Security Solutions against Computer Networks Threats

Fatemeh Soleimani Roozbahani
PhD Candidate for IT Management, Islamic Azad University, Science and Research Branch of Tehran, Iran
Email: Fa.Solaymani@gmail.com
Reihaneh Azad
Master Student of IT Management, Farabi Institute of Higher Education, Karaj, Iran
Email: Azad.mit92@hotmail.com

ABSTRACT

The spread of information networks in communities and organizations have led to a daily huge volume of information exchange between different networks which, of course, has resulted in new threats to the national organizations. It can be said that information security has become today one of the most challenging areas. In other words, defects and disadvantages of computer network security address irreparable damage for enterprises. Therefore, identification of security threats and ways of dealing with them is essential. But the question raised in this regard is that what are the strategies and policies to deal with security threats that must be taken to ensure the security of computer networks? In this context, the present study intends to do a review of the literature by using earlier researches and library approach, to provide security solutions in the face of threats to their computer networks. The results of this research can lead to more understanding of security threats and ways to deal with them and help to implement a secure information platform.

Keywords - **Computer Network, Security, Threats.**

Date of Submission: June 26, 2015 Date of Acceptance: July 17, 2015

1. INTRODUCTION

The increasing development of communication and information technology has doubled the need for exchange of information and data [1] the emergence of computer networks in all industries in the 70's improve the production of knowledge and gave it a high acceleration. Since then, the individual wisdom has turned into plural wisdom and the private thoughts of intellectuals became the great minds of the elite Global Village [2]. According to the statistics, from 2020 onwards, human knowledge will be doubled every 72 days [3]. The cost of information processing is cheap today and communication costs are decreasing as the world's exchanging is increasing [4]. The role of information in organizations therefore can be clearly seen as one of the most vital assets [5].

With the development of the Internet and its use in different dimensions, organizations and institutions have faced invasion with new issues related to information security and computer networks [6] in a way that technology information industry and communication are looking for security solutions for these networks [7]. So it can be said that security in the real world in individual and social scale is a dynamic concept interpreted by the effect of the new national and international opportunities and threats [8] and a secure network must be protected against intentional and unintentional attack and have a good response time, availability or high readiness, reliability or high reputation, integrity and be flawless and provide scalability as well as accurate information [7]. The vulnerability of computer networks as IT infrastructure, is one of the major problems in this area [9] and the intensive competition and the increasing volume of data traffic, have had the telecommunications providers to reload and review the existing network [10]. Vizandan et al. (2011) controlling vulnerabilities and security threats have been considered one of the most serious issues [11]. Azarpour et al (2012) have also mention the acceptable level of security as a key requirement for a lot of people who use computer networks in earnest [12]. The question that arises is: what solutions and technologies should be taken into account against computer network threats to ensure the security and confidentiality of information on individuals and organizations?

Given the necessity and in order to respond to the mentioned question, the current study aims to use library approach and reviewing the earlier investigations to provide solutions for securing computer networks. The results of this study can be used to identify the threats to network security to implement an effective and secure computer platform.

2. THEORETICAL FOUNDATIONS OF RESEARCH

2.1 Computer Networks

The term network means a set of serial lines that are used to connect the terminals to large computers [13]. Thus, the definition of the computer network is a set of independent computers that are connected to a single technology. Two computers are connected to each other when they can exchange information [14]. Basically a computer network consists of two or more computers and peripherals such as printers, scanners, etc. that are directly related to share hardware, software and information resources [12]. Computer networks are classified according to various factors including: longitude, interconnection, management and architecture [15]. Some computer networks are called local area network or LAN (network within home, office buildings, health care facilities, or in academia), metropolitan area network, or MAN (in a geographic area such as a city or metropolitan provinces) and wide Area Network or WAN (wide area network for the geographic area like a state). WAN networks are formed from LAN's in several different ways, which are connected by routers. The Internet is a final WAN [16]. Fig 1 shows an image of computer networks [17]:

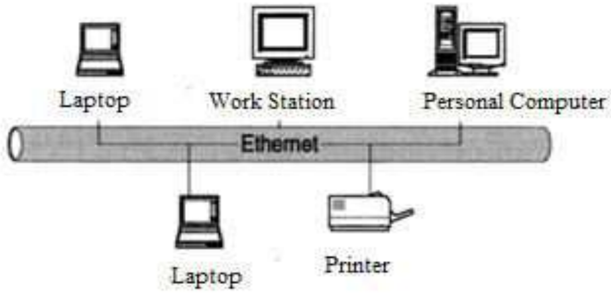

Fig 1 - Computer Networks[17].

2.2 Computer Security

Computer security is a generic name for a set of tools designed to protect data and thwart hackers [18]. This concept includes many aspects of physical protection equipment to protect the electronic bits and bytes that make up the network information [19]. Computer security has four main key goals which include confidentiality, accuracy, privacy and availability [20].

- **Confidentiality**: This term covers a related concept:
  Confidentiality of information ensures that private and confidential information is not accessible to unauthorized persons.
- **Privacy**: ensures the information which have been collected and saved by people is accessible by them and who this information can be revealed to.
- **Accuracy**: The term covers two related concepts:
- *Accuracy of the information* ensures that data and applications are allowed to change only on a specific procedure.
- *Accuracy System* ensures that a desired function runs in the correct manner, free from deliberate or inadvertent unauthorized manipulation.
- **Availability**: ensures that the system works quickly and does not exclude authorized users [21].

3. RESEARCH HISTORY

Security of computer networks is a complex problem that is considered by managers of organizational centers more and more every day [22]. A lot of research has been done in this regard. Among these Hojaji's study (2008) can be noted which has provided security framework for services in next generation networks, from his perspective, the simple and traditional infrastructure replacing with integrated and multilayered infrastructure will make the service network operators face security challenges and data privacy issues and suppliers from this platform are exposed to new risks [10]. Vizendan et al (2011) have investigated the symmetric encryption algorithms which have many applications in the secure network and communications infrastructure [11]. Azarpour et al (2012) also examined the importance of Honey Pot technology in establishing network security and how the hackers have been trapped by network specialists [12]. Results from Javadzadeh et al (2013) investigation for design and construction of the knowledge of systems expert for network security test suggest lack of a proper user interface, the interaction between humans and computers has been the problem [9]. Gholipour et al (2014) also provide a process for testing the security of web-based intranet applications. In their opinion, security test must be precisely done based on a rigorous process that he and his colleagues proposed in 10 stages [8]. Results from the Sayana investigation (2003) on the approach on network security audits indicate that good security will not be achieved only through high investments and the use of sophisticated tools, but this area requires an information system able to point the systematic management of security devices through a well-defined processes [23]. Alabady (2009) in a research on the design and implementation of network security has presented a checklist that assesses the amount of network security and confidential data [24]. Daya (2010) in an article entitled Network Security has the history and importance of network security in the future. In his opinion to deal with security threats in the future, network security needs to rapidly changing [20].

4. NETWORK SECURITY

Network security is a process in which the security of a network against internal and external threats is supplied to better meet the organization's set of security mechanisms and provide safe and reliable network that is called a secure computer network [25]. In fact, security is a series of security dimensions designed to express and manage specific aspects of network security [7]. Security thinking in network is to achieve three important factors that together constitute the security triangle. These include confidentiality and trusteeship, integrity and being constantly available. The three basic principles form the information security in the network or outside it so that all necessary measures taken for the security of the network or the equipment made, are all due to the need to apply these three parameters in the maintenance and exchange [12].

