Privacy Impact Assessment Methodologies for Protection of Personal Data

Okyar TAHAOĞLU, Yalçın ÇEBİ

Abstract—**This paper presents a brief summary of the Privacy Impact Assessment (PIA) methodologies proposed for the protection of personal data against misuse, collection and process risks. The methodologies presented in this paper shed light on the professional community's effort and government's governance responsibilities to assess and control these inherent risks. Clearly, as Information and Communication Technologies become increasingly more complex, individual knowledge, judgment, and expertise will not suffice and systemic methodologies for risk management such as those presented in this paper become imperative. Our observation, which is based on the workforce spent by the government institutions to protect personal data and the benchmark of our country's draft Data Protection Act regulation with the developed countries, is further amplified by the fact that privacy risk is among the least measured or managed in a system today.**

Keywords —**Personal data protection, Privacy impact assessment**

I. Introduction

PERSONALLY identifiable information is defined as any information relating to an identified or identifiable individual. Such information includes, but is not limited to, the customer's name, address, telephone number, social security/insurance or other government identification numbers, employer, credit card numbers, personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records and similar information [1]. Personal data can be defined as all of the information that can express any opinion about an individual or corporate.

On the other hand protection of confidentiality and secrecy of personally identifiable information is basically called as privacy. Privacy has several more meanings and privacy in the context of personal data can be divided into the following separate but related concepts: [2]

--Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";

Manuscript received November 10, 2008.

Okyar TAHAOĞLU is with the Computer Engineering Department,Dokuz Eylül University, İzmir, 35160 Turkey (okyar.tahaoglu@turkcell.com.tr).

Yalçın ÇEBİ is with the Computer Engineering Department, Dokuz Eylül University, İzmir, 35160 Turkey (yalcin@cs.deu.edu.tr).

--Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;

--Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and

--Territorial privacy, which concerns the setting of limits on intrusion into domestic and other environments such as the workplace or public space.

In this paper we will use privacy as "information privacy of personal data" and we will investigate on how personal information can be protected by organizations under an assumption that privacy legislations exist in Turkey. On the other hand in several papers it is criticized that "information systems security" is not discussed sufficiently in Turkey [3]. Accordingly we hope this paper may initiate a discussion in security of personally identifiable information.

II. Legislations

A. Data Protection Legislations

The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970 [4]. The Council of Europe's "Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data 1981 (Directive 108)" is a reference for today's data protection legislation [5].

Other current directives force the member states of the European Union (EU) to prepare and deploy their own data protection laws. These legislations aim to keep the security level of data used and shared among the states for commercial, legislative and social objects [6]. The baseline of the security level is set by the Directive 108. Each country must look for a data protection act from the other member while sharing personal data.

B. Turkish Draft Data Protection Act

Every Turkish citizen has rights protected by the organic law about protection of private and family life [7]. Additionally, Turkey has signed the Directive 108 in the same year it has been approved by the EU. Therefore a privacy and data protection act is expected from Turkey since then. A draft "Personal Data Protection Act" is currently being prepared but has not been enacted yet. The draft act is a regulation that draws the boundaries of usage and processing practices of data

[8]. It is expected that this draft act will be in action in the following years. Compliance with the privacy laws always took long time for the private and government organizations. Therefore authorities who are responsible for the governance of privacy protection usually give a considerable time for the organizations to ready. When this period is considered organizations must begin using privacy protection methodologies without waiting for the legislation. Some acts especially related to specific sectors (telecommunication, finance, health etc.) also force protection of private information. On the other hand, we see that socially developed nations which have high human development indexes and freedom of information levels like Canada prepare methodologies which include best practices and management guidelines for organizations to help them assure compliance with data protection legislations. This enables the legal bodies to act as corrective, detective and preventive controls rather than penalty authorities. Management of personal data in safe harbors requires fully implementation of selected technical and organizational controls. Thus selection of controls must be done in a systematic way.

III. PRIVACY IMPACT ASSESSMENT

In this section we examine general approaches to Data Protection Framework and we will use Canadian framework as a guide to make conclusions for a successful data protection practice in Turkey. Office of the Privacy Commissioner of Canada has a privacy framework including information center for individuals and businesses, e-learning tools for the public, privacy and personal data processing policies, system audit procedures and guidelines for Privacy Impact Assessments. We believe investigating the Canadian experience can give us clues about the facts we will face in the future in Turkey.

Privacy Impact Assessments (PIAs) are methodologies to help determine whether technologies, information systems and processes of a project meet privacy regulation requirements. It measures technical compliance with privacy legislation and defines the gaps between the practices and requirements. PIAs are used to identify privacy vulnerabilities and risks of new or redesigned programs, products or services. Canadian government uses PIA as a tool to assess government projects against privacy risks. PIAs take a close look at how government departments protect personal information as it is collected, stored, used, disclosed and ultimately destroyed. These assessments help create a privacy-sensitive culture in government departments [9]. All federal departments, agencies and institutions conduct PIAs for new or redesigned programs and services that raise privacy issues. The governmental institutions which must implement PIA as a tool in new system designs are listed in the Canadian Privacy Act of 1985 in detail [10].

A. Fundamental Principles of PIA

In order to have a standard privacy baseline for PIAs ten fundamental principles are defined. The fundamental principles of Canadian PIAs are shown in Table I. These fair information principles are included in the Personal Information Protection and Electronic Documents Act, Canada's private-sector privacy law [11]. Therefore organizations must consider these principles and should assure that computer systems which collect, use, store and transfer personally identifiable information are assessed accordingly.

TABLE I
TEN PRINCIPLES OF PIAS

Principle	Code for Protection of Personal Data
Accountability	Each government organization is responsible for personal information under its control and shall designate an individual who is accountable for the organization's compliance with privacy regulations.
Identifying purposes	Individuals must be informed during the collection of personal information.
Consent	Knowledge and consent is required for the collection, use, or disclosure of personal information.
Limiting collection	Minimum required information shall be collected by fair and lawful means.
Limiting use, disclosure and retention	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information should only be kept as long as necessary.
Accuracy	Personal information shall be as accurate, complete, and up-to-date.
Safeguards	Information shall be protected against unauthorized Access, copying, disclosure, use or modification.
Openness	Personal information management policies and practices must be available to the public.
Individual access	An individual shall be able to ask the status of his/her own information and have access for any update.
Challenging compliance	An individual shall be able to address a challenge concerning compliance with the above principles.

Government organizations must perform a PIA in order to assess privacy risks in new programs, acquisition of new software programs and integration of distributed systems in different government agencies. Major changes to existing programs, changes in technology architecture, additional systems linkages, new channel release for a governmental service, database design change, a new plan to collect citizens' personal data and outsourced operations are some examples where PIAs must be initiated.

Usually two kinds of PIAs are used; preliminary PIA and full-cycle PIA. Preliminary PIA is used at the initial phase of a project to determine whether a full-cycle PIA is needed. If personal data is not used or processed or transferred in the corresponding system preliminary assessment may find there are no or minimal privacy risks. This approach saves resources and time for the project.

Another way to save resources is using self-assessment where individual government departments conduct their own PIAs. Therefore each governmental agency must have educated professionals from various departments (Information Technology, legal, business analysis, project management etc.) of the organization.

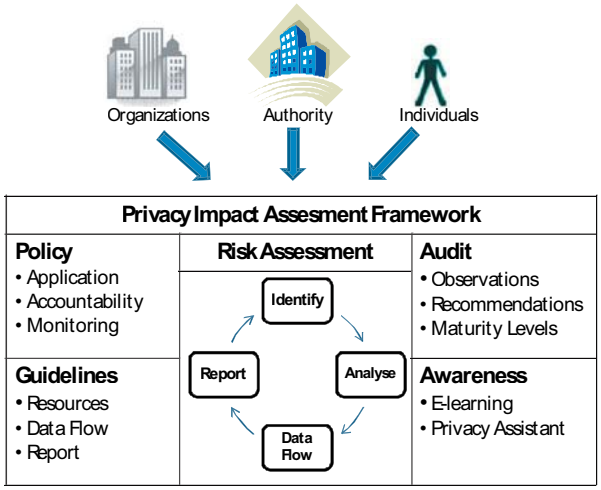


Fig. 1. Privacy Impact Assessment Framework components.

B. *Role of the Authority*

As previously defined an independent authority is responsible for the governance of data protection practices in each country. The authorities are responsible for building infrastructures to make the acts possible by preparing the supporting regulations, registry systems and the audit mechanisms. Each European Union member gives different names for this authority like, regulator, commissioner, supervisor or commissioner. For example EU, UK and Greece name their central authorities as European Data Protection Supervisor, Information Commissioner, and Data Protection Authority respectively.

The role of the authority in PIAs is establishing a framework to assess the impacts effectively and make sure that privacy issues are clearly covered by the assessment. Authority acts a consultant and program director body for organizations. During the annual risk assessment planning, each organization is expected to submit their draft plan to the authority. The authority may provide comments and recommendations to these departments. These recommendations help the organizations to decide the scope of their privacy assessment plans and to appoint necessary resources for PIAs.

Authorities are also responsible for auditing whether government organizations and agencies are giving importance to personal data privacy and assures that PIAs are conducted as planned. It may not always be possible to make on site audits in organizations but authorizes use self assessment and reporting techniques to audit such organizations.

C. *PIA Life Cycle*

Several system and methodologies are integrated to form PIA framework. The building blocks of a PIA framework as shown in Fig. 1 are policy and guideline documentation, a risk assessment life cycle, audit system and awareness program for the related parties.

The PIA policy helps to improve the awareness of privacy within government institutions. It has focuses on the potential privacy issues of a number of government programs. A PIA is a tool that helps ensure privacy protection is a core consideration when a project is planned and implemented. The whole process aims to force organizations to conduct PIA in case of new system development, integration and acquisition.

Guidelines prepared by the Authorities intend to provide instructions for completion of PIA. It includes checklists to determine whether a full PIA is required, measurement tools to identify required set of skills and expertise (security, legal, operational, and technology), and questionnaires assuring that PIA seeks for the entire Privacy Act principles.

Risk management process must include at least these key steps: [12]

1) Scope of the PIA must be determined. It must not be too wide thus it will be impractical to assess the entire system but also must not be too narrow where personal data may be out of scope. As a result of this Preliminary Privacy Impact Assessment process organizations decide conducting a full PIA. This step can be repeated if a design change takes place in the project.
2) Data flow must be analyzed. A detailed data flow diagram must be prepared covering the business processes and system architecture. The purpose of this step is to depict the personal information flows.
3) Privacy Analysis must be conducted from a risk management perspective. The privacy analysis examines the data flows in the context of applicable privacy policies and legislation. Checklists are used in this stage to identify major privacy risks and or vulnerabilities.
4) PIA report must be published. A document including the evaluation of the privacy risks, implications and possible mitigating and reducing countermeasures is published as a result.

The PIA report is designed as an effective communications tool used by a variety of stakeholders. If PIA system is a product then the individuals would be the customers of this system. Therefore result reports of PIAs must be available to the public. On the other hand, a national wide privacy protection framework can only be achieved by raising the awareness of individuals of the citizenry. Online leaning can be the most effective and economic way of an awareness program. Individuals must be able to ask to the Authority for assistance.

Periodic audits must be performed periodically to review that privacy directives are applied by organizations. Audits must assess; PIAs are done for necessary projects, risks are reported to the organizations' managers, recommended countermeasures are implemented, result reports are accurate, available and understandable for public. The Authority must be able to conduct on-site and off-site audits specific for each sectors (finance, communication, health, government, education etc.).

IV. CONCLUSION

Even though the government institutions are advised to implement PIAs, all organizations which are in the scope of the draft Turkish Data Protection Act must implement PIA methodologies in their organizations. E-Government infrastructure must also include PIA tools since it consists of multiple distributed systems and it interconnects these systems under single architecture. E-Government activities are also in planning phase in Turkey and it is expected to be in action soon. It is known that e-Government transition has an access point for the citizens called "e-gate". It includes identification, authentication and authorization functionalities and these controls enable protection of personal data. This is an international problem, thus the relationship between information security, individual privacy and service delivery is complex and dependent to a significant degree on the level of trust accorded to the public sector by the citizenry. Turkey, like all governments must address both the perceptions and realities of privacy within a broader spectrum of information and identity management that is at the core of both better client centric responsiveness externally and the corresponding need for new forms of coordination internally. There are two interrelated components in doing so: putting in place an infrastructure of reliable interoperability and ensuring mechanisms for accurate identity authentication [13].

Today, organizations are faced with many different and changing types of risk. Changes in new technologies (like Radio Frequency Identification, social networking sites, new online payment systems, etc.) must be followed very closely and new privacy risks must be added to PIA policies, guidelines and checklists by the Authority.

Personal data of public must be assessed as a valuable asset and be protected necessarily. Government agencies, universities, public bodies, financial institutions, telecom operators, hospitals, insurance companies and other private companies must implement and continue maintaining practical PIA tools and methods without waiting privacy legislations. This will increase valuation of the entire information systems in Turkey by raising confidence among individuals.

REFERENCES

[1] T. Karol, "Cross-Border Privacy Impact Assessments: An Introduction", *Information Systems Control J.*, vol. 3, 2001.
[2] *Overview of Privacy*, Privacy International, London, UK, 2005.
[3] G. Canbek, Ş. Sağıroğlu, "A Review on Information, Information Security and Security Processes", *J. of Polytechnic*, vol. 9, no. 3, pp. 165-174, 2006.
[4] C. J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Cornell University Press, 1992, pp. 48.
[5] *Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data,* Council of Europe, European Treaty Series, 1981, no. 108.
[6] Y. Çebi, O. Tahaoğlu, "Personal Data Protection in Turkey: Technical and Managerial Controls", in *Proc. First International Conference on Security of Information and Networks*, Gazimagusa, pp 220-227.
[7] Organic Law of Turkish Republic, Grand National Assembly of Turkey, Nov. 7, 1982, Available: http://www.tbmm.gov.tr/Anayasa.htm
[8] Current Draft Acts in the Commission, Ministry of Justice Official Web Page, Nov. 2, 2005, Available: http://www.kgm.adalet.gov.tr/tbmmtas.htm
[9] *Fact Sheet*, Officer of the Privacy Commissioner of Canada, Feb. 2, 2007, Available: http://www.privcom.gc.ca/fs-fi/02_05_d_33_e.asp
[10] *Canadian Privacy Act*, Department of Justice Canada, R.S., 1985, p-21.
[11] *Canadian Personal Information Protection and Electronic Documents Act*, (2000, c. 5), Department of Justice Canada, schedule.1, sec. 5.
[12] *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*, Treasury Board of Canada Secretariat, 2002.
[13] *UN e-Government Survey 2008*, United Nations, New York, 2008.

Kriptografik Modüllerin Güvenlik Gereksinimleri

Oğuz YAYLA

Özet*— Bu çalışmadaki amacımız açık anahtar altyapısında kullanılan kriptografik modüllerin FIPS PUB 140 standardı çerçevesinde sağlaması gereken minimum gereksinimlerin temel itibariyle neler olduğu ve bu gereksinimlerin standardın ilk sürümünden son sürümüne kadar nasıl değiştiğini göstermektir. Bunun yanında, hala FIPS PUB 140-1 standadına uyumlu kriptografik modül ile hizmet veren elektronik sertifika hizmet sağlayıcısının daha güncel ve üst seviyelere çıkışını kolaylaştıracak bilgileri vermektir. Ayrıca, kriptografik modül sağlayıcılarının ilgili modüllerinin yeni sürümlere onaylı hale nasıl geterebileceğine değineceğiz.

Anahtar sözcükler—**Kriptografik Modüller, Güvenlik Gereksinimleri, FIPS PUB 140**

I. GİRİŞ

Kriptografik algoritmalar ve anahtar üretme gibi önemli güvenlik işlemleri yapan donanım ve/veya yazılım bileşenlerine kriptografik modül denilmektedir. Modüller diğer bir çok güvenli kriptografik işlemler yapan bileşen gibi bir onay sürecinden geçmektedir. Bu ulusal[1] ve uluslararası[2] tebliğlerde de belirtilmiştir. Bir kriptografik modülün neden onaylanması gerektiği şu şekilde açıklanabilir:

- Onay, modülün, kabul gören güvenlik şartlarını sağladığının garantisidir.
- Onay programı ile modülün tasarım gereklerine göre en uygun güvenliği yerine getirmesi sağlanır.
- Güvenilir bir onay standardı tarafından onaylanmış kriptografik modül kullanıcılarına/müşterilerine gerekli olan güveni verecektir.

[1,2]'de belirtildiği üzere kriptografik modüller

> " *i. FIPS PUB 140–1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzerinde veya*
> *ii. CWA 14167-2'de belirtilen kriteriere uygun veya*
> *iii. CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olmalıdır.* "

Oğuz Yayla Uygulamalı Matematik Enstitüsü, Orta Doğu Teknik Üniversitesi 06531 Ankara e-posta:yayla@metu.edu.tr
Bu çalışma TÜBİTAK 105G126 Nolu proje tarafından desteklenmiştir.

şartını sağlamalıdırlar. Bu çalışmada birinci maddedeki Federal Information Processing Standards Publication(FIPS PUB) 140 standartlarını[3,4,5] inceleyeceğiz. Açıkcası, [2] 'nin yeni sürümlerinde FIPS PUB 140-1'e uygun olabilme seçeneğini kaldırılmıştır. Ancak Türkiye'de hala FIPS PUB 140-1'e uyumlu kriptografik modüller kullanılabilmektedir.

FIPS PUB 140 standartları, ana başlıkları ile, modülün doğru çalışmasını, standartlara uygunluğunu, testlerini ve güvenliğini incelemektedir. İlk sürümü 1994 yılında yayınlanmıştır. Daha sonraki sürümü 2001 yılında yayınlanmış ve daha taslak halinde olan son sürümü kullanıma açılmış ve yakın zamanda son halinin verilmesi beklenmektedir. Bu çalışmanın ikinci bölümünde bu standartın ilk sürümünün genel özelliklerini açıklayacağız. Üçüncü bölümde standartın ikinci sürümünün ilk sürümünden farklarını belirteceğiz. Dördüncü bölümde de standartın son sürümünün gerektirdiği yeni gereksinimlere değineceğiz. Beşinci bölümde ise yeni sürümlere veya seviyelere uyum sağlamak isteyen elektornik setifika hizmet sağlayıcıların ve kriptografik modül sağlayıcıların önceki bölümlerde bahsedilen farklardan yola çıkarak neler yapabileceğini belirteceğiz.

II. FIPS PUB 140-1 1994

Bu standart, bilgisayar ve haberleşme sistemlerindeki (örneğin bilgi depolama, erişim denetleme ve kimliklendirme, radyo, video, faks gibi) kriptografik modüllerin (örneğin akıllı kartlar) sağlaması gereken güvenlik gereksinimlerini tanımlamaktadır. Kriptografik modül, sağladığı kriptografik hizmete (örneğin şifreleme, kimlik doğrulama, e-imza, anahtar yönetimi gibi), kullanıldığı alana ve bulunduğu ortama göre çeşitli güvenlik gerektirmektedir; bu yüzden standart artan güvenlik seviyeleri belirtip bu seviyelerin maliyetine uygun gereksinimleri açıklamaktadır.

Bu güvenlik gereksinimleri, temelde kriptografik modülün güvenli tasarım ve uygulamasını kapsamaktadır:

- temel tasarım ve belgelendirme,
- modül ara yüzleri,
- fiziksel güvenlik,
- yazılım güvenliği,
- işletim sistemi güvenliği,
- anahtar yönetimi,
- kriptografik algoritmalar,
- elektromanyetik güvenlik ve
- testler.

Kriptografik modüller, yalnızca donanım değil, aynı zamanda yazılım, sürücü ve bunların birleşimini içermektedir.

Etkili bir güvenlik sistemi tasarlamada temel amaç sisteme yapılacak atağın sistemin kaybedeceği bilgiden daha pahalı olmasıdır.

Standardın yedi temel amacı vardır:

1. Kriptografik modülünü istenmeyen işlemlerden ve kullanımdan korumak.
2. Kriptografik modülündeki gizli bilgilerin yetkisiz kişi veya programlar tarafından açığa çıkmasını engellemek.
3. Kriptografik modülündeki yetkisiz değişiklikleri engellemek.
4. Sınıflandırılmamış bilginin korunmasında onaylı güvenlik yöntemlerini uygulamak.
5. Kriptografik modülünün işlem durumunun bilgisini sağlamak.
6. Kriptografik modülünün düzgün çalıştığından emin olmak.
7. Kriptografik modülünün işlem hatalarını algılamak ve bu hatalar yüzünden, önemli güvenlik bilgilerinin açığa çıkmasını engellemek.

Güvenlik Seviyeleri

Bu alt bölümde FIPS PUB 140-1 standartının belirlediği güvenlik seviyelerinin gereksinimlerini kısaca belirteceğiz.

Seviye 1

Kripto modülünde, FIPS onaylı kriptografik algoritmaların kullanılmasını şart koşmak gibi donanımsal güvenlikten bağımsız kişisel bilgisayar üzerinde çalışan sistemler için temel güvenlik öngörmektedir.

Gizli anahtarların yetkisizce değiştirilmesi veya açığa çıkarılması; ayrıca, açık anahtarların değiştirilmesi engellenmelidir. Eğer bu anahtarların üretilmesi modül içerisinde yapılıyorsa, FIPS onaylı üretme algoritmaları kullanılmalıdır. Üretme algoritmasında rastgele sayı üreteci kullanılmalı, gerekli testlerden (rastgelelik testleri) geçmiş olmalı ve bu üreteçteki besleme değerleri ve ara durum değerleri gizli anahtar gibi korunmalıdır. Anahtar dağıtımı onaylı elden, otomatik veya birleşimi yöntemlerle yapılmalıdır. Elden dağıtılan anahtarların modüle girilmesi veya modülden çıkışı yine elden veya elektronik yöntemlerle yapılmalıdır. Elden girilen anahtarların doğru ve ilgili kişiye girildiğinden emin olunmalıdır. Gerekirse şifreli metinin açık halini göstermemek şartıyla kısa süreli gösterimi olabilir. Elden dağıtılan gizli anahtarlar açık veya şifreli yöntemlerle modüle girilmeli veya modülden çıkarılmalıdır. Ancak elektronik dağıtılan gizli anahtarlar şifreli yöntemlerle modüle girilmeli veya modülden çıkarılmalıdır. Anahtar arşivleme yapılıyorsa şifrelenmiş arşivler tutulmalıdır.

Sistem üzerinde çalışan yazılımların detayları raporla belirtilmelidir.

İşletim sistemi yürütülür kod formatında olmalı, onaylı kimlik doğrulama tekniğini kullanmalı, aynı anda sadece bir kullanıcının modülü kullanmasına izin vermeli ve modül birden fazla hizmeti aynı anda vermemelidir.

Modül kendi kendine düzgün çalıştığını test edebilmeli ve bu test seviyesine çalıştırılır çalıştırılmaz geçebilmeli ve hemen kriptografik algoritmaların herbirinin doğru çalıştığını örneğin önceden bilenen değerlerle, yazılım ve sürücü bileşenlerinin doğru çalışabildiğini örneğin e-imza algoritmasıyla ve diğer önemli fonksiyonları kendi içlerinde test edebilmelidir.

Ayrıca, eğer modül anahtar ikililerini üretiyorsa anahtar ikililerinin uyumluluğunu örneğin şifreleme veya e-imza algoritmalarıyla, dışardan yüklenen yazılım ve sürücülerinin güvenliği testini yine örneğin e-imza algoritmasıyla, elle girilen anahtarlarda hata belirleme kodlarıyla ve rastgele sayı üreteci koşan modüller ardaşık ürettikleri rastgele sayı bloklarının farklılıklarını test edebilmeli ve geçmelidir.

Seviye 2

Seviye 1'e ilave olarak,

1. Kriptografik modüldeki fiziksel zorlama ve işlemlerin olduğunu belli edecek fiziksel güvenliği artırmaktadır.
2. Modül üzerinde işlem yapanın rolüne özgü kimlik doğrulama yapılmalıdır.
3. İşletim sistemi erişim kontrolünü sağlamalı ve önemli güvenlik bilgilerine yetkisiz erişimi engelleyebilmelidir.

Seviye 3

Seviye 2'ye ilave olarak,

1. Kriptografik modüldeki önemli gizli bilgilerin, fiziksel zorlama ve işlemlerle ulaşılmasını engelleyecek fiziksel güvenliği sağlamalıdır. Gerekirse içindeki önemli bilgileri sıfırlayabilmelidir.
2. Sistem üzerinde çalışan yazılımlarda yüksek seviye diller kullanılmalıdır.
3. Modül üzerinde işlem yapanın gerçek kimliğine özgü kimlik doğrulama yapılmalıdır.
4. Veri kablo ve yuvaları fiziksel olarak diğer kablo ve yuvalardan ayrılmalıdır. Modüle bilgi girişi ve çıkışı şifreli yapılmalıdır.
5. İşletim sistemi kriptografi yazılımına ve önemli güvenlik bilgilere sistem üzerinde çalışan diğer güvenilmeyen yazılımlar tarafından erişilmesini engellemelidir. güvenilir haberleşme yolu sağlayabilmelidir.
6. Modül çalıştırıldığında rastgele sayı üretecinin düzgün çalıştığını test edebilmelidir. Ardaşık 20000 bit için monobit, poker, runs ve long runs testlerinden geçebilmelidir. Bu testlerin ayrıntıları [3]'de verilmiştir.

Seviye 4

Seviye 3'e ilave olarak,

1. Kriptografik modülünün herhangi içine sızmaya karşı içindeki önemli bilgileri yok ederek tepki vermesini sağlamalıdır ve gerekiyorsa modül çalışmamalıdır.
2. Modülü çalışmaz hale getiren en düşük ve en yüksek arası voltaj ve -100°C ile 200°C arası sıcaklık değişimlerinde modülün güvenliğinin tehlikeye girmesini engelleyebilmelidir.

3. Sistem üzerinde çalışan yazılımların matematiksel yapıları ilk ve son koşulları ile beraber raporla belirtilmelidir.
4. Sadece onaylı işletim sistemleri üzerinde çalışılmalı, kullanılan işletim sistemi doğru işleyebildiğinin güvenliğini sağlayabilmelidir.

III. FIPS PUB 140-2 2001

Kriptografik modül onay programı standarda eklenmiştir. Bu program modülün bu ve diğer kriptografik standartlara uygunluğunu onaylamaktadır.

Müşterek Ölçütler (Common Criteria) EAL 2/3/4, sırasıyla seviye 2/3/4'e eklenmiştir.

"*Önemli bilginin korunması için onaylı güvenlik işlemleri doğru bir şekilde uygulanmak ve çalıştırmak*" amacı standardın amaçları arasına eklenmiştir.

İşletim Sistemi Güvenliği (Operating System Security) başlığı İşlemsel Çevre Güvenliği (Operational Environment Security) ile, Yazılım başlığı Tasarım ile ve Çevresel Etkiler başlığı Fiziksel Etkiler ile değiştirilmiştir; ancak, içerdikleri güvenlik gereksinimleri benzer tutulmuştur.

Kriptografik algoritmalar, kriptografik modül özellikleri altında verilmiştir.

Belgelendirmeye daha fazla önem verilmiş ve her türlü ayrıntının belgesini onay almak için istenmektedir.

140-1'de modül üzerinde işlem yapmak için kimlik doğrulama ve bunun için de PIN, parola, biyometrik gibi mekanizmalar kullanılıyordu. Ayrıca, 140-2'de 10^{-6} olasılıkla rastgele kimlik doğrulayabilme olabileceğini belirtmiştir. Dakikadaki çoklu erişim için daha yüksek bir olasılık (10^{-5}) da belirtilmiş. Ayrıca, açık parola girilmemesi gibi kimlik doğrulama geri beslemesi de açık olmamalıdır.

Rastgele sayı üretecinin güvenlik seviyesi kriptografik algoritmalarla aynı seviyeye çıkarılmıştır.

