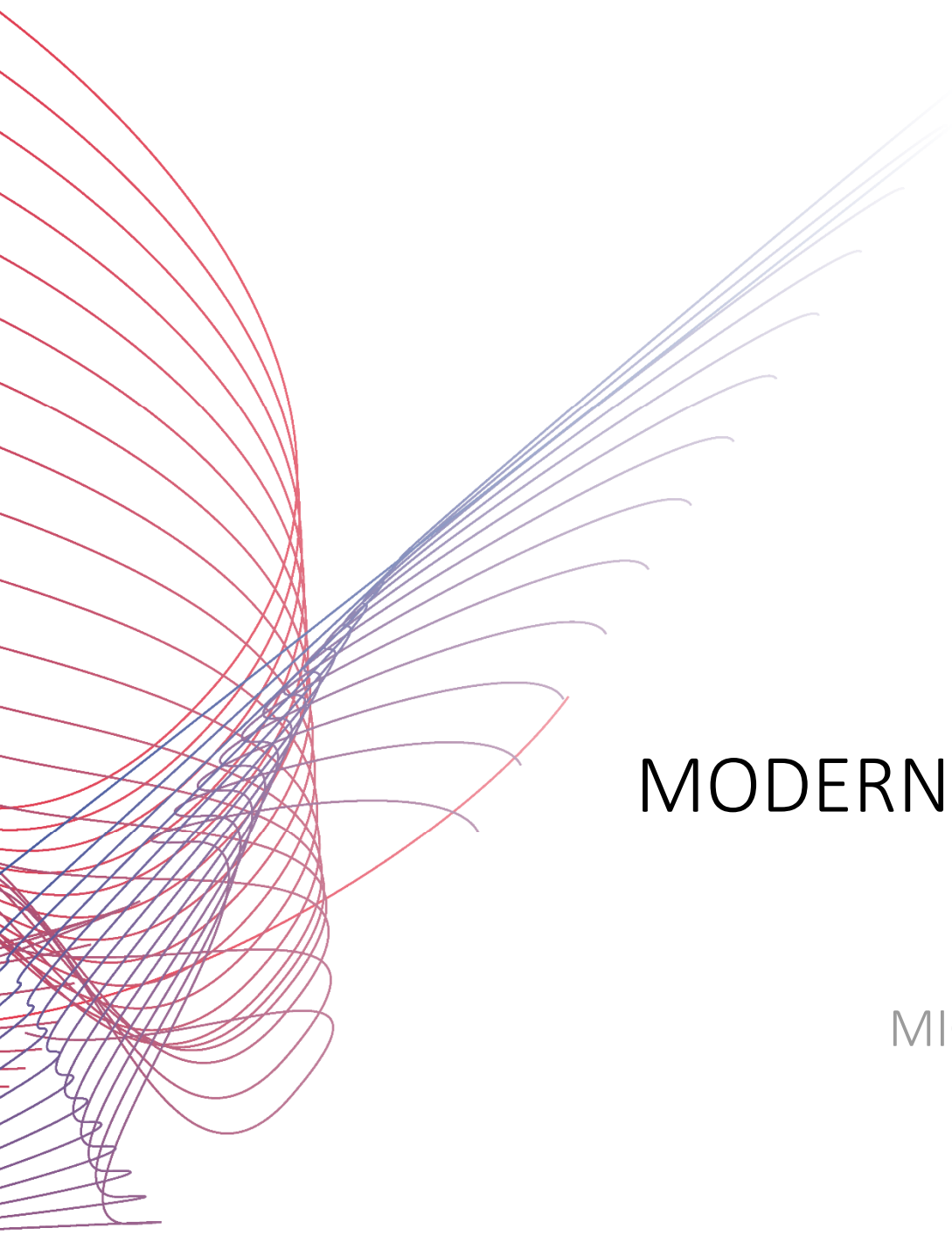
en
cs de
sk es

TECH
pedia



MODERN SECURITY SYSTEMS

MIGUEL SORIANO

Title: Modern security systems
Author: Miguel Soriano
Published by: Czech Technical University of Prague
Faculty of electrical engineering
Contact address: Technicka 2, Prague 6, Czech Republic
Phone Number: +420 224352084
Print: (only electronic form)
Number of pages: 42
Edition: 1st Edition, 2017

ISBN 978-80-01-06207-4

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Explanatory Notes

	Definition
	Interesting
	Note
	Example
	Summary
	Advantage
	Disadvantage

ANNOTATION

This module contains some necessary information for the basic orientation of students in the field of network security, including security services, security mechanisms, types of attackers, security threats and the description of the components of a network security system.

OBJECTIVES

This module provides an overview of the modern security systems. It is divided into six blocks or chapters.

The first chapter introduces the concepts of network security, security services, mechanisms, … The second one is an overview of network security threats introducing the concepts of viruses, worms, trojan horses; spyware and adware; zero-day attacks; denial of service attacks; data interception and theft; spoofing and identity theft …

The third chapter contains a description of some components of a network security system (anti-virus, firewalls, intrusion detection systems, VPN, …). The fourth chapter presents other network secure solutions (i.e., strong authentication methods, hardening the operating system, protecting web service, …)

Finally, there is a chapter devoted to mobile security. Smartphones play a very important role in modern communications; nobody doubts about the importance of smartphones in our lives. Because of the nature of these devices, they are open to new types of attack. In this chapter is shown how a hacker can profit from a compromised smartphone.

LITERATURE

[1] CVE. A dictionary of publicly known information security vulnerabilities and exposures. http://cve.mitre.org; 2015

[2] W. Cheswick and S. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 1994. ISBN

[3] E. D. Zwicky, S. Cooper, and D. B. Chapman. *Building Internet Firewalls.* O'Reilly and Associates, 2nd edition, 2000. ISBN.

[4] João Porto De Albuquerque , Paulo Lício De Geus "A Framework for Network Security System Design" .

[5] L. Bilge and T. Dumitraș, "Before we knew it: An empirical study of zero-day attacks in the real world," in ACM Conference on Computer and Communications Security, Raleigh, NC, 2012, pp. 833–844.

