Information Security Threats and Information Assurance

Yildiray Yalman[1], Murat Yesilyurt[2]

[1]*Computer Engineering Department, Turgut Ozal University, Ankara, Turkey*
[2]*Computer Engineering Department, Sakarya University, Sakarya, Turkey*

***Abstract* – Today, the benefits of rapidly developing technology, as well as come to the fore the problems brought about. For this reason, individuals, institutions and organizations take measures to ensure the security of information. Information assurance is the practice of managing risks related to the use, processing, storage and transmission of information or data and the systems and processes used for those purposes. Thus, information security is now provided with information assurance measures. The presented work, especially in today's digital and networking technologies in order to ensure effective information security threats and describes the scope of what required for information assurance.**

***Keywords* – Information security, Information assurance**

1. Introduction

Developed western societies in particular, serious steps are taken throughout the world in order to become an information society and many studies are made in this direction. In this context, individuals, institutions and organizations carry out their transactions electronically. Among those, making tax, bill and fine payments, performing money transfers, shopping and reaching all the documents and information by using a personal computer or cell phone may be ranked. As a natural consequence of this situation, information security (IS) concepts have gained great importance in many areas such as banking, e-commerce, e-signature, distance learning, e-state applications, and personal communications. The fact that individuals or states could not become effective separately in an information society increasingly becomes a current issue. As a part of the interdependence principle, an efficacious security approach will be exhibited by providing the security of all individuals, organizations and countries [1].

Information-centric security approaches are generally addressed in two main topics such as personal and corporate IS. Gradual increase in security breaches in the IS field divert individuals or institutions to develop new security approaches by taking into account the software, hardware, and environmental factors. At this point, single safety measures to ensure the IS such as network security or software security, are regarded as very insufficient applications although they are all important. For this reason, in order to ensure an effective IS, all needs in this respect should be met with a lump sum point of view, by taking measures such as the security of hardware, software, network and communication, emission (tempest), staff, crypto, physical space, document etc. [2]. The presented study gives up-to-date information about the current situation of internet technologies, as well as today's information and communication technologies while we elaborated the concept of information assurance (IA) covering all measures to be taken in order to ensure IS. Within this scope, sections are organized as follows:

In Section 2, the present state of web technologies has been described, the risks caused by them in terms of IS and the measures taken by countries against possible risks have been presented. The details on the measures for IA in order to ensure a full IS have been provided in Section 3. In Section 4, general assessments have been offered.

2. Information Security Threats and The Legal and Administrative Studies by Countries on This Subject

When it comes to the information and communication technologies, primarily, the services provided by the internet technology comes to mind. Since the internet has recently become integrated with cell phones, it has been an essential part of daily life, and is preferred by an increasing number of user. The number of internet users around the world which was 360 million by the end of 2000, had an increase of 566% and has reached to 2 billion and 405 million of people by June, 2012 [3]. Besides, the number of websites which was 20000 in 1995, has reached to 146 million by July 2013 [4]. Given that each website has 273 pages on average [5], one can say that there are almost 40 billion web pages in the internet world and their contents are constantly transferred from one point to another. It is indispensable that such an enormous communication world also accompany a number of security problems. Among the above mentioned problems,

what takes the lead is the information loss as a result of packet losses arising from the traffic density in private/wide area networks, the noise in the communication environment and the communication technologies in use, due to the nature of digital communication (Table 1). While loses are compensated by means of communication protocols (TCP/IP) in some application; in real-time applications, the compensation of information becomes impossible because of the protocols used (UDP, RTP, etc.).

E-mail communication is among the busiest use areas of Internet. Today, 94% of e-mail traffic is composed of the e-mails called spam which are unnecessary and often with a harmful content.

	Asia	North America	Europe	Australia	South America
Average Packet Loss (%)	33	25	9	0	0
Response Time (ms)	104	51	140	151	172

Table 1. Average packet loss rates and response times [6].

Especially trojans and viruses are the software that seriously poses a threat. Since the early 2000s when the Internet began to be used extensively, a large number of harmful software has been created. Knowing no bounds, this software has caused irreparable damage in the computer and network systems all over the world (Table 2). The current situation shows that conducting joint studies through an international cooperation is an important obligation in order to ensure IS.

Year	Harmful Software	Target	The Estimated Damage
2000	I Love You	Deleting system files	8,7 billion $
2001	Code Red	Creating a back door in the White House	200 million $
2003	Sobig.F	Affecting e-mail traffic	35 billion $
2004	MyDoom	Affecting e-mail traffic	38 billion $
2008	Conficker	Making computer an open door	3 billion $

Table 2. Harmful software and the estimated damages

According to a research conducted by the FBI, it is stated that about 70,000 viruses today has spread actively in the global network and about 85% of the internet service providers existing in the world is exposed at least one time to a cyber-attack [7]. Cyber-attack statistics in 2012 can be seen in Figure 1.