5. THREATS AND SECURITY VULNERABILITIES IN COMPUTER SECURITY

When talking about network threats, these threats can be events or people that lead to harm any network data. Network threats can be natural, such as wind, lightning, flooding, or may be accidental, such as accidental deletion of files [26]. Threats to the security of information systems can be classified in three main categories of disclosure of confidential information (the threat of disclosure), damage to the integrity of information (the threat of manipulation) and the lack of information (damaging services threats)[27]. From one perspective, attacks are divided into two categories: passive and active and in another perspective they can be divided in destructive and nondestructive categories and in another views they can be classified on their basis. The common attacks on the network are as follows [28]:

- Stop service attack (DOS): In this type of attack other users can use the resources and information and communication. This type of attack is active and can be used by internal and external users.

- Eavesdropping: a passive attack, the attacker hears the exchange of data, information and messages.

- Traffic Analysis: this is a passive attack; the attacker analyzes network traffic based on the number of packets and gains valuable information.

- Message and Data Manipulation: active attack, the attacker disturbs the comprehensiveness and accuracy of the information with unauthorized changes [28].

On the other hand the vulnerability of computer networks as IT infrastructure is one of the major problems in this area. The majority of the vulnerabilities are due to improperly configured software and network organizations [9]. In general, system vulnerabilities, flaws or weaknesses are in the design or implementation of an information system (including the security procedures and security controls associated with the system), which can be through loss of confidentiality, integrity or availability, as willingly or unwillingly adversely affect the operations or assets of the organization [29]. In other words, the organizations identify security merely as a technological issue or the software and security tools do their job properly without failure, even though the biggest source of security disasters is human error. In other words, in most cases users without the knowledge of what they are doing would provide network intrusion, so that even blind people can be deceived through typical social engineering tricks and use their lack of knowledge to penetrate the network abuse [30]. Table 1 summarizes the various threats and their consequences [31]:

Table 1: Summary of Various Threats and Their Implications [31].

Threat	Domestic/Foreign	Threat Consequences
E-mail containing virus	Foreign origin, domestic use	Can infect system's reading email and subsequently spread throughout the organization.
Network Virus	Foreign	Can enter through unprotected ports and affect the entire network.
Web-based viruses	Internal views of external sites	Can affect the system that does the visit and then also affect other internal systems.
Attack on the server	Foreign	If the server is compromised by a hacker he can gain access to internal network systems.
Service rejection attacks	Foreign	If the router is attacked the entire network can fail and external services such as web, email and FTP can be cumbering.
Network User Attack (internal employee)	Internal	Traditional firewall network edge can prevent the attack. Internal segmentation firewalls can help internal damage.

6. WAYS OF DEALING WITH SECURITY THREATS AND VULNERABILITIES IN COMPUTER NETWORKS

Network security is vital to restrict internal and external threats to an organization at different levels which with appropriate security policy, these threats can be reduced to a minimum. In other words, prevention includes all mechanisms and policies to limit the scope of security incidents and threats [32]. Security policies are rules electronically programmed and saved to control some areas as access privileges in security [33].

6.1 The Use of Encryption Techniques

No technique has ever provided 100% security. But the most widely used technique is encryption. Encryption is a technique that encrypts simple data and the text and makes it difficult to understand or interpret. Currently there are several encryption algorithms, secret key encryption, public key encryption and encrypted message [15]. The encryption systems can be divided into two broad categories: first, symmetric encryption system in which the receiver and transmitter agree on a private key that nobody else must know. The second type, asymmetric encryption with a public key which's major cause of creation was problems related to the key encryption distribution [11].

6.2 Layered Security

Layered Security is a combination of several security measures to ensure that not all security measures are at one level. So it protects the network from resources and threats [34]. The use of layered security is to ensure that all possible ways of attacking are blocked where prevention is not an option, but always identifying threats is [35].

6.2.1 Layers of Security

- Layer- 1 DNS: domain name system acts like a phone book for a computer to find the name of the website. This system is usually ISP Provided. But for better security DNS server can be used.

- Layer 2- Firewall: firewalls act as a filter between the network and the outside world and scan all the network traffic and decide what traffic is allowed to enter or exit [34]. Firewalls also convert internal IP to IP addresses on the Internet, providing a more secure network. This prevents disclosure of important information about the structure of the network covered by the firewall [1].