[6] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown Publishers, 2014. ISBN: 978-0-7704-3617-9

[7] Adeyinka, O., "Internet Attack Methods and Internet Security Technology,", 2008. AICMS 08. Second Asia International Conference on Modeling & Simulation pp.77-82, ISBN: 978-0-7695-3136-6

[8] Thomas W. Shinder The Best Damn Firewall Book Period (Second Edition), Syngress Publishing Inc. 2007. ISBN: 978-1-59749-218-8

[9] Karen Scarfone, Paul Hoffman. Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-41, Revision 1. Sept. 2009

[10] Eric Geier “Intro to Next Generation Firewalls” http://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html September, 2011

[11] Cliff, A.: “Password Crackers - Ensuring the Security of Your Password”, Security Focus, Feb. 19, 2001. http://online.securityfocus.com/infocus/1192

Index

1 Introduction

The world is becoming more interconnected with the advent of the Internet and new networking technology. Over the past few years, Internet-enabled business, or e-business, has drastically improved efficiency and revenue growth. However, as networks enable more and more applications and are available to more and more users, they become ever more vulnerable to a wider range of security threats. Therefore, to combat those threats and ensure that network transactions are not compromised, network security has become more important not only for business and the military, bur also for organizations and personal computer users.

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies. Many organizations try to classify vulnerability and their consequence: one the most famous vulnerability database is National Vulnerability Database from MITRE corporation [1].

The entire field of network security is vast and in an evolutionary stage; security incidents are rising at an alarming rate every year. Despite significant advances in the state of the art of network and computer security in recent years, systems more vulnerable than ever. Each major technological advance in computing raises new security threats that require new security solutions, and technology moves faster than the rate at which such solutions can be developed. As the complexity of the threats increases, so do the security measures required to protect networks.

1.1 What is network security

Network security refers to any activities designed to protect the network. Specifically, these activities protect the usability, reliability, integrity, and safety of the network and data. Network security has become a requirement for all communications including businesses, especially those that rely on the Internet.

The customers, vendors and business partners need the protection of all shared information, especially that information that is considered sensitive, such as credit card numbers or confidential business details.

Network security does not only concern the security in the computers at each end of the communication. When transmitting data, the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data and decrypt them and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

Network security is a prerequisite for the proper functioning of any business in the Internet. An important security requirement is to avoid denial of services; network downtime is costly to all types of businesses. Effective security allows a business to add new services and applications without disrupting the performance of the network. Safeguarding data is a necessary proactive approach to avoid interrupting customer services even when changes are being modified.

Some of the benefits that a business gets through secure networks are: customer trust (user privacy), mobility (secure access without introducing viruses or other threats), improved productivity (e.g., less time wasted on non-productive tasks such spam or dealing with viruses), and economy (network downtime is costly to all types of businesses).

1.2 What is network security system?

A network security system is a set of devices, either hardware of software-based, that uses secure protocols and cryptographic algorithms to protect the information and communication systems of a company

Some functions of these devices are to monitor and control incoming and outgoing network traffic, detection of attacks, data theft and network infrastructure protection including network bandwidth performance; service security and continuity defending against denial of service attacks, …

As the security needs of organizations get more complex, so do the network security systems and the traditional approaches, like firewalls, have to go through several changes to get adapted, being necessary the incorporation of distributed mechanisms to enforce security, decentralized trust management, and the widely spread use of cryptographic techniques (like IPSec and Virtual Private Networks).

Moreover, the network security system is just a small part (although an important one) of an organization's information security infrastructure and must be considered together with "several other fields, such as physical security, personnel security, operations security, communication security, and social mechanisms"

1.3 Security services

A security service is a service that ensures adequate security of the systems or of data transfers. Security services are implemented by security mechanisms according to security policies.

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles of information security. Later, other elements of information security were added to the three classic security attributes of the CIA triad. These elements are authentication, access control, non-repudiation, and privacy. Nevertheless, this classification is subject of debate among security professionals.

- Confidentiality refers to the protection of information from disclosure to unauthorized entities (organizations, people, machines, processes). No one may read the data except for the specific entity (or entities) intended. Information includes data contents, size, existence, communication characteristics, etc.

- Data integrity is the protection of data against creation, alteration, deletion, duplication or reordering by unauthorized entities (organizations, people, machines, processes). Integrity violation is always caused by active attacks. More specifically, integrity refers to the trustworthiness of information resources.

- Availability means having timely access to information. For example, a disk crash or denial-of-service attacks both cause a breach of availability. Any delay that exceeds the expected service levels for a system can be described as a breach of availability. An information system that is not available when you need it is at least as bad as none at all. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure.

- The authentication service is concerned with assuring that the communicating entities are provided with assurance and information of relevant identities of communicating partners (people, machines, processes). There are three separate categories of authentication factors typically, the knowledge, possession and inherence categories. Knowledge factors include things a user must know in order to log in. Possession factors include anything a user must have in his possession to log in. Inherence factors include any biological traits the user has that are confirmed for log in.

- Access control is the protection of information resources or services from access or use by unauthorized entities (organizations, people, machines, processes). That is to say, access control refers to the prevention of unauthorized use of a resource (i.e., this service controls who can have access to certain resources, under what conditions access can occur, and what those accessing the resources are allowed to do).

- Non-repudiation is the security service that uses these evidences to provide protection against denial by one of the entities involved in a communication of having participated in all or part of that communication.
- Data privacy is the security service that allows an individual to maintain the right to control what information about him is collected, how it is used and who uses it.

1.4 Security mechanisms

Security mechanism is a process that implements security services based on a hardware (technical), software (logical), physical or administrative approach. Security mechanisms support the security services and execute specific activities for the protection against attacks or attack results.

The security mechanisms are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service. Some of the security mechanisms are:

- Encipherment is a mechanism aimed at protecting a message's information content by using mathematical algorithms that transform data into a form that is not readable by unauthorized subjects.
- Digital signature is the mechanism that uses the cryptographic transformation of a data unit to prove the source and integrity of the data unit and protect against forgery.
- Access control overs a variety of mechanisms that enforce access rights to resources. This mechanism involves authorization to access some resources.
- Data integrity covers a variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- Authentication exchange is a mechanism intended to ensure the identity of an entity by means of information exchange.
- Traffic padding is a mechanism that inserts bits into gaps in a data stream to frustrate traffic analysis attempts.
- Routing control enables selection of particular physically secure routes for certain data and allows routing changes, especially when a security breach is suspected. This mechanism also involves perimeter security.
- Notarization is a mechanism that uses a trusted third party to assure certain properties of a data exchange.
- Perimeter security is a mechanism that allows accepting or denying data from or to a particular address or service located outside of the local network.

