Int. J. Nonlinear Anal. Appl.
Volume 12, Special Issue, Winter and Spring 2021 , 415-424
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/IJNAA.2021.5279

A study and analysis of attacks by exploiting the source code against computer systems

Ahmed Badrulddin[a*]

[a] *Department of Law Affairs, Baghdad University Presidency, University of Baghdad, Iraq.*

(Communicated by Madjid Eshaghi Gordji)

Abstract

An avalanche of threats from malicious used information and communication technologies (ICT) in political, military, economic and social affairs led to a deep awareness of the fact that new technologies may pose additional risks to international peace and safety. Thus, the problem of international information security, that is, the state of the spread of information among the countries of the world, with which excludes the possibility of violation of the rights of the individual and users in various state agencies and in all fields of knowledge. In the field of knowledge, as well as destructive and illegal impact on elements of the national critical information infrastructure, became an integral part of international security as a system of international relations based on the observance by all states of generally recognized principles and norms of international law and excluding the solution of controversial questions and disagreements between them through force or threat of force, in general. Thus, the principles of international security providing for promoting peaceful coexistence, being ensuring equal security for all states, the creation of effective guarantees in the military, political, economic and humanitarian spheres, preventing the race of nuclear and space weapons, respect for the sovereign rights of every people, fair political settlement of international crises and regional conflicts certainly include the creation of a system of international information security. At the same time, under the IIB system, designed for countering threats to strategic stability and ensuring equal partnership in the global digital environment, we understand the totality international and national norms and institutions, chief among which are the UN Regulated activities of various actors worldwide.

Keywords: Source Code, DNS Spoofing, DoS (Denial of Service).

1. Introduction

Attacks against computer systems tend to increase in frequency and complexity. Attacks, which were a way in which attackers called hackers showed their perfect motives and seek attention in the

[*] Corresponding author: Ahmed Badrulddin

Email address: Hmag462@gmail.com (Ahmed Badrulddin[a*])

Received: April 2021 *Accepted:* June 2021

early days, have become an industry due to the vulnerabilities in computer and computer networking systems today. Spyware is the most complex, obfuscated, and targeted class of malware, which has grown dramatically in recent years. Spyware is designed for secret, long-term, and persistent missions [5]. As reported by the country statistics in 2010, the number of attacks was 4400 and after that it increased by 6 times, reaching 26400 in 2019; approximately 15,000 attacks were detected. Figure 1 shows the number of attacks reported between 2010 and 2020 [3].

