University Mohamed Khider of Biskra

Computer Science Department

CYBER SECURITY COURSES

LEVEL: 3RD YEAR, BACHELOR'S DEGREE

Lecturer : Dr. Somia Sahraoui

Outline

1. Introduction and generalities
2. Introduction to cryptography
3. Public key infrastructure

Introduction and generalities

Introduction & generalities

➔Terminology related to cybersecurity (1)

➔ Vulnerability

Any weakness or flaw in information systems/communication networks is a vulnerability in cyber security. Cybercriminals and Hackers may target these vulnerabilities and exploit them to attack the system/network.

- **Examples of vulnerabilities :**

- Missing data encryption.
- Unrestricted upload of dangerous files.
- Using broken algorithms. -URL Redirection to untrustworthy websites.
- Weak and unchanged passwords. -Website without SSL.

Introduction & generalities

➔Terminology related to cybersecurity (2)

- **Risk** : the probability of exposure or loss resulting from a cyber attack or data breach in a system/network. A better, more encompassing definition is the potential loss or harm related to the exploitation of existing vulnerabilities.
  - *The more vulnerabilities a system or network has, the greater potential for threats and the higher risk we will have and vice versa.*
- **Threat/Attack:** refers to any possible malicious action that seeks to unlawfully damage, access data or disrupt digital operations. Cyber threats can originate from various actors, including terrorist groups, hostile persons, criminal organizations, hackers and even dishonest employees.
  - *Examples of attacks: Malware, Denial of Sevice (DoS), Man in the middle, spying, etc.*

Introduction & generalities

➔Terminology related to cybersecurity (3)

➔ **Attacker** = Adversary = Intruder = Hacker = Cybercriminal

➔ **Target** = Victim

➔ **Legitimate entity** ≠ (Attacker & Target)

➔ **Countermeasure** : any security solution or defense strategy that aims to protect the system against cyber-attacks. Counter measures can be preventive or detective.

Introduction & generalities

→ Objectives of cybersecurity

1. Confidentiality
2. Authentication
3. Non repudiation
4. Integrity
5. Access control
6. Availability

Introduction & generalities

➔Objectives of cybersecurity (1)

- **Confidentiality**

Confidentiality ensures that only authorized entities can access the information, while preventing others from discovering anything about its contents. It ensures that vital information does not reach the wrong people while also ensuring that the appropriate ones receive it. Data encryption is a wonderful example of how to keep information private.

Introduction & generalities

➔Objectives of cybersecurity (2)

- **Authentication**

- An authentication procedure is one that ensures and confirms a user's identity or role. Authentication is a must for all companies because it allows them to safeguard their networks by allowing only authenticated users to access protected information.
- In the context of communications, authentication refers to any mechanism that checks the validity of the pretended source of information / data messages.
- It can be ensured by means of digital signatures, Message authentication codes (MACs), digital fingerprint

Introduction & generalities

➔Objectives of cybersecurity (3)

- **Non-repudiation**

It refers to a situation where someone cannot deny the validity of something. In the context of communications, a sender of an authenticated message cannot thereafter deny the act of having sent that message.

- It is usually guaranteed by strong authentication tools like digital signatures

- **Integrity**

The means for guaranteeing that data is real, correct, and protected against unauthorized modification/alteration is referred to as integrity. It is a property that information has not been tampered with in any manner and that the information's source is legitimate.

- It can be esured by tools like: Hash functions and checksums.

Introduction & generalities

➔Objectives of cybersecurity (4)

- **Access control**

Access control refers to the set of rules and procedures that govern who has access to a system or to physical or virtual resources. It is the process of granting users access to systems, resources, or information, as well as particular privileges.

Users of access control systems must present credentials such as a person's name, passwords, digital fingerprint, or a computer's serial number before granting access.

These credentials can take numerous forms in physical systems, but credentials that cannot be transferred provide the best security.