1.5 Classification of attackers

The security threats are potentially realized by attackers, which generally differ in their ability and activity. We will briefly summarize the properties pertaining to attackers' abilities and activities, and the resulting class scheme.

Ability: The ability of an attacker is typically determined by the following:

- Cost. It relates to the cost an attacker is required to spend in terms of equipment to carry out an attack successfully. This can range from extremely cheap, where only a soldering iron and some cables are required, to prohibitively high, where top-of-the-line semiconductor test equipment is needed.
- Skills. It generally relates to the skills and knowledge that an attacker has to possess for a successful attack. Some attacks might be carried out by a kid after proper instruction, while others might require extensive knowledge of the particular application of the network, or a person trained in the use of special equipment. (This property can also be modelled as cost.)
- Traces. This relates to the traces left behind by the attack. If after the attack the node is left in the same state as before the attack, including unaltered memory contents, then this is harder to notice than an attack, which causes physical destruction of the node.

Activity. Attacking activities can generally be classified as passive versus active:

- Passive Attacks. They extract information from the network merely by monitoring of communications. These attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.

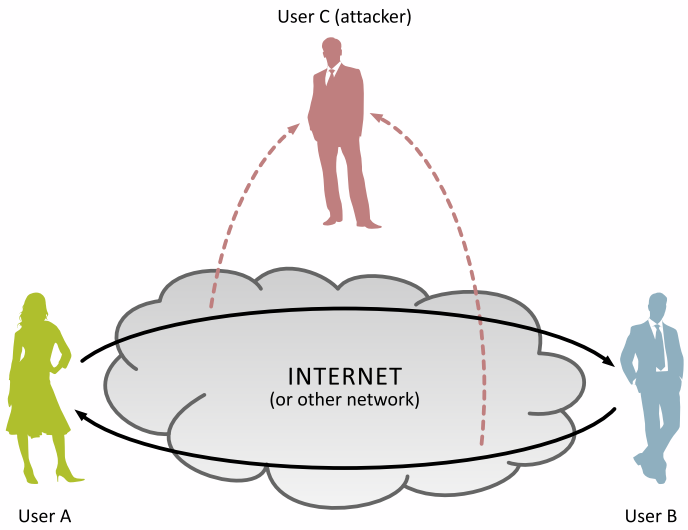


Fig. 1.1 – Passive attack

- Active Attacks. The objective of these attacks is to alter system resources (including data) or affect their operation. These attacks include the injection, modification or block of data network packets and the manipulation (tampering) of the any device that participate in the communication. Sometimes, passive attacks are preparatory activities for active attacks.

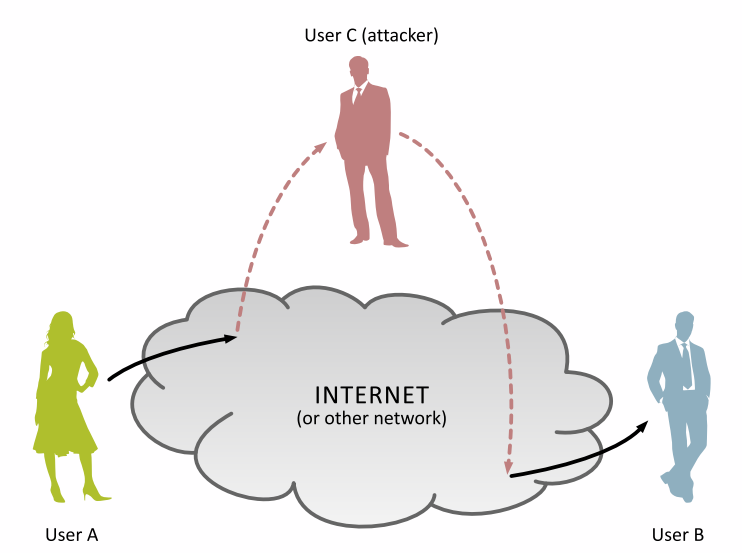


Fig. 1.2 – Active attack

And also as non-invasive versus semi-invasive versus invasive:

- Non-Invasive Attacks. They do not manipulate the device.
- Semi-Invasive Attacks. Tamper with package of the device but do not make direct electrical contact with the chip's surface.
- Invasive Attacks. They have practically no limits to the measures which can be taken to extract the information of the device (e.g. probing station).

Note that not all semi-invasive or invasive attacks are active attacks. For instance, passive semi-invasive attacks may try to just read sensitive data from memory components, and passive invasive attacks can use a probe station to sense valuable data signals. Examples of passive attacks are traffic analysis and camouflaging. The majority of attacks, however, are active attacks, such as routing attacks, spoofing, denial of service, man-in-the middle, eavesdropping, node replication, physical attacks...

Class. To grasp both ability and activity, IBM has introduced the following taxonomy on the class of attackers:

- Class I (clever outsiders). They are often very intelligent but may have insufficient knowledge of the system. They may have access to only moderately sophisticated equipment. They often try to take advantage of an existing weakness in the system, rather than try to create one.

- Class II (knowledgeable insiders). They have substantial specialized technical education and experience. They have varying degrees of understanding of parts of the system but potential access to most of it. They often have highly sophisticated tools and instruments for analysis.

- Class III (funded organizations). They are able to assemble teams of specialists with related and complementary skills backed by great funding resources. They are capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced analysis tools. They may use Class II adversaries as part of the attack team.

1.6 Terminology

It is not possible to provide a complete glossary of security-related terms within the scope of this chapter, but this section contains some of the more common words and phrases that the reader may encounter as she introduces into network and computer security:

- Attack. In the context of computer/network security, an attack is an attempt to access resources on a computer or a network without authorization, or to bypass security measures that are in place.

- Audit. To track security-related events, such as logging onto the system or network, accessing objects, or exercising user/group rights or privileges.

- Breach. Successfully defeating security measures to gain access to data or resources without authorization, or to make data or resources available to unauthorized persons, or to delete or alter computer files.

- Buffer. A holding area for data.

- Buffer overflow. A way to crash a system by putting more data into a buffer than the buffer is able to hold.

- Countermeasures. Steps taken to prevent or respond to an attack or malicious code.

- Cracker. A hacker who specializes in "cracking" or discovering system passwords to gain access to computer systems without authorization.

- Denial of Service attack. A deliberate action that keeps a computer or network from functioning as intended (for example, preventing users from being able to log onto the network).

- Exposure. A measure of the extent to which a network or individual computer is open to attack, based on its particular vulnerabilities, how well known it is to hackers, and the time duration during which intruders have the opportunity to attack.

