COMPUTER SECURITY

3rd Year Computer Science

Chapiter 1 :

Introduction to Security

Introduction

- An information system is an organization of activities consisting of acquiring, storing, processing, and distributing information. One of the technical means of operating an information system is the use of computer systems.
- guaranteeing information security therefore implies guaranteeing the security of computer systems.
- The problem of protecting information on computers has become even more critical and difficult since the adoption of the Internet. The Internet has become the primary route for unauthorized users to penetrate systems and perform malicious actions.
- It is therefore essential to know the system resources to be protected and to implement protection mechanisms.

1. Definitions

1. Information Security

This includes all the technical, organizational, legal, and human resources implemented to minimize a system's vulnerability to accidental or intentional threats.

2. Safety and Security

Information security covers two areas:

"Safety": protecting computer systems against accidents caused by the environment and system malfunctions.

"Security": protecting computer systems against intentional malicious actions.

2. Key concepts of computer security

- **Vulnerability:** A vulnerability (sometimes called a flaw or breach) is a point where a system is susceptible to a malicious attack. It is a security weakness, either logical or physical, that can be exploited to cause loss or damage.

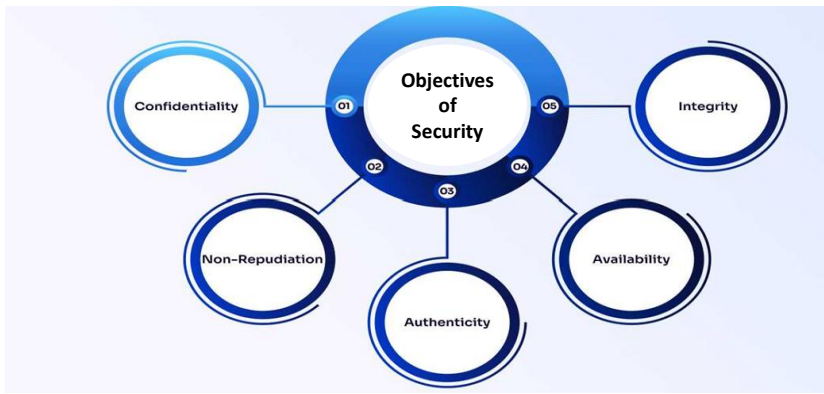
- **Threat:** A threat represents the type of malicious action that can harm a system by exploiting its security vulnerabilities (weaknesses). A threat is a potential danger to the system.

- **Attack :** An attack is a deliberate attempt to violate one or more security properties.
- **Contrmeasure :** An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
- **Risk :** An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

3. Objectives of Computer Security

The objectives (properties, requirements, services, etc.) of information security define what users of computer systems expect in terms of security.

Five main objectives to guarantee:



1. Confidentiality

This is the property that ensures only authorized users, under predefined conditions, have access to information. In other words, it keeps information secret except from the people for whom it is intended. One way to guarantee data confidentiality is through data encryption and cryptography.

2. Authentificity

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Among the means used to guarantee authentication are login/password, digital certificates, etc.

3. Integrity

This property ensures that data is not corrupted or modified in an unauthorized manner. One way to ensure integrity is through the use of digital signature.

4. Availability

This property ensures that the data or services of a system are accessible when needed by authorized users.

5. Non-repudiation

This property ensures that the perpetrator of an act cannot later deny having done it; They take responsibility for it. For example, preventing the sender or receiver from denying the transmission or receipt of a message.

4. Threat classification

Before you can implement a security solution, you must first start by knowing the different dangers and their motivations in order to plan how to protect them and limit the risks.

The different threats that exist can be classified according to several classes:

- **Threat source**
- **Threat agents**
- **Threat motivation**
- **Threat intention**
- **Threats impacts**

4.1 Threat Source Classification

The origin of threat either internal or external.

4.1.1 Internal threats

Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. A threat can be internal to the organization as the result of employee action or failure of an organization process.

4.1.2 External threats

External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. The most obvious external threats to computer systems and the resident data are natural disasters: hurricanes, fires, floods and earthquakes. External attacks occur through connected networks, physical intrusion, or a partner network.

4.2 Threat agents Classification

The threat agent is the actor that imposes the threat to the system.

4.2.1. Human Threats

This class includes threats caused by human actions such as insiders or hackers which cause harm or risk in systems.

4.2.2 Environmental threats

It comes, first, from natural disaster threats like earthquakes, flood or fire and, also, due to animals and wildlife which cause severe damage to information systems . Indeed, this class includes other threats such as riots and wars.