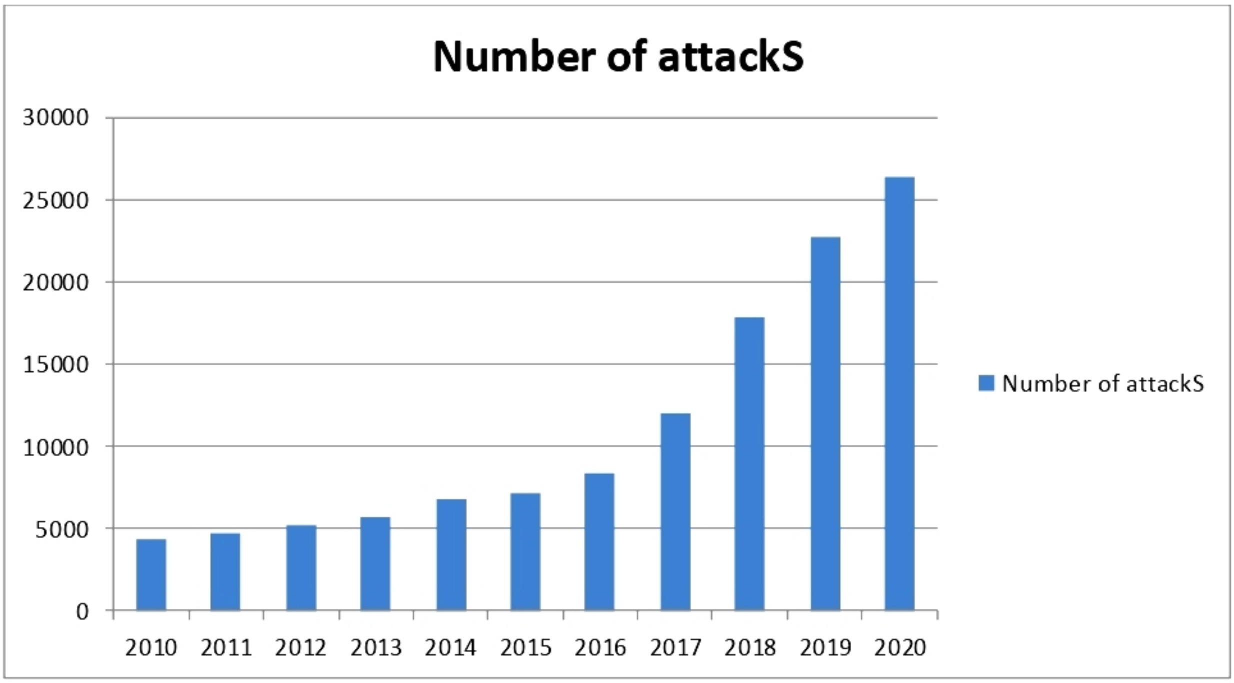

Figure 1: Number of attacks between (2010-2020)

Apart from the preliminary theoretical studies in determining the security processes to be developed against these increasing attacks; Attacks that have occurred or may occur against existing systems need to be examined and analyzed more than just a number. After all; security processes rather than prevent imaginary attacks; it is the review and design of the system for attacks that may actually be encountered [11].

We can classify the security goals into two goals: main and secondary. The main goals include security objectives that should be available in any system (confidentiality, availability, integrity and authentication) [9]. For this, the attacker checks for vulnerabilities in the system and acts accordingly. Vulnerability means compromising the security of the system, network, application or protocol in question; the presence of a vulnerability that may cause an unexpected and unwanted event is defined as a design or implementation error. To understand the methods developed for the security of computer systems, it is necessary to identify the types of attacks (attacks) that target these vulnerabilities and to develop actions that can be taken against these attacks.

In this paper, the attack phenomenon is defined via source code exploits, the point at which the attacks have reached in time and the reasons why attackers do so, the evolution of attacks over time and the essential features that all common attacks are discussed are examined. Then, the factors that can be classified according to the attacks are examined. Then, the simplest types of attacks were discussed. Finally, the present study is generally evaluated and its results are discussed.

2. Attacks on computer systems

In information and computer security; the other part generally considers evil people (hackers) and their attacks bypassing or circumventing existing information and computer security system; to weaken; harming people directly or indirectly. Attempts made on computer systems for malicious purposes such as damaging systems, disrupting, stopping, crashing or destroying systems are called attacks. Attackers are carrying out attacks that include many different methods to achieve their goals. By presenting all forms and classifications of attacks, analyzing them accurately, and determining the required procedures, these procedures are of great importance in order to obtain the security of complete information [7].

Understanding why attacks are carried out on computer systems will provide important data in determining the attacks and the measures to be taken. In general, the reasons for the attacker to take this path should be followed. In this regard, the statistics of the formation of Zone-H, which classifies and maintains information about attacks on web servers on the Internet after verification, about one million servers, based on previous years, also shows the reasons why the attacker attacks . The reasons for the attack between (2010-2020). It is classified as, "for political reasons", "challenge", "patriotism", and "Electronic blackmail". Figure 2 shows distributions of attacks based on these causes between 2010 and 2020. It also illustrates the distributions of attacks based on these reasons between 2010 and 2020.