- Hacker. A person who spends time learning the details of computer programming and operating systems, how to test the limits of their capabilities and identify vulnerabilities.

- Malicious code. A computer program or script that performs an action that intentionally damages a system or data, that performs another unauthorized purpose, or that provides unauthorized access to the system.

- Reliability. The probability of a computer system or network continuing to perform in a satisfactory manner for a specific time period under normal operating conditions.

- Risk. The probability that a specific security threat will be able to exploit a system vulnerability, resulting in damage, loss of data, or other undesired results. That is, a risk is the sum of the threat plus the vulnerability.

- Risk management. The process of identifying, controlling, and either minimizing or completely eliminating events that involve a threat to system reliability, data integrity, and data confidentiality.

- Sniffer. A program that captures data as it travels across a network. Also called a packet sniffer.

- Threat. A potential danger to data or systems. A threat agent can be a virus; a hacker;a natural phenomenon, such as a tornado; a disgruntled employee; a competitor, and other menaces.

- Trojan horse. A computer program that appears to perform a desirable function but contains hidden code that is intended to allow unauthorized collection, modification or destruction of data.

- Virus. A program that is introduced onto a system or network for the purpose of performing an unauthorized action (which can vary from popping up a harmless message to destroying all data on the hard disk).

- Vulnerability. A weakness in the hardware or software or even the security plan, that leaves a system or network open to threat of unauthorized access or damage or destruction of data.

- Worm. A program that replicates itself, spreading from one machine to another across a network.

2 Network security threats

Wherever there is a network, there are threats. The types of potential threats to network security are always evolving, and constant computer network system monitoring and security should be a priority for any network administrator. If the security of the network is compromised, there could be serious consequences, such as loss of privacy, and theft of information.

It is important to point out that not all the security threats are malicious. Non-malicious threats usually come from employees who are untrained in computers and are unaware of security threats and vulnerabilities. Errors and omissions can cause valuable data to be lost, damaged, or altered. Moreover, natural disasters are non-malicious threats. In this chapter, only malicious security threats are detailed.

Malicious threats consist of inside attacks by malicious employees and outside attacks by non-employees just looking to harm and disrupt an organization. The most dangerous attackers are usually insiders (or former insiders), because they know many of the codes and security measures that are already in place

Network attack tools and methods have evolved. Back in the days when a hacker had to have sophisticated computer, programming, and networking knowledge to make use of rudimentary tools and basic attacks. Nowadays, network hackers, methods and tools has improved tremendously, hackers no longer required the same level of sophisticated knowledge, people who previously would not have participated in computer crime are now able to do so.

The definition of "hacker" has changed over the years. A hacker was once thought of as any individual who enjoyed getting the most out of the system he or she was using. Now, however, the term hacker refers to people who either break in to systems for which they have no authorization or intentionally overstep their bounds on systems for which they do not have legitimate access. The correct term to use for someone who breaks in to systems is a "cracker." Common methods for gaining access to a system include password cracking, exploiting known security weaknesses, network spoofing, and social engineering.

There exists a “communication gap” between the developers of security technology and developers of networks. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. In contrast to network design, secure network design is not a well-developed process. There is not a methodology to manage the complexity of security requirements.

Many network security threats today are spread over the Internet. It is important to point out that smart mobile terminals have come to be an integral part of the Internet. A close inspection of the features of both smart mobile terminals and human behaviours can be used to define a protection scheme in this environment.

2.1 Malware: viruses, worms, trojan horses and zombies

Malicious software (malware) is software deliberately designed to infiltrate or damage a computer system without the owner's consent. It can cause losses or damages in the system. Computer viruses are a large class of malicious codes that can spread among computers and perform detrimental operations.

The execution of malware can cause the disruption of computer operations and can be also used to gather sensitive information or gain unauthorized access to computer systems. Malware is not the same as defective software, which is software that has a legitimate purpose but contains harmful bugs that were not noticed before release. In fact, computer viruses are actually a subset within the larger malware family, like other specimens such as worms, Trojan horses, adware, spyware, adware, rootkits, etc...

According to PandaLabs during 2014 more than 75 million of new malware samples were detected, representing the 34 % of all malware and also is more than twice higher than the amount recorded in the previous year, 30 million. Following, there is a definition of some of the most relevant types of malware:

- Viruses are self-replication programs that use files to infect and propagate. Once a file is opened, the virus will activate within the system.

- A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate. The primary purpose of the worm is to replicate. These programs were initially used for legitimate purposes in performing network management duties, but their ability to multiply quickly has been exploited by hackers to create malicious worms that may also exploit operating system weaknesses and perform other harmful actions. There are two main types of worms: mass mailing worms and network aware worms. Mass mailing worms use email as a means to infect other computers. Network aware worms select a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

- Trojans appear to be benign programs to the user, but in fact, performs actions that the user of the program did not intend or was not aware of. Basically, the Trojan can perform any action that the user has privileges and permissions to do on the system. This means a Trojan is especially dangerous if the unsuspecting user who installs it is an administrator and has access to the system files. A type of malware that typically propagates as a Trojan is ransomware. This kind of malware infects the computer system, restricts the access to this computer and demands that the user pays a ransom to the operators of the malware to remove the restriction.

- A zombie is malicious software that is propagated through the network. After its successful penetration into a computer system, the infected computer can be remotely controlled and administered. When several computers are infected by the same sort of malicious software, this is known as botnet. The botnet can be

controlled from one remote computer and force infected computers to carry out the same orders. This enables DDoS (Distributed Denial of Service) attack.

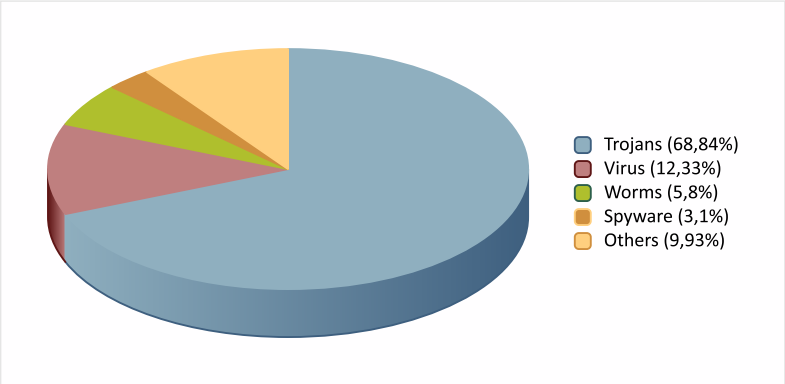


Fig. 2.1 – Types of new malware created during 2014

2.2 Spyware and adware

The term adware refers to software that displays advertisements and is given to the user embedded into another application.