Modül içerisindeki herhangi bir servisin durması halinde sistemin dışarıya istenmeyen bir bilgi verip vermeyeceğini test eden by-pass testi eklenmiştir.

Modülün hem kullanıcı hem de yönetici yardım belgelerinin olması gerektiği eklenmiştir.

IV. FIPS PUB 140-3 2008

140-3'de rastgele kimlik doğrulayabilme olasılığı 10^{-6}'dan 10^{-8}'e indirilmiştir. Dakikadaki çoklu erişim için ise 10^{-5}'den 10^{-7}'e indirilmiştir. Parola uzunluğu üzerinde kısıtlama olması ve basit parolaların kullanılmasının da engellemesi istenmiştir. Ayrıca, doğrulamada geri besleme yapılmaması önerilmiştir.

Her türlü geçici önemli güvenlik bilgisi, parolaların özeti ve test anahtarları da sıfırlanmalı ve geri dönüş olmamalıdır.

Ayrıca güvenlik seviyelerinde 140-2'ye ek olarak şunlar ilave edilmiştir:

1. Seviye 3'deki kriptografik modül
   a. Önemli kriptografik bilgilerini zaman ölçümü atağına karşı koruyabilmelidir.
   b. Üzerinde çalışılan işletim sistemi, kullanıcıları, kripto yazılımını ve güvenlik bilgilerini değiştirebilmesini engelleyebilmeli ve işlemlerini denetleyebilmelidir. Güvenlik verileriyle güvenilir bir kanal üzerinden haberleşmelidir ve bunları denetleyebilmelidir. Ayrıca, işletim sistemi uzaktan yönetime izin vermemelidir.
2. Seviye 4'deki kriptografik modül
   a. İki seviyeli kimlik doğrulamasıyla işlem yapanı denetleyebilmelidir: gizli parola, fiziksel anahtar/token veya biyolojik özellik(biyometrik).
   b. Önemli güvenlik bilgileri basit ve değişmeli güç ölçüm ataklarına karşı koruyabilmelidir. Ayrıca, modül kullanılmıyorken bile içerisindeki önemli güvenlik bilgilerinin dışa çıkmasını engellemek için bu bilgileri şifrelemeli ve erişim kontrolü sağlamalıdır.

140-3'de yeni bir güvenlik seviyesi tanımlanmıştır:

Seviye 5:

Bu seviyedeki bir modül, seviye 4'e ilave olarak modül kullanılmıyorken bile içerisindeki bütün güvenlik bilgilerinin dışa çıkmasını engellemek için bu bilgileri şifrelemeli ve erişim kontrolü sağlamalıdır.

Sıcaklık ve voltaj dalgalanmalarında hatalara karşı dayanıklı olmalıdır. Görünmez radyasyona karşı dayanıklı olmalıdır. Ayrıca, fiziksel mukavemet algılayıcı ve sıfırlama devrelerinin işlemez hale getirilmesine karşı korunaklı olmalıdır. Sıfırlama gerektiğinde, içindeki bütün güvenlik bilgilerini sıfırlamalıdır.

V. TAVSİYELER

Bölüm III ve IV'den anlaşılacağı üzere standartın güncel sürümlerinin bir önceki sürümünden çok fazla farklılıkları yoktur. Ancak, dikkat edilmesi gereken "FIPS Onaylı algoritmaların" sürekli değişim ve gelişim içinde olmasıdır. Simetrik kriptosistemlerinde DES[6]'ten AES[7] veya TDES[8]'e geçilmesi zorunlu hale gelmiştir. Yine simetrik kriptografide kullanılan şifreleme modları değiştirilmiştir[9]. Açık anahtarlı kriptosistemlerde ise RSA'nın Bleichenbacher'ın geliştirdiği ataklara açık olduğu anlaşılmış ve 2002 yılında RSA'nın uygulama yöntemi değiştirilmiştir[10]. Ayrıca, 2009 yılından itibaren en az 2048 bit açık anahtar uzunluğu kullanılacaktır[13]. Diğer e-imza sistemlerinden, DSA sisteminin kullandığı değerlerin nasıl üretileceği detaylandırılmıştır[11]. EDSA sisteminin ise nasıl uygulanacağı ilk kez detaylı halde açıklanmıştır[11]. Ayrıca, aynı standartın güncel sürümü[12] taslak halinde olmasına rağmen yaklaşık iki yıldır yorumlara ve tavsiyelere açıktır. Geliştirilecek RSA/DSA/EDSA e-imza sistemlerinin, bu taslak da göz önüne alınarak geliştirilmesinde gelecek uygulamalar için faydalı olacağı kaçınılmazdır. Özetleme algoritması MD5 kullanımdan tamamen kaldırılmış ve 2011 yılından itibaren en çok kullanılan SHA-1 özetleme algoritması da kullanımdan kaldırılacaktır[13]. Yerlerine SHA-256/SHA-384 veya yeni bir algoritma kullanılacaktır. Rastgele sayı üreteci için kararlı yöntemlerin önemli bilgilerin korunması işlemlerinde kullanılması önerilmiştir[14].

Dolayısıyla, elektronik sertifika hizmet sağlayıcı veya kriptografik modül sağlayıcı temel anlamda modül üzerinde işlem yapmak için kimlik doğrulama verisini (PIN vb.) en az sekiz basamaklı tanımlarsa, modül içerisinde kullanılan rastgele sayı üreteçlerini [15]'de belirtilen yöntemlere göre tanımlarsa ve güncel kriptografik algoritmalarını (AES, RSAPSS, SHA256 vb.) da tanımlarsa modülün güncel sürümlere; hatta üst seviyelere uygun olmasını sağlamış olur.

VI. SONUÇ

Bu çalışmada kriptografik modüllerin güvenlik gereksinimleri FIPS PUB 140 standardına göre verilmiştir. Yeni nesil kriptografik modüllerin daha fazla anahtar boyu ve daha dayanıklı kriptografik algoritmalar ile son kullanıcıya daha uygun güvenlik çözümleri sunacağı anlaşılmaktadır. Çalışmanın bütününü bozmamak için kriptografik algoritmalarda(DES, RSA, DSA, SHA-1, rasgele sayı üreteçleri vb) olan değişiklikler detaylı verilememiştir. Ancak, böyle bir çalışmanın bu çalışmanın devamı olabileceği görülmektedir.

VII. TEŞEKKÜR

Bu çalışmanın şekillenmesinde büyük katkıları olan TÜBİTAK 105G126 nolu projedeki yöneticilerime ve arkadaşlarıma teşekkür ederim.

KAYNAKLAR

[1] Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ T.C. Telekomünikasyon Kurumu 06.01.2005.
[2] ETSI TS 101 456 V1.4.1 Electronic Signatures and Infrastructures 2006
[3] Federal Information Processing Standards Publication Securıty Requırements For Cryptographıc Modules 1994
[4] Federal Information Processing Standards Publication Securıty Requırements For Cryptographıc Modules 2001
[5] Federal Information Processing Standards Publication Securıty Requırements For Cryptographıc Modules DRAFT 2008
[6] National Institute of Standards and Technology, Data Encryption Standard (DES), Federal Information Processing Standards Publication 46-3, October 25, 1999.
[7] National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001
[8] National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004.
[9] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001.
[10] RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard, June 14, 2002.
[11] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2 with Change Notice 1, October 05, 2001.
[12] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-3 DRAFT March, 2006.
[13] National Institute of Standards and Technology, Cryptographic Algorithms and Key Sizes for Personal Identity Special Publication 800 -78-1, August 2007.
[14] National Institute of Standards and Technology, Annex C: Approved Random Number Generators for FIPS 140-2, Security Requirements for Cryptographic Modules, March 17, 2003.
[15] National Institute of Standards and Technology, Special Publication 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006.

Siber Savunma: Ülkeler ve Stratejiler

Mehmet MERAL

***Özet*-1980'lerde bilgisayarların birbirleriyle iletişim kurmasıyla başlayan siber mekan kavramı muazzam bir gelişme kaydetmiştir. İnternet yakın zamana kadar bireyler ve iş çevreleri tarafından önem verilen ancak ulusal güvenlik veçhesi olmayan bir olgu olmakla birlikte, son zamanlarda milyarlarca internet kullanıcısı tarafından oluşturulan bu siber mekan güvenlik açısından etkin bir şekilde kontrol edilememektedir. Bu nedenle siber-savunma, siber-güvenlik, siber-saldırılar gibi kavramlar ulusal güvenlik bakımından önem arzetmeye başlamıştır. Bu çalışmada önde gelen ülkelerin siber savunma alanında yaptığı çalışmalar ve siber saldırılara karşı uyguladıkları stratejiler tanıtılmıştır.**

***Anahtar kelimeler*- Siber savunma, siber güvenlik, siber saldırı, strateji**

I. GİRİŞ

Siber bilişim yapılarının bankacılık, ulaşım, iletişim gibi temel alanlardaki ağırlığı, bu yapıların ve bu yapılarda saklanan bilgilerin güvenlik boyutunu konunun ayrılmaz bir parçası hailne getirmiştir. Küreselleşme ve bilgi teknolojilerinin yayılmasıyla birlikte özellikle düşük maliyetli olması, çok sayıda insan üzerine etki edebilmesi gibi nedenlerle siber saldırıların aynı zamanda teröristlerce artan bir şekilde tercih edildiği görülmektedir. Uzmanlar siber-güvenlik konusunda "uluslararası işbirliği, ulusal bilinçlenme ve bireysel bilinçlenmenin" elzem olduğunu ifade etmektedirler. NATO gibi uluslararası kuruluşlar siber-güvenliğe ilişkin ulusal sorumluluklara büyük önem vermektedir. Bu büyük tehiditlerin farkında olan gelişmiş ülkeler ise ulusal anlamda yaptıkları örgütlenmelerle siber savunmaya yönelik yasal düzelemeler, strateji belgeleri ve eylem planları hazırlayarak olası bir siber saldırı, siber savaş durumuna karşı hazırlıklı olmak için ulusal önlemler ve uluslararası işbirliği temelinde önemli adımlar atmışlardır.

Bu çalışmanın ikinci bölümünde konuyla ilgili tanımlar verilmiş, üçüncü bölümünde gelimiş ülkelerde siber savunma bağlanımda yaplan çalışmalar tanıtılmış, dördüncü bölümünde ise genel bir değerledirme sunulmuştur.

MEHMET MERAL, Dışişleri Bakanlığı 06100 Balgat Ankara (e-mail: mehmet.meral@mfa.gov.tr)

II. TANIMLAR: SİBER MEKAN, SİBER TERÖRİZM, SİBER SAVUNMA

Siber mekan: Network sistemleri ve ilgili fiziksel alt yapıyla bilgi depolamak, değiştirmek için kullanılan elektronik ve elektromağnetik ortamdır.

Siber terörizm: Bilgisayarlara ve içlerinde depolanan bilgilere karşı siyasi, sosyal veya ekonomik amaçlarla girişilen kanunsuz saldırılar veya saldırı tehditlerdir.

Siber savunma: Siber mekanı siber saldırılara ve siber terörizme karşı korumak için uygulanan güvenilk yöntemleridir.

III. DÜNYA ÜLKELERİ VE SİBER SAVUNMA STRATEJİLERİ

A. NATO

NATO, 21. yüzyılda dönüşüm sürecinde güvenliğe ilişkin hususlara büyük önem vermektedir. Enerji güvenliği ve siber güvenlik gibi yeni küresel tehditlere karşı NATO üyeler bağlamında savunma stratejileri geliştirmektedir. 2005 yılında Estonya ve Rusya arasında yaşanan gerginlikten sonra ise NATO Estonya'da Siber Savunma Mükemmelliyet Merkezi kurmuş, faaliyetlerini bu organizasyon çerçevesinde yürütmektedir. 2007 yılında hazırlanmaya başlayan Siber Savunma Siyasası ise taslak halinde olup henüz üzerinde mutabakat sağlanmamıştır.

B. ABD

ABD'nin siber savunma alanındaki faaliyetlerine ilişkin temel belgeyi Şubat 2003 tarihli "The National Strategy to Secure Cyberspace" oluşturmaktadır. Federal Yönetim, yerel makamlar ile özel sektörü içermesi nedeniyle ulusal nitelikte ve geniş kapsamlı olan anılan belgede, kendi görev alanları itibarıyla öncü rol üstlenecek devlet kurumları da belirtilmektedir. Bu çerçevede, örneğin bankacılık sektörü için Hazine Bakanlığı, elektrik ve gaz şebekeleri için de Enerji Bakanlığı esas makam olarak gösterilmektedir. Bahsekonu strateji belgesinin, "National Strategy for Homeland Security" belgesinin uygulama boyutunu oluşturduğu ve "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" belgesini tamamlayıcı nitelikte olduğu belirtilmektedir.

Gerek anılan belge gerek 17 Aralık 2003 tarihli İç Güvenliğe ilişkin Başkanlık Direktifi uyarınca, İç Güvenlik Bakanlığına (Department of Homeland Security) siber savunma konusuda önemli sorumluluklar verildiği anlaşılmaktadır.

C. ALMANYA

Almanya'nın elektronik ortamda gerçekleştirilebilecek saldırılara karşı almakta olduğu önlemler Federal İçişleri Bakanlığı tarafından hazırlanan "Enformasyon Altyapı Savunması İçin Ulusal Plan" başlıklı belgede tanımlanmıştır. Alman makamları, elektronik saldırıların başlıca hedefini büyük şirketler, bankalar veya kamu kuruluşları olarak tanımlamışlardır. Ulusal Plan'ın uygulanmasının koordinasyonu, "Enformasyon Güvenliğinden Sorumlu Federal Ofis" (BSI) tarafından yürütülmektedir. Bu saldırılara karşı koyabilmek için Federal Hükümet, Ulusal Plan'da üç stratejik hedef belirlemiştir:

1. Önleme: Bu başlık altında, enformasyon altyapısının, güncel ve güvenli teknoloji ürünlerinin kullanımı ve mevcut risklerlerin bilinciyle uygun şekilde korunması öngörülmektedir.
2. Hazırlıklı olma: Meydana gelebilecek elektronik saldırılara etkin şekilde karşı koyabilmek için BSI bünyesinde Enformasyon Teknolojisi Kriz Müdahale Merkezi tesis edilmesi planlanmakta, bu merkezin ulusal komuta, kontrol ve analiz merkezi görevlerini üstlenmesi ve bu amaçla bir algılayıcı ağı kurulması hedeflenmektedir. Aynı şekilde, Federal Hükümet, halkın ve özel sektörün mevcut riskler ve alınabilecek önlemler hakkında bilinçlendirilmesini hedeflemektedir.
3. Sürdürülebilirlik: Bu başlık altında, Almanya'nın elektronik güvenlik alanında yeterliliğinin artırılması amaçlanmaktadır.

Sözkonusu belgenin uygulanmasında gerekli önlemlerin Federal Hükümet tarafından alınması öngörülmektedir. Bununla beraber, uygulamaların sadece yetkili makamlar tarafından yerine getirilmesinin yeterli olmayacağı gerçeğiyle özel kuruluşlarla işbirliği hedeflenmektedir. Bahsekonu belgede, özel kullanıcıların da mevcut risklerin bilincinde olmalarının ve gerekli bireysel önlemlerin alınmasının önemine dikkat çekilmekte, öte yandan ülkelerarası işbirliğine de vurgu yapılarak, Almanya'nın uluslararası standartların ve normların tesis edilmesini savunduğu kaydedilmektedir.

D. DANİMARKA

Danimarka'da sanal alemden gerçekleştirilen saldırılara karşı koymakla görevli tek bir otorite bulunmamakta, görev ve yetki;

- Danimarka İstihbarat ve Güvenlik Servisi (PET),
- Savunma Bakanlığı'na bağlı Danimarka Kriz Yönetim Makamı (DEMA),
- Bilim, Teknoloji ve Yenilik Bakanlığı'na bağlı Danimarka Ulusal Bilgi Teknolojileri ve Telekomünikasyon Kurumu (ITST) ve
- Bağımsız idari otorite statüsünde bulunan ve teknoloji ile ilgili konularda, parlamento ile kamu kurumlarını bilgilendirmekle görevli Danimarka Teknoloji Kurulu arasında paylaştırılmış durumdadır.

Danimarka Teknoloji Kurulu himayesinde "IT- security Beyond Borders" adıyla kurulan bir çalışma grubunca 2007'de sınırı aşan bilgi teknolojileri güvenliği meselelerine dair bir rapor yayımlanmıştır. Raporda, bu alanda uluslararası yardımlaşmanın önemine ve somut adımlar atılması gerektiğine özel vurgu yapıldığı anlaşılmaktadır.

Danimarka İstihbarat Servisi konuya dair kamu kurum ve kuruluşlarına rehberlik ve yardım hizmetlerinde bulunmakta, yine korunmasında kamu yararı bulunan bilgileri haiz kişilere de gerekli yardımları yapmaktadır. Öte yandan, son yıllarda elektronik verilerin depolanması ve iletilmesindeki artışın sonucu olarak PET bünyesinde bilgi teknolojileri güvenliği kısımı (IT security section) tesis edilmiştir. Bu bağlamda PET ulusal ve uluslararası makamlarla (istihbarat makamları dahil) işbirliği halinde faaliyetler yürütmektedir.

E. FİNLANDİYA

Finlandiya'da elektronik ortamdaki saldırılara karşı savunma konusunda yetkili makam Fin İletişim Düzenleme Kurulu (Finnish Communications Regularity Authority)'dur. Elektronik ortamdaki saldırılarla mücadele dahil olmak üzere, bilgi güvenliğinin sağlanması için önlemler alınması ve bilgi güvenlik durumunun geliştirilmesinde yetkili ve sorumlu en üst makam Hükümet'tir. Hükümet, Eylül 2003'te Ulusal Bilgi Güvenliği Stratejisi hakkında kararı kabul etmiştir. Sözkonusu stratejinin desteklenmesi ve kaydedilen gelişmelerin gözetimi, Ulusal Bilgi Güvenliği Danışma Kurulu (National Information Security Advisory Board) tarafından 2007 yılı başlarına kadar yerine getirilmiştir. Anılan Kurul'un 2004 yılında Hükümet'e sunduğu "Creating a Safer Information Society" başlıklı raporunu sunmştur.

Bilgi güvenliğinin sağlanması için 2008 yılında Bakanlıklararası bir çalışma yapılarak yeni bir strateji belgesi hazırlanmaktadır. Bu çalışmayı "Ubiquitous Information Society Advisory Board" (Geniş Bilgi Toplumu Danışma Kurulu) altında kurulan yeni bir bilgi güvenliği grubu yerine getirmektedir.

Olağan durumlarda, bilgi güvenliğinin sağlanması ve bu konuda yapılacak düzenlemelere öncülük edilmesi, Ulaştırma ve İletişim Bakanlığı, sözkonusu Bakanlığa bağlı Fin İletişim Düzenleme Kurulu ve Ekonomi ve İstihdam Bakanlığı tarafından gerçekleştirilmektedir. Kamu sektöründe bilgi güvenliğinin geliştirilmesi ise, temel olarak Maliye Bakanlığı ile İçişleri Bakanlığı'nın sorumluluğundadır. Ulaştırma ve İletişim Bakanlığı, iletişim hizmetlerinde bilgi güvenliğiyle ilgili mevzuat ve strateji geliştirmeden sorumludur. Anılan Bakanlık, bu çerçevede, Fin halkına, iş dünyası ve kamu sektörüne bilgi toplumunda sunulan tüm hizmetlerin kullanılabilirliği ve güvenliğini, ayrıca özel bilgilerin korunmasını sağlamakla yükümlüdür.

CERT-FI, Fin İletişim Düzenleme Kurulu'nun bilgi güvenliği ihlalleri ve bu ihlallerin önlenmesi konularında yetkili birimidir.

F. FRANSA

Fransa'da elektronik ortamda gerçekleştirilebilecek suç ve saldırılarla mücadeleden sorumlu tek bir birim bulunmamakta; suçun niteliğine göre farklı birimlere sorumluluk verilmektedir. Bunlar arasında en önemlileri

- Başbakanlığa bağlı Milli Savunma Genel Sekreterliği
- İçişleri Bakanlığı'nın Adli Polis birimine bağlı olarak faaliyet gösteren "Bilişim Teknolojileri ile İlgili Suçlarla Mücadele Dairesi" - Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information de la Communication (OCLCTIC) dir.

Yukarıda kayıtlı iki kurumun dışında, Ekonomi, Maliye ve Çalışma Bakanlığı'na bağlı Telekom idaresi, Adalet Bakanlığı ve Jandarma Kuvvetlerinin de siber suçlarla mücadelede görevleri bulunmaktadır. Siber suçlar, Ceza Kanunu'nun (Code Pénal) 226. ve 323. maddeleri çerçevesinde cezalandırılmaktadır. Posta ve Elektronik Haberleşme Kanunu (Code des Postes et des Communications Electroniques) ise, siber haberleşme alanına bazı düzenlemeler getirmektedir.

G. GÜNEY KORE

İnternet kullanımının son derece yaygın olduğu Güney Kore'de elektronik ortamdaki saldırılara karşı savunma, farklı yönleriyle farklı kuruluşları ilgilendirmektedir. Toplantılarını Cumhurbaşkanı başkanlığında gerçekleştiren ve Cumhurbaşkanına iç ve dış politika ile askeri konuların ulusal güvenlik boyutu hakkında bilgi vermekten sorumlu olan "Ulusal Güvenlik Konseyi"nin sekreteryası, ulusal kriz uyarı sisteminin işleyişi ve geliştirilmesi, ulusal kriz durumlarına ilişkin bilgilerin toplanması, özetlenmesi ve dağıtılması ile siber tehdit uyarısı yayınlanmasından da sorumludur. "Ulusal Güvenlik Konseyi" bünyesinde yer alan "Ulusal Siber Güvenlik Strateji Konseyi" (National Cyber Security Strategic Council) ise ulusal siber güvenlik sisteminin kurulması ve geliştirilmesi, siber güvenlik politikaları ve çeşitli kuruluşlar arasında eşgüdümün sağlanması ve Cumhurbaşkanının siber güvenliğe yönelik kararlarının uygulanmasından sorumludur. Güney Kore Ulusal İstihbarat Servisinin başkanı aynı zamanda bu Konseyin de başkanıdır.

"Ulusal Siber Güvenlik Strateji Konseyi"nin altında, "Ulusal Siber Güvenlik Konseyi" (National Cyber Security Council) yer almaktadır. Siber güvenliğin sağlanması ve "Ulusal Siber Güvenlik Strateji Konseyi" tarafından alınan kararların uygulanması "Ulusal Siber Güvenlik Konseyi"nin görev alanına girmektedir. Konseyin başkanlığını, Güney Kore Ulusal İstihbarat Servisinin başkan yardımcısı yapmaktadır. Konsey, "Ulusal Güvenlik Konseyi Kriz Yönetim Merkezi" (NSC Crisis Management Center) Müdürü, "Ulusal Siber Güvenlik Merkezi" (National Cyber Security Center) Müdürü, Savunma Bakanlığı Enformasyon Dairesi Genel Müdürü ile Enformasyon ve Haberleşme Bakanlığı Enformasyon Planlama Yetkilisinden oluşmaktadır.

Elektronik ortamdaki saldırılara karşı savunma politikalarının hayata geçirilmesinden özel sektörü ilgilendiren konularda Enformasyon ve Haberleşme Bakanlığı bünyesindeki "Kore Enformasyon Güvenlik Ajansı"na (Korea Information Security Agency) bağlı "Kore Internet Güvenlik Merkezi" (Korea Internet Security Center); ülke savunmasını ilgilendiren konularda Savunma Bakanlığına bağlı "Enformasyon Savaş Müdahale Merkezi"(Information Warfare Response Center), ulusal güvenliği ve kamu sektörünü ilgilendiren konularda ise Ulusal İstihbarat Servisine bağlı "Ulusal Siber Güvenlik Merkezi" (National Cyber Security Center) sorumludur. Ayrıca, Güney Kore ulusal polis teşkilatı bünyesinde de "Siber Terör Müdahale Merkezi" (Cyber Terror Response Center) bulunmaktadır.

H. İNGİLTERE

İngiltere'deki uygulamada, elektronik ortamdaki saldırılara karşı savunma konusu "bilgi güvenliği" (information assurance) kapsamında ele alınmaktadır. Bilgi güvenliği konusundaki çalışmalar, teknolojik gelişmelere paralel olarak İngiltere'de 1999 yılından sonra ağırlık kazanmıştır. Kamu ve özel sektörün bu kapsamdaki ihtiyaçlarının karşılanması amacıyla üçlü bir yapı tesis edilmiştir.

Başbakanlık ofisine (cabinet office) bağlı olarak görev yapan "Central Sponsor for Information Assurance", "cyber defense" konusunda politika, strateji ve siyasa geliştirme çalışmalarını yürütmektedir. Hazırlanan sözkonusu politikaların uygulamasından ise "Center for Protection of National Infrastructure" (CPNI) ve "The Communications-Electronics Security Group" (CESG) sorumludur.

CPNI özel sektör ve iş çevrelerinin, CESG ise kamu kuruluşlarının bu alandaki ihtiyaçlarının karşılanmasında rol almakta, elektronik altyapı ve bilgi ağlarına yönelik olarak gerçekleştirilebilecek saldırılar konusunda ilgili kurumlara tavsiyelerde bulunmaktadır. Bu iki kuruluş, hükümetin bilgi güvenliği genel stratejisinin uygulanmasının genel gözetimini gerçekleştirmekte ve bilgisayar ağlarına ve elektronik ortamdaki işlemlere karşı olabilecek saldırılar konusunda erken uyarı işlevi görmektedir. Elektronik ortamdaki bilgi, belge ve işlemlerin güvenliğinin sağlanması amacıyla IT çözümleri geliştirilmesinin, temelde her bir kamu veya özel sektör kuruluşunun kendi sorumluluğunda olduğu kabul edilmektedir. Bu alanda önleyici işlev gören yazılım ve donanımların serbest piyasa koşullarında bu kuruluşlar tarafından temin edilmesi beklenmektedir.

Bu alandaki çalışmaların koordine edilebilmesi amacıyla "Chief Information Officer's Council" (CIOC) kurulmuş olup, ayda bir düzenli olarak toplanan sözkonusu Konsey'e CPNI ve CESG'e ilaveten silahlı kuvvetler ve istihbarat servisinin ilgili birimleri katılmaktadır. Buna ilaveten, daha kapsamlı eşgüdüm ihtiyacının karşılanması için "Information Assurance Policy and Programme Board" (IAPPB) ihdas edilmiştir. Kamu ve özel sektörle ilgili bilgi güvenliği politikası uygulamalarının ele alındığı sözkonusu Kurul, üç ayda bir toplanmakta ve toplantılara CIOC'a ilaveten Savunma Bakanlığı, Dışişleri Bakanlığı ve İş,

Girişim ve Reform Düzenlemeleri Bakanlığı'ndan yetkililer iştirak etmektedir.

Bilgi güvenliği konusunda İngiltere'de üç temel belge yürürlüktedir. Bunlardan "Transformational Government Agenda", çeşitli kamu kuruluşlarında görevli üst düzey IT uzmanlarından oluşan "Chief Information Officers' Council" ve teknolojik dönüşüm faaliyetlerinden kamu sektörünün azami ölçüde yararlanmasını sağlamakla yükümlü devlet görevlilerinden müteşekkil "Service Transformation Board" tarafından 2005 yılında dönemin Başbakanı Tony Blair'in talimatı üzerine hazırlanmıştır. Sözkonusu belge doğrudan bilgi güvenliğiyle bağlantılı olmayıp, İngiliz vatandaşlarının devlet kurumlarıyla gerçekleştireceği işlemlerde teknolojik imkanlardan azami ölçüde yararlanılmasını hedeflemekte ve bu amaçla gerçekleştirilecek çalışmaların esaslarını belirlemektedir. Bu çerçevede, bilgi güvenliği konusuna da değinilmektedir.