4.2.3 Technological Threats

Technological threats are caused by physical and chemical processes on material.

4.3 Threat motivation Classification

Attackers normally have a specific goal or motive for an attack on a system. These goals can cause malicious or non malicious results.

4.3.1. Malicious threats

consist of inside or outside attacks caused by employees or non-employees to harm and disrupt an organization like viruses, Trojan horses, or worms.

4.3.2 Non-malicious threats

Non-malicious attacks occur due to poor security policies and controls that allow vulnerabilities and errors to take place. It is caused by ignorant employees with the aim not to harm the system.

4.4 Threat intent Classification

Threat intent represents the intent of the human who caused the threat:

4.4.1. Intentional Threats

It represents threats that are result of a harmful decision. For example computer crimes, or when someone purposely damages property or information. Computer crimes include espionage, identity theft and credit card crime.

4.4.2 Unintentional Threats

It represents threats that are introduced without awareness. These threats basically include the unauthorized or accidental modification of software. Accidental error includes corruption of data caused by programming error, user or operator error.

4.5 Threat impacts Classification

A security threat can cause one or several damaging impacts to systems, we divide them into seven types:

- **Destruction of information,**
- **Corruption of information,**
- **Theft or loss of information,**
- **Disclosure of information,**
- **denial of use,**
- **Elevation of privilege,**
- **Illegal usage.**

5. The different types of attacks

Cyberattacks encompass various intentional cyber threats. These attacks can be grouped into four categories: malware, email attacks, exploits and intrusions, and web attacks.

5.1. Malware

5.2. Email Attacks

5.3. Exploits and Intrusions

5.4. Web Attacks

5. The different types of attacks

5.1. Malware

- **Virus**

A malicious program that attaches itself to a legitimate program or file and spreads from one computer to another when the infected program is executed. Viruses require user action to propagate and can damage files, corrupt data, or consume system resources.

- **Worm**

A self-replicating malware that spreads independently across networks without requiring user intervention or a host program. Worms exploit network vulnerabilities and can consume bandwidth, overload servers, and spread rapidly across the internet.

5. The different types of attacks

➢ Trojan Horse

Malicious software disguised as legitimate programs that users are tricked into installing. Unlike viruses, Trojans don't self-replicate but provide attackers with backdoor access, steal data, or perform other malicious activities. Examples include remote access Trojans (RATs) and banking Trojans.

➢ Spyware

Software that secretly monitors and collects user information without their knowledge. Spyware can track browsing habits, capture keystrokes (keyloggers), steal credentials, and transmit sensitive data to attackers. It often comes bundled with free software or is installed through malicious websites.

5. The different types of attacks

➢ Spyware

Spyware is a spy program responsible for collecting information about the user of the computer in which it is installed. It generally installs at the same time as other software (most often freeware or shareware, often legal mentioned in the license).

Spyware records all the activity of the infected computer and transmits it to someone else. It allows tracking URLs of visited sites, tracking keywords entered in search engines, analyzing purchases made via the internet, even banking payment information, ...

➢ Sniffer

A sniffer is a particular type of spyware that allows listening to and retrieving data circulating on the network (passwords, bank cards, ...).

5. The different types of attacks

➢ Keylogger

A keylogger (keystroke recorder) is a spy program responsible for recording keyboard keystrokes and saving them, without the user's knowledge.

➢ Ransomware

It is malicious software that takes personal data hostage. To do this, it encrypts personal data then asks the victim to send money in exchange for the decryption key. It can also block access to the machine until the user pays a sum of money.

➢ Adware

It is a free program funded by advertisements that appear in independent windows or in a toolbar on the computer or in the browser.
Most adware is annoying but safe. However, some are used to collect personal information, websites visited, ...

5. The different types of attacks

5.2. Email Attacks

➢ Spam

Spam (junk mail, unsolicited mail) is the mass sending of electronic mail to recipients who have not requested it.

Spammers generally collect email addresses on the internet (in forums, on websites, in discussion groups, ...).

➢ Phishing

Phishing is a fraudulent technique used by hackers to retrieve information (generally banking) from users.

Users receive an email that appears to come from a trusted company, typically a bank or a commerce site (exact copy of the original site).

5. The different types of attacks

➢ Hoax

A hoax is an electronic email spreading false information and pushing the recipient to spread the false news to all their friends or colleagues. In appearance, hoaxes are not harmful but they can have other consequences such as network congestion, the spread of false rumors and the cluttering of electronic mailboxes with the massive distribution of emails.