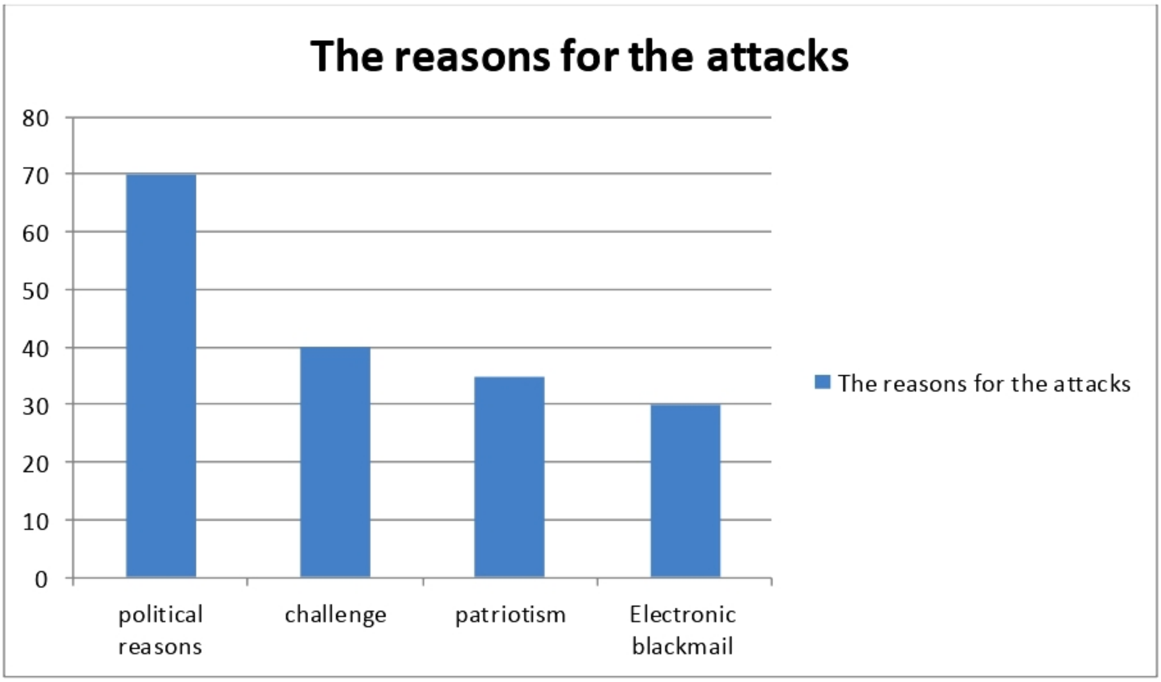

Figure 2: The most important reasons for the attacks

As shown in Figure 2, it appears that one of the most important reasons for the attacks is the political motive, as it is the biggest motive for the attackers.

The level of technical knowledge that attackers have and also the size of their attacks changes over time. As shown in Figure 2, attacks vary greatly over time and as technology evolves. Simple attacks such as guessing passwords or shuffling paper notes in the workplace are now being replaced by more comprehensive cross-site scripts and automatically coordinated, distributed, and structured attacks. As the attacks or tools used in the attacks are becoming more technically sophisticated, the level of information that the attacker needs to carry out the attacks also decreased. While this situation increases the number of attacks and attackers, and the damage that will be done as a result of the attacks, it also makes it difficult to do what needs to be done to prevent the attack [12].

3. Classification of attacks

Attacks can be classified and studied in various ways. Attacks according to the number of attackers, target type, path used, intent and means. These attacks are classified as shown in Figure 3.

