. Clusters occur when multiple sectors conjugate. Also the cluster size varies with the type of the operating system. Files are recorded in clusters.

There exist 2 different cases, one is the size of the file and the cluster are the same. This is the ideal case and the probability of the occurrence of this case is extremely low. The second case is the size of the file is larger or smaller than the cluster size. In this case, it is certain that the file will not fit into the cluster. There will be overflows to other clusters. The space between the end of the file and the end of the cluster is called the slack space and the information hidden in this space is called slack space data. For instance, if a file is 200 bytes long, the file has to allocate a 2048-byte data unit, and the remained 1848 bytes will be slack space considering an NTFS file system with a 2048-byte cluster. Figure 5 illustrates the slack space.

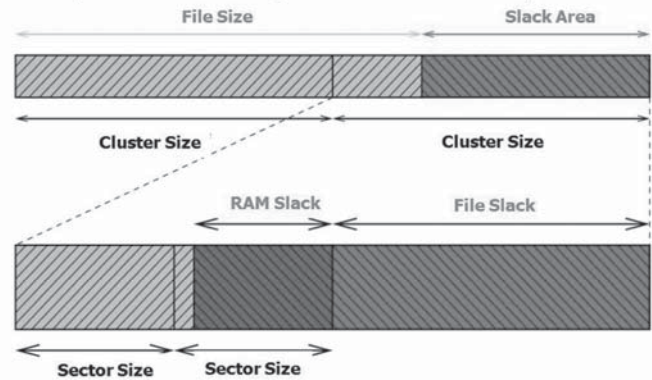


Figure 5: Illustration of slack space

Slack area or slack space consists of two types of slacks: RAM slack and File slack. Remember that clusters contain multiple sectors. RAM slack is defined as the space between the end of the file and the end of the sector. File slack is defined as the space between the beginning of the next sector and the end of the cluster.

When you press delete button on a file in a computer, you actually do not delete the whole file, only the pointer which indicates the beginning of the file is deleted. If this pointer is deleted, then the computer may write another information in that data unit. Slack space is not emptied in most computers, so this space contains information or data from previous files or from memory. Those data can be used by baleful people. Also this space may be used in steganographic methods. However, it is probable that the operating system may overwrite on those slack areas.

Another method of hiding information in file systems is to use hidden partitions. If the user knows the file name and password, then he/she can access to the file, otherwise the file seems not to exist in the system.

The aim of the Metasploit Anti-Forensics Project, developed by Vinnie Liu, is to develop tools so as to remove forensic evidence from computers. One of those tools is slacker.exe. by means of this executable, one can hide messages by using slack areas in NTFS file systems. Slacker.exe can be reached from and the usage is given in Figure 6.

```
C:\Windows\system32\cmd.exe
Hiding a file in slack space:
slacker -s <file> <path> <levels> <metadata> [password] [-dxi] [-n] [-k] [-f] <xorfile>
e)
-s store a file in slack space
-f file to be hidden
-p path root directory in which to search for slack space
-l levels depth of subdirectories to search for slack space
-m metadata file containing slack space tracking information
-p password passphrase used to encrypt the metadata file
-dxi dumb, random, or intelligent slack space selection
-nkf none, random key, or file based data obfuscation
-xorfile the file whose contents will be used as the xor key

Restoring a file from slack space:
slacker -r <metadata> [password] [-o outfile]
-r restore a file from slack space
-m metadata file containing slack space tracking information
-p password passphrase used to decrypt the metadata file
-o outfile output file, else original location is used, no clobber
```

Figure 6: Use of slacker.exe

We have already used notepad.exe in Windows operating systems. Now let us examine how to hide information by using this exe. Our aim is to hide information stored in secret.txt by using clear.txt. We have non-important information in clear.txt and sensitive data in secret.txt. so as to create secret.txt, go to the folder where clear.txt exists in the command prompt and write the following command: notepad clear.txt:secret.txt

Thereby, you can create a txt file and write your sensitive data down in it, however you can not see this file in the computer. In order to see the content of this file, go to the command prompt and write the command above again. Figure 7 illustrates this case.

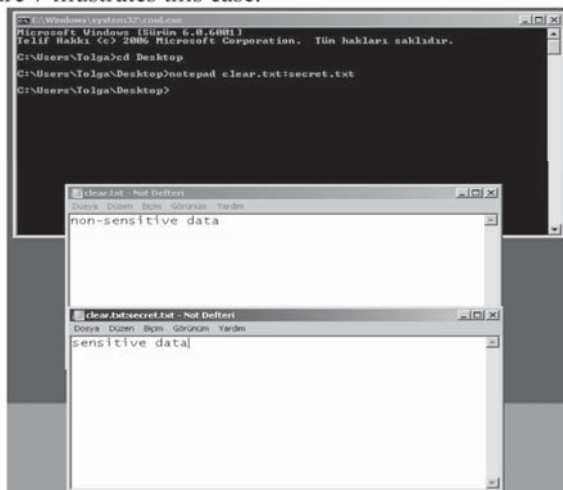


Figure 7: clear.txt and secret.txt files

This property comes with NTFS file systems and is called alternate data streams (ADS). If you want to copy this file into a system using FAT32 (most of the USB memory cards use this type of file system), you will get the warning window in Figure 8.