Adware is considered a legitimate alternative offered to consumers who do not wish to pay for software. There are many ad-supported programs, games or utilities that are distributed as adware (or freeware). Today there is a growing number of software developers who offer their goods as "sponsored" freeware (adware) until the user pays to register.

In the case of legitimate adware, when the user stops running the software, the ads should disappear, and the user always has the option of disabling the ads by purchasing a registration key.

Spyware is a general term used to describe software installed via the Internet on a computer without the consent of the user that performs certain behaviours such as advertising, obtaining information about her browsing habits or changing the computer configuration.

The gathered information can be sent though Internet to a server somewhere, normally as a hidden side effect of using a program and it may be collected for different purposes. Typical tactics include delivery of unsolicited pop-up advertisements, theft of personal information (including passwords to online accounts or financial information such as credit card numbers), monitoring of Web-browsing activity for marketing purposes, and routing of HTTP requests to advertising sites

Spyware may be installed along with other software or as the result of a virus infection. In some infections, its presence is hidden from the user; sometimes are designed to be difficult not only to remove but also to detect. Other kinds of spyware make changes to the computer that can be annoying and can cause this computer slow down or crash.

Users frequently notice unwanted behaviour and degradation of system performance. A spyware infestation can create significant unwanted CPU activity, disk usage, and network traffic.

The anti-spyware programs can work by providing real-time protection or scanning on a regular schedule. In the first case, they scan all incoming network [https://en.wikipedia.org/wiki/Computer_network] data for spyware and block any threats in a manner similar to that of antivirus [https://en.wikipedia.org/wiki/Anti_virus] . In the second case they can be used solely for detection and removal of spyware software that has already been installed into the computer.

2.3 Zero-day vulnerability, zero-day attacks

There are a few common, but slightly different definitions of zero-day vulnerabilities. Some definitions refers this term as software flaws that leave users exposed to cyber attacks before a patch or workaround is available or made public, while others define them as a security vulnerability on the same day that the vulnerability becomes publicly known (zero-day). In the first definition, a zero-day vulnerability can be unknown to anyone but a cyber attacker (or a supplier who sells zero-day discoveries on the black market); some authors refer to the attacks to these vulnerabilities as 'less than zero-day'. In other cases, the software vendor knows about the vulnerability but has not yet issued a fix.

These attacks are rarely discovered; in fact, it often takes not just days, but months, and sometimes years before a developer learns of the vulnerability that led to an attack.

In either case, the result is the same: users are wide-open to attack. As L. Bilge and T. Dumitras state in [5] "While the vulnerability remains unknown, the software affected cannot be patched, and anti-virus products cannot detect the attack through signature-based scanning". Software vulnerabilities may be discovered by crackers, by security companies or researchers, by the software vendors themselves, or by users. If discovered by crackers, an exploit will be kept secret for as long as possible and will circulate only through the ranks of crackers/hackers, until software or security companies become aware of it or of the attacks targeting it.

Fig. 2.2 – Vulnerability period of a zero-day attack

Zero-day exploits have enabled some of the most destructive and high-profile attacks in recent years. For instance, operation Aurora (2009) exploited an Internet Explorer vulnerability with more than 20 targets including Morgan Stanley, Google, Yahoo, Dow Chemical, Adobe Systems, Juniper Networks and even a software for security company like Symantec.

Probably, the most famous zero day attacks was Stuxnet (2010). In fact, Stuxnet worm used four separate zero-day exploits to damage industrial controllers and disrupt Iran's Natanz uranium enrichment facility. Stuxnet was designed to manipulate industrial programmable logic controllers (PLCs) made by the German firm Siemens that control and monitor the speed of the centrifuges. The remote attackers could not reach directly these devices because the computers were not connected to the Internet. So the attackers designed their attack to spread via infected USB flash drives, and they first infect computers belonging to five outside

companies that are believed to be connected in some way to the nuclear program. The use of four zero-day vulnerabilities is extraordinary and is unique to this threat. Moreover, Stuxnet also uses a variety of other vulnerabilities which shows the extraordinary sophistication, thought, and planning that went into making this attack.

2.4 Scanning and Spoofing. Identity theft

In this context, the term scanner refers to a software program that is used by hackers to remotely determine possible vulnerabilities of a given system.

Administrators also use scanners to detect and correct vulnerabilities in their own systems before an intruder finds them. Many scanning programs are available as freeware on the Internet.

A good scanning program can locate a target computer on the Internet (one that is vulnerable to attack), determine what TCP/IP services are running on the machine, and probe those services for security weaknesses.

A spoofing attack is when a malicious party impersonates another device or user on a network.

There are several different types of spoofing attacks; including e-mail spoofing, IP address spoofing attacks, ARP spoofing attacks, DNS server spoofing attack.

E-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user. Most e-mail servers have security features to prevent sending messages from unauthorized users; nevertheless, it is possible to receive e-mail from an address that is not the actual address of the person sending the message.

In an IP address spoofing attack, an attacker sends IP packets from a false (or "spoofed") source address in order to disguise itself. IP spoofing consists in sending the address from a computer but using as a source address the one of a trusted computer.

There are many tools and practices that organizations can employ to reduce the threat of spoofing attacks. Common measures that organizations can take for spoofing attack prevention include packet filtering, the use of spoofing detection software and the use of cryptographic network protocols.

Denial of Service Attacks (DoS) and Distributed DoS (DDoS)

As it is detailed in [8], "Denial of Service attacks are one of the most popular choices of Internet hackers who want to disrupt a network's operations. Although they do not destroy or steal data as some other types of attacks do, the objective of the DOS attacker is to bring down the network, denying service to its legitimate users. DOS attacks are easy to initiate; software is readily available from hacker websites that will allow anyone to launch a DOS attack with little or no technical expertise".

In this kind of attacks, the system receives too many requests and it is not able to return communication with the requestors. The system then consumes resources

waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

Distributed DoS (DDoS) attacks use intermediary computers called agents (that are compromised systems), which are often infected with a Trojuse an. These systems constitute a botnet and are used to target a single system causing a DoS attack.