Bu alandaki çalışmalara ışık tutmak üzere ilk defa 2003 yılında hazırlanan rehber belge ise "Ulusal Bilgi Güvenliği Stratejisi"dir. Geçtiğimiz yıl tekonolojik gelişmeler ve bu kapsamdaki yeni ihtiyaçlar çerçevesinde güncellenen örneği ekli belgeyle, hükümet ve kamuoyunun çıkarlarını yakında ilgilendiren elektronik ortamda bilgi güvenliğinin sağlanması konusuna ilişkin genel ilkeler ve bu alanda İngiltere'de uygulamaya konulacak kurumsal yapı tespit olunmaktadır.

"Information Assurance Governance Framework" başlıklı belgede ise, bilgi güvenliğinin sağlanmasına riayet edilecek ulusal standartlar ve bu sorumluluğun ilgili kurumlar bünyesinde nasıl paylaştırılacağı ortaya konulmaktadır. Buna göre, İngiltere'de bilgi güvenliği alanındaki sorumluluk dağılımı şu şekildedir.

Kabine Sekreteri (Bakan düzeyinde) Edward Miliband: Başbakana karşı sorumludur. Bakanlık Müsteşarı (Permanent Secretary): Kabine Sekreterine karşı sorumludur.

Kıdemli Bilgi Riski Yetkilisi (Senior Information Risk Owner): Her bir kamu kuruluşunda yürütülen bilgi güvenliği çalışmalarından sorumlu üst düzey yetkilidir. Bakanlık Müsteşarına karşı sorumludur.

Bakanlık Güvenlik Yetkilisi (Departmental Security Officer): Kamu kuruluşları bünyesinde bilgi güvenliği politikası ve rehber ilkelerinin uygulanmasını gözetmek, meydana gelebilecek saldırıları rapor etmek ve araştırmakla yükümlüdür. Kıdemli Bilgi Riski Yetkilisine karşı sorumludur.

IT Güvenlik Yetkilisi (IT Security Officer): Bakanlık Güvenlik Yetkilisine yardımcı olmak üzere atanabilir.

I. İSVİÇRE

İsviçre'de elektronik ortamdaki tehdit unsurlarına karşı kontrol ve mücadele, türlerine göre farklı kurumlarca yürütülmektedir. Devlet kurumları, kamu kuruluşları ve ulusal güvenliği alakadar eden bilişim atakları ile mücadele hususunda görevli olan birim Federal Analiz ve Önleme Dairesi'dir ve bu kuruluş (DAP) sivil ve askeri istihbarat kapasitelerinden yararlanmaktadır. Federal İnternet Suçları ile Mücadele Koordinasyon Dairesi (CYCO) koordinasyonunda faaliyet gösteren Federal Polis Teşkilatı, elektronik ortamdaki bireysel ve örgütsel tehdit unsurlarının araştırması, takibi ve ele geçirilmesi çalışmalarını yürütmektedir.

İş dünyası ile münferit internet kullanıcılarının elektronik ortamdaki saldırılara karşı korunması, bilgilendirilmesi, olası saldırıların algılanıp karşı önlemlerin alınması ile yasal ve idari düzenlemelerin yapılması hususlarında Bilgi Güvenliği Analiz ve Bildirim Servisi (MELANI) sürekli araştırmalar yapmakta, gelen ihbarları ilgili birimlere yönlendirmekte ve yılda iki kez, ülke içi ve uluslararası internet güvenliği durum raporu düzenleyerek kamuoyunun bilgisine sunmaktadır.

İsviçre Hükümeti 1 Ekim 2004 tarihinden beri MELANİ servisini İsviçre'nin özellikle iletişim ve veri toplama hususundaki hassas kurumlarını korumak ile görevlendirmiş ve önlemler hususunda Zürih ETH üniversitesi ile müşterek çalışılmasını sağlamıştır.

Uluslararası elektronik ortam saldırıları tehditi ile mücadele konseptinde uluslararası işbirliğine ve özellikle ek değişiklik protokolünün yürürlüğe girmesinin ardından bu hususta etkinlik kazanan EUROPOL teşkilatı ile eşgüdüm içinde çalışılmasına önem verilmektedir.

Elektronik ortamdaki saldırılara karşı icra edilen faaliyetlerin konsept ve stratejisini saptayan üs kurulun adı Federal Enformasyon Stratejisi Kurumu ISB' dir.

İnternet sayfalarındaki güvenlik boşlukları, işletim sistemlerindeki zayıf noktaların tehlike arz etmemesi için hazırlanan güvenlik yamaları bir liste halinde Bilgi Güvenliği Analiz ve Bildirim Servisi (MELANI) web sitesinde yayınlanmakta, söz konusu yamalar buradan indirilerek bilgisayarlar daha güvenli hale getirilmektedir. Aynı şekilde internette yayınlanan ve şüpheli görülen web siteleri bu kuruma ihbar edildiğinde sayfa araştırılmakta ve sonucu halka duyurulmaktadır.

İ. İTALYA

İtalya'da Telekomünikasyon ve Bilgi İşlem sistemlerini kapsayan konular Telekomünikasyon Bakanlığı ile Yenilikler ve Teknoloji Bakanlığının yetki alanlarına girmektedir. Bu cihetle, telekomünikasyon ve bilgi işlem sistemleriyle ilgili ulusal kanunlar ve AB mevzuatı çerçevesinde Yenilikler ve Teknoloji Bakanlığı, Telekomünikasyon Bakanlığının mutabakatıyla, 16 Ocak 2002 tarihinde bir kararname yayımlayarak Kamu Sektörünün elektronik ortamlarda savunulması için Ulusal Güvenlik Komitesi kurulmasına karar vermiştir.

Sözkonusu iki Bakanlık 24 Temmuz 2002'de imzalanan müşterek bir kararname ile bahsekonu Ulusal Güvenlik Komitesi aracılığıyla uluslararası güvenlik standartlarına uyum ve risklere karşı konulması gibi gereksinimleri yanıtlayacak bilgi işlem ve telekomünikasyon güvenlik planları oluşturulmasında müşterek programlar izlenmesi konusunda da mutabık kalmışlardır. Yenilikler ve Teknoloji Bakanlığı ile ilintili sözkonusu komite beş kişiden oluşmaktadır. Başkan ve bir üye Telekomünikasyon Bakanlığı, diğer üç üye ise Yenilikler ve Teknoloji Bakanlığınca atanmaktadır.

Komitenin belli başlı görevleri arasında bilgi işlem güvenlik sistemlerinin uluslararası standartlara uyması için

proje ve öneriler hazırlamak, kamu kurumlarında güvenlik sistemlerinin oluşturulması için programlar oluşturmak, yapılan çalışmaları değerlendirmek ve gerektiği hallerde uyarılarda bulunmak, kamu personelinin güvenlik konusunda eğitimi için programlar hazırlamak gibi hususlar yer almaktadır. Komite her dört ayda bir yaptığı çalışmalara ve elde edilen somut neticelere ait bir rapor hazırlar ve bunları Telekomünikasyon Bakanlığına ve Yenilikler ve Teknoloji Bakanlığına göndermektedir.

Sözkonusu kararname kapsamında tüm kamu kuruluşları kendi bünyelerinde bilgi işlem güvenliği için bir birim oluşturmakla yükümlü kılınmışlardır. Komite ayrıca, "Computer Emergency Response Team" adlı bir birim oluşturmuştur. Sözkonusu birim içerisinde bilgi işlem hataları ve elektronik saldırılar konusunda kamu idarelerine destek vermek için özel bir birim bulunmaktadır (GovCERT). GovCERT „Computer Emergency Readiness“ görevi yapmakta ve her bir Kamu idaresi bünyesinde kurulan yerel birimlere destek vermektedir. Yerel Birimler, risk yaratan durumların çözülmesi ve savunma yazılımlarının güncelleştirilmesi konularında GOVCERT ile temas etmektedirler.

J. İSPANYA

İspanya'nın siber savunma politikasını CCN-STIC 001 "Bilgi Teknolojisi Güvenliği ve Kamu İdaresinde Gizli Ulusal Bilgiler İçeren Yazışmalar" belgesi kamu idari sistemlerinde kullanılan gizli bilgilerin doğru bir biçimde korunmasına ilişkin temel ilkeleri ve asgari gereklilikleri belirleyerek bu konudaki çerçeveyi oluşturur. . Kamu İdaresinde kullanılan sistemler için yasal çerçeve kısmen oluşturulmuş olup, uygulama kanalları ve kuralları belirlenmiştir. Bilgisayar sistemlerinde asgari güvenlik kurallarının belirlenmiş olduğu yetki kullanılan uygulamalarda bilgi güvenliği, kullanımı ve saklanması konusunda genel kriterler geçerlidir. Bu konuda uyulması gereken bir zorunluluk ya da denetim mekanizması bulunmamaktadır. 11 sayı ve 22 Haziran 2007 tarihli vatandaşların Kamu Hizmetlerine elektronik ortamda erişimine ilişkin yasa uyarınca Kamu İdaresinde kullanılan sistemlerinde kullanılacak temel ilkeler ve asgari gereklilikleri oluşturmayı amaçlayan Ulusal Güvenlik Şeması geliştirilme aşamasındadır. Stratejik önem arz eden altyapı şirketlerinin sistemleri için bir düzenleme halihazırda bulunmamaktadır. Bununla beraber 2007 yılında İçişleri Bakanlığı, Güvenlik Devlet Sekreterliğine bağlı Stratejik Önem Taşıyan Altyapıları Koruma Ulusal Merkezi (CNPIC) stratejik açıdan ulusal önem taşıyan altyapıların güvenliğinin sağlanması konularını koordine eden bir organ olarak kurulmuştur. Bu merkezin görev alanına giren sektörlerden biri de Bilişim Teknolojileri sektörüdür. CCN, tüm devlet kurumları (merkezi, özerk, yerel) ile işbirliği yapmak ve onlara yardımcı olmakla görevli ulusal uyarı merkezi konumundaki CCN-CERT aracılığıyla doğabilecek güvenlik sorunlarına hızlı ve etkili bir biçimde çözüm bulmayı ve günümüz şartları içinde doğan yeni tehditlerle etkin şekilde mücadele etmeyi hedeflemektedir. Siber savunma politikası, halihazırda sadece devlet kurumlarının sistemlerini kapsamaktadır. Sanayi Bakanlığı tarafından Telekomünikasyon hizmeti veren şirketler için belirlenen yasal engellemeler ve idari gerekliliklere ilişkin uygulama hariç devlet kurumlarınınkiler dışında kalan sistemler için yasal düzenleme mevcut değildir.

K. TÜRKİYE

Ülkemizde ise konuyla ilgili doğrudan bir çalışma bulunmakla birlikte konunun bir düzene bağlanmasına yönelik genel nitelikli kurumsal ve mevzuat anlamında bir dizi çalışmalar yapılmıştır. 15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu, 4 Mayıs 2007 tarihli ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi hakkındaki kanun konuyla ilgili düzenlemelerdir. 5651 sayılı kanun internet ortamında işlenen suçları sekiz ayrı kategoride değerlendirmekte, bilgi güvenliği, siber terörizm gibi suçlara yer vermemektedir. E-dönüşüm Türkiye Bilgi Toplumu Strateji Belgesinin Eylem Planında ise 88 numaralı eylem Ulusal Bilgi sistemleri Güvenlik Programı olarak belirlenmiş ve 2008 Aralık ayına kadar tamamlanması amacıyla TÜBİTAK-UEKAE görevlendirilmiştir.

IV. STRATEJİLERİN VE ÜLKELERİN DEĞERLENDİRİLMESİ

Bu çalışma kapsamında, ABD, Almanya, Danimarka, Finlandiya, Fransa, Güney Kore, İngiltere, İspanya, İsviçre ve İtalya'daki siber saldırılara karşı savunmaya yönelik ulusal anlamda yapılan hazırlıklar, kurumsal düzenlemeler, hazırlanan yasal mevzuatlar açıklanmıştır. Ülkelerdeki çalışmalar genel olarak incelendiğinde;

- Siber savunma konusunda ülkelerin tamamının duyarlı ve tehlikenin farkında olduğu,
- Konu ile ilgili yasal düzenleme yoluna giden ülkelerin çoğunlukta olduğu, bazılarında ise düzenleme olmasına rağmen yasal zorunluluk getirilmediği,
- Ulusal anlamda siber savunma sorumluluğunun bazılarında bağımsız bir organa verilmesine rağmen bazılarında Bakanlıklar düzeyinde çok sayıda kurumun sorumluluğuna dağıtıldığı,
- Ülkelerin tamamında hazırlık olmasına rağmen olası bir saldırı durumunda atılması gereken adım konusunun açıklığa kavuşturulamadığı,
- Herbir ülkenin tamamen farklı yöntem ve stratejilerle konuya yaklaşım sergileyebildikleri,
- Ülkemiz gelişmiş ülkelere göre yapılan düzenlemeler ve kurumsallaşmalar bağlamında geri kaldığı, gereksinimlerin karşılanmasına yönelik adımların hızlandırılmasında yarar olacağı

değerlendirilmektedir.

KAYNAKLAR

1. The National Strategy to Secure Cyberspace
2. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
3. http://www.dhs.gov/index.shtm
4. İç Güvenliğe ilişkin Başkanlık Direktifi www.whitehouse.gov/mews/relases/2003/12/20031217-5.html
5. IT- security Beyond Borders http://www.tekno.dk/pdf/projekter/it-sec2007/2007_it-security-across-borders-summary.pdf
6. Creating a Safer Information Society www.mintc.fi/scripts/cgiip.exe/WService=lvm/cm/pub/showdoc.p?docid=2433&menuid=431
7. http://www.telecom.gouv.fr/fonds_documentaire/rapports/cybercriminalite.pdf
8. Korea Information Security Agency-www.kisa.or.kr
9. Korea Internet Security Center-www.krcert.or.kr
10. Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency) http://www.enisa.europa.eu/index.htm
11. http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2008/0097
12. http://www.csae.map.es/csi/pg3428.htm
13. E-Dönüşümde Türkiye Nerede? Y. Turan Çetiner, Uluslararası Ekonomik Sorunlar Dergisi, T.C. Dışişleri Bakanlığı, Kasım 2008

Türk Patent Enstitüsü E-imza Uygulamaları

Mustafa ÖZLÜ

***Özet*—Türkiye'de sınaî mülkiyet haklarının tescilini gerçekleştiren tek kamu kurumu olan Türk Patent Enstitüsü, internet üzerinden başvuru sistemine güvenlik ve hukuksal geçerlilik kazandırmak amacıyla elektronik imza ve zaman damgası entegrasyonunu gerçekleştirmiş, Ağustos 2007'de e-imza ile çevrimiçi marka başvurusunu, ardından Ocak 2008'de e-imza ile çevrimiçi patent ve endüstriyel tasarım başvurularını ve Nisan 2008'de mobil e-imza ile marka, patent ve endüstriyel tasarım başvuru uygulamalarını hizmete sokmuştur. Bu makalede Enstitü'nün e-imza uygulamaları, e-imza altyapısı ile e-imzalı başvurulara ilişkin istatistikî bilgilere yer verilecektir.**

***Anahtar Kelimeler*—E-devlet, E-imza, Mobil E-imza**

I. GİRİŞ

Türkiye'de son yıllarda gerek kamu gerekse özel sektörde internet üzerinden gerçekleştirilebilecek çevrimiçi işlemlerde önemli oranda artış görülmüştür. Bu gelişmelere paralel olarak çevrimiçi işlemlerin kullanım oranları artmış, artan bu oranlar teknik ve yasal açılardan bir takım sorunları da beraberinde getirmiştir. Burada yaşanan yasal sorunlar noktasındaki eksikliklerin giderilmesi amacıyla ıslak imzaya eşdeğer ve ıslak imza ile aynı sonucu doğuracak elektronik imza kullanımına geçilmiş ve gerek Avrupa'da gerekse Ülkemizde çevrimiçi e-devlet uygulamaların önemli bir kısmında bu entegrasyon gerçekleşmiştir.

Türk Patent Enstitüsü, sınai mülkiyet bilincini ve bilgisini ülke genelinde yaymak, yasal, teknik ve beşeri altyapıyı güçlendirerek, müşteri odaklı, hızlı ve kaliteli hizmet sunmak suretiyle etkin bir sınai mülkiyet sistemi oluşturmayı hedefleyen bir kamu kurumudur. Bu bağlamda müşterilerin sınaî mülki haklarının tescillerini daha etkin ve kolay yapabilmeleri, çevrimiçi başvuru sistemine güvenlik ve hukuksal geçerlilik kazandırmak amacıyla elektronik imza ve zaman damgası entegrasyonunun gerçekleştirilmesi için bir dizi teknik çalışmalar yapılmış, bu çalışmalar sonucu e-imza ile çevrimiçi patent, marka ve endüstriyel tasarım başvuru uygulamaları devreye alınmıştır.[1]

TPE E-imza uygulamaları ile e-imza sahipleri daha önce hiç bir bildirime ihtiyaç duyulmaksızın sahip oldukları sınai mülkiyet haklarının tescil başvurularını internet üzerinden web portalımızın çevrimiçi işlemler bölümünden (online.tpe.gov.tr) e-imzalarını kullanarak çevrimiçi gerçekleştirebilme imkanına kavuşmuşlardır. [2]

M. ÖZLÜ, Türk Patent Enstitüsü, Ankara

II. GENEL BİLGİLER

A) Uygulamalar Hakkında

Türk Patent Enstitüsü E-imza uygulamaları ve uygulama adımları içerisindeki E-imzalama işlemleri kurum içi uygulamalara da entegre bir yapıyla, istemci ve sunucu mimarisine göre, J2EE programlama teknolojisi ile programlanmış ve Oracle veritabanı üzerinde çalışmaktadır.

E-imzalama işlemi, istemci de TÜBİTAK e-imza kütüphanesini kullanan bir Java Appleti tarafından gerçekleştirilir. Kullanılan E-imza Appleti ile Türkiye'de faaliyet gösteren tüm ESHS sertifikaları desteklenmektedir.

Türk Patent Enstitüsü E-imza uygulamaları aynı zamanda Zaman Damgası hizmetini de desteklemektedir. Zaman Damgaları belli bir verinin belirtilen bir tarihte var olduğunu kanıtlarlar. Zaman Damgası Sunucusu, zaman damgalarını imzalamak için açık anahtar teknolojisini kullanarak, verinin bütünlüğünü ve belirli bir tarihteki varlığını onaylar.[3] Sınaî mülki hak başvurularında zaman damgası teknolojisinin kullanımı, tescil önceliğinin belirlenebilmesi açısından büyük önem arz etmektedir.

Türk Patent Enstitüsü E-imza uygulamaları 3 uygulamadan oluşmaktadır:

1) E-imza ve Mobil imza ile Marka başvurusu
2) E-imza ve Mobil imza ile Patent/Faydalı Model başvurusu
3) E-imza ve Mobil imza ile Endüstriyel Tasarım başvurusu

B) Uygulama İş Akışları

E-imza uygulamaları, Marka, patent/faydalı model ve endüstriyel tasarım başvuruları, açısından iş akışları ve işlem adımları açısından benzerlik göstermektedir. Bu sebeple bundan sonraki bölümlerde başvuru en kapsamlısı olan marka başvurusuna yer verilmesi uygun görülmüştür.

E-imza ile Marka Başvurusu İşlem Adımları

a) Başvuruyu gerçekleştirecek olan vekil ya da başvuru sahibi sisteme giriş yapar, varsa ön yazı talebi belirtir,
b) Başvuruyu eğer vekil ise vekâletname bilgisini girer,
c) Başvuru yapılacak marka adı ve örneği girilir,
d) Markanın sahibi/sahiplerine ilişkin bilgiler girilir
e) Markanın mal ve hizmet sınıfları seçilir,

f) Eğer varsa markanın rüçhan bilgileri girilir,
g) Ödemeye ilişkin bilgiler girilir,
h) Başvuru dokümanı ön izleme yapılır,
i) E-imzalama / Mobil İmzalama işlemi gerçekleştirilir,
j) Başvuruya ilişkin başvuru ve evrak kayıt bilgileri görüntülenir, form çıktısı alınabilir.

Bu işlemlerden sonra başvuruya ilişkin başvuru numarası verilmiş, evrak sistemine giriş yapılmıştır. Marka başvurusu için anında, patent ve endüstriyel tasarım başvuruları için bir süre sonra çevrimiçi işlemler sayfasında yer alan dosya takip işlemlerinden dosya durumu takip edilmeye başlanabilmektedir. [2]

E-İmzalı Uygulamalar Kullanıcı Tipleri

1) Başvuru şartlarını sağlayan Patent veya Marka Vekilleri
2) Başvuru şartlarını sağlayan herhangi bir vatandaş

Sistem gereksinimlerini sağlayan e-imza sahibi her patent/marka vekili veya vatandaş başvuru gerçekleştirebilmektedir. Başvuru gerçekleştirmeden önce yapılması gereken başka bir işlem yoktur. TPE E-imzalı uygulamaları bu yönüyle diğer kurum ve kuruluşlardan farklılık arz etmektedir. Ayrıca yapılan başvururu hiç bir ara işleme girmeden kalmadan direkt evrak sistemine ve oradan da ilgili uygulamaya geçmektedir. Bu da bürokratik/hiyerarşik işlemlerden kaybedilebilecek zamanı kazandırmaktadır. [2]

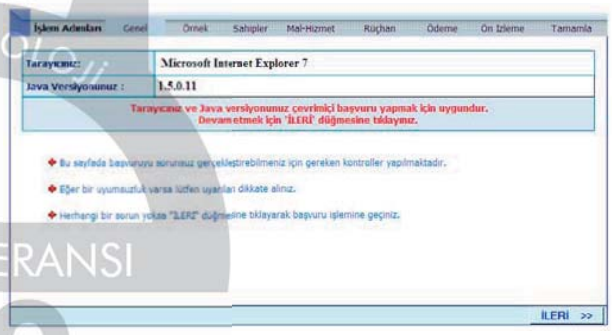
C) E-imza ve Mobil İmza ile Marka Başvurusu Adımları

Türk Patent Enstitüsü çevrimiçi işlemler sayfası sadece e-imza ile marka, patent, endüstriyel tasarım başvurusu değil, başvurmadan önce araştırma ve başvuru sonrası dosya takibi işlemlerine de imkan tanır.

Şekil 1: Türk Patent Enstitüsü Çevrimiçi İşlemler Sayfası (online.tpe.gov.tr)

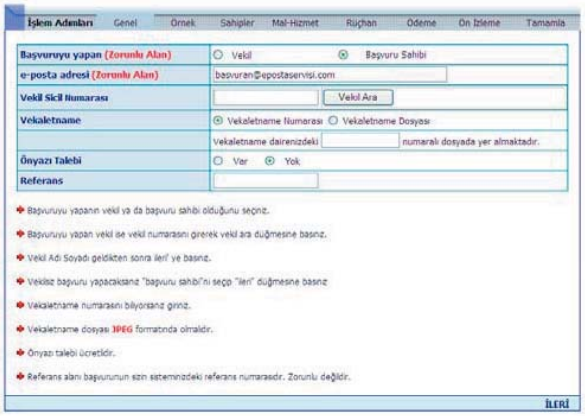
Şekil 2: Marka Başvuru uygulaması karşılama ekranı

Marka Başvuru uygulaması karşılama ekranında başvuruya ilişkin yasal geçerlilik hatırlatılır, e-imza sahibi olunabilecek yerler ve başvurunun gerçekleşebilmesi için gereken sistem ihtiyaçları hakkında bilgi verilir. [4]



Şekil 3: Marka Başvuru uygulaması sistem gereksinimleri testi ekranı

Bu test ekranı işlemlerin daha sağlıklı gerçekleştirilebilmesi için istemci bilgisayarından var olması gereken sistem gereksinimlerini kontrol etmekte, ortaya eksik veya yanlış değerler çıkması durumunda uyarı vererek gereksinimleri tekrar hatırlatmakta, işleme devam ettirmemektedir.

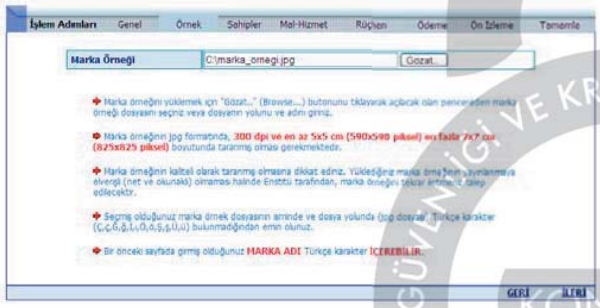


Şekil 4: Marka başvuru uygulaması başvuran bilgileri giriş ekranı

Bu ekranda başvuru gerçekleştirecek marka/patent vekili ya da başvuru sahibi sisteme e-posta adresini tanıtmaktadır. Vekil aynı zamanda sistemde kendi bularak ve vekâletname referans numarası ya da vekâletname dosyası yükleme adımları ile vekillik durumunu tanıtmaktadır. Ayrıca başvuru sahibi ya da vekil eğer varsa başvurularına ilişkin ön yazı talebini gene bu ilk adımdan belirtmektedirler.

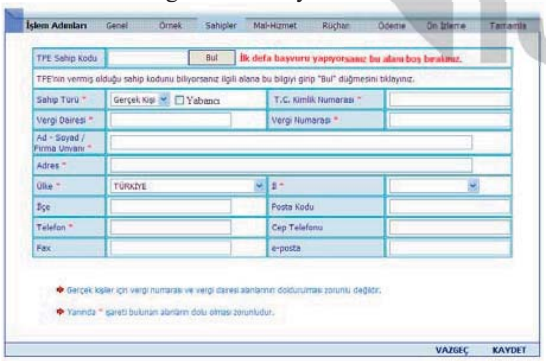
Şekil 5: Marka başvuru uygulaması marka bilgileri giriş ekranı

Bu ekranda başvuru yapılacak markanın adı ve koruma kapsamı (kelime, şekil, kelime+şekil) müşteri tarafından girilmektedir.



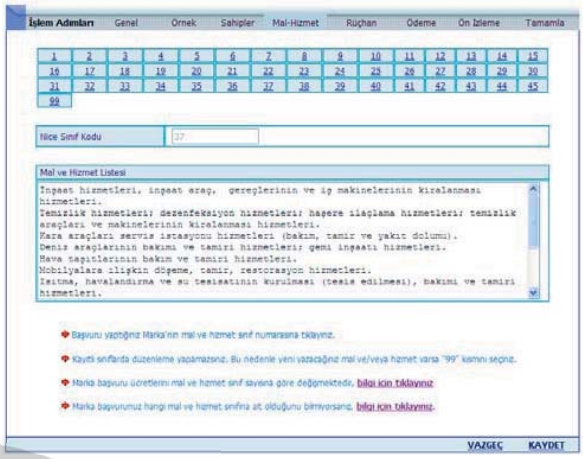
Şekil 6: Marka Başvuru uygulaması marka örneği giriş ekranı

Marka örneği, markanın logosunun örneğini anlatmaktadır. Müşteri bu adımda markasının logosunu imaj dosyasını belirlenen kıstaslara göre sisteme yüklemektedir.



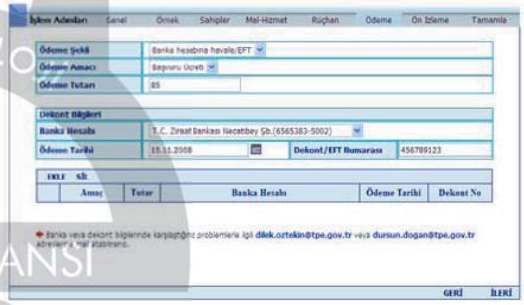
Şekil 7: Marka başvuru sahip bilgileri giriş ekranı

Başvuru sahibi bilgi ekranı marka sahibine ilişkin bilgilerin girişinin yapıldığı ekrandır. Bu ekranda müşteriye ilişkin, TC kimlik, vergi dairesi, vergi numarası gibi servisler aracılığı ile doğrulanacak bilgilerde girilmektedir. Müşteri daha önce TPE'de gerçekleştirdiği bir başvuru işlemi varsa kendisine verilen TPE sahip kodunun girerek bilgilerin otomatik doldurulmasını sağlayabilir.