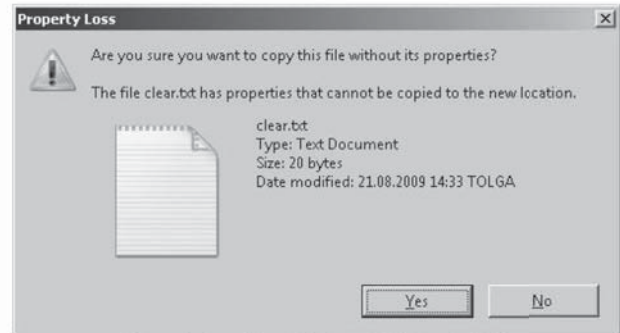


Figure 8: Copying ADS from NTFS to FAT32

Now let us do the same exercise by using two different executables. We will use winmine.exe (minesweeper) and calc.exe (calculator). You may consider that winmine.exe is an innocent program, however calc.exe is a malicious program like a virus will merge calc.exe into winmine.exe. Figure 9 gives us the commands so as to do this:

```
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>type calc.exe > uinmine2.exe:calc.exe
C:\WINDOWS\system32>start c:\WINDOWS\system32\winmine2.exe:calc.exe
C:\WINDOWS\system32>
```

Figure 9: Merging calc.exe into winmine.exe

Finally, let us explain how the files with alternate data streams can be detected and removed. One of the famous tools for this purpose is Microsoft's streams.exe. Notice that there exists a logo in the address bar in Figure 10:

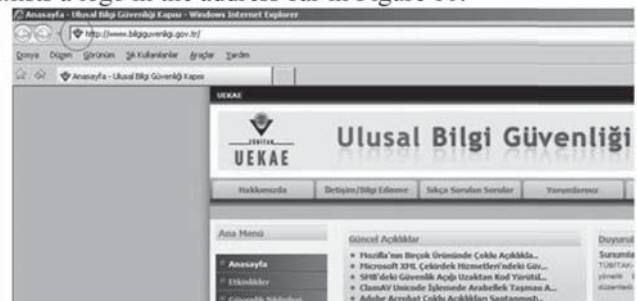


Figure 10: The logo

After adding this site to the Favorites in Internet Explorer, run the first command in Figure 11, so you can detect ADS's in the relevant directory.

```
C:\Documents and Settings\Administrator\Desktop>streams -s "C:\Documents and Settings\Administrator\
Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Documents and Settings\Administrator\winmine.exe:
:calc.exe:$DATA 0
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\
Content.IE5\39EFSK\Tolga_Mataracioglu_Lab_Assignment_1(1).pdf:
:Zone.Identifier:$DATA 26
C:\Documents and Settings\Administrator\S7k Kullan\lanlar\Anasayfa\Ulusal Bilg
i G'venli?i Kap?s?.url:
:Favicon:$DATA 3638
```

Figure 11: Detection of ADS's

One can see the line about the logo in the last line in Figure 7 and conclude that this logo has been merged in bilgiguvenligi.gov.tr URL. If you open that file in notepad, you may see the merged information seen in Figure 12.

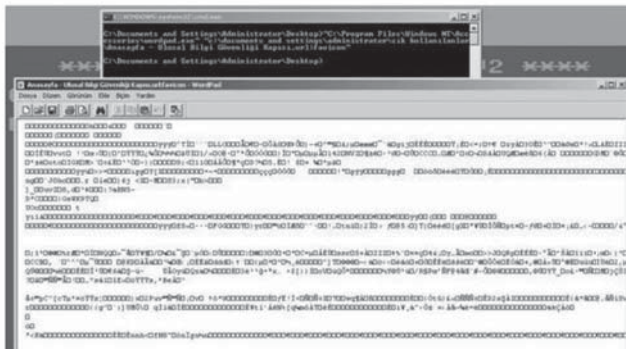


Figure 12: Logo format seen in notepad

So as to remove those ADS's, you can run the same command by using `-d` parameter.

D. Hiding in Image Files

Hiding data into the image files is another type of steganography. This method is the most common steganographic technique. There are several methods for hiding data into images. Most common methods for image steganography are least significant bit method and masking and filtering

In this project paper we will deal with only least significant bit method.

1) Image Files

Each image file in digital form is composed of pixels. Every pixel is similar to a very small point in picture. A pixel is either 24-bit or 8-bit. A common image size is 640X480 and such a file is 300 000 pixels.

Each pixel represents a color and each color is composed of red, green and blue. Different amount of these colors defines the value of pixel in 1 and 0s. For a 24-bit image, 8-bit is used for red, green and blue, total is 24 bits. This means that each pixel can have 16,777,216 (2^{24}) different colors.

Image files, like jpg files, can be compressed. Compressed files have two forms of compression: lossless and lossy compression. In lossless compression, you can retrieve the original file but in lossy compression you can not retrieve original file but only compressed form.

2) Least Significant Bit (LSB) Method

We have two files in hiding information in an image file: Cover image which is carrier of the hidden message and the other file is hidden message. After inserting the hidden message into cover image we have the stego image file.