5. The different types of attacks

5.3. Exploits and Intrusions

➢ Backdoor

A backdoor represents a secret functionality of software allowing monitoring or taking control of a computer. It is due to an accidental or intentional design flaw (generally Trojan horse). For example, a backdoor could be a flaw in the MySQL DBMS that allows connection as administrator.

➢ Intrusion

An intrusion represents a technique that allows infiltrating a computer system or network in order to carry out an attack. It can be carried out using malicious software or messaging tools.

5. The different types of attacks

➢ Exploit

An exploit is a program allowing an attacker to exploit a computer security flaw. We distinguish two types of exploit (Remote Exploit and Local Exploit).

➢ Rootkit

A rootkit is a set of programs allowing the installation of malicious software on a system and making them difficult to detect.

A rootkit provides administrator access to a computer without the user's knowledge by exploiting a backdoor.

5. The different types of attacks

5.4. Web Attacks

➢ 5.4.1. Cookies

A cookie is a text file placed on the local hard drive by a Web server. It contains identification information, and cannot be executed as a program, nor spread viruses.

In itself, a cookie cannot harm a computer, as it does not contain and cannot contain code. However, a cookie can contribute to malicious actions occurring on the system on which it is hosted. Being a simple text file, it is also vulnerable and can be read by other applications.

5. The different types of attacks

➢ Code Injection

Code injection consists of injecting code to divert the normal use of a program in order to execute arbitrary code or command. It can take multiple forms:

- **XSS Injection (Cross Site Scripting)**
- **SQL Injection**
- **LDAP Injection**
- **Xpath Injection**

6. Attack Techniques

Several attack techniques exist, we will focus in what follows on the main computer techniques:

➢ 6.1. Password Attacks

A password attack consists of trying to find the password allowing access to an account, system or program, ...

➢ 6.2. Denial of Service Attacks

A denial of service attack (DoS) is a type of attack aimed at making services or computer resources unavailable for an indefinite time. In general, DoS attacks are against servers, so that they cannot be used and consulted.

6. Attack Techniques

➢ 6.3. Identity Spoofing Attacks

Identity spoofing is a technique that consists of impersonating an entity that one is not (protocol, application, website, ...). It can take various forms that are difficult to detect. In general, the attacker no longer tries to directly deceive the user but rather the software and automated procedures of the operating system.

Identity spoofing techniques are:

- **IP address spoofing (IP spoofing)**
- **DNS hijacking (DNS spoofing)**
- **ARP Spoofing**

6. Attack Techniques

➢ 6.4. Man-in-the-Middle Attacks

The man-in-the-middle attack (or interceptor attack), sometimes noted MITM, is an attack technique in which a hacker listens to communication between two interlocutors and falsifies exchanges in order to impersonate one of the parties.

Most "man in the middle" attacks consist of listening to the network using a sniffer.

➢ 6.5. Buffer Overflow Attacks

Buffer overflow is a technique that consists of executing arbitrary code by a program by sending it more data than it is supposed to receive.

6. Attack Techniques

➢ 6.6. XSS Injection Attacks

An XSS (Cross Site Scripting) injection attack is a code injection attack executed on the client side of a web application.

➢ 6.7. Hardware Flaw Attacks

Hardware flaws are rare but they can prove very dangerous. This type of attack consists of exploiting vulnerabilities of various equipment and hardware peripherals such as: routers, servers, Bluetooth, wireless equipment (Wi-Fi), processors (virtualization technique flaws), fingerprint readers and facial recognition...

6. Attack Techniques

➢ 6.8. Social Engineering Attacks

Social engineering sometimes makes it possible to compensate for the absence of a flaw and extract information from the user of a computer without them being aware of opening their PC to an unwanted person.

7. Defense Methods

Antivirus Software

Firewalls

Encryption

Virtual Private Networks (VPN)

Intrusion Detection and Prevention Systems (IDS/IPS))

7. Defense Methods

➢ 7.1. Antivirus

Antiviruses are software designed to identify, neutralize and eliminate malicious software (e.g. computer viruses).

Antivirus software checks files and electronic mail, boot sectors (to detect boot viruses), but also the computer's RAM, removable media (USB keys, CDs, DVDs, etc.), data transiting on possible networks (including internet), etc.