Şekil 8: Marka mal ve hizmet sınıfları seçim ekranı

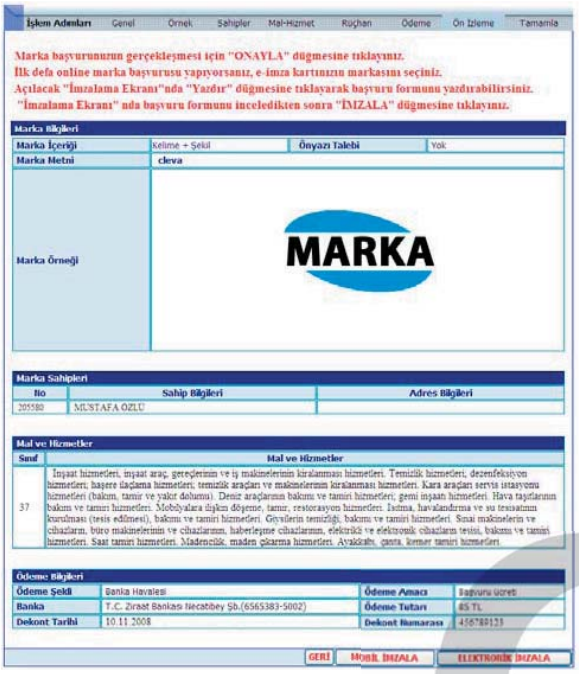
Bu ekranda müşteri markasının tescil edilmesini istediği 45 adet mal ve hizmet sınıflarından dilediklerini seçer, ayrıca 99 kodlu özel sınıfa mevcut sınıflarda yerleştiremediği mal ve hizmetlerini ekleyebilir.



Şekil 9: Ödeme Bildirimi ekranı

Ödeme bildirimi ekranında müşteri yapmış olduğu başvuruya ilişkin başvuru ücreti, ön yazı talebi ve rüçhan talebi ile ilgili ücretlerin ödeme bildirimlerini gerçekleştirmektedir.

15/01/2004 tarih ve 5070 sayılı e- imza Kanunu hükümleri gereğince elektronik ortamda yapılan, patent ve faydalı model başvurularında 10 YTL, endüstriyel tasarım başvurularında 20 YTL ve marka başvurularında 30 YTL toplam başvuru ücretinden indirilir.[2]



Şekil 10: Başvuru bilgileri kontrol ekranı

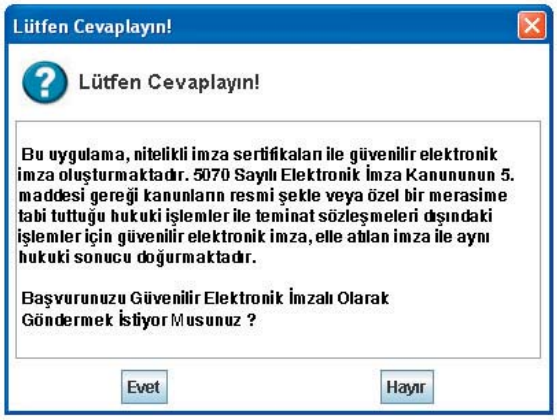
Bu ekranda müşteri marka başvurusu için girmiş olduğu bilgileri kontrol eder, bilgilerde bir yanlışlık ya da eksiklik varsa geri butonuna tıklar ve gerekli düzeltmeleri yapar. Eğer başvuru bilgilerinde herhangi bir sorun yoksa Elektronik İmzalama ya da mobil imzalama seçeneklerinden kendine uygun olanı seçerek imzalama işlemini başlatır.

D) E-imzalama Adımları ve E-imza Modülü Özellikleri

1) E-imza İşlem Adımları

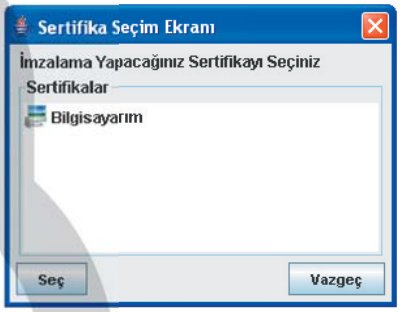
Şekil 11: Başvuru imzalama ekranı

Bu ekran e-imzalama işleminin gerçekleştiği ekrandır. Müşteri bu ekranda kendisine görüntülenen PDF dokümanı imzalamak için imzala butonuna tıklar.



Şekil 12: E-İmzalama onay diyalogu

Eğer gösterilen PDF dokümanının imzalanmasına onay veriliyorsa evet seçeneğiyle işleme devam edilir.

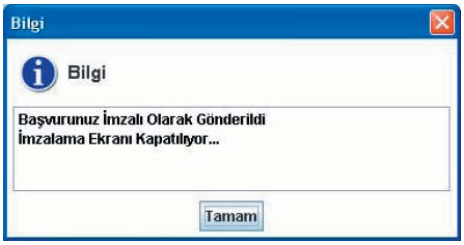


Şekil 13:Sertifika seçim ekranı

Müşteri sistemden kullanmak istediği sertifikayı seçer. Eğer mobil imza ile başvuruluyorsa telefon numarasını girer.

Şekil 14: E-İmza pin kodu giriş ekranı

E-imzaya ilişkin pin kodu girilir ve böylelikle imzalama işlemi başlar.



Şekil 15: Başarılı bir elektronik imzalama işleminin son ekranı

Bu ekrandaki tamam butonuna tıklandığında başvuru imzalanmış, zaman damgası alınmış demektir. Başvurunun değerlendirmeye alınmasıyla birlikte alındı bilgisi, başvuru numarası ve evrak numarası başvuru sahibi görüntülenir ve başvuru sırasında belirttiği e-posta adresine iletilir.

2) E-imza Teknik Özellikleri

Türk Patent Enstitüsü'nün Internet üzerinden e-imza ile başvuru uygulamalarına elektronik imza ve zaman damgası entegrasyonu özel bir firmanın sağlamış olduğu yazılım bileşenleri ve teknik desteği ile uluslararası standartlar kullanılarak gerçekleştirilmiştir. [CEN (Comité Européen de Normalisation), ETSI (European Telecommunications Standards Institute), ITU (International Telecommunication Union)]

Kurum E-imza uygulamalarında Kriptografik işlemler ve AAA hizmetlerinden faydalanmak için TÜBİTAK e-imza kütüphanesi kullanır. TÜBİTAK e-imza kütüphanesinden elde edilen imzaya ilişkin veriler, başvuru için hazırlanan PDF dokümanına eklenir ve bu doküman müşteriye gösterilir.

Müşteri gördüğü dokümanı elektronik olarak imzalayarak kurum sunucusuna gönderir. İmzalı gelen başvuru formları kurum merkezinde önce doğrulanır. Eksiksiz ve e-imzası doğrulanan başvurular kuruma giriş tarihini kesinleştirmek amacıyla zaman damgası da alarak kaydedilir ve başvuru onaylanarak değerlendirmeye alınır.

E-imzalı dokümanların doğrulanmasında, imza atıldığı tarihteki SİL (Sertifika İptal Listesi)'in kontrolü yapılır. O tarihteki SİL'lere ulaşılabilmesi için, bütün ESHS (Elektronik Sertifika Hizmet Sağlayıcısı)'ler tarafından yayınlanan SİL'ler sistemde depolanır.[1]

Türk Patent Enstitüsü E-imza Uygulamaları 24 Eylül 2008 tarihinde TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) tarafından hazırlanan E-imza Uygulaması Kontrol Listesi'ne göre yapılan, CWA 14170, CWA 14171[5] ve ETSI[6] 101733 standartlarına uygunluk denetimini başarılı bir şekilde geçmiştir böylelikle TÜBİTAK UEKAE bünyesinde faaliyet gösteren Kamu Sertifikasyon Merkezi'nce E-imza entegrasyonunu gerçekleştirmiş olan kamu kurumları listesine girmiştir.[7]

III. İSTATİSTİK VERİLER

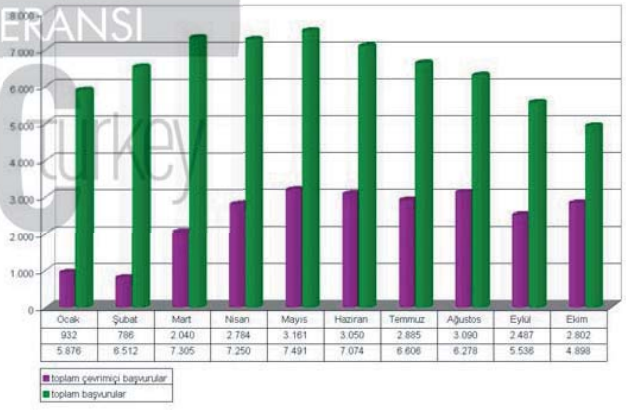
Türk Patent Enstitüsü, proje başlangıcında sadece marka için yıllık 60.000 civarında seyreden marka başvuruların %50'sinin internet üzerinden alınması hedeflemiştir.

TABLO 1
ÇEVRİMİÇİ PATENT, TASARIM, MARKA BAŞVURU ADETLERİ
(OCAK-EKİM 2008)

Tarih	Patent	Tasarım	Marka
2008/01	17	27	888
2008/02	8	17	761
2008/03	59	86	1.895
2008/04	71	127	2.586
2008/05	138	122	2.901
2008/06	80	147	2.823
2008/07	92	116	2.677
2008/08	111	110	2.869
2008/09	111	92	2.284
2008/10	85	105	2.612
Toplam	772	949	22.296

Ekim 2008 sonu itibariyle 772'si Patent, 949'u Endüstriyel Tasarım, 22.296'sı Marka olmak üzere, Toplam 24.017 çevrimiçi başvuru alınmıştır. Yine aynı dönemde toplam 64.826 adet başvuru gerçekleşmiştir. Toplam başvuruların %37'si çevrimiçi gerçekleşmiştir.

Çevrimiçi başvuru sonrası araştırma ve dosya takibi işlemleri de yoğun şekilde kullanılmaktadır. 2008 Ekim sonu itibariyle 656.052'si Patent, 685.397'si Endüstriyel Tasarım, 14.006.830'u Marka olmak üzere, toplam 15.348.279 araştırma ve dosya takibi yapılmıştır. Aylık ortalama 1.534.000'in üzerinde araştırma ve dosya takibi yapılmaktadır.[8]



Grafik 1: Çevrimiçi marka başvuruları ve toplam marka başvuruları

Yukarıdaki grafikte de görüldüğü gibi çevrimiçi marka başvurularının toplam başvurulardaki oranı, artış eğilimi içindedir. 2008 Eylül ayında bu oran %48 iken, 2008 Ekim ayı sonunda %62'ye yükselmiştir. [8]

IV. SONUÇ

Türk Patent Enstitüsü E-İmza Uygulamaları ile Marka, patent/faydalı model ve endüstriyel tasarım başvuruları artık yakın olan önceliğinde değil teknoloji sayesinde Ülkenin her yerinden herkese eşit imkânlarla sunulabilmektedir. Hem başvuru konusunda teknolojiden faydalanarak zaman ve para kazancı sağlanmış, hem olası haksızlıklar engellenmiş, hem de kuruma elden teslim edilen dosya sayısı azaldığından personelin iş yükü hafiflemiştir. Vatandaşlar ile patent ve marka vekillerinin işlerini daha kolay ve hızlı yapabilmeleri için gerekli ortam sağlanmıştır. E-İmza Uygulamaları ile başvurular elektronik ortamda daha ekonomik, anlık izlenebilir, güvenli ve hukuksal geçerli hale gelmiştir. Bununla birlikte vatandaşların kuruma elden teslim veya posta yoluyla ulaştırdığı başvurular da anlık izlenebilir hale gelmiştir.

Ayrıca Enstitü, e-imza kanunu hükümleri gereğince elektronik ortamda yapılan işlemler için uygulanması gereken indirimleri de gerçekleştirerek kullanıcıların başvurularda e-imzayı kullanmalarını teşvik etmiştir. Müşterilerin uygulamayı en iyi şekilde kullanabilmeleri için işlem adımlarını içeren kullanım kılavuzları, sıkça sorulan sorular vb. dokümantasyon sağlanmıştır. Müşterilerle kurulan iyi iletişimin sonucu, müşteriden gelen, uygulama kullanımı sırasında karşılaşılan problemler ile kullanım kolaylığı amaçlı geri bildirimlere ilişkin düzenlemeler kısa sürelerde uygulamaya yansıtılmıştır.

Bütün hizmetlerinde müşteri memnuniyetini ön planda tutarak yaptığı atılımlara bir yenisini daha ekleyen Enstitü; çevrimiçi uygulamalar ile e-kurum olma yolunda önemli bir adım daha atmış, diğer kamu kurumlarına örnek teşkil eder duruma gelmiştir.

Türk Patent Enstitüsü E-İmza Uygulamaları temel olarak teknolojiden faydalanmak suretiyle zaman, para ve iş gücü açısından büyük kazanımlar sağlamıştır. Bu kazanımlar çevrimiçi e-imzalı uygulamaların gerek kamu gerekse özel kurum ve kuruluşlarca kullanılması, uygulama alanlarının genişlemesiyle Ülke ekonomisine büyük katkılar sağlanabileceğini göstermiştir.

V. KAYNAKLAR

[1] http://www.tpe.gov.tr/portal/default2.jsp?sayfa=701 Türk Patent Enstitüsü Haber ve Duyuruları
[2] http://online.tpe.gov.tr/SSS_Cevrimici.pdf TPE çevrimiçi işlemlerle ilgili sıkça sorulan sorular ve cevapları
[3] http://www.kamusm.gov.tr/tr/Hizmetler/Zamandamgasi/ TÜBİTAK UEKAE, Kamu Sertifikasyon Merkezi, Zaman Damgası
[4] http://online.tpe.gov.tr/Online_Basvuru_Kullanim_Kilavuzu.pdf TPE Çevrimiçi Marka Başvurusu Kullanım Kılavuzu
[5] CWA 14171 CEN. Workshop Agreements: "Procedures for Electronic Signature Verification".
[6] ETSI TS 101 733 V1.5.1 (2003-7 12) : "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".
[7] http://www.kamusm.gov.tr/tr/Kurumsal/Musterilerimiz/ TÜBİTAK UEKAE, Kamu Sertifikasyon Merkezi, E-İmza Uygulaması Kontrol Listesi
[8] http://online.tpe.gov.tr/istatistikler.htm Çevrimiçi Başvuru, Araştırma ve Dosya Takibi İstatistikleri

Secure Embedding Communication Channels: An Exploration of the Use of Simulated Quantum Electro Dynamic Systems

Najib SAYLANI

Abstract--**This paper proposes a novel approach that would complements traditional encryption based methods used to secure the flow of sensitive and confidential information traveling the different channels that exist in embedded systems. The paper outlines the use of techniques adopted from the field of Quantum Electro Dynamic used to simulate weak perturbations through wave scattering. New and logical communication paths are simulated through the process of particles scattering phenomena. Information is encoded as waves packets transmitted through the same generated channels.**

Keywords-- **Quantum Electro Dynamic (QED), Security, Wave scattering.**

I. INTRODUCTION

Common embedded systems in use today to support various critical IT infrastructures implemented for both government and industries require, in addition to encrypting information, a more robust environment for the dissemination of critical and confidential information. Unsecure internal communication channels in a given system represent a so often ignored danger of compromising any system. We outline in the next section an approach from Quantum Electro Dynamic that is actually part of a large security system we are working on for the past six years. Paper referenced in [7] outlines the overall system. This is a tiny subset of such system that target securing communication paths taken by information within an embedded system. The idea is to make these paths invisible to hacking by mapping the whole process to the simulated process of waves' propagation through scattering process. We claim that this process, while is not a form of encryption, is a way to increase challenges for any potential hackers and to thwart attacks that have as a purpose the interception of embedded communication channels and the compromise of information within the system itself. The approach is to create chaotic but controlled phenomena that are extremely hard to determine by attackers.

II. BACKGROUND AND THE PROPOSED APPROACH

Quantum Electro Dynamic (QED) is the quantum field theory of electrons, positrons and photons. The techniques adopted for the proposed systems are limited to the case of weak perturbations when wave scattering occurs. The discussion related to QED is completely adopted from [5].

The scattering simulates a multi-treaded environment where information between CPU, BUS, RAM, and various ports on the system is already encrypted. We believe that this technique will efficiently complement techniques surveyed in the paper by Elbaz et Al [3]. The referenced paper is selected because it outlines traditional techniques based on encryption and it is one of several research paper s that inspired us to work on this area. We also claim that low overhead through using the proposed approach in systems where information is not encrypted at all.

We are aware of the fact that processors, bus, and main memory architecture and the associated ports used in internal communications are not secret. This same knowledge may make this environment a source of security compromises.
The following is a summary of the main points of such system:
-Information to be secured is encoded as a wave packet and propagated from source to destination within a given system.

N. SAYLANI, Hosftra University, USA

-The process of encoding and propagation is randomly generated and mapped to a certain number of threads managed through Inter Process Communication (IPC) schema.
-In this case, a single known channel of communication is mapped to multiple 'virtual' or 'logical' channels maintained through simulated oscillations kept alive through simulated local potentials (energy).
-The propagation/scattering process is assumed to happen in real or simulated real time through the introduction of artificial delays. The process is represented by the following $Schr\ddot{o}dinger$ wave equation [4]:

$$i\eta\frac{\partial(x,t)}{\partial t}=-\frac{\eta^2}{2m}\nabla^2\Psi(x,t)+V(x,t)\Psi(x,t)$$

The equation describes the interaction of a particle of mass *m* with a potential constant in space. (In our case the potential is not fixed-which would cause it to have different equations for different generated paths, with different potentials at various given times).

The question is how the information is retrieved later at destination? The answer is that, in QED, it is well established that:

If Ψ is known at position x, and at time t then Ψ is also know at t_0 <t and t'>t.

In the proposed model generated paths (i.e. channels) is achieved through a true simulation of a comparable physical system exhibiting identical phenomena. QED supports real world physical systems where past and future behavior of the scattering can be determined. In QED analyzing the behavior of the scattered waves across different paths (generated logical channels) is helped by the use of the *Green's Function*.
Green's Function describes the probability amplitude associated with the scattering process.
In our model, defining a specific path of scattering will help determine the solution to all $Schr\ddot{o}dinger$ equations involved. Across all generated paths the solutions to a specific $Schr\ddot{o}dinger$ equation would be linearly superposed on the *Green's Function*. In order to analyze the process of scattering we need to introduce the Huygens Principle:

$\Psi(x,t)$ at time t' position x' is known if $\Psi(x,t)$ is known at source x at time *t.*

$$\left[\Psi(x',t')=i\int d^3xG(x',t';x,t)\Psi(x,t)t'>t\right. \quad (1)$$

The intensity of Ψ at (x',t') is proportional to Ψ at $\Psi(x,t)$

Here $iG(x',t';x,t)$ is the constant of proportionality in (1)
$G(n',t';x,t)$ is the *Green's Function* of the *Hamiltonian* $\hat{H}$ or *Hamiltonian operator*

$$\hat{H}=-\frac{\eta^2}{2m}\nabla^2+V(x,t)$$

Backward and Forward propagations are considered. This assumes that within our model if the path is defined then one can proceed by assuming either a forward or backward propagation.
For that case there are two types of *Green's Function*:

- *Forward or retarded Green's Function*

$$G^+(x',t';x,t)=\begin{cases}G(x',t';x,t) & t'>t\\ 0 & t'<t\end{cases}$$

That is a causal backward or evolution of $\Psi(x,t)$ from $\Psi(x',t')$

- *Backward or advanced Green's Function*

$$G^-(x',t';x,t)=\begin{cases}G(x',t';x,t) & t'<t\\ 0 & t'>t\end{cases}$$

This is a causal backward or evolution of $\Psi(x,t)$ from $\Psi(x',t')$
Determination of a resulting wave packet backward or forward necessitates the introduction of step-function θ.

$$\theta(\tau)=\begin{cases}1\ for\ \tau>0\\ 0\ for\ \tau<0\end{cases}$$

The causal evolution of $\Psi(x',t')$ from $\Psi(x,t)$ where $t'>t$ can be represented by $\theta(t-t')\Psi(x',t')=-i\int d^3xG^-(x',t';x,t)\Psi(x,t)$
It is noted that the *Green's Function* is considered only when a potential V of a scattering position x and at time t is not zero. $(V(x,t)\neq 0)$. If $V(x,t)=0$ we speak of a *free Green's Function* noted G_0.

As stated before, when a scattering path is chosen in our model at time t_1 and at position x_1 (a node x, of a given path) the corresponding scattered wave can be found by solving the following *Schrödinger* equation:

$$i\eta\frac{\partial}{\partial t_1}\Psi(x_1,t_1)+\frac{n^2}{2m}\nabla^2\Psi(x_1,t_1)=V(x_1,t_1)\Psi(x_1,t_1)$$

And if $V(x_1,t_1)$ is on during a fraction time Δt_1:

$$\Psi(x_1,t_1)=\phi(x_1,t_1)+\Delta\Psi(x_1,t_{1)}$$

ϕ: free wave

$\Delta\Psi$: scattered wave

if $\mathrm{V}(\mathrm{x}_1,t_1)$ is off after Δt_1:

$$\Delta\Psi(x_2,t_2)=i\int d^3x,\nabla G0(x_2,t_2;x,t,)\Delta\Psi(x_1,t_1)$$

Other computations lead to:

$$\Delta\Psi(x_1,t_1)=\frac{1}{\eta}V(x_1,t_1)0(x_1,t_1)\Delta t_1$$

The *Green's Function* and *Huygen's Principle* will enable us to compute a wave function at a given position at a given time when the wave is known at a former position and time (in the same scattering process).

The choice of scattering' paths within the system are critical in reconstructing the waves and, by the same process, retrieve the encoded information. There are different equations to solve across different paths. The idea is to compute or construct the wave $\Psi(x,t)$ at a position x along a given path at time t during a potential V. We note that by $V(x,t)$

Assume $\phi(x,t)$ is the initial wave associated with the incoming particle; it is established that $\phi(x,t)$ is a solution of the *Schrodinger* equation for a free particle.

Therefore, if no interaction affected $\phi(x,t)$ then it is stated that $\Psi(x,t)=\phi(x,t)$. In the future at position x' and time t' we have the following result:

$$\Psi^{(+)}(x',t')=\phi(x')+\int d^4x_1G_0^+(x';x_1)V(x_1)\Psi^{(+)}(x_1)\quad(2)$$

$(+)$: future scattering

Here $\Psi(x_1)$ is the original wave packet. The second term of (2) is the scattered wave.

Following specific rules of waves' superposition, coherence and given local oscillations maintained by a local energy, the techniques outlined here makes it easier to trace back along any path the whole wave (information/pattern) by only using partial or chunks of waves at any time at the level of any point or group of points along a given generated path.

The simulation is to be conducted using mathematical and programming tools presented in [1][4][6].

The following is a summary of steps to be taken in this process:

-Determine source and destination of information within the system (embedded system).

-Determine all devices partners in such communication.

-Encrypted or not information set is determined.

-Encode information by using initial states of original waves at the source.

-Randomly generate a set of virtual/logical channels between source and destination through the creation of multiple processes residing in randomly selected and available areas in system memory.

-Start simulation the propagation of original waves through these virtual/logical channels.

-The simulated scattering of waves cannot be predicted ahead of its occurrence. The selected set of paths is determined through multiple random processes that mimic the scattering process of a real world physical system.

-Determine and compute all related equations at destination to assemble original waves through processing partial states of each to regenerate the original information back at destination.

-Repeat for each transmission by resetting the simulation each time.

Because the process of scattering is a 'pseudo non-deterministic' set of events, it represents a kind of black boxes whose contents (processes, information, paths) cannot be determined.

III. CONCLUSION

We should acknowledge the fact that this approach adds an extra layer of protection to existing traditional layers (i.e. encryption). Another inspiring research article is referenced in [3] and we feel our approach may complement such work. Theoretical analyses of such system through the already proven techniques in QED fully support the claim that the new environment is robust and extremely challenging to the would-be hackers/attackers. This environment adds a very large number of unknown to a specific

physical topology (known communication channels) through the creation of simulated logical topology (simulated and claimed to be invisible channels of communication). A much more in depth study of the effect of such approach on the over-all performance of the system must be undertaken. Some of the challenges depicted in [8], although not directly related to the challenges faced by our system, should be considered especially at the hardware design level. For now, we are limited to simulating a system using existing architecture. And, as with any security system, a paradox does exist; how to secure the simulation process itself? A paradox similar to the one related to the storage of passwords and other similar concerns. In the case of the proposed system, a hacker/attacker can only disturb the system without gaining access to the information being transmitted. The hacker/attacker cannot determine what channel to intercept.

REFERENCES

[1] Brandt, S., Dahmen, H. D., Quantum Mechanics on the Personal Computer Third Edition, SpringerVerlag, New York, (1994).

[2] Coburn J., et Al, SECA: security-enhanced communication architecture, Proceedings of the international conference on Compilers, architectures and synthesis for embedded systems, 2005

[3] Elbaz, R. et Al, Hardware Engines for Bus Encryption: a Survey of Existing Techniques, Proceedings of the conference on Design, Automation and Test in Europe - Volume 3, 2005

[4] Feagin, J. M., Quantum Methods with Mathematica, Springer-Verlag, New York, (1994).

[5] Greiner, Reinhardt, Quantum Electrodynamics, Springer-Verlag, New York, (1994).

[6] Hockney, R. W., Eastwood, J. W., Computer Simulation Using Particles, Mc Graw-Hill, New York, (1989).

[7] Najib Saylani, "A Proposal for an Automated Approach to Real Time Profiling of IT Security Compromises", The 2004 International Multi-conference in Computer Science & Computer Engineering (June 2004)

[8] Remond, F., Physical design challenges for multi-million gate SoC's: an STMicroelectronics perspective, Proceedings of the international symposium on Physical design, 2006

Saldırı Tespit Sistemleri Üzerine Bir İnceleme

Esra N. GÜVEN, Şeref SAĞIROĞLU

***Özet*—Bu çalışmada, Saldırı Tespit Sistemleri (STS) hakkında literatür araştırması yapılarak, bilgi ve bilgisayar güvenliği açısından önemi değerlendirilmiştir. Araştırma sonucunda elde edilen bilgiler doğrultusunda STS'lerin sınıflandırılmasında kulllanılan genel kriterlere ve STS'lerin geliştirilmesi için kullanılan klasik ve zeki yöntemler araştırılmıştır. STS'de kullanılan zeki yöntemlerden günümüzde en çok dikkat çekenlerden biri olan Yapay Sinir Ağlarının (YSA) STS'lerde kullanılmasının üstünlükleri gözden geçirilmiş ve STS'ler genel olarak değerlendirilmiştir.**

***Anahtar Kelimeler*—Saldırı tespiti, saldırı tespit sistemleri (STS), zeki STS, yapay sinir ağı.**

***Abstract*—In this paper, intrusion detection systems (IDSs) which are important tools for providing information and computer security were analyzed, the methods used in developing IDSs were reviewed, the studies on classical and intelligent IDSs were revised. Artificial neural networks, one of the intelligent techniques, used in IDS design were also summarized. IDSs were finally evaluated in general.**

***Keywords*—IDS, Intrusion Detection Systems, intelligent IDS, artificial neural network.**

I. GİRİŞ

BİLGİ çağını yaşadığımız şu günlerde, e-devlet, e-imza, e-ticaret gibi kavramlardan oldukça sık bahsedilmektedir. Gerek hız ve verimlilik artışı, gerekse kolaylık sağlaması nedeniyle birçok bilgi elektronik ortamlara aktarılmıştır. Ancak, kişisel veya kurumsal açıdan önemli bir bilginin, başkalarının eline geçmesi ile maddi ve manevi zararlara yol açabileceği görülmüştür. Geliştirilen e-devlet, e-kurum gibi projelerde güvenliğin en üst düzeyde tutulması ulusal bir amaç haline gelmiş, bu konuda hukuki ve teknolojik önlemler geliştirilmiştir [1].