Introduction & generalities

➔Objectives of cybersecurity (5)

- **Availability**

Availability is the property of being able to access and modify information in a timely manner by those who are allowed to do so. It ensures that only authorized personnel have access to the sensitive data on a consistent and dependable basis. The availability principle is operated by employing the following tools:

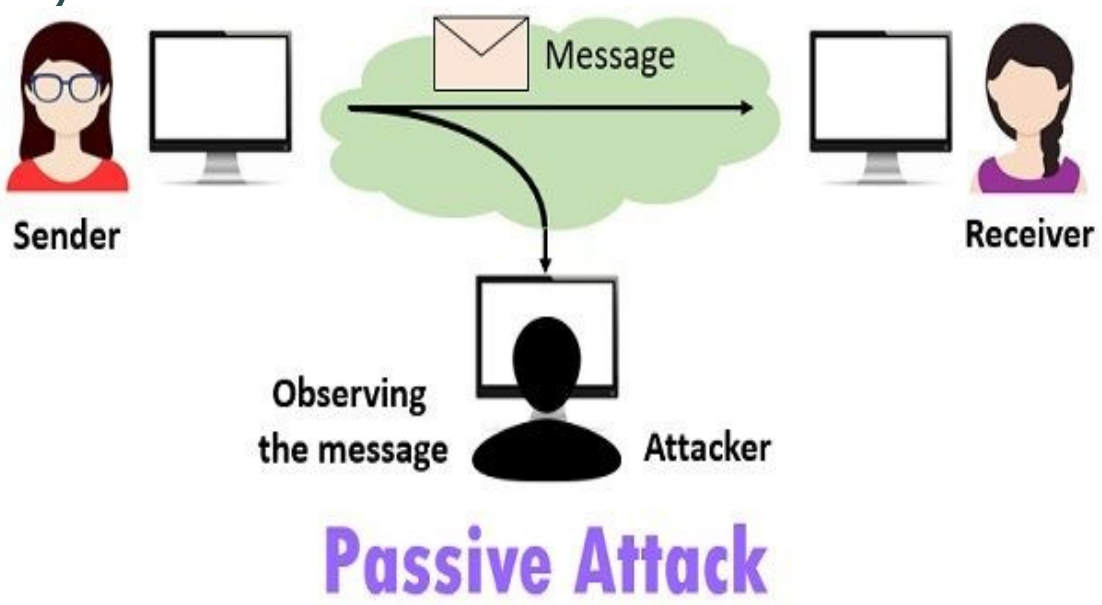
- **Physical Protection:** the ability to keep information accessible even when faced with physical difficulties. It ensures that sensitive data and important information technologies are kept in safe places.
- **Computational Redundancy:** used as a fault-tolerant system against intentional and unintentional failures.