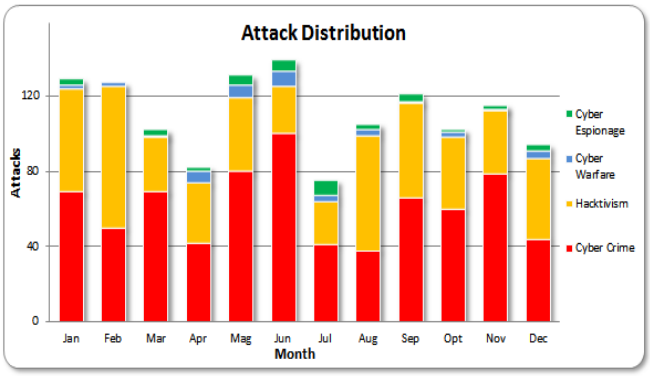


Figure 1. Cyber-attacks statistics

Especially the European Union (EU) countries and the USA take serious measures in order to avoid problems arising from above mentioned harmful software. The IA guidelines prepared in order to ensure IS and the decisions taken on this subject are the most important ones among these measures. Particularly, U.S. Department of Defense (DoD) has brought IA into the forefront thanks to a set of information prepared and implemented by them (Table 3).

Number	Subject	Date
O-8530.1	Security of Computer Networks	January 8, 2001
8500.01E	Information Assurance	October 24, 2002
8500.02	Information Assurance Application	February 6, 2003
8570.01	Information Security Training, Certification and Workforce Management	April 23, 2007

Table 3. Information assurance guidelines published by the U.S. Department of Defence.

Despite the fact that its existence is denied, thanks to a global communication response system, ECHELON, a group of countries led by the U.S. (Australia, Canada, New Zealand and the United Kingdom) have formed an organization where military and civilian communications throughout the world are followed and recorded. All tracing information and records obtained by this system are directly sent to National Security Agency (NSA) and Central Intelligence Agency (CIA). Besides, the possibility of having similar systems used for the same purpose in other countries such as Russia, China and France, is mentioned in the reports of EU parliament [8]. This system and all other suchlike systems (Carnivore, Coolminer etc.) are mainly used for the purposes of IS and national security although full details of them were not released to the public. In order to ensure IS, USA forms units within the Ministry of Internal Security and Justice and organizes related studies through these units [9].

As the United States, EU has also taken a series of decisions regarding ensuring IS and keeps studying in line with these decisions (Table 4). Among EU countries, the UK and France carry out these studies under favour of electronic security and information system security units, as well as their subsidiaries [1], [10].

Date	Decision	Content
1987	Green Paper	IS in the telecommunications sector has been pointed out.
1992	EU Council Dec.92/242/EC	Ensuring IS
1995	EU Directive 95/46/EC	Personal data processing and protection of individuals in respect of the free movement of such information
1997	EU Directive 97/66/EC	Processing and protection of the confidentiality of personal data in the telecommunications sector
1999	EU Decision 99/276/EC	Safer use of the Internet by struggle against illegal content on the global networks
2000	EU Directive 2000/31/EC	Determination of the standards applied within the framework of cryptography and electronic signature technologies
2001	EU Regulation 2001/45/EC	Processing of personal data, protection of individuals and free movement of information by community institutions
2002	EU Directive 2002/58/EC	Protection of the confidentiality in the electronic communications sector and processing of personal data
2003	EU Council Dec. 2003/48/EC	Determination of the EU's approach on network and IS
2003	EU Council Decision 2003/2256/EC	Improvement of network and IS and following the e-Europe Action Plan on the spread of the application
2004	EU Regulation 2004/460/EC	Establishment of the European Network and IS Agency
2006	EU Directive 2006/24/EC	Content of all communication activities and making the storing of all details obligatory between 6 months - 2 years

Among Far East countries, Japan carries out these studies by favour of the national IS centre connected to the Prime Ministry. The related studies are carried out under four main titles such as central and local authorities, key/critical units used by the public (airports, railways, nuclear power plants, etc.), medias used in business life [11].