Teknolojik önlemlerin geliştirilmesi sırasında bir varlık olarak bilgiyi, tehdit ve saldırılara karşı korumak için güvenlik duvarları, antivirüs yazılımları, saldırı tespit sistemleri (STS), saldırı engelleme sistemleri (SES) gibi araçlar geliştirilmiştir. Bu araçların belirlenen kural ve politikalara göre yapılandırılması, bilgi güvenliğimizi büyük ölçüde sağlayacaktır.

Günümüzde bilgi ve bilgisayar güvenliğinin öneminin kavranmasıyla, geliştirilen araçlardan biri olan Saldırı Tespit Sistemleri (STS), saldırılara karşı sistemimizde "alarm" niteliği taşıyan yazılım ve donanımlardır. STS'lerin kullanılması ile sistemlere yapılan yetkisiz erişimler ve kötüye kullanımlar tespit edilerek, bunların yol açabileceği zararlar engellenmiş olur. Bilgisayar sistemlerinde STS'lerin kullanılması ile birlikte, sisteme ne tür saldırıların daha çok yapıldığı, sistemdeki mevcut açıklar ve saldırganlar hakkında daha detaylı bilgiler elde edilebilir.

Esra N. GÜVEN is now PhD Student in Boston, USA e-mail: enguven8@hotmail.com
Şeref SAĞIROĞLU is now with the Department of Computer Engineering, Gazi University, Ankara, TURKEY (e-mail: ss@gazi.edu.tr).

II. SALDIRI TESPİT SİSTEMLERİ

Saldırı tespiti kavramı ilk olarak Anderson'un "Bilgisayar Güvenliği Tehdit Gözetleme ve İzleme (Computer Security Threat Monitoring and Survaillance)" makalesi ile 1980'de ortaya atılmıştır [9]. Bu çalışma, STS'lerin tanımlanması ve tanınması açısından büyük bir öneme sahiptir.

İlk nesil STS'ler, basit bilgisayar sistemleri üzerine düşünülmüştür. İkinci neslinde ise günümüzde STS'lerin vazgeçilmezi olan "denetleme izi (audit trail)" kavramı ve veritabanı mantığının bilgi güvenliği alanındaki önemi ortaya çıkmıştır. Bunu izleyen çalışmalarda, güvenlik konusundaki çalışmalara yardımcı olmak amacıyla günlük denetleme verilerinin otomatik araçlar ile elde edilmesi konusunda çalışmalar yapılmıştır [10]. 1985'ten itibaren bu akımla geliştirilen projelerde denetleme verileri üzerinde özenle durulmuş ve istatistiksel yaklaşımlar temel alınarak saldırı tespit modelleri geliştirilmiştir. Bu çalışmalardan biri olan IDES (intrusion detection expert system), Denning tarafından geliştirilmeye başlanan ve 1988-1992 yılları arasında yapılan çalışmaların birçoğunu üzerinde barındıran bir sistemdir [8]. Daha sonra ismi NIDES (next-generation intrusion detection systems) olarak değişen bu sistem, ikinci nesil saldırı tespit sistemlerinin en eski ve en bilinen çalışmalarından biridir. IDES, saldırı senaryolarının kural kümelerinin çıkarılmasıyla dizayn edilmeye başlanan kural tabanlı bir STS'dir. Denning çalışmasında 3 farklı istatistiksel model tanımlamıştır. Bu modeler [2];

- kullanıcının belirli aralıklarla bir işlemi tekrar etmesine izin veren ve eşik değerine göre anormallik olduğunu tespit eden model,
- istatistiksel momentlerin bilindiği varsayılarak tespit edilen sapmalar ile anormallik olduğunu tespit eden model ve
- anormalliklerin tek olaya değil bir diziye bağlı olduğu Markov modeliolarak verilmektedir.

STS'lerin geliştirilmesinde günümüze kadar istatistiksel yöntemlerin dışında, kural tabanlı (rule based), eşik değeri belirleme (threshold value), durum geçiş diyagramları (state transition diagrams), yapay sinir ağları (artificial neural

networks), veri madenciliği (data mining), yapay bağışıklık sistemi (artificial immune system), bulanık mantık (fuzzy logic) gibi farklı birçok yaklaşım uygulanmıştır [11, 12].

STS'ler, bilgisayarlar ve veri ağları için yeni bir güvenlik yaklaşımı sunmaktadırlar. Daha önce de belirtildiği gibi STS'lerin amacı, saldırı, yetkisiz kullanım, suistimal, sistem içi ve dışından davetsiz misafirlerin sisteme zarar vermesi gibi durumların teşhis edilmesidir. Saldırı tespit problemi, bilgisayar ağlarının hızlı şekilde artması ve bu artışın sonucu olarak sisteme erişiminin çoğalması ile davetsiz misafirlerin kimliklendirmeyi kolaylıkla reddetmesinden sonra büyük önem kazanmıştır [3].

STS'ler günümüze kadar farklı birçok kritere göre sınıflandırılmıştır. Bunlardan en çok bilinen sınıflandırma türü saldırı tespit yöntemine göre olup, anormallik tespiti ve kötüye kullanım tespiti olarak ikiye ayrılır [8]. Ancak STS'lerin mimari yapısı, korunan sistemin türü, verinin işlenme zamanı gibi farklı sınıflandırmalar da yapılabilir [6]. Bu sınıflandırma kriterlerinden en yaygın olanları şunlardır;

Veri İşleme Zamanı

STS'ler için veri işleme zamanı, izlenen olaylar ve olayların analizi arasında geçen zamanı ifade eder. STS'ler "gerçek zamanlı" ve "gerçek zamanlı olmayan" şeklinde ikiye ayrılırlar [6].

Mimari Yapı

STS'lerin mimari yapısı, fonksiyonel bileşenlerin birbirlerine göre nasıl yerleştirildiklerini anlatır [13]. Temel fonksiyonel bileşenler; izlenen sistem, analizin yapıldığı sunucu ile çevresi ve problemler için izlenen hedef olarak sıralanabilir.

Bilgi Kaynağı

STS'ler, bilgi kaynaklarını analiz ve karşılaştırma yapmak için kullanırlar. Bilgi kaynakları, bilgisayar veya ağ paketlerinin dinlenmesinden elde edilebildiği gibi, kullanıcı profillerinin davranış modellerinden de elde edilebilir. Bilginin nasıl ve nereden toplanacağı, geliştirilecek olan STS'nin amaçlarına göre değişir. Bunlar; denetleme izi, ağ paketleri, uygulama kayıt dosyalarıdır.

Saldırı Tespit Yöntemi

STS'lerde, saldırı tespit yöntemi olarak anormallik tespiti ve kötüye kullanım tespiti olmak üzere iki farklı yaklaşım kullanılır [8]. Anormallik tespitine dayanan yaklaşım, sistemdeki kullanıcı davranışlarını modellerken, kötüye kullanım (imza) tespitine dayanan yaklaşım, saldırganların davranışlarını modeller.

Korunan Sistem

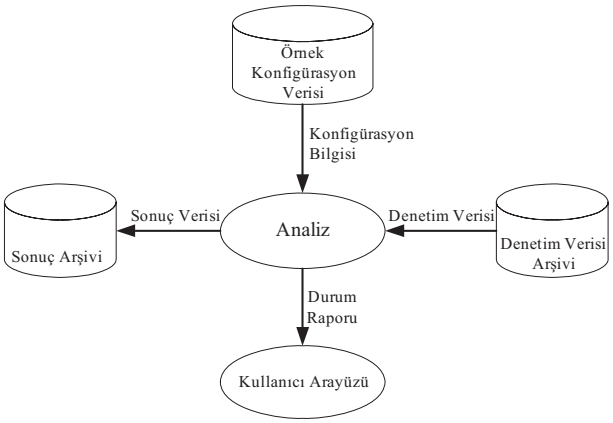
STS'ler korudukları sisteme göre üç gruba ayrılırlar. Korumak istenen sisteme göre; ağ, sunucu ya da uygulama temelli STS'ler olarak adlandırılırlar [14].

En genel anlamıyla, saldırı tespiti işini yapmak için geliştirilen sistemlere "saldırı tespit sistemleri" denir. Ancak günümüze kadar yapılan araştırmalar ve çalışmalar incelendiğinde, saldırı tespit sistemlerinin farklı tanımları olduğu görülmüştür. Yapılan bu tanımlara göre STS'ler;

- Bilgisayar sistemlerine yapılan atakları ve kötüye kullanımları belirlemek için tasarlanmış sistemlerdir [2].
- Tercihen gerçek zamanlı olarak, bilgisayar sistemlerinin yetkisiz ve kötüye kullanımı ve suistimalini tespit etmek için kullanılırlar [3].
- Saldırıyı durdurma girişiminde bulunmayan ve olası güvenlik ihlali durumlarında, sistem güvenlik çalışanlarına uyarı mesajı (alarm) veren sistemlerdir [4].
- Bilgisayar sistemlerinin kaynaklarına veya verilerine yetkisiz erişimleri belirler [5].
- Bilgisayar güvenliği alanındaki "hırsız alarm"larıdır [6].
- Bilgisayar veya ağ sistemine yapılan yetkisiz erişimleri tespit etmek için kullanılan yazılım araçlarıdır. STS'ler kötü niyetli ağ trafiği ve bilgisayar kullanımını tespit etme yeteneğine sahiptir. Bir STS, olası güvenlik açıklarını belirleyebilmek için bilgisayar veya ağ içerisinde değişik alanlardan bilgileri toplar ve analiz eder. Güvenlik duvarının statik izleme kabiliyetini tamamlayan dinamik izleme elemanıdır [7].

Yukarıda sunulan tanımlardan yola çıkarak, biz de STS'leri, bilginin elektronik ortamlarda taşınırken, işlenirken veya depolanırken başına gelebilecek tehdit ve tehlikelerin ortadan kaldırılması amacıyla, bilgiye yetkisiz erişim veya kötüye kullanım gibi girişimleri tespit edebilme ve bu tespiti sistem güvenliğinden sorumlu kişilere iletebilme özelliğine sahip yazılımsal ve/veya donanımsal güvenlik araçları olarak tanımlayabiliriz. Aynı zamanda STS'ler, ağ cihazlarını izleyerek anormal davranışları ve kötüye kullanımı tespit ederler.

Literatürdeki STS çalışmaları incelendiğinde, STS'lerin yapısı ile ilgili birçok gösterim yapıldığı görülmüştür. STS çalışmalarından biri olan NIDES'in geliştirilmesi sırasında çizilen örnek Şekil 1'de gösterilmiştir [8].



Şekil 1. STS'lerin temel yapısı [8]

Şekil 1'de sunucu tabanlı bir STS'nin temel yapısına bir örnek gösterilmiştir. Bu örnekte, bilgi kaynağı olarak denetim verileri kullanılmıştır. Denetim verisi arşivinden alınan denetim verileri, örnek konfigürasyon verileri ile karşılaştırılıp analiz edilerek, elde edilen sonuçlar, sonuç arşivine aktarılmaktadır. Aynı zamanda, olası saldırıların, kullanıcı tarafından görülebilmesi için kullanıcı arayüzüne de analiz sonuçlarını içeren durum raporu gönderilmektedir. İstenildiği takdirde, sonuç arşivi incelenebilir veya örnek konfigürasyon verileri güncellenebilir [8].

III. STS'LERDE KULLANILAN TEKNİKLER

Günümüze kadar STS'lerde birçok farklı teknik kullanılmıştır. Bu teknikler, elde edilen verilerin modellenmesi, sınıflandırılması veya kural tablolarının oluşturulması için geliştirilmiştir. Kullanılan tekniklerden elde edilen veriler sayesinde, saldırı tespit yaklaşımlarının uygulanması için gerekli olan platform oluşturulmuştur. Bu tekniklerden en çok kullanılanları, veri madenciliği, kural tabanlı sistemler, açıklayıcı istatikler, eşik değeri tespiti, durum geçiş analizi, uzman sistemler, örüntü eşleme olmuştur.

Veri Madenciliği

Veritabanındaki saklı olayları ortaya çıkarmak için yapılan bilgi açılımıdır. Paternleri ve veriler arasındaki ilişkileri bularak kural çıkarmak için kullanılır. Bu şekilde, hesap izlerini kullanarak normal kullanıcı aktiviteleri tanımlanır [15].

Kural Tabanlı (Rule Based) Sistemler

Sistem trafiğini inceleyip kurallar oluşturur ve saldırı tespiti sırasında belirlenen kurallara göre davranışlar sınıflandırılır [16].

Açıklayıcı İstatistikler (Descriptive Statistics)

Kullanıcı veya sistem davranışları farklı değişkenlere göre ölçülerek istatistiksel bir model oluşturulur. Bu değişkenlerden bazıları; kullanıcı oturum girişi, oturum kapatma, belli bir zaman periyodunda erişilen dosya sayısı, kullanılan disk alanı ve hafıza olarak sıralanabilir. Kullanıcı profilleri ve hesap izleri kullanılarak normal davranışların modeli oluşturulur ve anormallik tespit edilir [17]. Kullanıcı profilinin basit istatistiklerle oluşturulup, buradan uzaklık vektörlerini (distance vector) kullanarak karar alan sistemlerdir. Davranış profili oluşturulurken, kullanılan işlemci zamanı, bir zaman periyodundaki ağ bağlantı sayısı gibi farklı ölçütler de kullanılabilir. İstatistiksel yaklaşımların dezavantajlarından biri, saldırganın bu istatistikleri öğrenerek ona göre davranış sergileyebilmesidir [18].

Eşik Değeri Tespiti

Bu model oluşturulurken spesifik olayların tekrarlama sayısı ve spesifik zaman periyodu dikkate alınır. Karşılaşılan en büyük sorun; eşik değerinin belirlenmesi ve spesifik olaylar için pencere boyutunun belirlenmesidir. Örnek olarak; yanlış girişler, giriş/çıkış hata sayısı veya silme sayıları verilebilir. Tek başına pek güçlü değilse de büyük STS'lerde alt bileşen olarak kullanılır.

Durum Geçiş Analizi

Durum değişimi serileri oluşturularak gerçekleştirilir. Bir işin yapılması için birbirini takip eden durum sırası olduğu varsayılır ve buna göre bir seri oluşturulur. Sızmaların senaryosu çıkarıldıktan sonra, anahtar hareketler, imza hareketler olarak tanımlanır. İmza hareketler, saldırının tamamlanması için gereken en küçük hareket kümesidir. Durumlar, geçişler ve imzalar, durum geçiş diyagramı olarak grafiksel biçimde sunulur [19]. Burada tüm davranışlar durumlara karşı düşer. Eğer bir davranış daha önceden tanımlı durumlara ve durum geçişlerine denk düşen hareketler yapıyorsa saldırı olarak tanınır.

Uzman Sistemler

Belirli bir alanda sadece o alan ile ilgili bilgilerle donatılmış ve problemlere o alanda uzman bir kişinin getirdiği şekilde çözümler getirebilen bilgisayar programları olarak tarif edilebilir. Saldırı tespit sistemlerinin ilkleri kural-tabanlı uzman sistemlerdir [6].

Örüntü Eşleme

Sistemde daha önceden karşılaşılmaması gereken durumların tanımlanarak, bu durumlardan biri ile eşleşilmesi halinde saldırı olduğunu algılamak amacı ile kullanılır. Yapısı itibariyle esnek birçözüm değildir fakat basittir [6].

IV. ZEKİ STS'LER

Bilgisayar veya ağ sistemlerine yapılan saldırıları tespit ederek güvenliğin sağlanması için geliştirilen STS'ler, her ne kadar yapılan saldırıların büyük bir çoğunluğunu tespit edebilseler de daha önce hiç karşılaşılmamış olan saldırıların büyük çoğunluğunun tespit edilememesi ve bu saldırıların sistemlerde büyük zararlara yol açması, yeni saldırı çeşitlerinin tespit edilebilme başarısının artırılması ihtiyacını getirmiştir. Bu ihtiyacın karşılanması ve hızla değişen saldırı tiplerinin karşısında, bilgi ve bilgisayar güvenliğinin sağlanması amacıyla, STS'lerin geliştirilmesinde yapay zeka yöntemleri kullanılarak STS performanslarının iyileştirilmesi hedeflenmiştir. Yapay zeka tekniklerinin öğrenilebilmesi hızlı hesaplama, genelleme matematiksel olarak modellenmesi zor olan problemlere çözüm sunabilmesi gibi özellikler, bu yaklaşımların STS'lerde kullanılmasının önemli gerekçelerindendir. Zeki yaklaşımların kullanılmaya başlaması ile birlikte anormallik tespiti yaklaşımı biraz daha ön plana çıkmış ve bu sayede anormallik tespitinin yeni saldırıları tespit edebilme yeteneği arttırılmıştır.

Yapay zeka araştırmacılarının baştan beri ulaşmak istediği ideal, insan gibi düşünen ve davranan sistemler geliştirmektir. Ancak buna ulaşmanın güçlüğü anlaşılınca çalışmanın yönü rasyonel düşünen ve davranan sistemlerin tasarlanmasına çevrilmiştir. Geleneksel yöntemlerle çözümü zor veya imkansız olan problemlerin çözümünde kullanılan, yapay zeka

teknikleri, yapay sinir ağları, bulanık mantık, sezgisel (genetik, tabu arama, karınca koloni, ısıl işlem (tavlama) benzetimi, bağışıklık sistemi, arı) algoritmalar olarak sıralanabilir.

Bulanık Mantık

Bulanık mantık metodunu uygulama girişimleri, STS'nin farklı bileşenlerinin geliştirilmesi için 2000'li yıllarda başlamıştır. Bu çalışmalarla ortaya çıkan FIRE (Fuzzy Intrusion Recognition Engine) ile ağ verileri işlendikten sonra atakları tespit etmek için bulanık mantık kullanılmıştır [12]. Ağ paketleri üzerinde çalışılan FIRE'de, TCP, UDP ve ICMP için otonom ajanlar kullanılır [20]. Aynı zamanda kural tabanlı bir sistem olan bu çalışmada, güvenlik yöneticisi ve edinilen tecrübe sayesinde belirlenen bulanık kurallar oluşturulmuştur [21]. 2002 yılında bulanık mantığın, anormallik tespiti yapan bir STS'nin karar verme aşamasında kullanılması önerilmiştir [22]. Bu çalışmada bulanık mantık, uzman tarafından tavsiye edilen, bulanık "if-then" kurallarını temel alarak çözüm sunmaktadır.

Genetik Algoritmalar

Genetik algoritmalar STS'lerde, trafik verilerine basit kurallar uygulamak için kullanılabilir. Bu kurallar, anormal trafik verilerinden normal verileri ayırmak içindir. Veri kümesi, tcpdump ya da snort gibi trafik dinleyiciler (sniffers) kullanılarak toplanır [13]. Genetik algoritmalar öncelikle küçük boyutlu rasgele üretilmiş kurallar kümesi ile başlar, daha sonra bu kural kümesi genişletilir.

Yapay Bağışıklık Sistemi

Literatürde insan bağışıklık sistemine dayalı birçok STS çalışması sunulmuştur. Bu çalışmalardan bazıları doğal bağışıklık sistemi karakteristiklerinden esinlenerek, bilgisayar sistemlerinde anormallik tespiti için biçimsel (formal) çatı (framework) önermişlerdir. Doğal bağışıklık sisteminin, bağışıklığı tanımladığını düşündükleri 4 önemli özelliğini kullanmışlardır. Bunlar; farklılık (diversity), doğal dağıtık yapısı (distributed nature), hata toleransı (error tolerance) ve doğal dinamik yapısıdır (dynamic nature) [23].

Destek Vektör Makinaları

DVM'ler STS'lerde, özellik vektörünün seçilmesinde sıkça kullanılmıştır. Hızlı olmaları nedeniyle STS'ler için oldukça kullanışlı bir yöntemdir. DVM'ler geniş bir örnek setini öğrenebilir ve iyi ölçeklendirirler [24].

Yapay Sinir Ağları

Zeki yaklaşımların STS'lerde kullanılmaya başlaması, farklı birçok zeki yöntemin de kullanılabilir olduğunu göstermiştir. Bu tekniklerden hemen hemen hepsi STS'lerin geliştirilmesi için kullanılmış olsa da, elde edilen başarılı sonuçlardan dolayı en çok kullanılanlardan biri YSA'dır [25, 26].

YSA'lar, giriş ve çıkış vektörleri arasında ilişki kurarak kendi algoritmalarını uygularlar ve genelleştirerek yeni giriş/çıkış ilişkilerini ortaya çıkarırlar. Bu yaklaşım, sistemdeki kullanıcıların davranışlarının öğrenilmesiyle gerçekleşir. Spesifik bir kullanıcı için önceki komutlardan yola çıkarak yeni komutu tahmin eder.

V. YSA'NIN STS'LERDE KULLANILMASI

Yapay sinir ağları (YSA), saldırı tespit sistemlerinde 1990'ların başında kullanılmaya başlanan zeki yaklaşım yöntemlerinden biridir. YSA'lar, anormallik tespiti yapan STS'ler için istatistiksel yöntemlere alternatif olarak önerilmiştir [26].

YSA'ların STS'lerde kullanımı, YSA'nın normal sistem davranış izleriyle eğitilmesi ile başlar. Normal veya anormal olarak sınıflandırılan olay akışları yapay sinir ağına verilir. Toplanan veriler ile sistemin davranışına bağlı olarak öğrenme değişimi yapılabilir. Yani eğitim, izin veriliyorsa sürekli hale getirilebilir. Buradaki yaklaşım, kullanıcının n adet hareket veya komutundan, sonraki hareket veya komutunun tahminen eğitilmesidir [18]. Bu tahminin yapılması için öncelikle eğitim veri seti oluşturulmalıdır, daha sonra da eğitim tamamlanmalıdır. Eğitim verileri, belirli zaman periyodunda (birkaç gün) her kullanıcı için, sistem hesaplarından toplanır. Her gün ve her kullanıcı için veriler vektörel forma sokulur ki bu vektör kullanıcının her komutu ne kadar sıklıkta yürüttüğünü gösterir. Eğitim aşamasında ise daha önce elde edilen vektörler, kullanıcıları tanımlamak için eğitilir.

YSA'lar, anormallik tespitinde kullanıldığı gibi kötüye kullanım tespitinde de kullanılan bir tekniktir. Ağ ataklarının sürekli değişen yapısı, ağ trafiğini geniş çapta analiz edebilen ve kural tabanlı sistemlerden daha esnek bir savunma sistemi ihtiyacını doğurmuştur. YSA tabanlı kötüye kullanım tespiti yapan sistemlerle, kural tabanlı sistemlerde var olan bu tür problemlere çözüm sağlanabilmektedir [26].

YSA'lar, kötüye kullanım tespitinde iki farklı şekilde kullanılmaktadır [26]. İlk yaklaşımda yapay sinir ağları, zaten var olan bir uzman sistemin bir parçası olarak kullanılmaktadır. Bu yaklaşımda, saldırı tespitinin daha etkin yapılması amacıyla gelen verilerin filtrelenmesi ve uzman sisteme gönderilmesinde YSA'lardan faydalanılır. İkinci yaklaşımda ise, YSA'lar tek başına bir sistem olarak kötüye kullanımı tespit etmekte kullanılır. Bu yaklaşımda YSA, ağ akış bilgilerinden, kötüye kullanım tespitinin analizinde kullanılır.

YSA'lar, STS'lerde karşılaşılan pek çok problemlere esnek çözümler sunabilirler, YSA'nın çözüm sunduğu temel iki problem, veri redaksiyonu ve sınıflandırmadır [27]. Veri redaksiyonu (azaltma), işleme zamanını, iletişim yükünü ve depolama gereksinimlerini azaltmak amacıyla veri koleksiyonunu analiz ederek en önemli girişleri tanımlama işidir. Sınıflandırma ise saldırganları ve atak yapanları tanımlama işlemidir. YSA'lar pek çok STS'lerde bu iki önemli problemi çözmek için kullanılmışlardır [27].

STS'lerde karşılaşılan diğer problemler, istatistiksel yayılımı doğrulama ihtiyacı, tespit ölçütlerinin değerlendirilmesinin zorluğu, algoritma geliştirmenin yüksek maliyeti ve ölçeklemede zorluk olarak sıralandırılabilir [28].

YSA'lar bu problemlere de çözüm sağladığından dolayı STS'ler için oldukça uygun bir tekniktir.

YSA'nın STS'lerde kullanılmasının avantajları

(1) Kötüye kullanım ataklarının karakteristiğini öğrenmesi ve daha önce ağda kaydedilen örneklere benzemeyenleri ayırt edebilmesi,
(2) Hızlı sonuç üretmesi sayesinde gerçek zamanlı uygulamalar için kullanışlı olması,
(3) Gürültülü verilerle de çalışabildiklerinden, gürültülü verilerin sonuçları diğer yöntemlere göre daha az bozması,
(4) Farklı sistemlerle beraber çalışabilmeleri,
(5) Genel olarak çözüm sağlayabilmeleri yanında kısmi olarak da STS'lerin tasarımında kullanılabilmeleri,
(6) Az örneklerde sistemin veya atağın genel davranışını öğrenebilme yetenekleri olarak sıralanabilir.

Tüm bu avantajların yanı sıra, en büyük problem yapay sinir ağlarının eğitilmesidir. Yapay sinir ağı, etkin şekilde çalışması için iyi eğitilmelidir ve geniş bir veri seti kullanılmalıdır [1].

VI. Bilgi Güvenliğinde STS'lerin Önemi

İnternetin ve iletişim olanaklarının artmasıyla birlikte saldırganlar tarafından saldırılabilecek daha çok sistem ortaya çıkmıştır. Bu saldırıların büyük bir bölümü kullanılan sistemin kusurları veya eksiklerinden faydalanılarak yapılır. Bu tür saldırıları engellemenin iki yolu vardır; ilki tamamen güvenli bir sistem ve ortam oluşturmak, ikincisi ise saldırıları tespit edip gerekli önlemleri almaktır. Bunlardan ilki pratik açıdan mümkün olmamaktadır. Bunların gerekçeleri ise [18],

- Kullanılan işletim sisteminde var olan açıkların genellikle ilk olarak saldırganlar tarafından fark edilmesi ve önlem alınana kadar bu açıkların kullanılabilmesi,
- Veri iletiminde kullanılan protokollerin yapısında var olan bazı kuralların saldırı amaçlı kullanılabilmesi,
- Kriptografik metotların ve anahtarlarının kırılabilmesi, kullanıcıların şifrelerini unutabilmesi veya kripto-sistemin kırılabilmesi gibi nedenlerle yüksek seviyede bir güvenlik sağlanamaması,
- Dış ortama karşı güvenliği sağlanan sistemin, iç ortamlardan suistimal edilerek güvenliğin ortadan kaldırılması,
- Güvenlik amacıyla kullanıcı yetkilerinin minimuma indirilmesi sonucu kullanıcı verimliliğinin düşmesi gibi nedenleri vardır.

Sistemlerini korumak isteyenler, genelde saldırı gelene kadar bekleme pozisyonunda kalmak, saldırı geldiğinde ise olabildiğince hızlı tespit etmek isterler. Bu ise STS'nin yaptığı iştir [18]. Bir saldırının hangi adresten veya hangi porttan geldiğini bilmeden engel olmak mümkün değildir. STS'ler saldırıları tespit ederken bu bilgileri de elde ederler. STS'ler, detaylı olarak topladığı ve depoladığı bilgilerden yararlanarak, saldırıları olabildiğince erken tespit etme özelliğine sahiptir. Yine aynı bilgilerin incelenmesi ile daha önce hiç karşılaşılmamış bir saldırıyı da tespit edebilir. STS'leri de cazip hale getiren bu özelliktir.

VII. Sonuç ve Değerlendirmeler

Bu çalışmada, STS'ler genel olarak incelenmiş, STS'lerde kullanılan klasik ve zeki teknikler gözden geçirilmiştir.