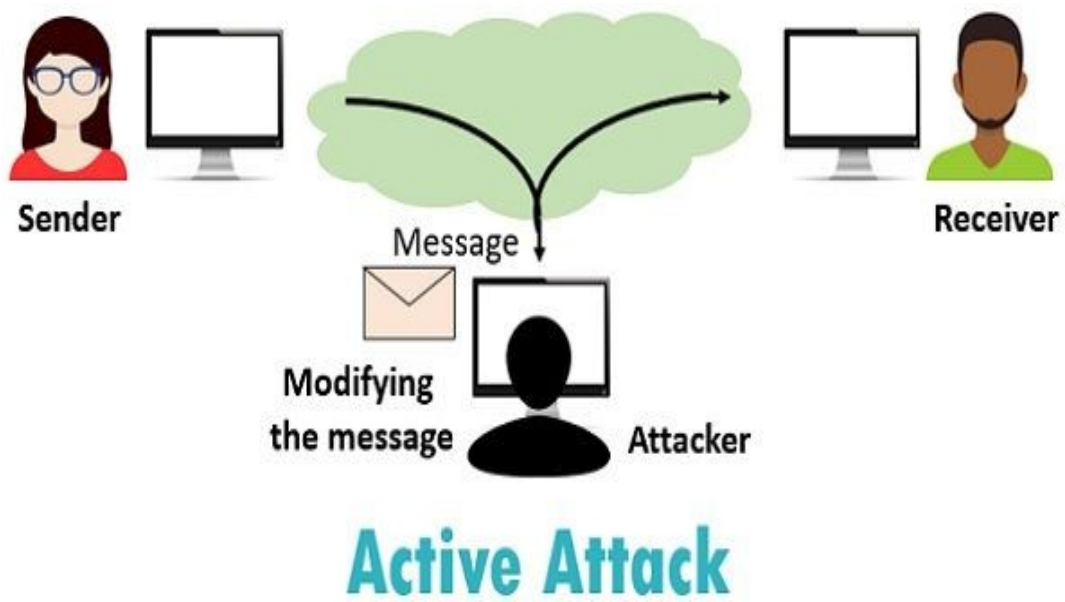
Introduction & generalities

➔Classes of attacks : There are several classes of cyber-attacks

- **Passive vs Active attacks**

In passive attacks, adversaries just attempt to analyze, capture network trafic (exchanged messages), spy on communications without changing or subverting anything. Whereas, with active attacks, the adversary performs malicious actions that cause damage, negative changing in communications, system resources or databases.





Introduction & generalities

→ Classes of attacks

- **Random vs deterministic attacks**

In random attacks the behavior of attackers is random; malicious actions can be of any type and they are launched at anytime. However, in deterministic attacks every action is performed at specific and well determined timing /phase.

- **Centralized vs distributed attacks**

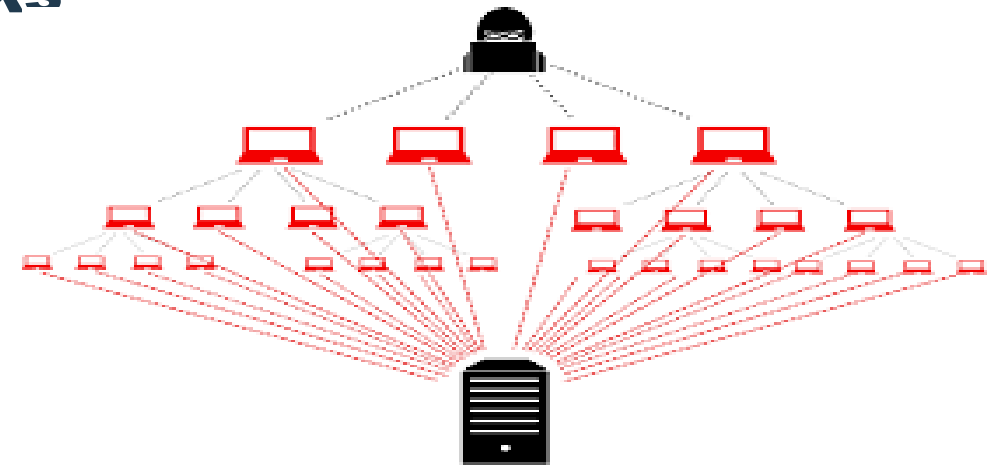
In centralized attacks, attacks are originated from one centralized source. Distributed attacks are launched by a group of adversaries that are generally supervised by one hidden attacker.

Introduction & generalities

➔Classes of attacks

- **Centralized vs distributed attacks**

Centralized attacks



Distributed attacks

Introduction & generalities

→ Classes of attacks

- **Intentional vs Unintentional / Accidental attacks**

Intentional attacks refer to actions carried out with the purpose of causing harm or disruption to a network, system, organization, or individual. These attacks are typically executed with some form of malicious intent, such as theft of data, disruption of services, or damage to infrastructure.

Unintentional or accidental attacks occur without malicious intent but still cause harm or disruption. Human error (lack of awareness), software bugs, or system misconfigurations, inadequate security practices are possible sources of unintentional threats.

Introduction & generalities

→ Classes of attacks

- **Internal vs external attacks**

Internal attacks are exercised by attackers that belong to the network or company's system. External attackers attack the network or the company's information system from the outside.