The difference with a classical DoS attack is due to the use of botnet in DDoS with many computers (can number in the hundreds or even thousands) and many Internet connections, often distributed globally in DDoS.

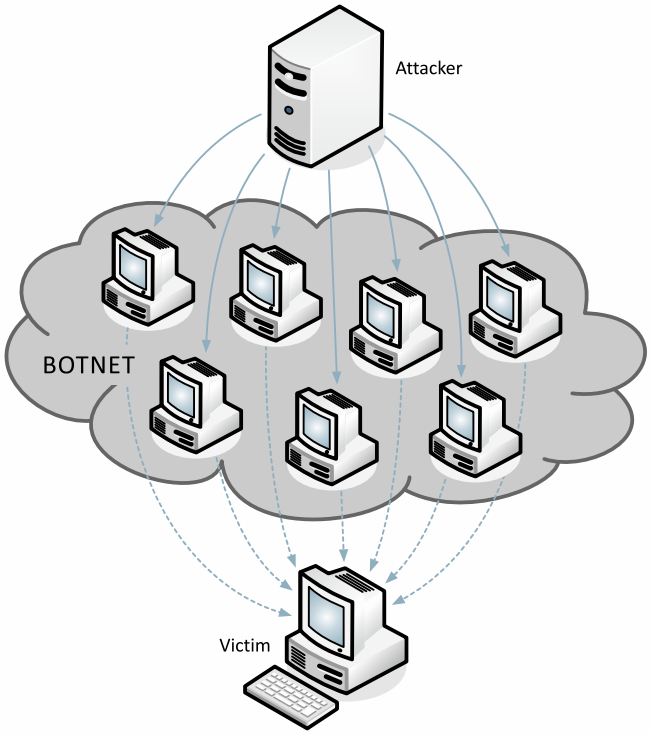


Figure 2.3. Scheme of a DDoS attack

The attacker activates remotely these Trojan programs, causing the intermediary computers to simultaneously launch the actual attack. This effectively makes it impossible to stop the attack simply by blocking a single IP address since the attack comes from computers, which may be on networks anywhere in the world. Moreover, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

It is important to note that DDOS attacks pose a two-layer threat. Not only could the network be the target of a DOS attack that crashes their servers and prevents incoming and outgoing traffic, but also their computers could be used as the "innocent middle men" to launch a DOS attack against another network or site.

DDoS attacks can be divided into volume-based attacks, protocol attacks and application layer attacks, according with the target of the attack. In the first case, the objective is to saturate the bandwidth of the network, in the second to consume server or intermediate communication equipment resources, and in the third case to crash the application server.

2.5 Social engineering attacks

Social engineering is defined as obtaining confidential information by means of human interaction.

The types of information that hackers are seeking can vary, but when individuals are targeted the hackers usually try to trick the victims in order to get their passwords, bank information, or access their computer to secretly install malicious software.

Unlike the other attack types, social engineering does not refer to a technological manipulation of computer hardware or software vulnerabilities and does not require much in the way of technical skills. Instead, this type of attack exploits human weaknesses – such as carelessness or the desire to be cooperative – to gain access to legitimate network credentials. The talents that are most useful to the intruder who relies on this technique are the so-called "people skills," such as a charming or persuasive personality or a commanding, authoritative presence.

Many security professional consider that the weakest link in the security chain is the human who accepts a person or scenario at face value. Some common social engineering attacks include email from a "friend" that contains a link or a file to download (with malicious software embedded), or asking for help; phishing attempts or baiting scenarios.

3 Components of a network security system

To lessen the vulnerability of the computer to the network there are many products available. Organizations have an extensive choice of technologies, ranging from anti-virus software packages to dedicated network security hardware, such as firewalls and intrusion detection systems, to provide protection for all areas of the network.

It is important to point out that no single solution protects a system from a variety of threats. A network security system usually consists of many components. Ideally, all components work together, and if one fails, others still stand, improving the security. These components can be hardware and/or software. The software must be constantly updated and managed to protect you from emerging threats.

Organizations today use combinations of firewalls, IDS, encryption, and authentication mechanisms to create “intranets” that are connected to the Internet but protected from it at the same time. Intranet is a private computer network that uses internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organization while extranets can generally be accessed by customers, suppliers, or other approved parties.

3.1 Anti-virus and anti-spyware

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-malware tools are used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worms, trojan horses, spyware and adware. Virus protection software is packaged with most computers and can counter most virus threats if the software is regularly updated and correctly maintained, otherwise it will fail to give protection against new viruses.

The anti-virus industry relies on a vast network of users to provide early warnings of new viruses, so that antidotes can be developed and distributed quickly. With thousands of new viruses being generated every month, it is essential that the virus database is kept up to date. The virus database is the record held by the anti-virus package that helps it to identify known viruses when they attempt to strike. Reputable antivirus software vendors will publish the latest antidotes on their Web sites, and the software can prompt users to periodically collect new data. Network security policy should stipulate that all computers on the network are kept up to date and, ideally, are all protected by the same anti-virus package —if only to keep maintenance and update costs to a minimum. It is also essential to update the software itself on a regular basis. Virus authors often make getting past the anti-virus packages their first priority.

No matter how useful antivirus software is, it can sometimes have drawbacks. Antivirus software can impair the performance of a computer. Inexperienced users may also have trouble understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach.

Eradicating a virus is the term used for cleaning out a computer. There are several methods of eradication: removing the code in the infected file which corresponds to the virus; removing the infected file or quarantining the infected file, which involves moving it to a location where it cannot be run.

A variety of strategies are typically employed.

Signature-based detection involves searching for known patterns of data within executable code. Viruses reproduce by infecting "host applications," meaning that they copy a portion of executable code into an existing program. So to ensure that they work as planned, viruses are programmed to not infect the same file multiple times. To do so, they include a series of bytes in the infected application to check if it has already been infected- this is called a virus signature. Antivirus programs rely on this signature, which is unique to each virus, in order to detect them. This method is called signature based detection, the oldest method used by antivirus software.

However, this method cannot detect viruses which have not been archived by the publishers of the antivirus software. Moreover, virus programmers have often given them camouflage features, making their signature hard to detect, if not undetectable. To counter such threats, heuristics detection approach can be used.

One type of heuristic approach, generic signatures, can identify new viruses or variants of existing viruses by looking for known malicious code, or slight variations of such code, in files. The heuristic method involves analysing the behaviour of applications in order to detect activity similar to that of a known virus.