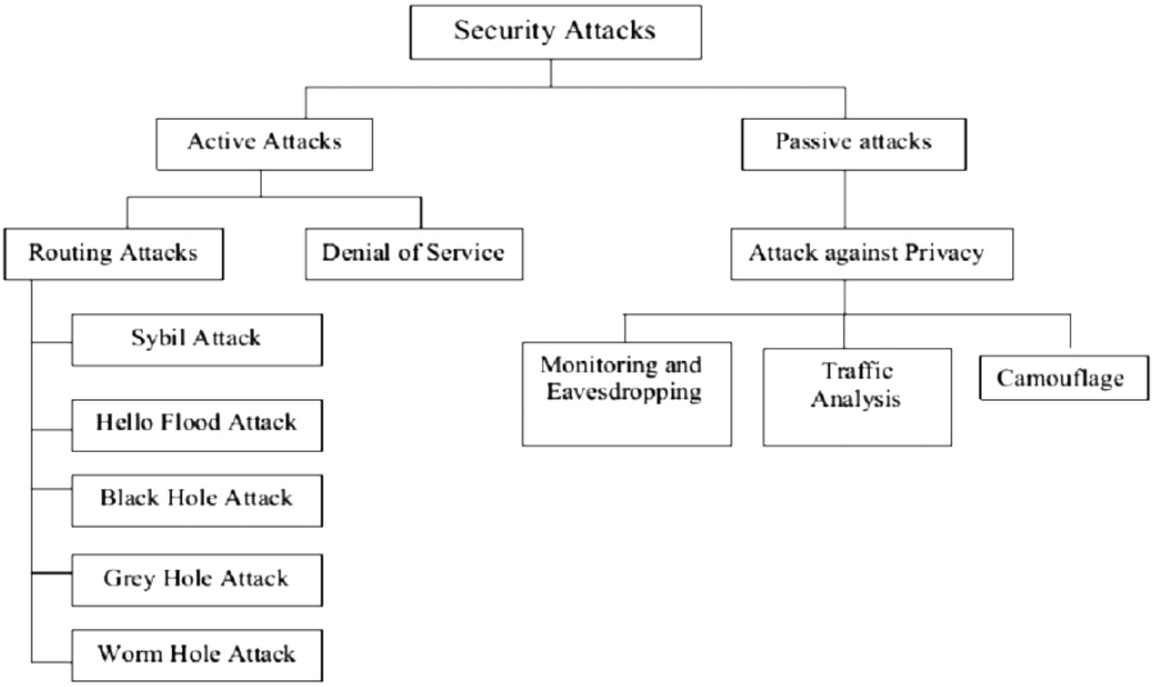

Figure 3: Classification of attacks

A solo attack by a single attacker is the most common type of attack and is easier to detect. System vulnerability attacks and unauthorized access are types of solo attacks. Attacks involving more than one attacker are called multi-attacks. IP spoofing, email bombardment and network flooding are such attacks. Attacks such as the ”Back Orifice” and Winnuke attacks are single-target attacks. Anomalous packet publishing attack, scanning attack, and anonymous FTP attack are multi-target attacks. DNS spoofing (DNS Spoofing), router attack and network DoS (Denial of Service) attack are types of network attacks. It is possible to count buffer overflow, ping to death attacks among direct attacks. Local attacks are carried out after login to the system.

4. Methodology

Software defects such as buffer overflow, CGI scripting errors, and encryption errors that may exist in all software used in the system (including system programs prepared for the operating system) can cause a computer system to take control or cause that computer to start unexpectedly. This is a vulnerability that has left the door open to many attacks, an issue that has been overlooked until recent years. Some software companies even released the product as soon as possible without debugging and correcting some errors they detected in the software packages they developed for reasons such as competition and profitability.

In the Microsoft Windows operating system, which is stated as the most used operating system, such source code flaws are announced to the users with the prepared security bulletins, very important fixes (”hot-fixes”) and service packs that are released at certain intervals are offered to the users both online and on CD. The abundance of these fixes points to the abundance of software flaws that were not foreseen or ignored during operating system development. In this regard, Microsoft has accelerated the work that focuses on security for the operating system software it has released. It is stated that Windows Server 2003, which was developed with the ”Security Development Lifecycle” approach, was released with much fewer security bulletins than Windows 2010. Microsoft perceived the importance of security and started to increase its investments and studies in this regard.

In Figure 4, a spyware attack with a ”drive-by download” source code exploit, which is used in a situation where the Internet browser security settings are not provided at a sufficient level or the current version is not used, and the activities that can be carried out against the system as a result of this attack are presented . Such attacks, source code vulnerabilities found in Internet browsers, are often used to hijack a computer system.

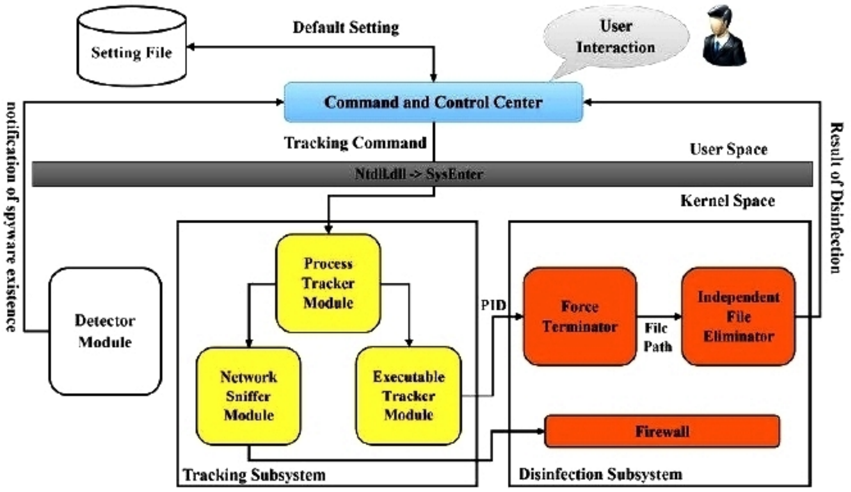

Figure 4: Spyware attack with a ”drive-by download” source code exploit

Accordingly, while browsing web pages on the Internet, the script codes on the pages of malicious sites manage to run a tiny installer program by taking advantage of an appropriate vulnerability detected in the client’s browser. This program starts its activities by negotiating with the system. Here, the desired spyware can be transferred to the server side without the user’s knowledge. In this context, there may also be a structure that constantly monitors the operability of running spyware. When this structure detects attempts to delete or dismantle the spyware, it can restore spyware through various techniques. For spyware running smoothly on the system, the purpose is to gather information. This information; It can be used for market research, identity theft, corporate spying, and even national security. This type of spyware also provides an external access to the host computer or use system resources to coordinate other attacks without the knowledge of the user.