In image steganography most common technique is least significant bit insertion technique. For instance, we want to hide letter 'A' in three pixels data. 'A' letter has 8 bits data. 'A' is equal to (1 0 0 0 0 1 1) in binary format.

Each pixel has 24 bit information. Assume following is the value of three pixels.

```
( 00100111 11101001 11001000 )
( 00100111 11001000 11101001 )
( 11001000 00100111 11101001 )
```

To hide data, we change last bits of each byte (8 bits), that means least significant bits of Red, Green and Blue colors of each pixel.

After hiding data, data in pixels is shown below.

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

In this example, only italic and bold digits changed, red ones are unchanged. Since data and cover image are composed of 1's and 0's probability of change of a bit cover image is about $\frac{1}{2}$.

If we use last two bits of RGB values of each pixel as in Figure 13, we can hide two times larger data in the image file and change in image is still undetectable by human eyes.

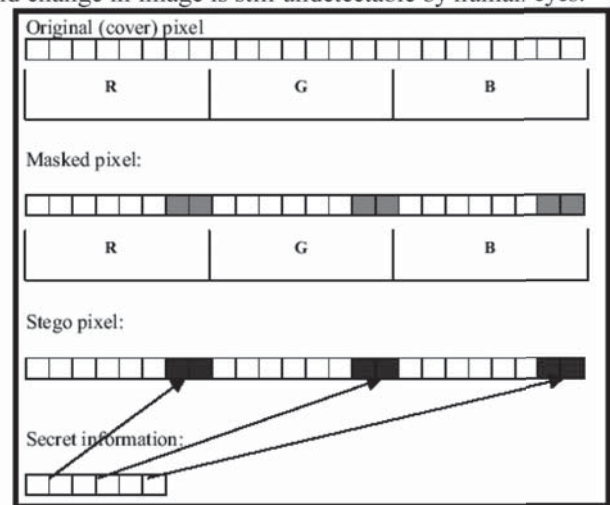


Figure 13: Hiding in last two bits.

3) An LSB Application

For this paper we implemented an LSB application. The program uses only 24-bit bmp image as cover media. In Figure 14, screenshot of the program is seen.

To hide a file:

1. Load Image: Click Load Image button on the left pane to select cover image file.
2. Load: Click load button to select guest data (hidden file)
3. Passphrase: Write a password to encrypt (DES algorithm) hidden data before hiding. This is optional.
4. Used Bits: Select Used Bits ruler to select how many bits used.
5. Hide Data: Click Hide Data button to hide hidden data in cover image
6. Save Image: Click Save Image button to save the modified image file.

To extract hidden data:

1. **Load Image:** Click Load Image button on the right pane to select image that contains hidden data.

2. Passphrase: Write the password to decrypt (DES algorithm) hidden data.
3. Used Bits: Select Used Bits ruler to select how many bits used.
4. Extract Data: Click Extract Data button to unhide the data.
5. Save: Click Save button to save the hidden data.



Figure 14: Screenshot of the LSB Steganography Program

When we used more than one bit deformation of the image increases. In the Figure 15 we hide a file in the same image file and we used last bits from 1 to 8.

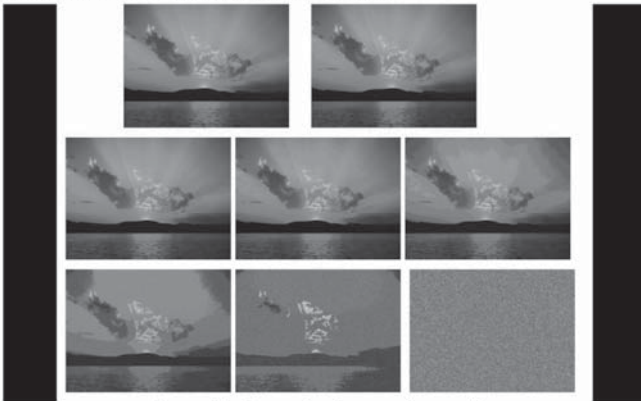


Figure 15: Corruption in cover image files

III. CONCLUSION

This paper aims to analyze distinct steganographic methods including hiding in text, hiding in audio file, hiding in file system, and hiding in image files. Further, implementations of those techniques have been performed.

REFERENCES

- [1] A. Ker: "Improved Detection of LSB Steganography in Grayscale Images", in J. Fridrich (ed.): Information Hiding. 6th International Workshop. Lecture Notes in Computer Science, vol. 3200, Springer-Verlag New York, pp. 97–115, 2005.
- [2] Avcibas, I.; Memon, N.; Sankur, B. "Image steganalysis with binary similarity measures"