However in Turkey, there is no public authority directly responsible for IS and IA applications. Nevertheless, according to the needs, cyber security exercises are carried out by TUBITAK within the body of the Ministry of Science, Industry and Technology and SPO Department of Information Society connected to the Prime Ministry carries out studies to determine information technology strategies. In addition to these institutions mentioned above, Information and Communication Technologies Authority (BTK) and Presidency of Telecommunication and Communication (TIB) connected to this agency perform the task of organizing information technology within the framework of their duties and responsibilities.

Preparation of regulations and directives in an intended manner and their implementation are inadequate if not accompanied, although they are essential. At this point, full and efficacious applicability of the relevant legislation gains great importance.

3. Information Assurance

By selecting IS as its centre, IA is an approach combining the sub-headings of confidentiality, integrity and availability. Based on the idea that IS cannot be provided only with some specific measures; main security headings and the details of IA approach that proposes activating all security mechanisms and effectively managing all processes such as conveying, storing and processing information, are given below.

A. Software/Hardware Security

The main reason for the use of safety standards and their guidelines is to ensure testing and evaluation of the software/hardware or systems produced in the relevant field by independent laboratories according to certain rules and accordingly, to mediate for giving guarantee to users in this respect. The main purpose of these tests and evaluations is to check full implementation of safety functions on the hardware/software and to determine whether the professed guarantee level is provided or not. Consequently, different security evaluation standards has been used in the different countries over the world. The first studies on the safety assessment of software/hardware, started with the publication of TCSEC (Trusted Computer System Evaluation Criteria) standard by U.S. Department of Defence in 1983 [12, 13]. Within the scope of IA, controlling the compliance of the software and hardware with the standards such as TCSEC and ITSEC (Information Technology Security Evaluation Criteria) and disallowing its use in a contrary situation will be the most appropriate approach. Especially, companies computerize all their applications, keep all information that is of vital importance for them such as income, expenditure, R&D, product, personnel, corporate policies in discs and transfer their backups into the data storage cassettes in the backup units. Likewise, everybody may keep his/her personal information such as income and expenses, bank transactions, medical information, personal picture/video files in his/her personal computer. As well, such information may be kept on their cell phones. Backups of these data are generally kept in a storage medium such as an external disk, CD, DVD

[14]. In terms of IA, it is of great importance whether the software controlling such information and the hardware hosting/storing them, are in a structure and environment complying with the standards or not.

B. Network and Communication Security

Network security technologies protect network against cyber-theft, use of confidential business information for malicious purposes and the attacks from viruses and worms arising from internet. As for the Communications Security (COMSEC), it is interested in secure transmission of information or news through channels of communication and focuses on the security technologies on the points connecting to the outside world with network inputs. In case that network and communication security is not provided, there becomes the risk of facing with the risks such as unauthorized intrusion, closure of the network, interruption of service, non-compliance with regulations and even legal action. When it comes to network security, IA applications comprising the topics such as continuous workableness of the system, authentication, data integrity, and data confidentiality, come to the forefront.

Network and communication security cannot be performed as based on a unique method. Instead, a number of obstacles are used in order to defend personal/corporate networks in different ways. Even if a solution fails, the remaining one can protect the network and the data against various network attacks. Security layers in the network signify exposure of valuable information used for the execution of the works/communications to the use of authorized persons and its protection. Basically, the ideal network security systems (firewall, antivirus, etc.), provides protection against internal and external network attacks. Possible threats may come from inside and outside of the entity and the four walls of the room. An ideal network security system signs the unusual behaviour by monitoring the effectiveness of the whole network and gives an appropriate response. It tries to ensure the confidentiality of all communications anywhere and at any time. What is important at this point is to enable individuals to access with the guarantee that their communication with the network will be confidential and under protection [15].

Network security system controls access to information by correctly identifying the users and the network structure. Individuals or entities can create their own rules about data access. Rejection or approval of the access be based on the identities of the users, job function or other business-specific criteria. For this reason, establishment of an ideal network security system, its adaptation to current developments and the measurement of its resistance against attacks by assaulting in certain periods are important elements in terms of IA.

After about one year-long preparation process in Turkey, between 24 December 2012 to 11 January 2013, National Cyber Security Exercise was carried out with the participation of 61 organizations under the coordination of Advanced Technology Research Centre (BILGEM) and Information and Communication Technologies Authority (BTK). Within the scope of USGT-2013, in addition to written injection more than 500, real attacks comprising of port scanning, distributed drop off service attacks (DDoS), control of web applications and analysis of log file, are performed. Studies have revealed the consequent that there is a considerable amount of deficiencies in terms of IS in the organizations involved in the exercise [16]. This situation points out the need to advance more in terms of the level of network security in Turkey.