Literatür incelemesinden elde edilen bilgiler doğrultusunda, çalışma genel olarak değerlendirildiğinde;

- Ülkemizde zeki saldırı tespit sistemlerine yönelik yeterli çalışma bulunmadığı,
- Ülkemizde geliştirilecek olan STS'lerin testinde kullanılabilecek bir veri kümesi bulunmadığı,
- Literatürde, veri kümesi oluşturmak için yapılan çalışmaların güncel olmadığı tespit edilmiştir.

Bu araştırmada elde ettiğimiz bilgi ve deneyimlere dayanarak, saldırıları tespit etme yöntemlerine göre ikiye ayrıldığını bildiğimiz STS'lerin, hangi yöntemin seçileceğine dair dikkat edilmesi gereken noktası, anormallik tespiti yönteminin, bütün kötü davranışları tespit etmeye çalışırken, kötüye kullanım tespiti yönteminin kötü olarak bilinen davranışları tanımaya çalışmak olduğudur. Her iki yöntemin de avantaj ve dezavantajları olduğu göz önünde bulundurularak, tasarımlarda avantajları bir araya toplayan hibrit yaklaşımlardan faydalanmanın daha gerçekçi olacağı değerlendirilmektedir.

KAYNAKLAR

[1] Ş. Sağıroğlu, M, Alkan, "Her yönüyle elektronik imza (e-imza)", Grafiker Yayınları, Ankara, 1-100 (2005).
[2] D. E. Denning, "An intrusion detection model", IEEE Transactions on Software Engineering, 13(2): 118–131 (1987).
[3] B. Mukherjee, L. T. Heberlein, K. N. Levitt, "Network intrusion detection", IEEE Network, 8(3): 26-41 (1994).
[4] M. Crosbie, E. H. Spafford, "Defending a computer system using autonomous agents", Technical Report 95-022, Dept. of Comp. Sciences, Purdue University, West Lafayette, 1-11 (1995).
[5] D. Endler, "Intrusion detection applying machine learning to solaris audit data", 1998 Annual Computer Security Applications Conference (ACSAC'98), 268-269 (1998).
[6] S. Axelsson, "Intrusion detection systems: A survey and taxonomy", Technical Report 99-15, Dept. of Computer Eng., Chalmers University of Technology, Göteborg, Sweden, 1-23 (2000).
[7] A. Patcha, J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends", Computer Networks, 51(12): 3448-3470 (2007).
[8] D. Anderson, T. F. Lunt, H. Javitz, A. Tamaru, A. Valdes, "Detecting unusual program behavior using the statistical component of the next-generation intrusion detection expert system (NIDES)", SRI-CSL-95-06, Menlo Park, California, 1-22 (1995).
[9] C. Endorf, E. Schultz, J. Mellander, "Intrusion Detection & Prevention", Jenn Tust, Jody McKenzie, Elizabeth Seymour, McGraw-Hill, California, 10-150 (2004).
[10] T. F. Lunt, "Automated audit trail analysis and intrusion detection: A survey", 11th National Computer Security Conference, Baltimore, MD, 65-73 (1988).
[11] S. A. Hofmeyr, "An immunological model of distributed detection and its application to computer security", Doktora Tezi, Computer Science, University of New Mexico, 1-69 (1999).
[12] J. E. Dickerson, J. A. Dickerson, "Fuzzy network profiling for intrusion detection" NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta, 301-306, (2000).

[13] A. Murali, M. Rao, "A survey on intrusion detection approaches", First International Conference on Information and Communication Technologies, IEEE Communications Society Press, 233-240 (2005).
[14] A. K. Jones, "Computer System Intrusion Detection: A Survey", Technical Report, Computer Science Dept., University of Virginia, Charlottesville, Virginia, 1-21 (2000).
[15] W. Lee, S. J. Stolfo, P. K. Chan, E. Eskin, W. Fan, M. Miller, S. Hershkop, J. Zhang, "Real time data mining-based intrusion detection", Second {DARPA} Information Survivability Conference and Exposition (DISCEX II), Anaheim, CA, 89-100 (2001).
[16] K. Ilgun, R. Kemmerer, P. Porras, "State Transition Analysis: A RuleBased Intrusion Detection System", Software Engineering, 21(3): 181-199 (1995).
[17] İnternet: Knowledge Discovery and Delivery, "KDD Cup 1999: General Information",http://www.sigkdd.org/kddcup/index.php?section=1999&method=info (2007).
[18] A. Sundaram, "An introduction to intrusion detection", Crossroads: The ACM Student Magazine, New York, USA, 2(4), 3-7 (1996).
[19] P. A. Porras, "STAT: A State Transition Analysis Tool for intrusion detection", Yüksek Lisans Tezi, Computer Science Department, University of California, Santa Barbara, 1-150 (1992).
[20] J. E. Dickerson, J. Juslin, O. Koukousoula, J. A. Dickerson, "Fuzzy intrusion detection", IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conference, Vancouver, British Columbia, 3: 1506-1510 (2001).
[21] K. Lee, L. Mikhailov, "Intelligent Intrusion Detection System", Second IEEE International. Conference on Intelligent Systems, 2: 497-502 (2004).
[22] S. B. Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection System", IEEE Transactions on Systems, Man, and Cybernetics, Part C 32(2): 154-160 (2002).
[23] F. Esponda, S. Forrest, P. Helman, "A formal framework for positive and negative detection schemes", IEEE Transactions on Systems, Man, and Cybernetics, Part B, Cybernetics, 34(1): 357-373 (2004).
[24] S. Mukkamala, A. H. Sung, A. Abraham, "Intrusion detection using ensemble of soft computing paradigms", Third International Conference On Intelligent Systems Design and Applications, Germany: Springer, 239-248 (2003).
[25] R. E. Wassmer, J. H. Fikus, "Advanced Intrusion Detection Techniques", Final rept., Defense Technical Information Center - ADA410454, 2. evre, 1-14, (2003).
[26] J. Cannady, "Artificial neural networks for misuse detection", Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), Arlington, VA, 443-456 (1998).
[27] J. Frank, "Artificial intelligence and intrusion detection: current and future directions", Division of Computer Science, University of California at Davis, 1-12 (1994).
[28] S. Peddabachigari, A. Abraham, C. Grosan, J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems", Journal of Network and Computer Applications, Elsevier, 30:114–132 (2007).

E-Sağlık/Tele Sağlık Yönetişiminde Uzaktan Eğitim ve Güvenli Bilgi Yönetim Sistemleri

Akın MARŞAP

***Özet*- 21 nci yüzyılda e-sağlık/tele sağlık yönetişim sistemi sağlık ve hastane yönetimin sürecinde giderek artan bir öneme sahip olduğunu göstermektedir. Bu anlamda yapılan tüm gayretler uzaktan eğitim ve güvenli bilgi yönetim sistemlerinin bütünlüğü içinde yenilenen bir yapıda ele alınarak değerlendirmelidir. Tele sağlık sistemi uygulamaları bilişim ve iletişim teknolojilerini etkin bir şekilde kullanarak büyük oranda bir gelişim göstermiştir. Organizasyonlar e-sağlık politikaları alanında birçok yenilikleri başarı ile yapıyor olsa da, bu sistemi kullananlar tarafından zaman zaman farklı biçimde algılanabilirler. Bu açıdan e-sağlık entegrasyonu ve uygulamaları araştırma ve gözden geçirmeler ışığında karşılaşılan engellerin zamanla aşılacağı açıktır. Buna karşın, e-sağlık sisteminin e-öğrenim sürecinde tam potansiyelinin anlaşılarak geliştirilmesi oldukça önemlidir. E-sağlık yönetişiminde uzaktan eğitim sistemi (UES), geleceğin e-öğrenim sürecinde yaşamsal bir öneme sahiptir. Bu bildirinin amacı e-sağlık yönetişim sürecinde uzaktan eğitim sisteminin yüz yüze eğitimle desteklenerek güvenli bilgi yönetim sistemlerinin önemi üzerinde durulmaktadır.**

***Anahtar kelimeler*- E-Sağlık/Tele sağlık yönetişimi, uzaktan eğitim, sağlık ve iyilik, güvenli bilgi yönetimi.**

***Abstract*- Overall, it is considered the issues identified the e-health/telehealth governance systems has an increasing role in good health and hospital management process in the 21 st century. For this reason every efforts must be made the combination of distance education systems and information security systems must be consider in modernisation of new conditions. The advent of telehealth has seen the rapid growth and application of information and communications technology in many areas of healthcare. Organisations may well have develop some e-health policy, but to the general e-health user, the reality appears different. Also, when implementing and integrating e-health, it is clear the focused literature searces and reviews, that tecnological barriers are no longer a major issue. Rather, policy related issues remain major impediments to the further development of e-health and realization of e-learning of full potential. Consequently, distance education systems(DES) has an critical role for e-health management systems. This paper is studied for to explain the major importance of distance education systems that including face to face (formal) education and security of information management systems.**

***Keywords*- E-Health/Telehealth govarnance, distance education systems, health and wellness, secure of information management.**

Akin MARSAP Yönetim ve Organizasyon Uzmanı, UE Danışmanı, Ankara, E-posta: akinmarsap@yahoo.com

I. GİRİŞ

Yönetim; işletmenin yada organizasyonun, elindeki kaynaklarını planlayarak, organize ederek, yürüterek ve kontrol ederek etkili ve verimli bir şekilde kullanıp amaçlarını gerçekleştirme sürecidir [1]. Bu anlamda yönetişim; yönetim, etkileşim ve iletişim işlevlerinin etkin bir biçimde bütünler. Kurumsal yönetişim, 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 yönetişim, işletmenin üst yönetiminin yönetilmesidir. Kurumsal yönetim etkinliği; yapılandırma, performans ve uygunluğu işlevleri ile sağlanabilir [2]. Bilişim toplumu çağdaş yönetişim süreci; e-sağlık/tele sağlık alanında açıklık, şeffaflık, paylaşım, güvenlik ve hesap verilebilirlik ilkelerini ön plana çıkarır. E-Sağlık/Tele sağlık işletmeciliğinde yeniden dönüşen dijital dünyaya öncülük edecek öncül nitelikteki ciddi adımlar UES içinde e-öğrenim sürecinden geçmektedir. Bilişim teknolojilerinin sağladığı yeni olanaklar e-sağlık yönetişiminde UE'de e-öğrenim için olduğu kadar, e-randevu, e-reçete ve dijital hastane sistemlerinin işlerliğini ve sürekli gelişimini hızlandırmaktadır. Bu açıdan değerlendirildiğinde, sağlık sektöründe insan kaynakları yönetimi/eğitimi konusu daha stratejik bir rol almış bulunmaktadır. Sağlık idarecileri, doktor, hemşire, hastabakıcı, diğer tıbbi ve idari personelden oluşan stratejik insan kaynaklarının hasta ve hasta yakınlarına yönelik tüm kritik işlemleri için eğitim/öğretim süreci artan bir önem kazanmıştır. E-Sağlık/Tele Sağlık yönetişimin temel amacı, genel sağlık sistemi organizasyonu açısından gerçek durumuna ilişkin tam/doğru ve zamanında yapılan açıklamalar, yönetimin özellikle tüm ilgili birimlerin çıkarlarını gözetecek şekilde çalışmasını dijital sistemlerin güvenli desteğinde kaliteli/verimli ve etkin bir biçimde sağlamaktır. Bu giderek yenileşen yaklaşım içinde, e-sağlık/tele sağlıkta sağlanan esneklik, birey-hastane-doktor/hemşire ve idari yönetim arasındaki işleyiş akışına; yaratıcılık, gelişim ve sürekli yenilikçi açılımlar sağlayabilir. Günümüzde e-sağlık/tele sağlık yönetiminde UES'nin 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 çıkmaktadır. Kısacası bu süreçte, tele tıp/tele sağlık eğitim sisteminde UES'de yatay akademik yaklaşımların, bilimsel, akademik ve dinamik süreçleri kapsayacak biçimde yeniden tasarımlanarak gelişimi önemlidir. Bu açıdan, sağlıkta

UE sürecinin yüz yüze eğitim sistemleri ile gelişimi sağlık UES mimarisinin güvenli bilgi yönetim sistemlerine dayalı çalışmalarında önemlidir. E- Sağlıkta UES'nin yönetim ve organizasyonu, insan kaynakları, akademik danışmanlık, yüz yüze eğitim ve sonuçların değerlendirilmesini de içeren e-öğrenim/dönüşüm süreçlerini kapsamaktadır. 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. Sağlık hizmetleri, insanların fiziki ve zihni durumlarının korunup onarılarak iyileştirilmesi amacı ile gerçekleştirilen bütünsel faaliyetlerdir. Sağlık hizmetleri; insanın sağlığına zarar veren çeşitli faktörlerin tesirinden korunarak hastaların tedavisi, bedeni ve zihni kabiliyetleri azalmışların sağlıklarına kavuşturulması amacıyla uygulanan tıbbi faaliyetlerdir [3].Koruyucu ve tedavi edici sağlık hizmetlerinde, toplumun sağlığını üst düzeyde tutmak sağlık yöneticilerinin en büyük hedeflerindendir. Sağlık kurumlarının istenilen amaçları başarmalarının temel koşullarından ilki, bilimsel esaslara göre eğitim ve yönetimidir. Başka bir deyişle sağlık kuruluşunda, yönetimin başarısının göstergesi, ne kadar hasta bakıldığı, yapılan tetkik ve ameliyatlar yanında; sürekli eğitim/öğretime verdiği önem, hizmet alanların ne oranda hizmetten fayda gördüğü ve memnun kaldığıdır. Sağlık hizmetlerinin yönetimi, sağlık kuruluşlarının mimarisinden başlayarak, laboratuar, ameliyathane, dosyalama ve arşiv, otelcilik, yeme-içme ve temizlik, eczane hizmetleri gibi çok geniş bir yelpazeye yayılan hizmetlerin yönetimi, İK planlaması ve yönetimi, finansal yönetim gibi birbirinden farklı pek çok faaliyetin bir arada yürütülmesini getirmektedir [4].Özetle, hastaneler açık dinamik bir sistemdir. Sistem, parçaların sağlık ve iyiliği sağlamak için bir araya gelen alt sistemlerden oluşan bir bütündür. Bütünü oluşturan bu parçaların her birisinin kendisine has işleyiş özelliği vardır ve aynı zamanda her birinin etkinliği de birbirine bağlıdır. Hastaneler iç/dış çevreleriyle sürekli olarak bir etkileşim halindedirler. Sağlık yönetiminde ilk aşamada çağdaş hastaneler ve hastane yönetimi gelmektedir. Hastaneler, sağlığı bozulan kişilerin muayene, teşhis ve tedavilerinin yapılıp sağlık bakımı hizmetlerinin sunulduğu işletmelerdir. İnsanın kendi bakımının başkası tarafından yapılması kabul edilmesi zor bir duygudur. Onun için toplumun en önemli ve ayrıcalığı olan, çoğu zaman da hiç ilgilenilmeyen ve en az verim alınan kurumları hastanelerdir. Hastanelerin birinci amacı hastaneye gelen hasta ve yaralılara için gerekli tıbbi yardım ve hemşirelik bakımını sunmaktır. [5]. Hastanelerin fonksiyonel yapısı; tıp hizmetleri, hemşirelik hizmetleri, para medikal hizmetler, destek hizmetleri olarak dört grupta incelenebilir. Sağlık hizmetlerinin diğer hizmetlerden ayrılan temel özellikleri vardır. Bu özellikler şu şekilde sıralanabilir[6]:Soyutluk, sosyal sorumluluk, yüksek iş birliği, yüksek maliyet, sağlık piyasalarında eksik rekabet şartları, hızlı değişim, belirsizlik, ikame edilemezlik, ertelenemezlik, değişimlere uyum zorluğu, homojen olmayan yapı, yönetimde otorite sorunu ve hata kabul etmeyen bir yaklaşımdır.

II. DEĞİŞİM SÜRECİNDE HASTANELER

Topluma sağlık hizmeti sunan bir kurum olarak hastaneler, gerek meslek dalı, gerekse uzmanlık alanları yönünden çeşitlenerek; uzaktan muayene, e-randevü, e-reçete ve diğer uzaktan eğitim sistemleri yoğun kullanılmaktadır. Bu nedenle hastaneler; tedavi ve tıbbi bakım 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. Hastane işletmeleri, bir açıdan diğer işletmeler gibi çevresinden farklı girdiler alıp bunları bir süreçten geçirip nihai olarak bir hayati öneme haiz bir hizmet sunarlar. Hastane işletmelerinde dış çevre ve ürün yelpazesi karmaşıktır. Süreç açısından işlevler değişiktir. Nihai ürünün geri bildirim mekanizması tam organize edilememiştir. Karmaşıklığın bir başka nedeni ise, her hasta için farklı uygulama gerekebileceği ve bunun sonucu girdilerin çeşitlenmesidir. Sağlık ve iyiliği sağlayan hizmetlerinin temel özelliği itibariyle eğitim/öğretim başta olmak üzere işlevsel süreçlerin her evresinde yüksek bir güven faktörünün ön planda olduğu yapılardır. Modern sağlık hizmetleri hastalara anında, çabuk, tam ve doğru yanıtlar verebilmelidir. Çünkü tüm sağlık hizmetinin sunumunda hastanın hayatı söz konusudur. Bunun yanında sağlık hizmetlerinde hastaların ihtiyaç ve beklentileri her geçen gün değişmektedir. Tıpta gelişen yeni buluşlar ve çözümlerin yanında bütün bunların hasta/hasta yakınlarıyla sağlıklı iletişim ve evrensel tıp etik ilkelerinin ışığında birleştirilmesi gereklidir. Bunun için hastane işletmesinin faaliyetine başladıktan sonrada yenilikleri çok yakından izlemesi gerekir.. Bunun için, hastanelerin tüm bu hızlı değişimleri anında takip edip cevap verebilmesi büyük bir önem taşımaktadır. Sağlık ve sağlık hizmetlerine olan talep diğer ürün ya da hizmetlere olan talepten farklılık içermektedir. Sağlık hizmetlerinin yapısal itibariyle gösterdiği çeşitli özellikler sağlık sektöründe talep analizi yapmayı engellemektedir. Çünkü kişilerin sağlık hizmeti için ne kadar ödeme yapmaya istekli ve ödeme yapabilir olduğunu tespit etmek güçtür [7]. Hastanelerde hizmetlerin özelliği, kesintisiz hizmet, hastanelerin mimari yapısı ve fiziksel özelliği ve karmaşık yapı, açık ve dinamik sistem özelliklerini taşımaktadır [8]. Bu temel ilkelerin yanı sıra, bilişim teknolojilerinin sunduğu yeni olanakları kendi bünyesinde değişim sürecine uyumlu geçişler sağlayan modeller sağlıkta hizmet kalitesi, etkin zaman kullanımı ve gelişimi de beraberinde getirmektedir.

III. E-SAĞLIK/TELE SAĞLIKTA UZAKTAN EĞİTİM SİSTEMLERİ

Genel anlamı ile eğitim bireylerdeki öğrenim eğilimlerini toplumun beklentileri doğrultusunda karşılayıcı davranışlar kazandırış süreci olarak düşünülebilir [9]. Ağ tabanlı öğretimde seslendirilen kalite ile ilgili sorunlar, sistemin işleyişi gereği ortadan kalkmaktadır. Katılımcılar sınıf geçmek için değil öğrenerek öğrendiklerini

bir işe dönüştürmek için çalışmaktadır. Sınıf geçmek için çalışan öğrencilerde görülen bir zaman baskısı, sınıfta küçük düşürülme, diğer arkadaşlarıyla kıyaslanıp rencide edilme gibi durumlar olmadığından, kendine uygun zamanlarda öğrencinin öğrenim için çalışması kaliteyi beraberinde getirmektedir [10]. E-Sağlık/Tele sağlık yönetişiminde bilişim teknolojilerinde tasarruf, ya da gelirleri artırmak amacı internet çağının hız faktörü kurumsal planların çok yönlü kullanımına avantajlar sağlayabilir. E-sağlık/Tele sağlıkta UES'nin yenileşiminde aktif katılımlı akademik etkileşim süreçlerinin zenginliği yaşam boyu eğitim sürecinde öncül rolü olan gerekli bir ögedir. UES'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 oluşturmasına katkıda bulunur. Her bireyin çalıştığı iş ya da kurumdaki durumuna ilişkin bir fikri vardır. Kurum ve yöneticilerin çalışanlara sürekli geribildirimi, farkındalık düzeyi açısından gerçekçi bir zemin sağlar. Aslında olumsuz geribildirim alımı, olumlu geribildirim almaktan daha zordur. Dolayısıyla yapıcı olumsuz geribildirimin değerini bilmek ve ondan yararlanmak gerekir [11]. 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 [12]. E-öğrenim, öğrenenin bireysel öğrenim etkinlikleri ile kendi başına bireyselleştirilmiş bir öğrenim pratiği yanında eş zamanlı ya da eş zamansız diğer öğrenen ve öğretenler ile birlikte bilgisayar ağları üzerinden kurulan bir etkileşim ortamının paylaşılır. Web'in eğitim ortamlarında kullanımında biricik özelliklerden bir tanesi katılımcılar arasında etkileşimdir [13]. 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 donanıma sahip araştırıcı 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[14]. Entegrasyonun yarattığı değişimin aşamaları, değişim benimseme, alışma, kabullenme ve kullanma olarak dört evreden geçmektedir [15]. Şüphesiz bu evrelerde izlenebilirlik yönetimi bilgi güvenliği için önemlidir. İzlenebilirlik yönetimi, bir ürünün üretildiği, dağıtıldığı ve bulunduğu yerler, geçirmiş olduğu işlem ve uygulamaların saptanarak raporlanmasını sağlayan yazılım bileşenlerini kapsar[16]. İnternet üzerinden iletişimi gerçekleşen bilgilerin güvenirliği, açık anahtar kriptografi olarak adlandırılan bir teknikle (şifreleme ve şifre çözme, kurcalama/sezme, kimlik doğrulama, inkar edememe) içeriğinde sağlanabilir. [17]. Güvenlik sürecinde kullanılan sayısal sertifikalar, bir kişi, sunucu ya da bir organizasyonun kimliğinin tanımlanarak bir açık anahtarın bu kimlikle ilişkilendirilmesinde kullanılan elektronik belgelerdir [18]. E-Sağlık/Tele Sağlıkta UE yeni bir ortamında ağ tabanlı eğitim kavramı, dijitalleşen hastanelere yönelik değişim sürecinde eğitimde yaşanan bu dönüşüme paralel öğretim ortamlarına ait kavramı temelden değiştirmiştir. Gerçek anlamda sağlıklı 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-Sağlık/Tele Sağlık alanında akademik değerlendirme kurulları arasında iletişimin arttırılarak eşgüdümün kazanımında yararlıdır. E-Sağlık alanında UES'de kalite odaklı çalışmaların çeşitli bakımlardan geliştirilmesinin uygun olacağı değerlendirilmektedir;

1. E-Sağlık/Tele Sağlıkta kaliteli yönetim, gözetim ve denetim
2. E-sağlık öğretim sürecinde katılımcı geribildirimleri
3. Akademik kaliteye yönelik işlemler ve yeni araştırmalar
4. E-Sağlık/Tele Sağlık eğitim destek kalitesinin artırılması
5. UE sürecinde yüz yüze eğitim katkısının sağlanması

E-Sağlık/Tele sağlık alanında yeni gelişimler UES' de kullanılan teknolojilerin, iletişim-ortam-etkileşim ve teknoloji ilişkilerinin entegrasyonu daha güvenli bir bilişim modeli boyutunda tasarımını ortaya çıkarabilir. Etkileşim iki ya da daha fazla taraf arasındaki iletişimdir. Ancak UES'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 [19]. UES 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. UES'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 [20]. 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 bir esnek ve 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 [21]. 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 [22].

IV. E-SAĞLIKTA E-ÖĞRENİM VE YÜZYÜZE EĞİTİM

UE süreci, çoklu öğrenim yaklaşımlarının aşamalı işletimini sağlayabilecek özelliktedir. Böylece; aktif, bireysel, katılımcı, keşfedici ve etkileşimli öğrenim süreçleri başarı ile uygulanabilir. UE derslerinde, öğrenci-içerik etkileşimi, öğrenci-eğitmen etkileşimi ve öğrenci-öğrenci etkileşimi olarak üç tür etkileşim tanımlanmıştır. UES'de katılımcıların katılımcı-danışman etkileşimi ve katılımcı-katılımcı etkileşimi sınırlı gerçekleştiğinden dolayı, katılımcı-içerik etkileşimi öğrenim hedeflerine erişim açısından kritik öneme sahiptir. UE katılımcılara sağlanan içerikle etkileşim olanakları e-öğrenimi kolaylaştırıp öğrenim sürecini olumlu yönde etkiler. Bir anlamda artan zenginliği sağlar. UE, genel anlamda, geleneksel eğitim kurumlarının eğitim hizmeti insan topluluklarına her düzeyde eğitimi amaçlayan bir eğitim yaklaşımıdır. UE temel öğretim malzemesi uzaktan öğretim teknikleriyle kendi kendine öğrenime uygun hazırlanmış dijital ders kitapları ve danışman öğretim üyelerinin rehberliğinde işlenir. UE sisteminde, bilgi teknolojilerine dayalı etkileşimli öğrenim ortamların tasarımı çok çeşitli yararlar sağlar. UES'de tasarlanan çeşitli e-öğrenim uygulamaları şöyle sıralanabilir,

1. UES'de; uzman ve aktif bir akademik danışmanlık birimi,
2. E-öğrenim sürecinde sanal sınıf ortamlarında etkileşim,
3. Dijital sesli kitaplar ve çoklu ortam alıştırma testleri,
4. İnternet üzerinden zamanlı ara, final ve deneme sınavları,
5. İnternet üzerinden yapılan ödevler, proje çalışmaları,
6. E-kütüphane hizmetleri ve ar-ge birimlerine erişim
7. E-öğrenimD akademik e-konferans ve e-seminerler
8. Yüz yüze eğitim/öğretimin %50 'si oranında sağlanmasıdır.

İnternet, daha katılımcı bir öğrenim ortamı için büyük bir kapasitedir, gelecekte e-öğrenim oranı internet üzerinden, internet öğretişimi sağlar. İnternet öğretimde sosyal iletişimi güçlendirip öğrencileri mobilize ederek, eğitim birimlerinin şeffaflığı, danışman ve öğrenciler arasındaki mesafeyi azaltarak doğrudan öğretimi kolaylaştırır. Klasik eğitim ortamı dışında yaşam boyu öğretim ilgisini çekmiş gruplar yeniden kazanılarak eğitime katılımcılık artacaktır.