- [3] B. Carrier, "File System Forensic Analysis", Addison-Wesley Publishing, 2005.
- [4] "Classical Steganography, Cardano Grille" URL: <http://library.thinkquest.org/27993/crypto/steg/classic1.shtml>
- [5] Counterintelligence News and Developments, Volume 2, June 1998 "Hidden in Plain Sight-Steganography" URL: www.nacic.gov/pubs/news/1998/jun98.htm
- [6] S. Dumitrescu, X. Wu, and Z. Wang: "Detection of LSB Steganography via Sample Pair Analysis", in: Petitcolas, F.A.P. (ed.): Information Hiding. 5th International Workshop. Lecture Notes in Computer Science, vol. 2578, Springer-Verlag New York, pp. 355–372, 2000.
- [7] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, July 1999, pp. 1062 – 1078.
- [8] H. Farid and L. Siwei: "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines", in: F.A.P. Petitcolas (ed.): Information Hiding. 5th International Workshop. Lecture Notes in Computer Science, vol. 2578, Springer-Verlag New York, pp.340–354, 2002
- [9] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics." *Security and Watermarking of Multimedia Contents, San Jose, Ca.*, February 2001.
- [10] J. Fridrich, M. Goljan, D. Hoge, and D. Soukal: "Quantitative Steganalysis: Estimating Secret Message Length," ACM Multimedia Systems Journal, Special Issue on Multimedia Security, vol. 9(3), pp. 288–302, 2003.
- [11] J. Zollner, H. Federrath, H. Klimant, A. P. Tzeman, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the security of steganographic systems," *2nd Information Hiding Workshop*, pp. 345–355, April 1998.
- [12] K. Bennett, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", Purdue University, CERIAS Tech. Report, 2004.
- [13] Kay, S. M., "Modern Spectral Estimation Theory and Application", Prentice Hall, Jan. 1988.
- [14] Kolata, Gina, "A Mystery Unraveled, Twice" URL: cryptome.unicast.org/cryptome022401/tri.crack.htm
- [15] M. Russinovich. Streams v1.56. URL: <http://technet.microsoft.com/en-us/sysinternals/bb897440.aspx>
- [16] Miroslav Goljan*, Jessica Fridrich, and Taras Holotyak "New Blind Steganalysis and its Implications"
- [16] N.F. Johnson, Z. Duric, S. Jajodia, "Information Hiding: Steganography and Watermarking – Attacks and Countermeasures", Kluwer Academic Publishers, 2001.
- [17] R. Anderson, R. Needham, A. Shamir, "The Steganographic File System", Lecture Notes in Computer Science, vol. 1525, Springer-Verlag, 1998.
- [18] Spam Mimic. URL: <http://www.spammimic.com/index.shtml>
- [19] Singh, Simon, "The Cipher of Mary Queen of Scots" URL: www.arch.columbia.edu/DDI/cad/A4513/S2001/r9/
- [20] S. Lyu and H. Farid "Steganalysis Using Higher-Order Image Statistics" IEEE Transactions on Information Forensics and Security, 1(1):111-119, 2006
- [21] Taras Holotyak I, Jessica Fridrich I, Sviatoslav Voloshynovskiy 2 "Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics"
- [22] T. Mataracioğlu, "Uygulamalarla Steganografi", National Information Security Portal. URL: <http://www.bilgiguvenciligi.gov.tr/teknik-yazilar-kategorisi/uygulamalarla-steganografi.html?Itemid=6>
- [23] T. Mataracioğlu, Ü. Tatar, "Spectral Estimation Methods: Comparison and Performance Analysis on a Steganalysis Application", 2nd Information Security & Cryptology Conference with International Participation, Ankara, Dec. 2007.
- [24] Trithemius, Johannes, "Steganographia: hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa" URL: www.esotericarchives.com/trithem/stegano.htm
- [25] "The Science of Secrecy, Steganography" URL: www.channel4.com/plus/secrecy/page1b.html
- [26] Van Trees, H. L., "Detection, Estimation and Modulation Theory Part-I", John Wiley, Jan. 1968.
- [27] V. Liu, Metasploit Anti-Forensics Project. URL: <http://metasploit.org/research/projects/antiforensics>

Prototype Development of VoIP Steganography

Azizah A. Manaf, Abdulaleem Z. Al-Othmani, and Akram M. Zeki

Abstract—Steganography is the process of hiding data inside any of multimedia objects, such as images, audio or video files, normally used for transmitted data. The main contribution of this study is developing a prototype of Voice over Internet Protocol (VoIP) steganography. VoIP is a technology that allows telephone calls to be made over computer networks like the Internet. VoIP converts analog voice signals into digital data packets and supports real-time, two-way transmission of conversations using Internet Protocol (IP). In this paper, VoIP steganography by using least significant (LSB) technique will be studied and tested. VoIP is considered a very effective and practical medium to hide data and transfer it secretly between two parties.

Index Terms— VoIP, Steganography, Real-time transmission

I. INTRODUCTION

VOICE over Internet Protocol (VoIP), or IP telephony, is defined as a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks [1]. VoIP converts analog voice signals into digital data packets and supports real-time, two-way transmission of conversations using Internet Protocol (IP). In [2], it is stated that through IP technology, voice communications are digitized and then segmented into standard digital data payloads (i.e., batches or collections of data) that are, in turn, encapsulated within IP packets so they can be transmitted via the IP transport network. This process allows voice and other information to coexist in a single IP data network so it can be transmitted using shared equipment and communications lines. VoIP systems usually interface with the traditional public switched telephone

network (PSTN) to allow for transparent phone communications worldwide. Although VoIP has existed for several years, it has only recently begun to take off as a viable alternative to traditional voice systems and PSTN networks.