C. Emission Security

Within the framework of intelligence, forms of access to data are divided into three groups such as intelligence based on human, imagery intelligence and signal intelligence. Among these intelligence forms, signal intelligence can be analyzed under four sub-title such as communication, electronic, telemetry, and radar intelligence [17].

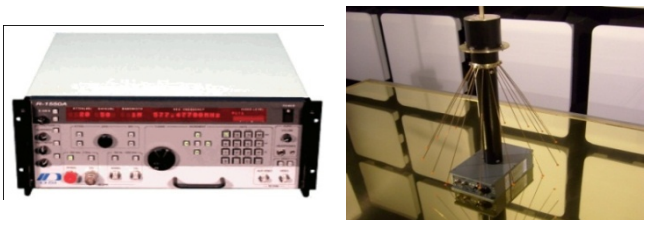
Communication intelligence includes all the operations of searching, capturing, monitoring and even decryption of the communication signals performed between two points as emitter and receiver through satellite, microwave, radio, radiotelephone, mobile phones and car phones. On the other hand, electronic intelligence includes the activities of making evaluation by obtaining electromagnetic waves involuntarily emitted by the devices belonging to the other side. In this intelligence method, they try to obtain information or data by analysing electromagnetic waves unintentionally emitted and in a free state in space [17].

The intelligence method by United States which is performed by analysing the data/information after recording all involuntary emissions has merged under the name of TEMPEST (**T**ransient **E**lectro**M**agnetic **P**ulse **E**manation **S**tandard) and almost all its standards are kept confidential. The most common example for the data/information intelligence TEMPEST is to analyse involuntary electromagnetic waves emitted from a computer screen by recording them in hundreds of meters away. For instance, every key pressed by a computer user in an office may be displayed on the screen of the TEMPEST receiver in a building outside the occupied space.

Since computers run with discrete impulsive signs, wideband emission comes into question. Thus, it is

possible for wideband sensitive receivers to obtain the recovery of the image from screen propagation without loss of information. Today, there are TEMPEST devices developed for this monitoring process (Figure 2) [17, 18]. Especially the undesirable leaks occurs on the computer screen, cables, keyboard, modem cable and even in ventilation panels are recorded and an image on a user's screen may be displayed on another screen with the help of very powerful algorithms. For this reason, all military or civilian institutions have to give importance to emission security defined as restraining unauthorized persons to obtain information from electromagnetic waves leaked from communications systems, information processing, and crypto hardware.

The emission security which is an important part of IA expressing the full complement of the measures taken in order to ensure effective IS and whose details were given above, can be achieved by taking a number of measures. Grounding of any kinds of cable and the use of ferrite filters commonly used in internal and external power cables of electronic circuits, plastic ribbon cables of portable and hard disks, internal and external data cables of computers (screen, printer, keyboard, CPU) are ranked among these. In addition, the emission security is provided by some simple measures: For instance, layout plan of the computer inside the room and avoiding computers from being located face to face with the window, keeping metal water and heating pipes, heaters, coolers, and metal shelves away from this environment, shielding of the entire room (isolating two medias in an electromagnetic sense from each other at a level of card, circuit or device) may be ranked among the measures that can be taken [19].



(a) (b)

Figure 2. TEMPEST receiver (a) and wideband antenna (b) [18].

D. *Employee Training and Physical Security*

Among the measures that should be taken by individuals, institutions or organizations within the scope of IA, training of the employees on related issues and providing physical security of the electronic media containing critical information are very important. Although measures for software, hardware, and emission security may be taken by expensive investment, all those measures can be in effective if the employee are in careless actions that may lead to a security vulnerability and the devices in which the information is stored are left on the places easily accessible. Therefore, the employee should be trained within the context of IA and storage devices and documents should be kept in suitable environments at the rate of confidentiality degree phase (identity card, biometric access system, storage media with a video surveillance system etc.).

E. *Other Safety Measures*

The use of cryptology, watermarking and steganography techniques are among the measures to be taken in order to ensure IS.

Cryptography is a set of techniques and applications based on the basis of mathematical methods, which allows two or more parties communicating with each other to make the exchange of information securely and grounds on a protection by transforming information into a form that unwanted people cannot understand (Figure 3) [20, 21].

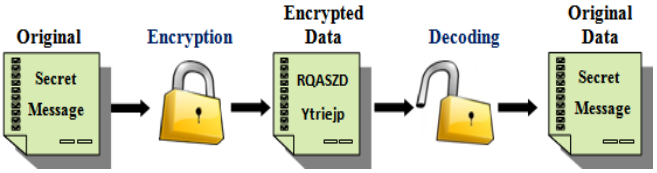


Figure 3. Encryption and decryption process.