- Layer 3- Network: this layer monitor signs of external threats [34]. In this level IDS[1] and IPS [2]are used; these technologies analyze the network traffic passing through the firewall in more detail [1].

- Layer 4- Equipment: the existence of the network firewall can ensure the protection of information, thus the use of firewall can ensure any of the equipment and systems that even if the network firewall fails the system will always be protected.

- Layer 5- Users: the user layer is often the most difficult one to manage because of the need to strike a balance between security and convenience. So the best way to defend the internal threat is awareness and training.

- Layer 6- Applications: the software to be installed from a reliable source and network operating systems and be up to date is very important to protect newly discovered exploits.

- Layer 7- Data: for increased security, data must be encrypted and have password [34].

6.3 Penetration Test

Penetration testing is the process of investigation and discovery of vulnerabilities and security weaknesses of a system or a computer network and the possibility of abusing the loopholes in order to carry out illegal activities, or sabotage the team. The test is divided into two categories: internal and external. Internal penetration test relates to a process in which the test team, through the organization's internal network, assesses the weaknesses and possibilities of taking advantage of them. In the external penetration test the team uses the internet remotely, and without physical presence, to assess the possible vulnerabilities and taking advantage of them [36]. On the other hand, the method of testing network security software based on the variety of vulnerabilities is very specific and it is suggested for flaws so that 10 defects are chosen, and by modeling a threatening tree it builds the attack tree and generalizes the test sequence in an algorith. According to the theory of defects, the method can be applied to a case to determine the validity of its performance [8].

6.4 Intrusion Detection Systems (IDS)

There are many reasons to use intrusion detection system as a necessary part of the system to protect it. Many traditional systems and applications have been developed without security [37]. Intrusion detection is a diagnostic procedure that attempts to identify unauthorized access to a network or the reduction of its performance [12]. Fig 2 shows a computer network intrusion detection system [37]:

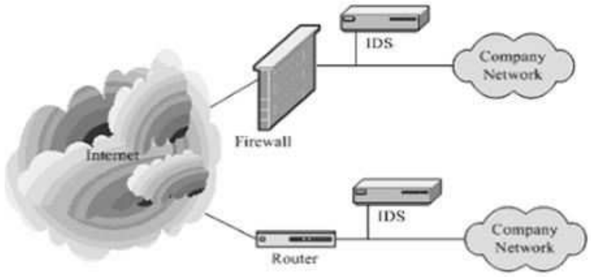

Fig 2: IDS in the computer network [37].

Intrusion detection system is divided into two main categories: host-based intrusion detection system (HIDS) and network-based intrusion detection system (NIDS). HIDS assesses the information content of operating systems, systems and software file and NIDS analyzes the information in network communications and evaluates the data packets that are exchanged over the network [38].

6.5 Intrusion prevention system (IPS)

IPS uses IDS algorithm for monitoring and allows network traffic to pass based on technical analysis. It usually works in different areas of the network and actively manages any

[1] Intrusion Detection System
[2] Intrusion Prevention Systems

suspicious activities that can bypass firewall [39]. In fact, this system is a device or software that detects signs of intrusion to the network. This includes generating alarms and intrusion blocking [40]. Generally, IPS is set into the network and monitors the information as they pass inside. An IPS has the ability to do more than just warning or log its decision. In addition, the system has the ability to be programmed to react to what the diagnosis is. This feature makes the response much better than the IDS and IPS [12].