5. Types of attacks:

The main types of attacks including code exploit are: eavesdropping, denial of service attacks (DoS), indirect attacks, backdoors, direct access attacks, social or social engineering, and cryptographic attacks. These attacks are described in turn below.

5.1. Eavesdropping

It is the interception of data transmitted over a network or channel by malicious third parties. In this attack type, it is even possible to obtain the data from the source to the target in the meantime and send it to the target by changing it. This attack, which is called "eavesdropping" (eavesdropping) in English, has many different application areas, contrary to what is believed. Even a stand-alone computer with no interaction with a computer can be eavesdropped on by tracking the electrical or electromagnetic emission from its electronic parts such as a microchip, display, or printer. In order to prevent these devices from allowing such eavesdropping, the American government developed a standard called TEMPEST starting in the mid-1950s.

5.2. Denial of Service Attacks (DoS)

Denial of service attacks are attacks that are carried out for a different purpose than attacks to gain unauthorized access or system control. The sole purpose of this attack is to place more load than a computer, server or network can handle; rendering the system unusable. These types of attacks usually consume computing resources such as bandwidth, free disk space or CPU time; It is done in the form of corruption of configuration information such as routing information and deterioration of physical network components. Such an attack on a key server on the network could render the entire network inoperable. Attacks are very difficult to prevent, as analysis of the entire network is required to prevent these attacks. Distributed Denial of Service (DDoS) attacks are a denial of service attack from multiple compromised hosts to a single target, not from a single source. Even very large and well networked websites can be disrupted by using enough attacking computers.

5.3. Indirect Attacks

These types of attacks include different types of attacks launched from a remotely inherited third-party computer. The use of another computer, called a zombie computer, in the attack makes it difficult to determine the actual source of the attack.

5.4. Rear doors

The methods that allow remote access to that computer to the person who by passing the normal identity verification processes or is aware of this established structure, which cannot be found with ordinary examinations on the computer, is called a back door. The backdoor can be in the form of an installed program (eg Back Orifice); it may be intentionally left in an existing legitimate program itself, in an undocumented form by the author of that program. Trojan horse programs are used extensively in such attacks.

5.5. Direct Access Attacks

Attacks made by a person who has direct physical access to a computer system are gathered in this group. The person providing physical access to the computer can make various future changes to the operating systems, such as designating a user for himself; software worms can install keyboard listening systems and eavesdropping devices on the system. Having direct access, the attacker can also copy a large amount of information to his side using backup units such as CD-ROM, DVD-ROM, floppy disks, memory cards, digital cameras, digital audio systems, cell phones and wireless/infrared connected devices. In this respect, a computer system should not be left to third parties, even for a short time.

5.6. Social Engineering

The human factor is the most important factor in computer systems security, as it is in every business. Albert Einstein ”Only two things are infinite, the universe and human stupidity, actually I am not so sure about the infinity of the universe.” He stated that social engineering will always be on the agenda.

Many security-related incidents encountered in computer systems are caused by the deliberate or deliberate intervention of the human factor. In computer security, social engineering is the general name given to the techniques for a hacker to obtain the information necessary to access the system by using psychological and social numbers on legitimate users who use or manage the computer system he is dealing with. Obtaining user and password information, especially by phone, is the most typical example. The hacker can obtain such information from system administrators like a regular company user. Many tactics can be considered in this regard, and the most important thing to do in order to get out of all these tactics without injury; It is the regular training of users and the implementation of security policies by all users, including system administrators, without exception .

Most damage to computer systems is due to human error. In-house users are actually the ones who cause the most damage to the system they use. Another point to be considered is the possibility that a person who leaves or is removed from a company may harm or attack the company he later worked for. For this, various security policies should be established for people leaving the company. The interesting methods used in social engineering, the risk area, the tactics used by the hacker and the things to be done in the fight against them are listed in Table 2. As can be seen from the list, social engineering uses various methods that cannot be thought of, from spying on a computer user while using their computer, to searching for useful documents among the paper waste in the workplace.