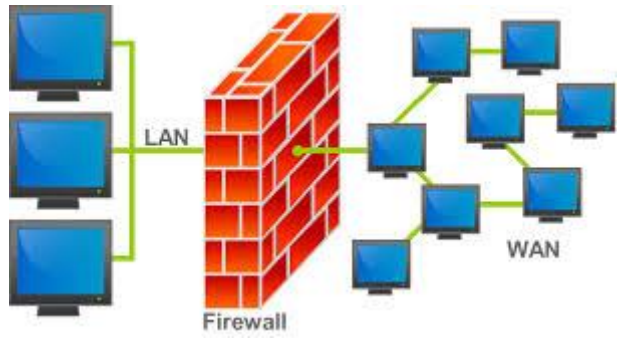
Among the methods used:

- **The main antiviruses focus on files and then compare the virus signature to the codes to be verified. The signature database must therefore be very regularly updated on the publisher's site.**
- **Another approach to locating viruses consists of detecting suspicious behaviors of programs. For example, if a program attempts to write data to an executed program or modify/delete system files, the antivirus will detect this suspicious behavior and notify the user who will choose the measures to follow.**

7. Defense Methods

➢ 7.2. Firewall

A firewall is a physical (hardware) or logical (software) system serving as an interface between one or more networks in order to control and possibly block the circulation of data packets, by analyzing information contained in layers 3, 4 and 7 of the OSI model.



7.2. Firewall

It is therefore a machine (specific machine in the case of a hardware firewall or a secured computer hosting a particular firewall application) comprising at minimum two network interfaces:

- **An interface for the network to be protected (internal network).**
- **An interface for the external network.**

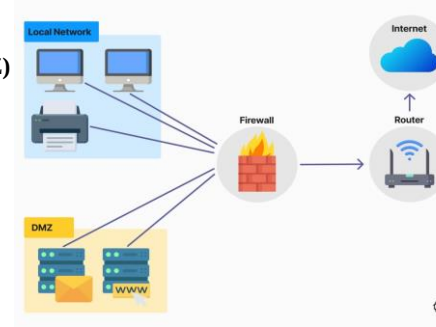
The firewall thus generally represents in companies a device at the network entrance . It acts as a protective barrier between a trusted internal network and untrusted external networks such as the Internet. It uses predefined security rules to allow or block traffic.

7.2. Firewall

Demilitarized Zone (DMZ)

When certain machines on the internal network need to be accessible from outside (for example for a web server, a messaging server, etc.) it is often necessary to create a new interface to a separate network, accessible both from the internal network and from outside, without however risking compromising the company's security.

We thus speak of a demilitarized zone (DMZ) to designate this isolated zone hosting applications made available to the public.



7.2. Firewall

Firewall System Operation

A firewall system contains a set of predefined rules allowing:

- To authorize the connection (allow).
- To block the connection (deny).
- To reject the connection request without notifying the sender (drop).

All these rules allow implementing a filtering method depending on the security policy adopted by the entity.

We usually distinguish two types of security policies allowing:

- Either to authorize only communications that have been explicitly authorized.
- Or to prevent exchanges that have been explicitly prohibited.

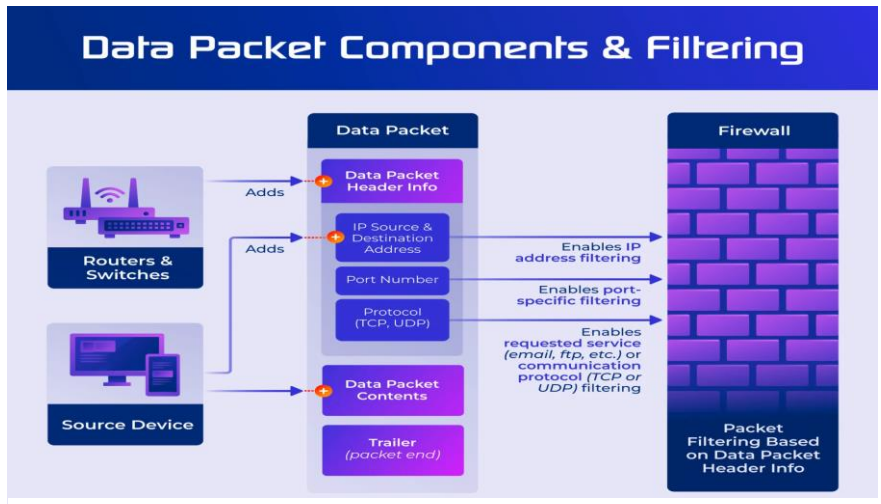
Types of Firewalls

1.Packet filtering firewalls

Also known as stateless filtering firewalls, This is the most basic and oldest type of firewall. It operates at the Network Layer (Layer 3) of the OSI model. It inspects packets individually and makes decisions based on the:

- **IP address of the sending machine.**
- **IP address of the receiving machine.**
- **Protocol (TCP, UDP, etc.).**
- **Port numbers (source port and destination port).**

Types of Firewalls



Types of Firewalls

Example of firewall rules:

#	Src IP	Dst IP	Src Port	Dst Port	Protocol	Action
1	Any	172.16.10.5	Any	80	TCP	ALLOW
2	172.16.10.5	Any	80	Any	TCP	ALLOW
3	Any	172.16.10.5	Any	443	TCP	ALLOW
4	172.16.10.5	Any	443	Any	TCP	ALLOW
5	Any	172.16.10.6	Any	53	UDP	ALLOW
6	172.16.10.6	Any	53	Any	UDP	ALLOW
7	10.0.0.0/8	Any	Any	80	TCP	ALLOW
8	10.0.0.0/8	Any	Any	443	TCP	ALLOW
9	10.0.0.0/8	172.16.10.7	Any	25	TCP	ALLOW
10	10.0.1.100	172.16.10.8	Any	22	TCP	ALLOW
11	172.16.10.0/24	10.0.0.0/8	Any	Any	Any	DENY
12	Any	10.0.0.0/8	Any	Any	Any	DENY
13	Any	Any	Any	Any	Any	DENY

Types of Firewalls

2. Stateful inspection firewalls

Stateful inspection firewalls monitor the state of active connections and use this information to determine if they should block or allow packets. They offer more in-depth security than packet filtering and circuit-level firewalls, as they can examine the entire data packet, including the payload.

Types of Firewalls

3. Application-level gateways

Also known as proxy firewalls, application-level gateways act as intermediaries between clients and servers. They inspect data packets at the application layer, ensuring they adhere to specific protocols and are free of malicious content. This type of firewall provides strong security but can be resource-intensive.

Types of Firewalls

4. Next-generation firewalls (NGFWs)

Next-generation firewalls (NGFWs) combine traditional firewall functions with advanced features like deep packet inspection, intrusion prevention system (IPS), and application awareness. They offer comprehensive security but might require more resources and management compared to simpler firewalls. NGFWs are often suited to large organizations that need to protect large volumes of data transfer.

7. Defense Methods

7.3. Encryption

Encryption is a cryptography process by which one wishes to make the understanding of a document impossible to anyone who does not have the decryption key.

Although encryption can make the meaning of a document secret, other cryptographic techniques are necessary to communicate securely.

Cryptology is essentially based on arithmetic: In the case of text, it involves transforming the letters that make up the message into a succession of numbers (in the form of bits in the case of computing), then doing calculations on these numbers to:

- **On one hand modify them in such a way as to make them incomprehensible.**
- **Ensure that the recipient will know how to decipher them.**

7. Defense Methods

7.4. Virtual Private Networks (VPN)

In computer networks, the virtual private network (VPN) is a technique allowing remote stations to communicate securely, while using public infrastructures (internet).

A VPN is based on a protocol, called tunneling protocol, that is to say a protocol allowing data passing from one end of the VPN to the other to be secured by cryptography algorithms

7. Defense Methods

7.5. Intrusion Detection System (IDS)

Even if the intruder manages to cross the protection barriers (firewall, authentication system, etc.), it is still possible to stop them before they attack. Intrusion detection tools detect any abnormal behavior or suspicious traffic.

An IDS (Intrusion Detection System) is a computer system, generally composed of software and possibly hardware, whose role is intrusion detection.

It is a mechanism listening to network traffic in a stealthy manner in order to spot abnormal or suspicious activities and thus allowing preventive action on intrusion risks.

There are two large distinct families of IDS: N-IDS and H-IDS.

7. Defense Methods

7.6. Intrusion Prevention System(IPS)

The IPS is an Intrusion Prevention/Protection System and no longer just recognition and signaling of intrusions as most IDS are. The main difference between an IDS (network) and an IPS (network) is mainly in 2 characteristics:

The positioning in cutoff on the IPS network and no longer just listening on the network for the IDS (traditionally positioned as a sniffer on the network).

The possibility to immediately block intrusions regardless of the type of transport protocol used and without reconfiguration of third-party equipment, which implies that the IPS is natively constituted of a packet filtering technique and blocking means (drop connection, drop offending packets, block intruder, ...).