V. E-SAĞLIK/TELE SAĞLIK VE GÜVENLİ BİLGİ YÖNETİMİ

E-Sağlık/Tele Sağlık alanında özellikle "E-Sağlık Kayıtları", "Teletıp Projeleri" e-Devlet ve e-Sağlık/Tele Sağlık uygulamaları ile ilgili yasal düzenlemeler, sağlıkta dönüşüm programı'nın en önemli bileşenleridir. Sağlık sektöründe en iyi bilinen sorunlar yaşlanan nüfus, artan maliyetler, kaynak ve bilgi yönetiminde yaşanan sıkıntılardır. Bu açıdan sağlıkta uzaktan eğitim e-sağlık stratejisinin temelinde sağlık-net omurgasını, standartları, veri elemanları, tanımlamalar ve kodları oluşturan ulusal sağlık veri sözlüğü, kan bankaları veri paylaşımı", "çevrimiçi sağlık hizmetleri, aile hekimliği ve hastane YBS temelini oluşturur. Ulusal sağlık YBS, yaşam boyu sağlık kayıtlarında sağlık bilgilerinin gizlilik, güvenlik ve mahremiyet ilkeleri doğrultusunda korunmasını sağlamak için sayısal güvenlik önemlidir. Özellikle radyoloji ve patoloji alanında çekilen görüntüler, uluslararası standartlara uygun bir şekilde sayısal görüntü haline çevrilir. Hastanelerde bilgi sistemi ile tam entegre sayısal görüntüleme sistemleri; yeni gelişen teleradyoloji, teleekg ve telebiyokimya servislerini de kapsamı içene alır. Çok çeşitli kronik hastalıkların izlenerek evde bakım teknolojileri, kuşkusuz sağlık bilgileri, özelliği nedeniyle, gizlilik, güvenlik ve mahremiyet ilkeleri doğrultusunda büyük bir titizlikle korunan bilgilerdir. E-sağlıkta 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 ögeler sisteme entegre edilmelidir. Bilginin güvenli tutulması, bilgi güvenliği politikaları ve teknik altyapı olmak üzere iki önemli safhayı içerir. E-sağlıkta UE organizasyonunda güvenlik stratejisi bu ölçütler doğrultusunda değerlendirilerek, ortaya çıkacak yeni gereksinimlere göre güvenlik ölçütleri değişik düzeylerde yeniden incelenmelidir. Bu anlamda e-vatandaşlık kartı güvenliğin en üst düzeyde sağlanarak, kişilerin e-sağlık kayıtlarına hasta izni doğrultusunda erişim yetkisi ile mümkündür. Ulusal doktor veritabanı, online randevu, laboratuar ve tahlil sonuçlarının sunumu önem kazanır. E/M imza yasası kapsamında e-hasta kayıtlarına erişim denetimi ve gizlilik ilkelerine yönelik yasal düzenlemelere yardımcıdır. Kişisel sağlık bilgilerinin dijital ortamlarda korunması, gerektiğinde kişinin izniyle istendiği yerden ulaşılabilmesi ve kişilerin tanınmasını önleyecek şekilde toplumsal bilgilerin istatistiki sonuçlarının yaygın kullanımı sağlık sektörünün verimlilik ve etkinliğini önemli ölçüde artırabilir. Kişilerin

aşıları, geçirdiği hastalıklar, teşhisleri içeren bilgiler kayıtlanabilir. Kişisel sağlık bilgilerinin ortak bir standart çerçevesinde, gerektiğinde paylaşılabilir bir sistemde saklanabilmesini sağlayacak e-sağlık sistemi çok önemli faydaları da beraberinde getirebilir. Hastaların sağlık geçmişi, alerjileri, kan grubu gibi önemli bilgilere acil durumlarda (örneğin hastanın bilincinin yerinde olmadığı bir durumda) hastanedeki görevli personel tarafından ulaşılabilmesi birçok hayatın kurtulmasına yardımcı olabilir. Hastalar kendileri ile ilgili teşhise temel olan bilgileri istedikleri başka doktorlarla da kolayca paylaşarak ikinci bir görüş alabilirler. İlaç firmaları belli rahatsızlıkları olanlara ya da belli ilaçları kullananlara gerektiğinde (örneğin üretim aşamasındaki bir sorun veya yeni elde edilen bir bilgi nedeniyle) kolaylıkla ulaşarak olası sağlık sorunlarını oluşmadan engelleyebilirler. Kişinin özel izni olmaksızın bilgilerin kişileri tanımlayacak bir şekilde paylaşılmaması ve bu konudaki gizliliğe özenle uyulması sistemin çok iyi denetimini gerektirir. Bilgilerin gerektiğinde kolaylıkla paylaşımında ortak standartlara, bilgilerin gizliliğinin korunabilmesi için de güvenilir denetim ve gözetim sistemlerine ihtiyaç vardır. Bu nedenle, e-sağlık/tele sağlık sisteminin kamusal bir niteliği olduğu göz önüne alınmalıdır. Özetle, sağlık sisteminin maliyetlerini kontrol ve etkinliğini artırarak yaşam kalitesini geliştirmek için başta kişisel sağlık bilgilerinin güvenli bir şekilde dijital ortamlarda saklanması e-sağlık uygulamalarına önemlidir. E-Sağlık/Tele Sağlık bilgi ve iletişim teknolojilerinin tüm fonksiyonlarını bireylerin hizmetine daha hızlı, doğru ve güvenilir bir biçimde sunabilir. E-sağlık insan sağlığı için tıp ve bilişimdir. Teknolojilerinin yapı taşı olarak, kimlik denetim sistemi kullanıcıların kimliklerini doğrularken servislere yetkisiz girişleri engellemek için önemli bir rol üstlenir. Bu karakteristiklere göre kimlik denetim sistemi tarafından karşılanması gereken ihtiyaçlar; sağlamlık, alan-kesiştirici kimlik denetimi, ölçülebilirlik ve performans olarak sıralanabilir [23]. 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 [24]. Çağdaş yönetişim sürecinde yöneticiler, e-iş hukukî ve teknik yönleri ile kullanımına ilişkin esasları dikkatlice izlemelidir. İnternetin yaygınlığı ve iletişim teknolojileri ilerlemeler e-devletin yaygınlığına büyük katkı sağlar. Bu yaygınlık e- ortamda yapılan işlemlere güven gereksinimini beraberinde getirmiştir. Dolayısıyla taraflar arası iletişimde bilginin gizliliği ve bütünlüğünü garanti edecek kimlik doğrulamayı sağlayacak hukuki zeminin hazırlanışı önem kazanmıştır [25]. Örneğin, bankacılık sektöründe, internetten kredi başvurusu yapılabilen, insansız, dijital ve mobil iletişimin iç içe geçtiği bir uygulama ile bankacılık işlemlerine yeni bir boyut getirir. Bankacılık işlemlerinde talimat vermekten, kredi işlemlerine kadar pek çok işlemin gerçek anlamda banka şubelerine gitmeden yapılabileceği bir dönem başlıyor. E-imzayı bankacılık sistemine adapte ederek kısa sürede kapsamı genişliyor [26]. Sonuç olarak sağlık alanında stratejik insan kaynaklarının yerinde ve zamanında kesintisiz eğitim/öğretimi ve gelişim/değişimi sağlanabilir. Bilişim toplumunda entelektüel sermayenin yönetiminde sağlıklı ve güvenli olarak işletimi esastır.

VI. SONUÇ VE DEĞERLENDİRMELER

Bu açıdan, e-Sağlık/Tele Sağlık yönetişiminde uzaktan eğitim uygulamaları oldukça farklı sistemlerin bütünsel ve hassas bir entegrasyonunu gerektirir. UES ile e-öğrenim olanakları kurumsal çapta teknoloji firmaları öncülüğünde, kendi çalışanlarına yönelik eğitimler güvenlik kültürünü de kapsayan bir yaklaşım içinde sağlar. Zaman-mekan tasarrufu ve kişilerin iş performanslarını da artırıcı etkileri tercih edilen bir konumdadır. E-sağlık sistemi öğrenim süreçlerinde ortaya çıkan zayıf yönlerin zamanında yüz yüze eğitim süreci ile desteklenerek giderilişidir. Sistemin olgunluğa erişimi, tasarım ve sistematiği, belli standartların kullanılışı, hazırlanan içeriklerin sürekli güncellenerek çekiciliğinin arttırılışı, çalışabilirliği, kalitesi, birbirleriyle uyumlu hale gelen internet alt yapısında, öğrencilerin derse katılımının artışında çekici bir model yapısına erişim esastır. UES bütünsel yapısında kişinin en kısa sürede davranış değişikliğine yol açan, kendine ve iş sonuçlarına pozitif etkili eğitsel aktivitelerin uyumlu birliğidir. Diğer yandan, UES içinde internet üzerinden, sanal sınıflarda yapılan derslerin yanı sıra, yüz yüze eğitim olanaklarının bireşimi karma eğitim modeli yapısında, etkinlik olumlu yönde artabilir. UES, modelinin işletiminde, sistemin kullanıcılar ile etkileşimi, tepkileri, eleştirileri ile karşılaştıkları sorunlar yakından izlenerek kişilerin kendisini sistemle baş başa ve yalnızlığı yerine, sistemin sürekli desteklendiği duygusunun yaşanırlığı sağlanabilir. Katılımcıların performans izlenimi ile düzenli raporların sonuçları katılımcılarla paylaşılarak kurumsal kültür kazanımı hızlanır. UES'lerinin daha net anlaşılırlığı 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 UES gelişimini hızlandırır. E-Sağlık/Tele sağlık alanında UES, derslik, televizyon ve kitabın yanında internet üzerindeki "sanal sınıflar" da eğitim gelişim dinamizmini arttırmaktadır. E-Sağlıkta 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-öğretmeninin sanal sınıfta canlı buluşması); sanal sınıflar, işitsel ve görsel konferanslar, internet üzerinden telefon bağlantısı, çift taraflı (interaktif) ve canlı uydu yayınlardır. UES programı yüz yüze eğitim ile birleştirilebilir. Sistemin, esnek, kullanıcı dostu ve kişisel nitelikte uyumlu tasarımı gerekir. Eğitimlerden istenen eğitimi parçalar halinde verilişi, 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. UES'de, eğitim-öğretim sanal bir organizasyon yapısındadır. Bilişim olanaklarının giderek artığı 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. E-sağlıkta 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. [27]. Bu açıdan iyi bir güvenlik politikası kullanıcının işini zorlaştırmamalı, kullanıcılar arasında tepkiye yol açmamalı, kullanaıcılar tarafından uygulanabilir olmalıdır. Politika, kullanıcıların ve system yöneticilerinin eldeki imkanlarla uyarak uygulayabilecekleri yeterli düzeyde yaptırım gücüne sahip kurallardan oluşmalıdır. Kurumsal bilgi güvenliği standartlarının yüksek seviyede bir güvenlik için gereklidir. Bunun ötesinde de sistemlerde açıklar olabileceği, özellikle web uygulamalarında daha dikkatli olunması gerektiği, yeni eğilim ve yaklaşımların keşfedildikçe kurumsal güvenliğin arttırılması yönünde hayata aktarılması gerektiği de asla unutulmamalıdır [28]. E-sağlık yönetim ve eğitiminde yenileşen teknolojiler katılımcılara yüksek etkileşim kalitesi sunmaktadır. UE'de internete dayalı etkileşimli e-öğrenim sürecinde örgün eğitimin eksikliklerini aşan; e-posta, etkileşimli veri tabanları, bilgisayar konferansı ile daha da kolaylaşabilir. Buna bağlı olarak, E-Sağlık/Tele sağlık alanında yeni ortak programlar, destek, network projeler, ek kredi transfer sistemleri, lisan eğitimleri, geniş konferanslar, potansiyel ortakların arttırılması esnek UES olanaklarını ve etkileşimi zenginleştirebilecektir. Sonuçta olarak, e-sağlık/tele sağlık yönetişiminde uzaktan eğitimin e-sağlık öğrenim sürecinde akademik etkileşimler artan oranda bir güven, katılım ve geleceğe doğru sürekli gelişen yeni ve yüksek güvenilirliği olan etkin ve kaliteli bir model oluşturabilecektir.

KAYNAKLAR

[1] Daft, R., Management, Dryden, s.7. (2000).
[2] Ülgen, H. ve Mirze, S.K., İşletmelerde Stratejik Yönetim, Arıkan, İstanbul, s.423,(2007).
[3] Köroğlu, E., Sağlık Mevzuatı. 2. Baskı Ankara, (1987).
[4] 4Hayran O., Sağlık Hizmetlerinin Yönetimi: Hekimler mi, Profesyonel Yöneticiler mi? http://www.merih.net/m1/wosmhay21.htm., (03.01.2008).
[5] Sözen, C "Sağlık Yönetimi", Palme Yayıncılık, Ankara, (2003).
[6] Sur, Haydar, Sağlık Hizmetlerinde İnsan Kaynakları Yönetimi, Hastane Dergisi, İstanbul, (2007).
[7] Tengilimoğlu, D. AYÜ Sağlık İşletmeciliği Ders Notları, (2007).
[8] Ak, B., Hastane Yöneticiliği, Özkan Matbaacılık, Ankara,(1990).
[9] Kuzgun, Y., Rehberlik ve Psikolojik Danışma, (5. Basım), Ankara, ÖSYM Yayını, (1997).
[10] Langford, P. David ve Barbara A. Cleary. Eğitimde Toplam Kalite, (1999).
[11] Yöney, H., Profesyonel Zeka, Remzi Kitabevi, İstanbul, s. 83, (2007).
[12] Onat, E., Mimarlığa Yolculuk, Yem Yayın, İstanbul, s. 54, (2006).
[13] Davidson-Shivers, G. and K.L. Rasmussen, Web-based Learning, USA: Merill-Prentece Hall, (2006).
[14] Öncü, A., ve Varol, S., "Uzman Sistem Teknolojisi ile Web Tabanlı Sınav Değerlendirme Modeli Geliştirmesi", IETC, 6th International Education Techlogy Conference", 19-21 April, North Cyprus. s.1327-1331, (2006).
[15] Ahire, S.L., Ravichandran, T., "An Innovation Diffusion Model of TQM Implementation, " IEE, Transactions on Emerging Management, Vol.48, No.4, November (2001).
[16] Cebeci, Z., ve diğ., "Karma Yem Sanayinde Ağ Tabanlı İzlenebilirlik Sistemi Tasarımı ve Uygulaması", Bilişim 08, Bildiriler Kitabı, Ankara, s.82-89(2008).
[17] Tanenbaum, A., Computer Networks, New Jersey:Prentice Hall, (1988).
[18] Laudon, K.C., E-Commerce, Prentice Hall, (2006).
[19] Trentin, G., The Quality-Interactivity Relationship in Distance Education, Educational Technology 40, 1: 17-27, Jenuary-February, (2000).
[20] Girginer, N., Uzaktan Eğitim Kararlarında Teknoloji, Maliyet, Etkinlik boyutları ve Uzaktan Eğitime Geçiş İçin Kavramsal Bir Model Önerisi. Doktora Tezi, Eskişehir, 2001.
[21] Moore, M.G. and Thompson, M.M., The Effects of Distance Learning. Pennsylvania: The Pennsylvania State University, (1997).
[22] Bates, A.W., Technology, Open Learning and Distance Education. London: Routledge, (1995).
[23] Zrelli, S., Medeni, T., Shinoda, Y., Medeni İhsan Tolga, Kurumlar Arasındaki Alan-Kesiştirici İşbirliği İlişkisi İçin Kerberos Güvenlik Sistemini Geliştirme: Gelişen Doğrulanabilir E-Toplum İçin Yenilikçi Bir Bilgi Teknolojisi Örneği, Ulusal E-İmza Sempozyumu, Ankara, s.105-115, 2006.
[24] Özbey, R. S., Akıllı Kart Teknolojileri, Ulusal E-İmza Sempozyumu, Ankara, s.208-211, (2006).
[25] İnalöz, A, Telekominakosyon Regulasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi, Telekominakosyon Kurumu Uzmanlık Tezi, (2003).
[26] Altay, H., İnsansız Bankacılık, http://www.e-imza.gen.tr/index.php?Page=Haberler&HaberNo=172, (25 09 2007).
[27] Özenç, K. "Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması", ISCTURKEY, Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, s. 183-190, (2007).
[28] Vural, Y. Ve Sağıroğlu, Ş. "Kurumsal Bilgi Güvenliği:Güncel Gelişmeler", ISCTURKEY, Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara,s. 191-199, (2007).

Elektronik Ticarette Güvenlik İlkeleri

Tolga MATARACIOĞLU, Ünal TATAR

Özet **– Son çeyrek yüzyılda teknolojinin üssel bir oranda ilerlemesiyle birlikte 21. yüzyıl, enformasyon çağı olarak adlandırılmaya başlanmıştır. Bu çağdaki en önemli gelişmelerden birisi de kuşkusuz elektronik ticaret olmuştur. Gerçek hayatta yapılan her olay, artık sanal ortamda da yapılabilir bir duruma gelmiştir. Fakat gerçek hayatta olduğu gibi sanal ortamda da karşılaşması olası pek çok sorun mevcut durumdadır. Bu tür sorunların önüne geçilmesi için ulaşılması gereken hedef, varolan güvenlik sistemlerini daha da geliştirmek olmalıdır.**

Anahtar Kelimeler **– E-ticaret, asimetrik anahtarlı şifreleme. simetrik anahtarlı şifreleme, sayısal imza, sayısal sertifika**

I. GİRİŞ

Elektronik ticaret, bilgisayar ağları aracılığı ile ürünlerin üretilmesi, tanıtımının, satışının, ödemesinin ve dağıtımının yapılması olarak tanımlanabilmektedir [1][2][3]. Yapılan işlemler, sayısal biçime dönüştürülmüş yazılı metin, ses ve video görüntülerinin işlenmesi ve iletilmesi işlemlerini içermektedir.

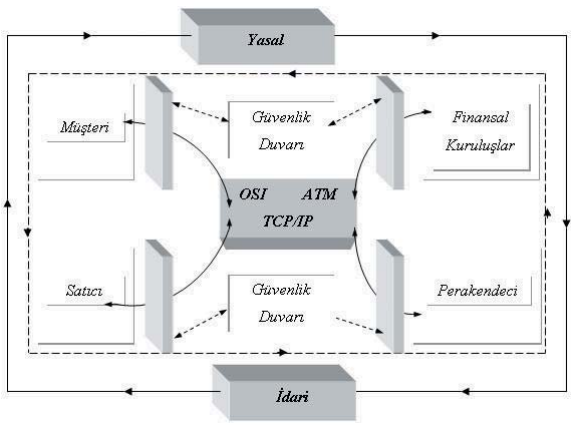
Elektronik ticaret, enformasyon analizi içeren ve bir şebekedeki ticari aktiviteleri destekleyen süreçler bütünüdür. Bu aktiviteler, enformasyon üretmekte ve olayları, hizmetleri, sağlayıcıları, tüketicileri, reklamcıları içine almaktadır. Aynı zamanda işlemleri, bir grup hizmet ve oturumlar için olan (örneğin ürünü bulmak ve ucuz ürünü bulmak) borsa sistemlerini, işlemlerin güvenliğini ve güvenilirliğini vb. destekler. Elektronik ticaret aynı zamanda bir ticari süreç içerisinde verimliliği ve etkinliği geliştirmek amacıyla ileri enformasyon teknolojisi tarafından desteklenen bir iş vizyonunun olmasına imkan verir [4].

Şekil 1'deki model, elektronik ticaretin çok disiplinli doğasını yansıtmaktadır [1]. Şekilden görüldüğü gibi bu model, birkaç ana bileşenden oluşmaktadır. İlk olarak ürünleri global bir elektronik pazar ortamının bir parçası olan satıcıdan elektronik olarak eşya satın almak isteyen tüketici ile modele başlanır. Ticaretin bu yeni modu, yeni iş modellerinin kabul edilmesine, çeşitli yasal ve idari konular tarafından etkilenmesine yol açar.

T. MATARACIOGLU, Elektrik-Elektronik Mühendisliği Bölümü, Orta Doğu Teknik Üniversitesi, 06531 Ankara, Türkiye
Ü. TATAR, Uygulamalı Matematik Enstitüsü, Kriptoloji Bölümü, Orta Doğu Teknik Üniversitesi,06531 Ankara, Türkiye,{e157307,e156699}@metu.edu.tr

Bu tür global bir elektronik pazar ortamını mümkün kılmak için; kaynakların paylaşılmasına olanak sağlayan, asimetrik protokoller üzerine kurulmuş, veri konumlarının ve karar desteğinin şeffaf olmasını sağlayan, çoklu ortam enformasyonunu destekleyen, çeşitli yazılım ve donanım platformlarının birleştirilip uyuşmalarına izin veren, mesaj tabanlı değiştokuş üzerinden haberleşmeyi destekleyen ve verinin güvenliğini ve bütünlüğünü garanti eden teknik bir mimariye gereksinim duyulmaktadır.

Elektronik ticaretin öncelikli hedefi; iş dünyasındaki işlemlerin ve süreçlerin hızını ve verimliliğini arttırmak ve müşteri hizmetlerinin geliştirilmesini sağlamaktır. Ayrıca iştirakçilerin yükseltilmiş rekabet, iş yaratma ve ekonomik büyüme gibi konulara önem vermesini teşvik etmek de elektronik ticaretin hedefleri arasındadır. Bilindiği gibi yüksek rekabet, eşya ve hizmet fiyatlarında bir ucuzlamaya sebep olmaktadır. Bu amaçlar, endüstri için ve aynı zamanda müşteriler için yeni seçenekler sunan yeni pazarlar geliştirilmelidir. Bu noktada elektronik ticaret, iş dünyasındaki süreçleri daha basit ve daha verimli yapmak zorundadır. Amerika Birleşik Devletleri, devleti küçültmek için büyük bir güç sarf etmektedir. Böylece tüm devlet işlemleri, yerini iş dünyasında görülen elektronik işlemlere bırakmaktadır. Bunlara ek olarak elektronik ticaretin; ürünü tedarik etme süreçlerinin gelişmesini sağlamak, ürün çemberinin uzunluğunda bir azalmaya neden olmak, teşebbüslerin komşu partnerlerle ilişkili olduğu kadar uzak mesafedeki partnerlerle de ilişkili olmasını sağlamak, küçük çaptaki işlere de yetki vermek, yeni hizmetler ve işler yaratmak ve iştirakçilerinin ufkunun genişlemesine yardımcı olmak gibi amaçları da mevcuttur.



Şekil 1. Çok disiplinli bir elektronik ticaret modeli

Bu bildiride güvenli bir elektronik ticaret için yerine getirilmesi şart olan kimlik doğrulama, yetkilendirme, güvenilirlik, inkar edememe, bütünlük ve elde edilebilirlik gibi fonksiyonlar ve gereksinimler, işlem ve şebeke güvenliğindeki teknolojiler, şifreleme türleri ve algoritmaları ile sayısal imza ve sayısal sertifika kavramları ele alınmıştır.

II. FONKSİYONLAR VE GEREKSİNİMLER

Kimlik doğrulama (authentication), bilgisayar ağları üzerinde iki tarafın birbirlerinin kimliklerini doğrulaması işlemidir. Bilgisayar ağlarında iletişim, istemci ile sunucu arasında gerçekleşmektedir [5][6]. İstemci kimlik doğrulama, istemcinin kimliğinin sunucu tarafından doğrulanması olarak tanımlanırken; sunucu kimlik doğrulama ise, sunucunun kimliğinin istemci tarafından doğrulanması olarak tanımlanmaktadır. Kimlik doğrulama metotları, aşağıda listelenen faktörler üzerine kurulmuştur:

- Parola (password) gibi özel bir enformasyonun bilinmesi
- Anahtar veya kart gibi özerklik belirten nesnelere sahip olunması
- Parmak izi gibi bazı biyometrik karakteristiklerin bilinmesi

Bir kullanıcının kimliğini ispatlamak için, bu faktörler tek başına kullanılmamakta; genelde birbirleriyle olan kombinasyonları denenmektedir.

Yetkilendirme (authorization) işlemi, kimliğin ispatlandığı andan itibaren kısmi bir enformasyona erişimin kontrolü olarak tanımlanmaktadır. Bazı oturumlar kısmi olarak ulaşılabilirlik gereksiniminde bulunsa da, bazı oturumlar hiçbir ulaşılabilirlik gereksiniminde bulunmamaktadır. Yetkilendirme işlemi, kimliği ispatlanmış kişilerin şebekeli bir çevrede yaptıkları hareket ve işlemlere bir sınır getirmektedir. Bu sınırlamalar, güvenliğin seviyesine bağlı olarak değişmektedir.

Güvenilirlik (confidentiality) işlemi, veri ve/veya enformasyonun gizliliği ve bu veri ve/veya enformasyona yetkisiz kişilerce ulaşılmasının engellenmesi olarak tanımlanmaktadır. Elektronik ticaret için güvenilirlik ise; bir organizasyonun veya şirketin finansal verisine, ürün geliştirme enformasyonuna, organizasyon yapılarına ve çeşitli tipte gizli enformasyona yetkisiz kişiler tarafından erişilebilmesini engellemek olarak tanımlanabilmektedir. Güvenilirlik kavramı, aşağıdaki iki konuyu garanti etmek zorundadır:

-Herhangi bir enformasyon, özel bir yetki olmadığı sürece; kesinlikle okunamaz, kopyalanamaz veya değiştirilemez.

-Şebekeler üzerinden haberleşme hiçbir şekilde kesilemez.

Kriptografi temelli şifreleme teknikleri, bu tür gereksinimleri karşılamak üzere tasarlanmışlardır.

İnkar edememe (nonrepudiation) işlevi, enformasyon göndericisinin sonradan gönderdiği bilgiyi inkar etmesini engellemektedir. Böylece orijinin, dağıtımın, arz etmenin ve verinin doğru gönderilmesinin ispatı da yapılmış olmaktadır.

Bütünlük (integrity) ölçütü, enformasyonun beklenmeyen yollarla güncellenememesini garanti etmektedir. Bütünlük kaybına insan hataları veya kasıtlı kurcalamalar neden olmaktadır. Şüphesiz ki herhangi bir işte yanlış enformasyonun kullanılması, istenmeyen sonuçlar doğurabilmektedir. Uygunsuz bir şekilde güncellenmiş bir verinin işe yaramaz veya tehlikeli olması gerçeği, verinin doğruluk ve tutarlılığının korunması için çok büyük bir çabanın sarf edilmesini gerektirmektedir.

Verinin geçerliliği çok önemli bir unsur olduğuna göre, bunu garanti edecek kontrollerin tasarlanması ve verinin doğruluğunun kontrol edilmesi gerekmektedir. Eğer veri bir şekilde çalınmışsa veya yetkisiz kişiler tarafından değiştirilmişse; bunun tespit edilmesi, sistemin bütünlüğü açısından gerekmektedir. Şifreleme verinin yetkisiz kişiler tarafından erişilmesi ve değiştirilmesini, veriyi gizli bir forma çevirerek, engellemede kullanılan bir yöntemdir.

Olgunlaşmış bir bilgi güvenliği politikası, etkin önlem alma ve tepki oluşturma işlevlerini içermelidir. Etkin önlem alma işlevi, kuvvetli güvenlik denetimlerinin konulmasını gerektirirken; tepki oluşturma işlevi, bu kontrollerin kayıtlanması ve izlenmesini gerektirmektedir. İyi bir sistem yöneticisi sistem içerisindeki hareketleri kayıt dosyalarından izleyerek, gerçekleşen olaylardan sonuçlar çıkarıp, yeni önlemler oluşturmalıdır.

Elde edilebilirlik (availability), kaynakların silinmesini veya erişilemez hale gelmesini engelleyen bir ölçüttür. Bu ölçüt sadece enformasyon için değil, diğer tüm teknoloji altyapısı ve şebekeye bağlı makineler için de geçerlidir. Bu gerekli kaynakları kullanamama durumu, hizmet dışı bırakma (denial of service) olarak adlandırılmaktadır.

Bir kurumun güvenlik stratejisi yukarıda belirtilen ölçütler doğrultusunda değerlendirilmeli ve kurumun ihtiyaçlarına göre ölçütler, değişik seviyelerde incelenmelidir [7]. Örneğin milli savunma sistemlerinde güvenilirliğe daha çok önem verilmesi gerekirken, fon aktarım sistemlerinde bütünlüğe daha çok önem verilmelidir.

III. GÜVENLİK TEKNOLOJİLERİ

İnternet üzerinden iletişimi gerçekleşen bilgilerin güvenilirliği, açık anahtar kriptografi olarak adlandırılan bir teknikle sağlanmaktadır [7][8]. Açık anahtar kriptografinin gerçekleştirdiği faaliyetler aşağıda listelenmiştir:

Şifreleme ve Şifre Çözme: Güvensiz bir ortamda birbirleriyle haberleşen iki tarafın, bilgiye sadece kendilerinin anlayacağı bir biçim vermesi tekniği olarak tanımlanmaktadır. Gönderilmeden önce gönderici tarafından şifrelenen veri, alıcı tarafından açılmakta ve orijinal veri elde edilmektedir. İletilen verinin şifreli olması, saldırganın veriye erişimini engellemektedir.

Kurcalama Sezme: İletişim sırasında veri üzerinde gerçekleştirilebilecek olası değişikliklerin sezilmesinde kullanılan teknik olarak tanımlanmaktadır.