At the present time, VoIP is one of the most popular services in the Internet. It was introduced to the telecommunication market and since then, changed it completely and gradually. As it is used worldwide more freely, the traffic volume that it generates is still increasing. VoIP became a natural target for steganography, it is appropriate to enable hidden communication throughout IP networks [3]. VoIP steganography covers a wide range of information hiding techniques; including popular techniques based on IP or TCP and other protocols. The main idea is to use free, redundant or unused fields of these protocols [4].

This prototype has been designed and implemented to work in a lab-based environment, this means, the VoIP call will be limited to two hosts using point-to-point connection with static IP addresses. This is different from the real life VoIP applications which use client-server calls. As a result, the system will be based on LAN network which provides an environment with almost zero noise. This will greatly help to get better VoIP steganography performance and correctness. Due to the complexity of VoIP steganography, only specific basic types of visual and statistical measures will be considered. The most important success factors of this study are keeping the overall changes of the VoIP stream very small so that they can be hardly noticed while embedding a large amount of covert data and providing maximum extraction of the hidden information.

II. METHODS OF AUDIO STEGANOGRAPHY

There are many audio steganography techniques that are applicable to VoIP covering time domain, frequency domain and integer transform domain. The time domain algorithms provide less complexity and higher capacity than others, while other domains focus on the robustness and invisibility. Because VoIP is simply audio signal transmission using IP networking, it is possible also to apply network steganography techniques during VoIP call session. It is possible to use redundant, unused and reserve bits of protocols packets to hide some data. Many of current audio and network steganography algorithms are theoretically applicable to VoIP streams. In practice only some of them are feasible or applicable to VoIP taking in mind available equipment and technology. There are also some techniques which are too complex to be applied on VoIP stream which needs real time embedding and extraction of secret data.

Azizah Abdul Manaf is a Professor of Image Processing and Pattern Recognition from University Technology Malaysia (UTM). She graduated with B. Eng. (Electrical) 1980, MSc. Computer Science (1985) and PhD (Image Processing) in 1995 from UTM. Her current areas of interest and research are image processing, watermarking, steganography and computer forensics and have postgraduate students at the Masters and PhD level to assist her in these research areas. She has written numerous articles in journals and presented an extensive amount of papers at national and international conferences on her research areas. Prof. Dr. Azizah has also held management positions at the University and Faculty level such as Head of Department, Deputy Dean, Deputy Director and Academic Director pertaining to academic development as well as on training for teaching and learning methodologies at the University. E-mail: azizah07@ic.utm.my.

Gopalan and Wennedt [5] presented a method of embedding covert data in a cover audio signal by insertion of low power tones. It is clear [6] that the flexibility of audio steganography is what makes it so potentially powerful. The five methods discussed provide users with a large amount of choice and makes the technology more accessible to everyone. A party that wishes to communicate can rank the importance of factors such as data transmission rate, bandwidth, robustness, and noise audibility and then select the method that best fits their specifications. For example, two individuals who just want to send the occasional secret message back and forth might use the LSB coding method that is easily implemented. On the other hand, a large corporation wishing to protect its intellectual property from "digital pirates" may consider a more sophisticated method such as phase coding, SS, or echo hiding.

Cvejic and Seppänen, [7], presented a high bit rate LSB audio watermarking method that reduces embedding distortion of the host audio. Using their proposed two-step algorithm,

watermark bits are embedded into higher LSB layers, resulting in increased robustness against noise addition. Furthermore, listening tests showed that perceptual quality of watermarked audio is higher in the case of this method than in the standard LSB method. Another aspect of audio steganography that makes it so attractive is its ability to combine with existing cryptography technologies. Users no longer have to rely on one method alone. Not only can information be encrypted, it can be hidden altogether.

III. PROTOTYPE DEVELOPMENT

The VoIP steganography prototype architecture contains few steps as illustrated in figure 1 below. Each covert data transmitted during VoIP call will be processed and embedded according to the architecture.