This kind of antivirus program can therefore detect viruses even when the antivirus database has not been updated.

On the other hand, they are prone to triggering false alarms.

3.2 Firewall

A firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to prevent unauthorized access to or from a network by blocking traffic from the outside or from the inside of this network.

All data entering or leaving the network pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria. Firewalls can be implemented in both hardware and software, or a combination of both [8].

Firewalls enforce the security policies of an organization by restricting access to specific network resources. In the physical security analogy, a firewall is the equivalent to a door lock on a perimeter door or on a door to a room inside of the building—it permits only authorized users, such as those with a key or access card, to enter. Firewall technology is even available in versions suitable for home use. The firewall creates a protective layer between the network and the outside world. In effect, the firewall replicates the network at the point of entry so that it can receive and transmit authorized data without significant delay. However, it has built-in filters that can disallow unauthorized or potentially dangerous material from entering the real system. Moreover, firewalls provide an important logging and auditing function; often, they provide summaries to the network administrator about what type/volume of traffic has been processed through it, including attempted intrusion.

The National Institute of Standards and Technology (NIST) 800-41, [9] divides firewalls into three basic types: packet filters, stateful inspection and proxys. These three categories, however, are not mutually exclusive, as most modern firewalls have a mix of abilities that may place them in more than one of the three.

Packet filter firewalls are essentially routing devices that include access control functionality for system addresses and communication sessions; they can also filter network traffic based upon certain characteristics of that traffic. They are normally deployed within TCP/IP network infrastructures. Their main strengths are speed and flexibility and the most relevant weakness is their inability to prevent attacks that employ application-specific vulnerabilities (since they do not examine upper-layer data).

Table 1 shows a sample packet filter firewall rule set, adopted from [9]

	Source Address	**Source Port**	**Destination Address**	**Destination Port**	Action	**Description**
1	Any	Any	192.168.1.0	> 1023	Allow	Rule to allow return TCP Connections to internal subnet
2	192.168.1.1	Any	Any	Any	Deny	Prevent Firewall system itself from directly connecting to anything
3	Any	Any	192.168.1.1	Any	Deny	Prevent External users from directly accessing the Firewall system
4	192.168.1.0	Any	Any	Any	Allow	Internal users can access External servers
5	Any	Any	192.168.1.2	SMTP	Allow	Allow External users to send email in
6	Any	Any	192.168.1.3	HTTP	Allow	Allow External users to access WWW server
7	Any	Any	Any	Any	Deny	Everything not previously allowed is explicitly denied

Stateful inspection firewalls, also known dynamic packet filtering, is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. These firewalls analyse packets down to the application layer. By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture by examining certain values in the protocols headers to monitor the state of each connection over a period of time. Outgoing packets that request specific types of incoming packets are tracked and only those incoming packets constituting a proper response are allowed through the firewall. Each new packet is compared by the firewall to its state table to determine if the state of the packet contradicts its expected state. Traditional stateful inspection firewalls do not inspect the data payload of network packets and they do not have the fine-grained intelligence to distinguish one kind of Web traffic from another (legitimate applications and attacks).

Proxy firewalls, or application gateway firewalls, are a fairly recent addition to mainstream security environments. Proxy firewalls, on the other hand, combine stateful inspection technology with the ability to perform deep application inspections. This capability allows the analysis of protocols at the application layer such as HTTP and FTP and monitor traffic to compare the behaviour of benign protocol activity against observed events to identify deviations (possible signs of

attack). This allows a firewall to allow or deny access based on how an application is running over the network.

Next-Generation Firewall (NGFW) is an integrated network platform that combines a traditional firewall with other network device filtering functionalities such as a proxy firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS) and/or other techniques such as SSL and SSH interception, website filtering, QoS/bandwidth management, antivirus inspection and third-party integration (i.e. Active Directory) [10]. In fact, they are, basically, a form of a unified threat management (UTM) solution. The main drawback of NGFW is that usually NGFW tend to use separate internal engines to perform individual security functions; therefore, a packet may be examined several times by different engines to determine whether it should be allowed into the network. That round-robin approach adds latency, which may affect network performance.

3.3 Intrusion detection systems (IDS)

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions, by monitoring the network traffic, working with signature database and using heuristic analysis to identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block it. In the physical analogy, an IDS is equivalent to a video camera and motion sensor; detecting unauthorized or suspicious activity and working with automated response systems, such as watch guards, to stop the activity

An IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. The IDS evaluates a suspected intrusion once it has taken place and signals an alarm. Moreover, the IDS watches for attacks that originate from within a system

IDS uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network. Intrusion detection functions include monitoring and analysis of both user and system activities, analysis of system configurations and vulnerabilities, assessing system and file integrity, analysis of abnormal activity patterns and tracking user policy violations. There are several ways to categorize an IDS:

- Misuse detection vs. Anomaly detection
    - Misuse detection: the IDS analyses the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. The intrusion detection technique based on attack signature consists in looking for “signatures” (a typical character sequence of an attack) in all communications going through the network. It can detect application level attacks, even if they conform to inter-application protocol standards; as such, it complements inter-application protocol decoding. Like a virus detection system, misusedetection software is only as good as the database of attack signatures that it uses to compare packets against, so it implies the maintaining and updating of the attack signatures database; the frequent update of this database on equipment using this technology is of utmost importance for the relevance of this technique.
    - Anomaly detection: the system administrator defines the baseline or normal state of the network’s traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

- Network-based vs. Host-based systems
    - Network-based system, or NIDS: the individual packets flowing through a network are analysed. The NIDS can detect malicious packets designed to be overlooked by a firewall's simplistic filtering rules.
    - Host-based system, or HIDS: the IDS examine all the activity on each individual computer or host.

3.4 Virtual Private Network (VPN)

VPN stands for "Virtual Private Network". A Virtual Private Network (VPN) is a network technology that makes it possible to use a public network such as the Internet for private communication by creating a secure (encrypted) network connection.

VPNs are often used to enable remote users to securely connect to a private network, and in this way, to extend intranets worldwide. In other words, a VPN enables sending data between two computers using the routing infrastructure provided by a shared or public internetwork (such as the Internet) in a manner that emulates the properties of a point-to-point private link. The secure connection appears to the user as a private network communication, despite the fact that this communication occurs over a public internetwork, hence the name virtual private network.