Social engineering attacks are possibly one of the most dangerous forms of security and privacy attacks since they are technically oriented to psychological manipulation and have been growing in frequency with no end in sight [1]. The Internet has become the largest communication and information exchange medium. In our everyday life, communication has become distributed over a variety of online communication channels. In addition to e-mail and IM communication [5].

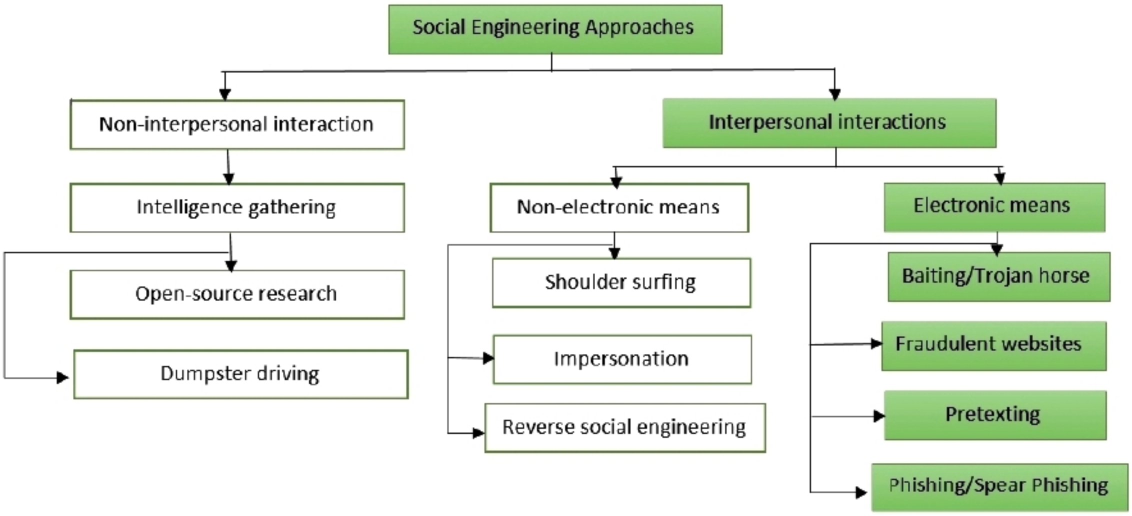

Figure 5: Common social engineering tactics and countermeasures

5.7. Cryptographic Attacks

Attacks to crack or decrypt encrypted information. These attacks are carried out by crypt-analysis methods. These include brute force attack, dictionary attack (dictionary attack) [2], man in the middle attack, ciphertext only, known plaintext, selected plain text or ciphertext. It is possible to count text (chosen plaintext, chipertext), adaptively chosen plaintext and related key attacks [4].

6. Discussion and Conclusions:

Eventually, the spread of information technologies and the rapid implementation of the work and transactions we do in our daily lives in electronic environments make information security mandatory. In order to ensure information security;

- Knowing the value of the information to be protected and protecting it accordingly,
- Taking into account the attacks, types and aggressive behaviors examined in this study in countermeasures and
- Implementation of the policies that will be determined in this framework.

It will greatly reduce the troubles and dangers to be encountered, prevent labor, time and financial losses, and will make great contributions to ensuring personal and corporate information security against malicious software or program particles that may come over the Internet.

In order not to encounter vulnerabilities in information security, individuals and institutions should take a series of measures from the simple to the most complex. However, even with all precautions taken, no one and no organization should think that systems are 100% secure due to constantly evolving attack techniques. It should not be forgotten that attacks can come from electronic media, as well as from friends and acquaintances.

In general, no matter how much precautions are taken regarding information and computer systems, it is useful to be aware that it is not possible to reduce the risks to zero. The most basic precautions to be taken can be listed as being constantly vigilant against risks, namely attacks, effectively creating and implementing security policies that will eliminate the attacks and their types described in this study, and minimizing the possibility of being affected by attacks by making the necessary updates in the light of new developments.

When the literature is examined, it has been determined that although there are many studies on the subject, ”information and information systems security” is not sufficiently discussed in academic environments and the necessary importance is not given to the subject. Such a study; It is thought that it will be important in terms of bringing the subject to the academic agenda.