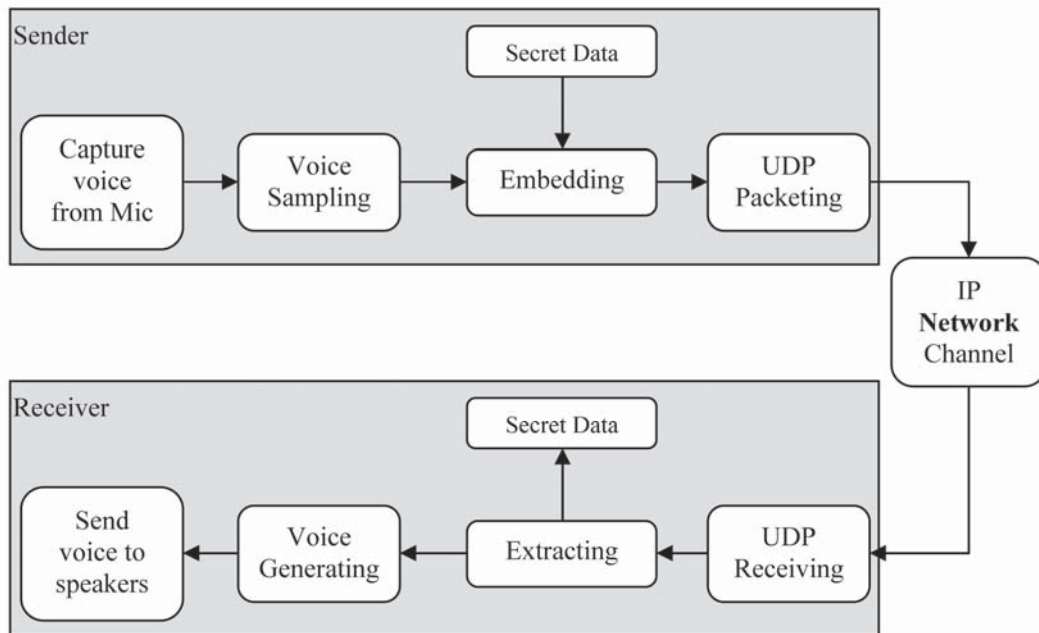


Fig 1. Prototype General Architecture

At the first stage of the prototype, is implementing VoIP call by client-server based and point-to-point based. The VoIP call in this prototype consists of three steps: initializing call, performing the conversation, and ending the call. The initialization of VoIP calls starts when the sender sends an INVITE message to the receiver using receiver's IP address. If the receiver accepts the invitation, the message will be sent

back to the sender. By receiving the message, the initialize step is done and the both parties will start the conversation.

In this prototype, the LSB technique will be used to embed the data into VoIP, different size of data going to be embedded within 1 LSB, 2 LSB, 3 LSBs, and 4 LSBs. Figure 2 shows the graphic user interface GUI for the developed prototype.

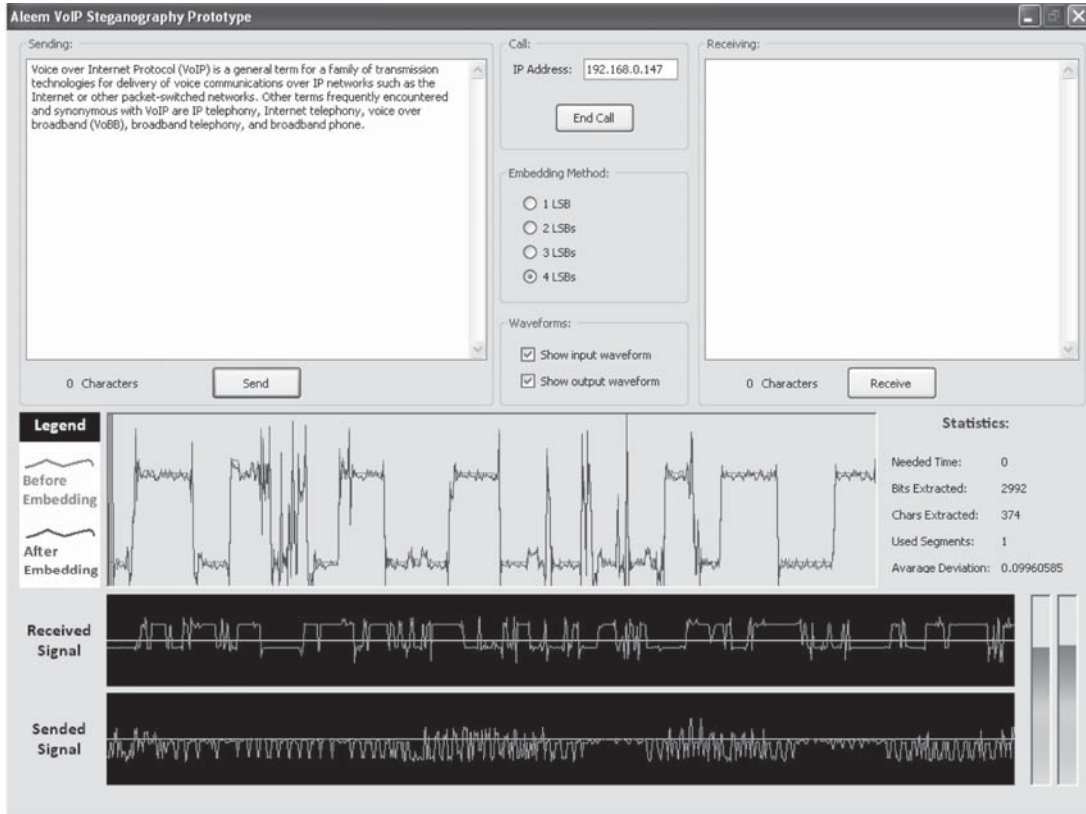


Fig 2. GUI for the developed prototype

A. Embedding Process

As the conversation session start, voice signals from microphone are captured and sampled into PCM codes. This task is done by Microsoft DirectSound. It will then compress the 16 bits PCM voice samples captured into 8 bits using G711 audio codec algorithm. The data will now be hiding using LSB, and the result will be Packet voice data into UDP packets which will be consequently send to the receiver, as described in Figure 3.