There are several motivations for building VPNs, but a common thread is that they all share the requirement to "virtualize" some portion of an organization's communications—in other words, make some portion (or perhaps all) the communications essentially "invisible" to external observers, while taking advantage of the efficiencies of a common communications infrastructure. The common uses of VPNs are: secure remote access to corporate resources over Internet and connecting networks over Internet. A VPN solution should provide the following security services:

- User authentication. The VPN restricts access to authorized users only; therefore their identity must be verified. Moreover, the VPN should provide audit records.
- Data encryption. The data that is exchanged over the public network must be unreadable to unauthorized users.
- Key management. Prior to data encipherment, it is required that users set up the details of the cryptography (algorithms, keys, …)

4 Network Secure solutions

A network is only as secure as its weakest link. In addition to using the components described in the previous section, detailed below a set of actions that users and / or network administrators should implement in order to enhance system security

4.1 Use of secure authentication methods

Several organizations require the use of "strong authentication methods" especially in online transactions that include payment service. There are several definitions of strong authentication. Some authors refer to it as the authentication method with multi-factor authentication that requires the use of solutions from two or more of the three categories of factors (knowledge, possession and inherence), already explained in the section 1.3. Other authors (A. J. Menezes, P. C. van Oorschot and S. A. Vanstone) consider in [11] that strong authentication methods require a cryptographic challenge response protocol … In any case, a strong authentication protocol could not be accomplished with the transmission of passwords.

It is important to know that the reliability of authentication is affected not only the number of factors involved but also how they are implemented. In each category, the choices made for authentication rules greatly affect the security of each factor. Poor or absent password rules, for example, can result in the creation of passwords like "guest," which completely defeats the value of using a password. Best practices include requiring inherently strong passwords that are updated regularly. Lax rules and implementations result in weaker security; alternatively, better rules can yield better security per factor and better security overall for multifactor authentication systems.

In the case of using passwords, it is essential creating a good quality password policy to prevent password guessing and cracking. The advent of password crackers has made it so much easier for hackers to "guess" passwords. There are also numerous password cracking tools available that any average person can use Unfortunately the average user is more inclined to make the password easy to remember than difficult to guess.

Password cracking is the process of figuring out or breaking passwords in order to gain unauthorized entrance to a system or account. Passwords can be cracked in a variety of different ways. The most simple is the use of a word list or dictionary program to break the password by brute force. These programs compare lists of words or character combination against password until they find a match. Therefore, it is obvious that passwords should not be dictionary words, proper nouns or foreign words.

Password crackers can be used to ensure that users are implementing secure passwords. Systems administrators can use them to test the strength of user's passwords. The system administrator can then notify users whose passwords are insecure.

Another way that intruders can use to discover passwords is through social engineering. Many users create passwords that contain personal information and therefore, they can be guessed by learning a minimal amount of information about them. So, passwords should not contain personal information.

Many users store the different passwords they use in computer files. If so, in order to mitigate the impact of password sniffing, it is necessary to encrypt these files. In

fact, this recommendation is useful not only for password files, but also for all files that contains sensitive information.

4.2 Hardening the operating system

Hardening of the OS is the act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services.

Hardening the operating system means making it more secure. This is typically done by removing all non-essential software programs and utilities from the computer, applying the latest patches, deleting unused files, locking down user accounts. While these non-essential programs may offer useful features to the user, if they provide "back-door" access to the system, they must be removed during system hardening.

Although they are important; removing applications, disabling services, patching, hotfixing, and installing service packs are not the only ways to harden an operating system. Administrative privileges should be used sparingly, and policies should be in place to enforce the rules of the organization.

There are hardening checklists available for popular operating systems that administrators can follow. While both Macintosh and Windows operating systems can be hardened, system hardening is more often done on Windows machines, since they are more likely to have their security compromised.

4.3 Physical Security

Ensuring a physically secure network environment is the first step in controlling access to the sensitive data and system files, but it is only part of a good security plan. This is truer today than in the past, because networks have more “ways in” than they once did. A medium or large network may have several access points, VPN servers, and a dedicated full-time Internet connection. Even a small network is likely to be connected to the Internet part of the time.

Virtual intruders never touch the computers or the target network. They can access the network from across the street or from halfway across the world. But they can do as much damage as the thief who breaks into the company headquarters to steal or destroy the data – and they are much harder to catch. To make a physical access control the “outer perimeter” means:

a) Controlling physical access to the servers

b) Controlling physical access to networked workstations

c) Controlling physical access to network devices

d) Controlling physical access to the cable

e) Being aware of security considerations with wireless media

f) Being aware of security considerations related to portable computers

g) Recognizing the security risk of allowing data to be printed out

h) Recognizing the security risks involving pen drives, external disks, CDs and other removable media

5 Mobile security

Mobile devices are rapidly replacing or complementing the personal computer at home and in the workplace. The rapid growth in smartphone and tablet usage over the past two years has led to the inevitable rise in targeting of these devices by cybercriminals. Moreover, some unregulated app markets increase the problems related with malware in these devices. Mobile malware writers know the best way to infect as many devices as possible is to attack central app markets.

There are many different ways that a hacker can profit from a compromised mobile device. Some of these, such as ransomware, botnet activity and data theft, have migrated from the traditional PC. Nevertheless, they are also open to new types of attack due to the nature of mobile devices. And, their very portability makes them vulnerable to being physically lost and the potential data loss as a result if the device is not encrypted or properly secured.

The continuing adoption of emerging apps for personal and business communication widens the attack surface, particularly for social engineering scams and data exfiltration attempts. The address book and social connections graph is a treasure for cyber-crooks of all sorts. Mobile and web applications control for business users will help mitigate this risk.

Today, the evolution of mobile banking poses a potentially even greater risk for users. Powerful mobile devices are already being actively targeted by malware designed to steal data and money since they make it easy for users to conduct financial transactions on the move. Therefore, protecting the smartphone from malware and keyloggers has to be a basic principle of secure mobile banking.

Security experts have been banging the drum about the threat of mobile malware for years. The fact that it has not yet materialized in a major attack has eroded the credibility of the claims, though, which means many users do not take it seriously and have let their guard down. The sheer volume of mobile devices, and the prevalence of new mobile malware threats only increase the likelihood that a major mobile malware attack will happen.

Kaspersky's Bermingham said, "As consumers and businesses shift to using mobile devices for a greater percentage of their daily activities, cybercriminals will place a larger emphasis on targeting these platforms—specifically Android and jail-broken IOS devices"