On the other hand, watermarking (invisible) and modern steganography are technically based on the placement of any data (message) into an object in confidential manner. So much so that, only the recipient to whom the message was addressed can find the message in the object and the other observers cannot even be aware of the existence of such a message in that object (Figure 4) [20].

(a) (b)

Figure 4. The original digital image (a) and its version on which data was hidden by using the science of steganography (b) [22].

The purpose of each three methods mentioned above, is to ensure IS and to take effective security measures. Even if encryption ensures reliability, in a sense, it cannot ensure the confidentiality of the

message (it can be dawned on). While information is encrypted in a way that no one other than the sender and the recipient can understand it, in encryption applications; in watermarking and steganography applications, information is hidden in a form only known by the sender and the recipient and an additional protection can be provided if necessary by encrypting it [20]. Thus, it would be a more successful approach to store or hide the data through watermarking and steganography algorithms after encrypting it. It should be noted that one of the most important factors improving IS by the related methods, is the confidentiality of the algorithms and keys used in codes.

4. Conclusion

The innovations brought by today's information and technology age noticeably increase their presence in the lives of communities. Especially the element of insecurity due to the nature of electronic media is one of the most important factors threatening the security of information. From this point of view, in the present study, we clarify the IA approach and its elements which are becoming even more prominent day by day in today's world and which lumps the sub-headings of confidentiality, integrity, availability, and we make a number of suggestions about this issue in order to ensure effective IS.

Considering the principle of "an effective IS media can be achieved by ensuring IS", the use of software/hardware in compliance with standard, employee training, the establishment of physical environment; a safe transmission of information by cryptography, watermarking, and steganography techniques have been recommended. Beyond question, besides taking some or all of these measures, it is possible to improve the related measures according to the needs.

References

[1]. Bensghir T. K., Altınsoy S. Ö., A *corporate restructuring proposal for the management of cyber security in Turkey*, 3rd International Conf. on Information Security and Cryptology, 14−20, Ankara, 2008.

[2]. Sevgi L., *11 September 2001 - Electronic wars, information security and national defense in changing world*, EMO special issue, 2001.

[3]. http://www.internetworldstats.com/

[4]. http://www.whois.sc/internet-statistics/

[5]. http://www.boutell.com/newfaq/misc/sizeofweb.html

[6]. http://www.internettrafficreport.com/main.htm

[7]. Ozenc K.., , *ensuring the security of personal and corporate information in information and communication technologies*, 2nd International Conf. on Information Security and Cryptology, 183−190, Ankara, 2007.

[8]. http://en.wikipedia.org/wiki/Echelon_(signals_intelligence)

[9]. http://www.dhs.gov/index.shtm

[10]. http://www.cesg.gov.uk/about_us/index.shtml

[11]. Japanese Government's Efforts to Address Information Security Issues (November 2007), http://www.nisc.go.jp/eng/

[12]. http://www.niap-ccevs.org/cc-scheme/cc_docs/

[13]. Kara M., S*oftware/hardware security evaluation in Turkey*, TÜBİTAK-UEKAE, 2009.

[14]. Kara M., Secure File Storage and Deletion in Computer Systems, TÜBİTAK-UEKAE, 2011.

[15]. http://www.cisco.com/web/TR/solutions/smb/products/security/security_primer.html

[16]. National Cyber Security Exercise in Turkey, 2013 http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usgt2013.php

[17]. Sevgi L., *Electronic wars, information espionage and tempest*, Endüstriyel & Otomasyon, January 2005.

[18]. http://www.comtestnl.com/tempest.shtml

[19]. Sevgi L., *EMC and prevention methods: (i) Screening*, Endüstriyel & Otomasyon, September, 2004.

[20]. Yalman Y., Erturk I., *A hidden data transfer system implementation within digital voice for wireless communications*, Journal of Polytechnic, Vol. 11: 319–327. 2008.

[21]. Bandirmali N., Erturk I., *WSNSec: A scalable data link layer security protocol for WSNs*, Ad Hoc Networks, doi:10.1016/j.adhoc. 2011.04.013.

[22]. Yalman Y., Erturk I., Karahan A., *Software design and implementation for revealing digital stego images*, 4th Int. Computer and Instructional Tech. Symposium (ICITS'10), 1082–1086, 2010.

Corresponding author: *Yildiray Yalman*
Institution: *Computer Engineering Department, Turgut Ozal University, Ankara, Turkey*
E-mail: *yyalman@turgutozal.edu.tr*