The detailed procedure of the embedding is based on the option of utilizing 1 LSB, 2 LSBs, 3 LSBs and 4 LSBs depending on user choice through GUI. The 1 LSB part of this function is working according to the following algorithm:

Step 1: Get secret data and convert it to an array of bits A1.
Step 2: Get a portion of voice data and save it into an array of bytes A2.

Step 3: Insert starting bytes (0, 255, 0, 255, 0) into voice data array.

Step 4: Insert 1 bit of secret data array into LSB of voice data array byte.

Step 5: Increment indexes of A1 and A2.

Step 6: repeat Step 4 and 5 until end of A1.

Step 7: Insert ending bytes (255, 0, 255, and 0,255) into voice data array.

The replacement of 1 LSB is being done according to figure 4.

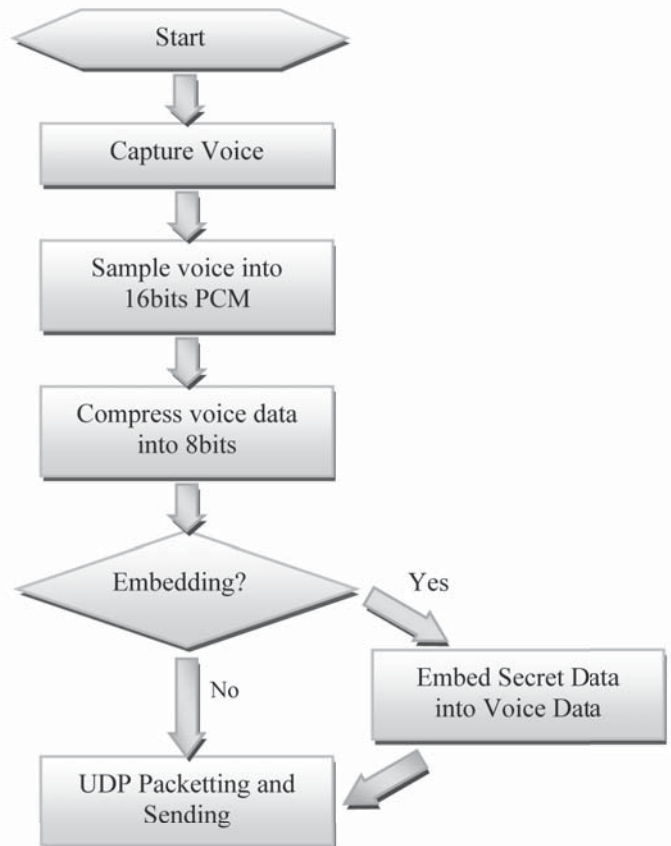


Fig 3. Flowchart of the embedding prototype.

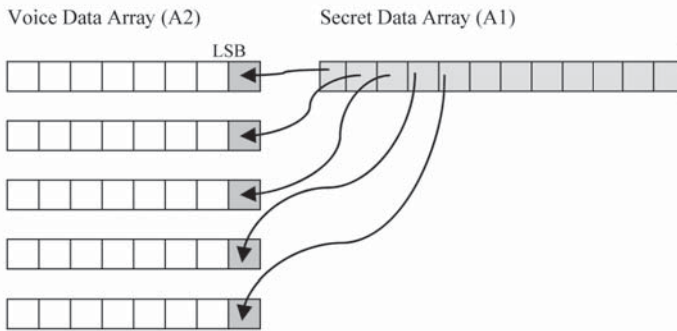


Fig 4. Replacement of 1 LSB in Embedding Function

B. Extracting Process

Receive UDP Packets from the sender are extracted by the use of extracting function. The data are first decompressed from 8 bits G711 data into 16 bits PCM voice samples using G711 audio codec algorithm. Regenerate audio signals from voice data are sent back to the speaker by Microsoft DirectSound, then the hidden data will be extracted. Figure 5 shows the flowchart of extracting process.

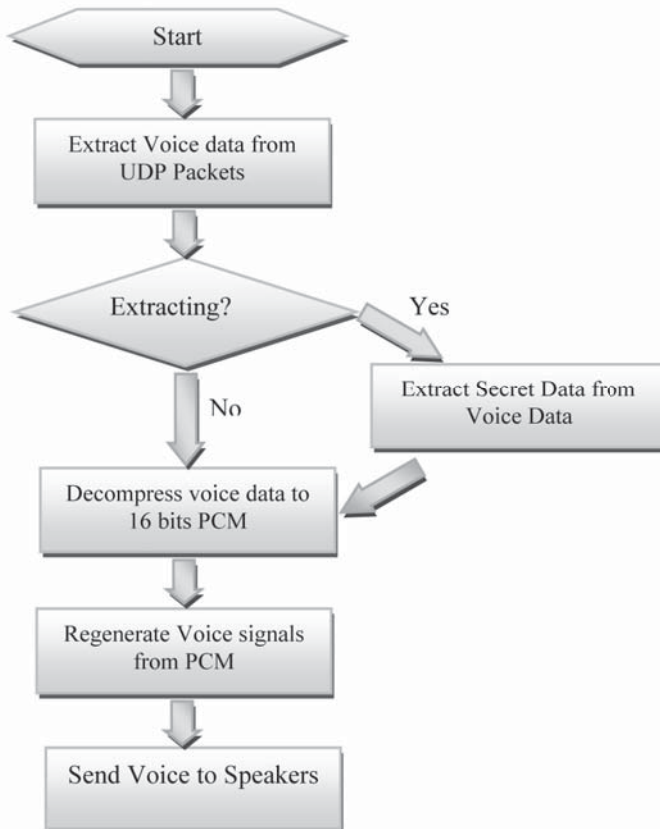


Fig 5. Flowchart of the Extraction

The detail procedure of the extracting is working according to the following algorithm:

Step 1: Get the received voice signal and save it into an array of bytes A2.

Step 2: Search the received voice data for the starting bytes (0,255,0,255,0).

Step 3: Extract the LSB of one byte of voice data array and save it into an array of bits A1.

Step 4: Increment indexes of A1 and A2.

Step 5: Repeat Step 4 and 5 until finding the ending bytes (255,0,255,0,255).

Step 6: Recombine array A1 into array of characters.

Step 7: Display the result (the array of characters) on the GUI.

IV. EXPERIMENTAL RESULTS

For the purpose of testing, each LSB steganography algorithm has been used to embed different size of data within different number of bits. Statistical measures include Time interval needed to receive, extract and display secret data, the number of bits transmitted, number of VoIP call sample or bytes used to embed such secret data, the signal-to-noise ratio SNR, and average deviation (AvDev) as shown in equation 1.

$$AvDev = \frac{1}{n} \sum_{i=1}^n \frac{S_i}{V_i} \quad (1)$$

Where:

AvDev = average deviation.

n = number of VoIP call data bytes used to hide the secret data.

S_i = value of the secret data hidden in the VoIP call data byte i.

V_i = value of the VoIP call data byte I used to hide secret data value S_i.

The first experiment is done by embedding a sample of 100bytes text message using LSB technique within 1, 2, 3, and 4 LSB. The embedded data sent by the sender is totally and correctly received by the receiver. The results of this experiment and statistical records are summarized in Table I below.

TABLE I
RESULT OF HIDING 100BYTES OF SECRET DATA

Measure	1 LSB	2 LSBs	3 LSBs	4 LSBs
Average Deviation	0.007109	0.0142429	0.039231	0.075223

Another experiment was done by using 100 bytes, 1KB, 4KB, 8KB of secret data. The results of this experiment and statistical records are summarized in Table II below.

TABLE II
RESULT OF HIDING DIFFERENT SIZE 1KB OF SECRET DATA

Measure	100 Byte	1 KB	4 KB	8 KB
Time hide the data in Sec	4	237	1378	2908
Used Voice Segments	1	4	15	30
Average Deviation	0.007109	0.007447	0.006822	0.004482

The above table shows that the quality of the voice by using one bit (1 LSB) is better than using 4 bits at the same time (4 LSB). And by comparing different size of secret data, the

above results shows that there is a difference the total number of voice segments required to send the desired secret message.

V. CONCLUSION

steganography is a fascinating and effective method of hiding data that has been used throughout history. The biggest challenge of steganography is to increase the amount of information to be embedded in the host channel without affecting the properties of that channel while keeping this secret transmission invisible to unauthorized parties. This study concerns available steganographic techniques that can be used for creating covert channels for VoIP streams. LSB technique of VoIP steganography was tested and evaluated throughout the phases of this research. The results of this study provide a reasonable tradeoff between the adequate information hiding requirement (good security and sufficient capacity) and the low latency requirement for VoIP.

REFERENCES

- [1] International Engineering Consortium. "Voice over Internet Protocol. Definition and Overview". http://www.iec.org/online/tutorials/int_tele/. White Paper. Accessed May 5, 2009.
- [2] US. Department of Justice. "Voice over Internet Protocol" <http://www.ncjrs.gov/pdffiles1/nij/217864.pdf>. Accessed May 7, 2009.
- [3] W. Mazurczyk and K. Szczypiorski, "Covert Channels in SIP for VoIP Signalling". Springer Verlag Berlin Heidelberg, Proc. of 4th International Conference on Global E-security 2008, London, United Kingdom, pp. 65-72, June 2008
- [4] J. Lubacz, W. Mazurczyk, and K. Szczypiorski. "Hiding Data in VoIP". In Proc. of: The 26th Army Science Conference, December 1-4, 2008, Orlando, FL, USA.
- [5] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. "RTP: A Transport Protocol for Real-Time Applications". RFC3550, July 2003.
- [6] M.D. Swanson, M. Kobayashi, and A.H. Tewfik. "Multimedia Data-Embedding and Watermarking Technologies". Proc. IEEE, Vol. 86, pp. 1064-1087, June 1998.
- [7] N. Cvejic, and T. Seppänen, "Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding". Journal of Universal Computer Science 11(1):56-65. 2005.
- [8] R. Thurston, "Steganography developers turn their attention to hiding information in VoIP". SC Magazine. July 04, 2008.