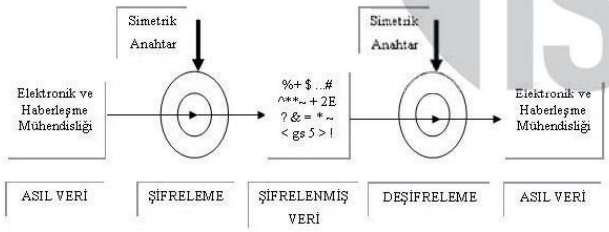
Kimlik Doğrulama: Enformasyon alıcısına, enformasyonun kaynağının ve göndericinin kimliğinin doğrulanması imkanını vermek olarak tanımlanmaktadır.

İnkar Edememe: Enformasyonun göndericisinin, daha sonraki bir zamanda, gönderdiği enformasyonu inkar etmesini engellemek olarak tanımlanmaktadır.

Şifreleme işlevi enformasyonun, alıcı haricindeki kişiler tarafından anlaşılmayacak bir şekle çevrilmesi olarak tanımlanmaktadır. Şifre çözme ise; özel bir anahtar yardımıyla anlamsız bilgiye, şifrelenmeden önceki anlamlı halinin geri verilmesi olarak tanımlanmaktadır. Şifreleme ve şifre çözme işlevleri, kriptografi algoritması olarak adlandırılan matematiksel işlevlerce gerçekleştirilmektedir. Şifreleme yönteminin kuvveti; algoritmanın bilinmezliği ile değil, kullanılan anahtarın uzunluğu ile ilgili olmaktadır. Şifrelenen veri; anahtar kullanımı ile rahatlıkla açılmakta iken, anahtarın bilinmemesi durumunda verinin elde edilmesi matematiksel işlemlerin yoğunluğu dolayısıyla imkansız olmaktadır.

Simetrik Anahtarlı Şifreleme

Simetrik anahtarlı şifreleme (Symmetric Key Encryption); şifreleme anahtarının deşifreleme anahtarından elde edilebildiği bir şifreleme yöntemidir. Şekil 2'den de görüldüğü gibi, çoğu simetrik algoritmalarda şifreleme ve deşifreleme (şifre çözme) anahtarları aynı olmaktadır. Simetrik anahtarlı şifreleme, verinin şifrelenmesinde ve deşifrelenmesinde herhangi bir gecikmeye neden olmamaktadır. Bu tarz şifrelemede bir anahtar ile şifrelenen veri, diğer bir anahtarla açılamadığından dolayı; anahtarın gizli tutulması durumunda bir derecede kimlik doğrulama işlemi sağlanmaktadır. Simetrik anahtarlı şifrelemede, simetrik anahtarın gizli tutulması vazgeçilmez bir şarttır. Simetrik anahtarın gizli tutulmadığı durumlarda, hem verinin güvenilirliği hem de kimlik doğrulama ölçütleri tehlikeye girmektedir. Başkasına ait bir simetrik anahtar; saldırganın hem kişiye ait gizli bilgilere erişmesine, hem de anahtar sahibinin kimliğiyle başkalarına veri göndermesine neden olmaktadır.



Şekil 2. Simetrik anahtarlı şifreleme

Genel olarak dört tip simetrik anahtarlı şifreleme algoritması kullanılmaktadır. Bu algoritmalar; veri şifreleme standardı (Data Encryption Standard – DES) algoritması, üçlü veri şifreleme standardı (Triple Data Encryption Standard – Triple DES) algoritması, uluslar arası veri şifreleme algoritması (International Data Encryption Algorithm – IDEA) ve RC4 algoritması olarak adlandırılmaktadır.

Ulusal Standartlar Bürosu (National Bureau of Standards) tarafından yayınlanmış veri şifreleme standardı (Data Encryption Standard – DES) algoritmasının aşamaları aşağıda listelenmiştir [9][10]:

-Mesaj 64 bitlik parçalara bölünür.

-Bu bölmeler bir başlangıç permütasyonundan geçirilir.

-56 bitlik anahtar kullanılarak, 16 adet 48 bitlik anahtar elde edilir.

-56 bitlik anahtar üzerinde permütasyon gerçekleştirilerek, 2 adet 28 bitlik anahtar elde edilir.

-Her iki bölme de; 1, 2, 9 ve 16'ncı aşamalarda sola doğru 1, diğer aşamalarda sola doğru 2 bit döndürme (rotate) işlemine tabi tutulur.

-Her bir bölme ayrı ayrı permütasyondan geçirilip; birinci anahtarın 9, 18, 22 ve 25'inci, ikinci anahtarın 35, 38, 43 ve 54'üncü bitleri elenir ve 48 bitlik anahtar elde edilir.

-DES aşamalarını gerçekleştirmek üzere, 16 adet 48 bitlik anahtarın her biri kullanılır.

-64 bitlik giriş değeri, 32 bitlik iki parçaya bölünür.

-DES aşamasına giriş değerinin sağ tarafı, aşama çıkış değerinin sol tarafı olur.

-Aşamaya giriş değerinin sağ tarafına parçalayıcı işlevi, aşamaya ait anahtarla uygulanır.

-Parçalayıcı işlevin sonucu, aşamaya giren değerin sol tarafı ile aşamadan çıkan değerin sağ tarafının EXOR işleminden geçirilmesi ile elde edilir.

-Dördüncü aşama 16 kez tekrar edilir.

-Sonucun sol ve sağ parçaları yer değiştirilir.

-Son permütasyon gerçekleştirilir.

Üçlü veri şifreleme standardı (Triple Data Encryption Standard – Triple DES) algoritmasında ise, DES algoritmasının üç kez çalıştırılması işlemini içeren üç adet anahtar kullanılmaktadır. Anahtar 1, anahtar 2 ve anahtar 3 olarak adlandırılan ve üç adet 56 bitlik bölmelere ayrılan 168 bitlik anahtar kullanılmaktadır.

Uluslar arası veri şifreleme algoritması (International Data Encryption Algorithm – IDEA) ise; 128 bitlik anahtar kullanarak, 64 bitlik açık metni 64 bitlik şifreli parçalar halinde şifreleyen bir algoritmadır. Bu algoritma, hesapsal olarak birbirinin aynı 8 aşama içermektedir. Uzun zamandır bilinen IDEA algoritması, herhangi bir saldırı teşebbüsüne maruz kalmamıştır. Biham, Shamir ve Biryukov tarafından IDEA'ya gerçekleştirilen saldırı teşebbüsü, algoritmanın ancak dördüncü seviyesine kadar ulaşmış; algoritmanın 8 aşamalık toplam bölümü yine güvenli olarak kalmıştır. Amerika Birleşik Devletleri ve birçok Avrupa ülkesinde patentlenmiş olan IDEA algoritmasının aşamaları kabaca aşağıda verilmiştir [9][10]:

-Şifrelenecek mesaj, 64 bitlik parçalara bölünür. Her bir açık metin parçası, şifreli parça haline dönüşecektir.

-64 bitlik parçalar, 16 bitlik 4 bloğa ayrılır.

-52 adet 16 bitlik anahtar oluşturmak üzere, 128 bitlik bir anahtar kullanılır.

-Tek sayılı aşamalarda dörtlü, çift sayılı aşamalarda ise ikili kümelerde anahtar kullanılarak 17 aşama gerçekleştirilir.

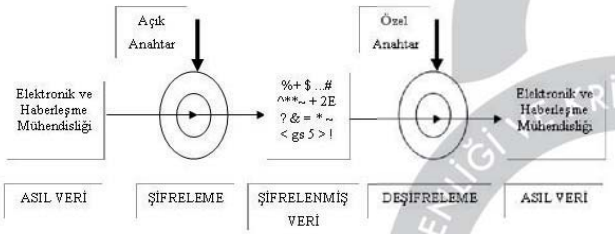
-16 bitlik bloklar, 64 bitlik şifreli bloklar olarak birleştirilir.

RSA Veri Güvenlik Firması ve Ron Rivest tarafından geliştirilen RC4 algoritması, çalışma hızının çok yüksek olması ve güvenlik seviyesinin bilinmemesine rağmen bazı

hız gerektiren uygulamalarda kullanılmaktadır. İstenildiği kadar anahtar uzunluğu kabul edebilen RC4 algoritması; bir sahte rastgele sayı üreteci ve bu sayı üretecinin çıktısının, şifrelenecek veri ile EXOR işlemine tabi tutulmasından ibarettir. Bu nedenle aynı anahtar, iki farklı veri kümesini şifrelemede kullanılmamalıdır.

Açık Anahtarlı Şifreleme

Anonim veya simetrik olmayan anahtarlı şifreleme olarak da adlandırılan açık anahtarlı şifrelemede (Public Key Encryption); biri açık anahtar, diğeri özel anahtar olarak isimlendirilen bir anahtar çifti kullanılmaktadır. Bu anahtar çifti; verinin imzalanması, şifrelenmesi ve kimlik doğrulama işlemlerinde kullanılmaktadır. Bu şifreleme yönteminde açık anahtar herkese dağıtılırken, özel anahtar sadece anahtar sahibi tarafından bilinmektedir. Açık anahtar ile şifrelenen veri sadece özel anahtar ile açılabilirken, özel anahtarla şifrelenen veri ise sadece açık anahtar ile açılabilmektedir. Şekil 3'ten de görüldüğü üzere; gönderici veriyi alıcının açık anahtarı ile şifrelemekte ve alıcıya göndermektedir. Alıcı ise, şifrelenmiş veriyi özel anahtarı ile açmaktadır.



Şekil 3. Açık anahtarlı şifreleme

Açık anahtarlı şifreleme, simetrik anahtarlı şifrelemeye göre daha fazla matematiksel işlem gerektirmektedir. Bu nedenle açık anahtarlı şifrelemenin, büyük uzunluklu verilerin şifrelenmesinde kullanılması uygun değildir. Bu tarz veri boyutlarında açık anahtarlı şifreleme ve simetrik anahtarlı şifreleme birlikte kullanılmalıdır. Çoğunlukla karşılaşılan yöntem; simetrik anahtarın değişiminde açık anahtarlı şifrelemenin kullanılması, verinin değişiminde ise simetrik anahtarlı şifrelemenin kullanılması şeklidir. Açık anahtarlı şifreleme, kimlik doğrulama işleminde de kullanılmaktadır. Kimliği doğrulanacak olan gönderici, özel anahtarı ile veriyi şifreler. Özel anahtar ile şifrelenen veri sadece açık anahtar ile açılabildiği için, göndericinin kimliği doğrulanmış olur.

1977 yılında Rivest, Shamir ve Adleman tarafından bulunan ve şifreleme ve şifre çözme işlemlerinin her ikisinde de kullanılan RSA algoritmasında, ilk önce şifreleme ve şifre çözmede kullanılacak açık ve gizli anahtar çiftinin oluşturulması gerekmektedir. RSA algoritmasının aşamaları aşağıda verilmektedir [9][10]:

-Tipik olarak 10000'den daha büyük p ve q gibi iki büyük asal sayı seçilir.

-n = p * q ve z = (p-1) * (q-1) işlemleri gerçekleştirilir.

-z sayısına göre aralarında asal bir d sayısı belirlenir.

-e * d = 1 (mod z) olacak biçimde bir e sayısı belirlenir.

-Şifrelenecek metin, 2k < n olacak şekilde k bit uzunluklu bloklara ayrılır ve her bir blok, P olarak adlandırılır.

-P mesajının şifrelenmesi için, $C = P^e \pmod n$ işlemi gerçekleştirilir.

-Mesajın deşifrelenmesi içinse, $P = C^d \pmod n$ işlemi gerçekleştirilir.

RSA algoritmasının işlem aşamaları ve sonuçları Tablo 1'de gösterilmektedir. Buradaki örnekte; p = 3, q = 11, n = 33, z = 20, d = 7 ve e = 3 olarak alınmıştır.

Şifreleme yönteminin kuvveti ise, anahtarın bulunması ile ilgili olmaktadır. RSA algoritmasında anahtarın bulunması, çok büyük basamaklı sayıların çarpanlarına ayrılması işlemidir. Şifreleme yönteminin kuvveti, anahtarın uzunluğu ile doğru orantılı olmaktadır. Farklı şifreleme yöntemleri, aynı şifreleme kuvvetini sağlamak için farklı uzunlukta anahtar uzunlukları gerektirebilmektedir.

TABLO 1

RSA algoritmasıyla şifreleme ve şifre çözme

Açık Metin (P)		$X = P^3$	Şifreli Metin (C)	$Y = C^7$	Şifre Çözme İşleminden Sonra	
Sembol	Sayı		X (mod 33)		Y (mod 33)	Sembol
K	11	1331	11	19487171	11	K
R	18	5832	24	4586471424	18	R
I	9	729	3	2187	9	I
P	16	4096	4	16384	16	P
T	20	8000	14	105413504	20	T
O	15	3375	9	4782969	15	O

Sayısal İmzalar

İncelendiği üzere şifreleme ve şifre çözme teknikleri, verinin internet üzerinde iletiminde karşılaşılan sorunlardan sadece gözetleme sorununu engellemektedir. Sayısal imzalar ise, kurcalama ve taklit etme sorunlarına çözüm getirmektedir [11][12][13]. Kurcalama sezme ve kimlik doğrulama teknikleri, tek yönlü çırpma (one-way hash) olarak adlandırılan matematiksel bir işleve bağlı olmaktadır. Tek yönlü çırpma işlevinin özellikleri aşağıda listelenmiştir:

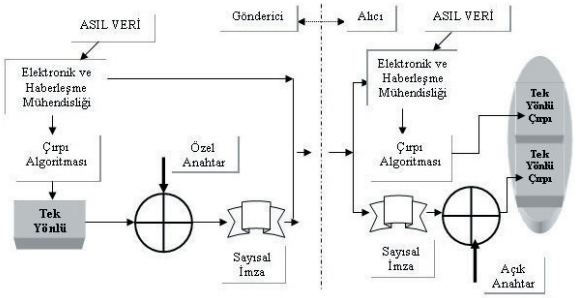
-Veriden elde edilen çırpı değeri tektir. Veride yapılan bir bitlik değişiklik bile çırpı değerini değiştirmektedir.

-Çırpı değerinden, çırpılan veri elde edilemez. Bu nedenle, çırpma işlevi tek yönlü bir işlev olarak adlandırılmıştır.

Sayısal imza veriye tek yönlü çırpı işlevi uygulanarak elde edilen çırpı değerinin, kullanıcının özel anahtarı ile şifrelenmesiyle elde edilmektedir.

Şekil 4'ten de görüldüğü gibi veri; tek yönlü çırpı işlevinden geçirilerek, tek yönlü çırpı değeri elde edilmektedir. Elde edilen çırpı değeri, özel anahtarla şifrelenmekte ve sayısal imza elde edilmektedir. Elde edilen sayısal imza, veri ile birlikte alıcıya gönderilmektedir. Alıcı, sayısal imzayı göndericinin açık anahtarı ile açmakta ve gönderici tarafından hesaplanmış tek yönlü çırpı değerini elde etmektedir. Daha sonra kendisine ulaşan veriden, tek yönlü çırpı değerini hesaplamakta ve diğer çırpı değeriyle

karşılaştırmaktadır. İki değerin eşitliği durumunda göndericinin kimliği doğrulanmaktadır.

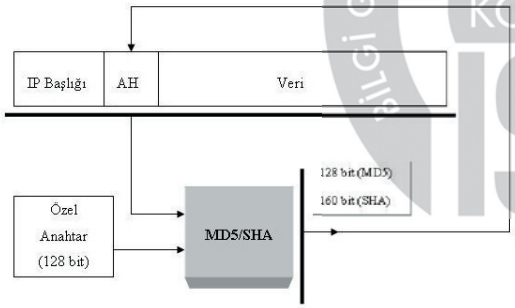


Şekil 4. Sayısal imza kullanımı

Çırpma Algoritmaları

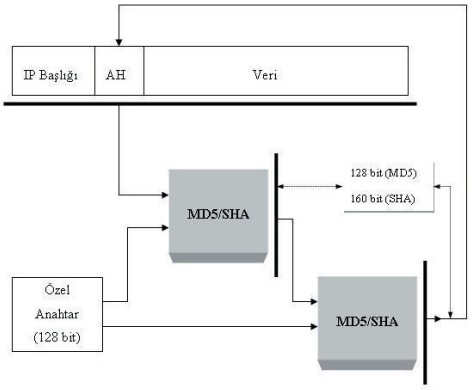
Geniş olarak kullanılan çırpı işlevleri, MD5 ve güvenli çırpı algoritması (Secure Hash Algorithm – SHA)'dır. MD5, Rivest tarafından tasarlanmıştır. Güvenli çırpı algoritması ise; MD5 algoritmasından esinlenilerek, Ulusal Standartlar Enstitüsü (National Institute of Standards) ve Ulusal Güvenlik Acentesi (National Security Agency) tarafından sayısal imzalama standardı (Digital Signature Standard – DSS) ile birlikte kullanılmak amacıyla tasarlanmıştır.

MD5 ve güvenli çırpı algoritmasında (Secure Hash Algorithm – SHA) 128 bitlik gizli bir anahtar ve veri birimi, çırpı algoritmasına giriş değeri olarak girmektedir. Algoritma sonucunda oluşan çıktı değeri, veri birimi başlığının kimlik doğrulama sahasına (AH) yerleştirilmektedir. Algoritmanın şekilsel gösterimi, Şekil 5'te bulunmaktadır. Güvenli çırpı algoritmasının MD5'ten tek farkı, oluşan çırpı değerinin 160 bit olmasıdır.



Şekil 5. MD5 ve SHA algoritması

Çırpılmış mesaj doğrulama kodu (Hashed Message Authentication Code – HMAC) MD5 ve SHA algoritmaları ise, IBM tarafından sunulmuş güçlü bir çırpı değeri oluşturma yöntemidir. Çırpılmış mesaj doğrulama kodu; kendi kendine bir çırpı işlevi olmaktan ziyade, mesaj doğrulama kodu hesaplaması için özel bir çırpı işlevi kullanan güçlü bir kriptografi yöntemidir. Örnek olarak MD5 algoritmasının kullanıldığı düşünülürse; HMAC, temel çırpı işlevinin üst üste iki kez uygulanmasından ibaret olmaktadır. İlk seferde veri birimi ve anahtar, çırpı işlevine giriş değerleri olurken; ikinci seferde birinci çırpı işlevinin çıktısı ve anahtar değerleri, giriş değeri olmaktadır. Algoritmanın şekilsel gösterimi, Şekil 6'da yer almaktadır. SHA için oluşan tek değişiklikse, oluşan ara değerlerin 160 bit uzunlukta olmasıdır.



Şekil 6. Çırpılmış mesaj doğrulama kodu MD5 ve SHA algoritmaları

Sayısal Sertifikalar

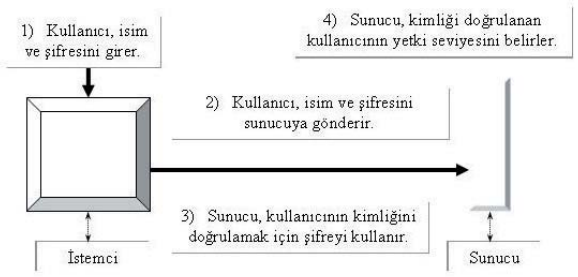
Sayısal sertifikalar; bir kişinin, bir sunucunun veya bir firmanın kimliğinin tanımlanması ve bir açık anahtarın bu kimlikle ilişkilendirilmesinde kullanılan elektronik belgeler olarak tanımlanmaktadır [14]. Sürücü belgesi, pasaport veya nüfus cüzdanı gibi belgeler; kullanıcının kimliğini kanıtlamak için kullanılan belgelerdir. Açık anahtarlı şifreleme, taklit etme sorununu çözümlemek amacıyla sayısal sertifikaları kullanmaktadır.

Sayısal sertifikalar; açık anahtarın yanında, nesneyi tanıtan isim, geçerlilik süresi, sayısal sertifikayı veren makamın ismi ve seri numarası gibi bilgileri içermektedir. Sayısal sertifikaların içerdiği en önemli bilgi ise, sertifika makamının sayısal imzasıdır.

Sayısal sertifikalar, istemci ile sunucu kimlik doğrulama işlemleri için kullanılmaktadır. İki tip istemci doğrulaması vardır. Şifre temelli kimlik doğrulamada sunucu, isim ve şifrelerden oluşan bir veri tabanı tutmaktadır. İstemcinin girmiş olduğu isim ve şifre, veri tabanındaki bilgilerle karşılaştırılarak kimlik doğrulama işlemi gerçekleştirilmektedir. Kimlik doğrulama işlemi; istemcinin girmiş olduğu isim ve şifre çiftinin, sunucunun veri tabanındaki çiftle aynı olduğu durumda başarıyla sonuçlanmaktadır. Tüm sunucu yazılımları, şifre temelli kimlik doğrulamayı desteklemektedir. Sertifika temelli kimlik doğrulama ise, SSL protokolünün bir parçasıdır. İstemci rastgele üretilmiş veriyi, sayısal imzası ile imzalamakta ve sayısal sertifikası ile birlikte sunucuya göndermektedir. Sunucu, açık anahtarlı kriptografi tekniklerini kullanarak sayısal imzayı doğrulamakta ve sayısal sertifikanın geçerliliğini onaylamaktadır. Şifre temelli kimlik doğrulamada yer alan aşamalar Şekil 7'de gösterilmiştir.

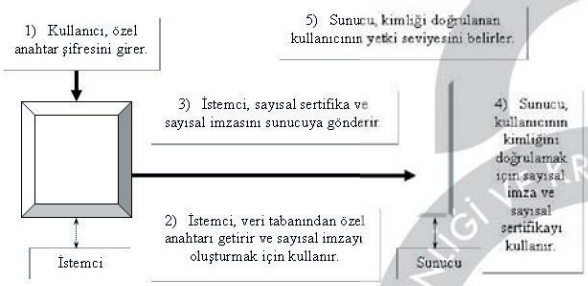
Sayısal sertifika temelli kimlik doğrulamada ise; istemci kimlik doğrulama, sayısal sertifika ve SSL protokolünün kullanımıyla gerçekleşmektedir. Kullanıcının sunucu tarafından doğrulanması için; istemci, rastgele üretilmiş veri parçasını sayısal imzası ile imzalamakta ve sayısal sertifika ile birlikte sunucuya göndermektedir. Sunucu ise sayısal imzasından, kullanıcının kimliğini doğrulamaktadır. Sayısal

sertifika temelli kimlik doğrulama; kullanıcının bildiği bir nesne (şifre) değil de, kullanıcının sahip olduğu bir nesne (özel anahtar) gerektirdiğinden dolayı; şifre temelli kimlik doğrulamaya göre daha çok tercih edilmektedir.



Şekil 7. Şifre temelli kimlik doğrulama

Şekil 8'de sayısal sertifika kullanarak istemcinin kimliğinin doğrulanması işleminin aşamaları verilmektedir.



Şekil 8. Sayısal sertifika temelli kimlik doğrulama

Sayısal sertifika içeriği, X.509 v3 standardına göre düzenlenmektedir. X.509 v3 sertifikası, fark edilebilir ismi (distinguished name) bir açık anahtar ile ilişkilendirmektedir. Fark edilebilir isim, bir nesneyi tekil olarak tanıtan bir dizi isim ve değer çifti olarak tanımlanmaktadır. Tipik bir sayısal sertifika, veri ve imza olmak üzere iki kısımdan oluşmaktadır. Veri kısmı, aşağıdaki bilgileri içermektedir [14]:

-Sürüm numarası
-Sertifika seri numarası
-Enformasyon
-Kullanıcının açık anahtarı ile ilgili enformasyon
-Sertifikayı dağıtan sertifika makamının tanınır ismi
-Sertifikanın geçerlilik süresi
-Sertifikanın fark edilebilir ismi
-Seçimlik sertifika uzantısı

İmza kısmı ise aşağıdaki bilgileri içermektedir:

-Sertifika otoritesi tarafından kullanılan kriptografik algoritma
-Sertifika otoritesinin sayısal imzası

IV. SONUÇ

Elektronik ticaret, 20. yüzyılın son döneminde bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ve gelişmelere paralel bir şekilde ve giderek artan ölçüde dünya genelinde tartışılan bir kavram olarak ortaya çıkmaktadır. Elektronik ticaret çerçevesinde yaşanan gelişmeler sonucunda pek çok ülke, uluslararası örgüt ve kuruluş; elektronik ticaret ve bu alanla bağlantılı konuları gündemlerine almışlar ve elektronik ticaret olgusunu çeşitli yönleriyle araştırmaya başlamışlardır. E-ticaretteki büyüme potansiyelinin gerçekleşmesini belirleyecek unsur, bazı konuların nasıl ele alınacağına bağlı olmaktadır. Bu konular arasında vazgeçilmez olanların aşağıdaki şekilde sıralanması mümkündür:

-Uygun bir telekomünikasyon altyapısı ile standartlarının sağlanması
-Altyapıya girişin arttırılması
-Yaptırımlar içeren bir yasal çerçeve oluşturulması
-Enformasyonun güvenliği ve gizliliğin temini
-Uygun bir vergi rejimi yaratılması
-Fırsat eşitliğini sağlayacak politikalarla, bilhassa gelişme yolundaki ve en az gelişmiş ülkelerde eğitim düzeyi ve internete giriş imkanlarının arttırılması

Yukarıda belirtilen koşullar sağlanabildiği takdirde, internet aracılığıyla yapılan elektronik ticaret açısından yeni ve değerli fırsatlar yaratılmış olacaktır.

Elektronik ticaret kavramında en önemli husus, enformasyon güvenliği olmaktadır. Ancak tam bir güvenlik ortamı sağlandığı takdirde taraflar, güvenilir olarak elektronik ticarete atılmaya başlayacaktır. Bu güveni sağlamak için de çeşitli şifreleme yöntemleri ve algoritmaları, sayısal imzalar ve sertifikalar gibi pek çok kavram ortaya çıkmıştır. Amaç hep aynı olup; kimlik doğrulama, yetkilendirme, güvenilirlik, inkar edememe, bütünlük ve elde edilebilirlik kavramları gibi pek çok fonksiyonun ve gereksinimin karşılanması olmuştur. Bu fonksiyon ve gereksinimlerin karşılanmasını sağlamak üzere geliştirilecek yeni teknoloji ve sistemler, elektronik ticaretin kullanılabilirlik ve güvenilirliğini de arttırmış olacaktır.

KAYNAKLAR

[1] N. Adam, O. Dogramaci, A. Gangopadhyay, Y. Yesha, *"Electronic Commerce: Technical, Business, and Legal Issues"*, New Jersey: Prentice Hall, 1999.
[2] W. Rajput, *"E-Commerce Systems Architecture and Applications"*, Boston: Artech House, 2000.
[3] http://www.e-ticaret.gov.tr/.
[4] A. Ghosh, *"E-Commerce Security: Weak Links, Best Defenses"*, New York: John Wiley, 1998.
[5] S. Garfinkel, *"Web Security & Commerce"*, Sebastopol: O'Reilly, 1997.
[6] R. Çölkesen, B. Örencik, "*Bilgisayar Haberleşmesi ve Ağ Teknolojileri"*, İstanbul: Papatya, 2000.
[7] A. Tanenbaum, *"Computer Networks"*, New Jersey: Prentice Hall, 1988.
[8] http://www.eticaret.org/.
[9] W. Davies, L. Price, *"Security for Computer Networks"*, Canada: John Wiley & Sons, 1989.
[10] J. Reynolds, R. Mofazali, *"The Complete E-Commerce Book:Design, Build & Maintain a Successful Web-based Business"*, New York: CMP Books, 2000.
[11] http://www.online-commerce.com/.
[12] E. Turban, *"Electronic Commerce 2008"*, Prentice Hall, 2007.
[13] J. F. Rayport, *"Introduction to E-Commerce"*, McGraw-Hill, 2001.
[14] K. C. Laudon, *"E-commerce"*, Prentice Hall, 2006.