7. CONCLUSION

The importance of utilizing the information in today's developed world will lead to security threats. It can be said that the protection of computer network of organizations, is important to create a competitive advantage. Results from this study showed that threats and damage computer networks can be any person or event that could damage the data. Computer network attacks can be divided into two categories: passive and active attacks or internal and external attacks. Attacks common to computer networks, include denial of service attacks, eavesdropping, traffic analysis, manipulation of messages and data, e-mails containing viruses, network viruses, Web-based virus attacks on Web servers and RAID network users. To deal with these threats and vulnerabilities there are techniques that exist, including encryption techniques where simple data is encrypted in text in such a way that it can be difficult to understand and interpret. This will reduce the possibility of network intrusion. On the other hand IDS and IPS techniques control the exchange of information in the network and prevent unauthorized access. After the implementation of the proposed techniques using internal and external penetration test can ensure security implementations. In this context, and based on the findings of this study to enhance the security of computer networks, the following suggestions are offered:

- Identifying security breaches of computer networks
- Using a combination of techniques of computer network security
- Periodical Penetration Testing
- Informing users of the computer network of common security threats
- Identifying further new security threats and ways of dealing with them
- Periodically update software and network operating systems

The above suggestions can be effectively used to create a secure platform for organizations.

REFERENCES

[1] N. Modiri, H. Arbasi. "Providing multiple layers to increase the layered e network security". The first national conference on new approaches in computer engineering and information retrieval. Gilan. 2013.

[2] M. Rahgozar. "Computer networks". Book of the Month Science and Technology, pp. 98-99, 2010.

[3] Sh. Ajudanian, M. Ahmadi, S. Tabatabaei. "Providing a model for the localization of the strategy of defense in depth in network security and its analysis using SWOT analysis". The National Conference on Science and Computer Engineering, Najaf Abad, 2012.

[4] M. Soufi, "Providing a new innovative and intelligent approach to use in the design of security systems detection engine to enhance the security of network infrastructure". The first Conference on computer intelligent systems and their applications, Tehran, 2011.

[5] Processor, "IT and computer networks security ".Processor monthly, pp. 32-36, 2012.

[6] Sakharavesh, "the role of human factors in computer network security". Processor Monthly, pp. 24-27, 2011.

[7] N. Mashayekhi, M. Ashoorian, M. Riahi Nasab, "Providing the security matrix as a layer in NGN networks" the Third National Conference on Information and Communication Technology, Tehran, 2008.

[8] F. Gholi Poor, N. Modiri, M. Riahi Kashani, Providing a process for testing the security of web-based intranet applications," the National Conference on Advances in science, engineering and basic electronics, Tehran, 2014.

[9] M. Javad Zadeh, M. Kangavari, S. Fathi, "to design and build the knowledge base of expert systems for network security test," Journal of electronic and cyber defense, pp. 43-51, 2013.

[10] F. Hohaji, "providing a framework of security for services in next generation networks," the Third National Conference on Information and Communication Technology, Tehran, 2008.

[11] A. Vizandan, A. Mir Ghadri, J. Sheykh Zadegan, "passive defense in infrastructure communications networks with an emphasis on the security assessment of flow encryption algorithms," Journal of passive defense, pp. 47-52, summer and fall of 2011.

[12] M. Azar Poor, A. Dahar, M. Jahani Mir, "the assessment of computer network security by Honey Pot technique in IDS & IPS systems"," journal of information technology era, pp. 78-84, 2012.

[13] L. Peterson and B. Davie, Computer Networks: A Systems Approach, USA: Elsevier, Inc., 2012.

[14] A. Tanenbaum and . D. Wetherall, Computer Networks, New Jersey: Pearson Prentice Hall, 2011.

[15] Tutorials Point (I) Pvt. Ltd., Data Communication and Computer Network, INDIA: www.tutorialspoint.com, 2014.

[16] K. Mansfield and J. Antonakos, Computer Networking for LANS to WANS: Hardware, Software and Security, USA: Course Technology, Cengage Learning, 2010.