As a result of the examination, the support of electronic environments where information and technology are intertwined and technology is developing and spreading at a dizzying pace, finding the vulnerability of systems, spyware written by malicious people such as hackers who will always be by our side, or by using these vulnerabilities and accessing systems It has been determined that they try to try almost every way in order to gain unauthorized access and to harm the systems and the people using the system, personal or institutional. It is among the findings that such attacks and the methods used should be constantly examined in order to take precautions against these attacks and threats.

It has been determined that attacks with malicious and spyware, which are the most important threats to information security in the world and in our country, are widely used, but users are mostly not aware of such attacks and threats. In order to avoid any harm, it is necessary to give the necessary importance to the subject, to increase the knowledge, to take the necessary precautions and briefly to raise awareness.

As described in this paper, in today's world, where the amount of attacks that can be performed on systems increases rapidly, while technological protection techniques increase, there is an increase in threats, as described in this paper; In today's world, where the amount of attacks that can be performed on systems increases rapidly, while technological protection techniques increase, there is an increase in threats .It changes shape according to technological innovations, people's weaknesses are mostly taken advantage of, many innocent methods are used that users cannot even think of, often overlooked social engineering approaches are often applied in addition to taking advantage of weaknesses in computer technologies, Web technologies and these programs can be used in a very short time and easily. They allow users to become widespread and widespread, from their computer usage habits, to scan their internet browsing history, to discover vulnerabilities in ports, to exploit operating system and program vulnerabilities, to send important and personal information to malicious people, to work on a computer system Unnoticed and without leaving any traces, malware scanners and spyware hide by hiding in different programs. It is considered that they use many methods, from bypassing the Internet, even deactivating these programs, opening system resources such as bandwidth and processor for unnoticed external use, and it is considered that great efforts should be made to create reliable systems for information and computer security.

Among the most important things that must be taken in order to strengthen the systems:

- has a dynamic rather than static process,
- It begins with protection and unification,
- A preparatory process is needed,
- That attacks must be responded to quickly after they are detected and
- We should not forget that improvements must always be made in the system.

As a result, for a high level of security of information and computer systems these things must be taken into account. Attacks on computer systems and the methods used in the attacks, the security elements the attacks target, the characteristics they exhibit, the weaknesses and vulnerabilities the attacks target, the profile of the attacker, and the factors that drive the attacker to attack, should always be taken into account. In mind, preventive countermeasures should be taken by applying a systematic approach, as mentioned above.

References

[1] D. Airehrour, *Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model,* mdpi, Information 2018, 9, 110; DOI:10.3390/info9050110.

[2] *Anatomy of an attack,* available online: http://blogs.rsa.com/anatomy-of-an-attack/, last accessed on 2013.

[3] T. Huang and Y. Zhao, *Revolution of securities law in the Internet age: A review on equity crowd-funding,* Comput. Law Secur. Rev., 33(6), 2017, pp. 802810

[4] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer,*Social phishing*, Communications of the ACM, 50(10) 2007 94-100.

[5] D. JAVAHERI, *Detection and Elimination of Spyware and Ransom ware by Intercepting Kernel-Level System Routines*, IEEE, 6, 2018.

[6] K. Krombholz, *Advanced Social Engineering Attacks*, Preprint submitted to Journal of Information Security and Applications, Journal of Information Security and Applications, 2014, DOI: 10.1016/j.jisa.2014.09.005.

[7] Dr. G. Padmavathi and D. Shanmugapriya, *A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,* International Journal of Computer Science and Information Security, 4(1&2), 2009.

[8] PriceWaterhouseCoopers. Adjusting the Lens on Economic Crime; PriceWaterhouseCoopers (PWC): Auckland,New Zealand, 2016.

[9] S. Suman and Shubhangi, *A Survey On Comparison Of Secure Routing Protocols in Wireless Sensor Networks,* International Journal of Wireless Communications and Networking Technologies, 5(3), April - May 2016.

[10] US Department of the Treasury. Financial Services Sector-Specific Plan; US Department of the Treasury: New York, NY, USA, 2015.

[11] G. L. White, *Education and prevention relationships on security incidents for home computers,* J. Comput. Inf. Syst., 55(3), 2015, pp. 29-37.

[12] K. Xing, S. S. R. Srinivasan, M Rivera, J. Li and X. Cheng, *Attacks and Countermeasures in Sensor Networks: A Survey,* Network security, Springer, 2005.