[17] J. Migga Kizza, Computer Network Security, New York: Springer Science+Business Media, Inc. , 2005.
[18] K. Krishnan, *Computer Networks and Computer Security,* North Carolina , United States: North Carolina State University, 2004.
[19] T. Shinder, Dr. Tom Shinder's ISA Server 2006 Migration Guide, Burlington: Elsevier, Inc., 2007.
[20] B. Daya, "Network Security: History, Importance, and Future," *University of Florida Department of Electrical and Computer Engineering,* 2010.
[21] W. Stallings, NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS, USA: Pearson Education, Inc. , 2011.
[22] Network, "just when it comes to network security," Network Magazine, 2013.
[23] A. Sayana, "Approach to Auditing Network Security," *INFORMATION SYSTEMS CONTROL JOURNAL,* 2003.
[24] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," *International Arab Journal of e-Technology,* pp. 26-36, 2009.
[25] S. Farahmand, "IT security and computer networks," Processor Monthly, pp. 32-36, 2010.
[26] N. Ahmad and K. Habib, Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution, Sweden : Blekinge Institute of Technology, 2010.
[27] Analysts's information age, "the performance of network security system in the municipality ICT," the information age analysts, pp. 54-55, 2011.
[28] Processor, "a security model for computer networks," Processor Monthly, p. 39, 2014.
[29] O. Awodele, E. Enyinnaya Onuiri and S. Okolie, "Vulnerabilities in Network Infrastructures and Prevention/Containment Measures," in *Proceedings of Informing Science & IT Education Conference (InSITE)* , California , 2012.
[30] B. Berner, "Seven unforgivable errors in network security," Binesh Magazine, pp. 53-55, 2011.
[31] C. Leidigh, "Fundamental Principles of Network Security," *American Power Conversion,* 2005.
[32] K. Mahmoudi, M. Ketabdari, M. Saybani, "the identification of penetration to military systems computer networks by anomaly detection method," Journal of Marine Science and Technology, pp. 17-27, 2013.
[33] Cisco, "Network Security," *Cisco Systems,* 2001.
[34] FORTINET, "A Look at Layered Security," *FORTINET High Performance Network Security,* 2015.
[35] M. Kedgley, "The Art of Layered Security - Data Protection in a Threatscape of Modern Malware," *A New Net Technologies Whitepaper,* 2012 .
[36] S. Nikookar, "penetration tests in computer networks," journal of information technology era, pp. 95-99, 2012.
[37] A. Anand and B. Patel , "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols," *International Journal of Advanced Research in Computer Science and Software Engineering,* pp. 94-98, 2012.
[38] M. Sazzadul Hoque, A. Mukit and A. N. Bikas, "AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM," *International Journal of Network Security & Its Applications (IJNSA),* pp. 109-120, 2012.
[39] N. DULANOVIĆ, D. HINIĆ and D. SIMIĆ, "AN INTRUSION PREVENTION SYSTEM AS A PROACTIVE SECURITY MECHANISM IN NETWORK INFRASTRUCTURE," *Yugoslav Journal of Operations Research* , pp. 109-122, 2008.
[40] S. Piper, Intrusion Prevention Systems, Indiana: Wiley Publishing, Inc., 2011 .

Biographies and Photographs

Miss. Fatemeh Soleimani Roozbahani has obtained B.S. degree in Nuclear Physics from Shahid Chamran University in 2009, and has obtained Master degree in Information Technology Management summa cum laude with a cumulative GPA of 19.76 [out of 20] amongst the graduates of this major who had been graduated in 2011 from Farabi University. Presently she is pursuing Ph.D. in Information Technology Management in SRBIA University. Her research fields are Information Business Intelligence, Systems Integration, Strategic Information Systems, e- Banking, e- Commerce, Knowledge Management and Security in Computer Networks. She is appointed as a Lecturer in Azad University, Deptt. of Information Technology.

Miss. Reihaneh Azad received her B.S Degree in Computer Engineering from Saeb University, Abhar, Iran in 2008. She's Master Student of IT Management in Farabi University, Karaj, Iran and works as software supporter expert in Pasargad Bank Electronic Payment Company, Tehran, Iran. Her research interest includes E-Commerce, Information Systems, Knowledge Management, Computer Network, Data mining and E-Banking. She has authored 6 research papers in proceedings & journals.