LEC1

Introduction to Cryptography
- Concepts
- Examples

2025-2026
Second semester
2026-2-4

Alaa Y. Taqa

تحليل الخطر Risk Analysis: هي عملية تحديد النظام المطلوب حمايته والتهديدات المحتملة له .

سلامة البيانات Integrity: التأكد من أن المعلومات لم يتم تغييرها من قبل وسائل غير معروفة او غير مخولة .

المتاحية Availability: يجب أن تكون المعلومات و الحواسب متاحة للأشخاص المخولين باستخدامها .

الخصوصية Privacy \ Confidentiality: الحفاظ على سرية المعلومات و عدم إظهارها ألا للأشخاص المخولين قانونا .

أثبات الشخصية Authentication: هو أثبات الشخص أو البرنامج أو الآلة انه من حقها استخدام رمز التعريف Identification الذي تم استخدامه.

عدم الإنكار Non-repudiation: منع إنكار الالتزام السابق بعمل ما .

السيطرة على الوصول Access Control: تحديد عملية الوصول إلى الموارد لكينونات مخولة.

أمنية الحاسوب Computer Security: هو اسم عام لمجموعة الأدوات المصممة لحماية البيانات من المتطفلين .

المتطفل Intruder : هو عبارة عن كينونة متواجدة بين طرفين متراسلين وهو ليس احدها (لا المرسل ولا المستلم) وهو يحاول القضاء على خدمة النظام الأمني الموجود بين المرسل والمستلم. توجد أسماء أخرى مرادفة للمتطفل وهي العدو ، المهاجم والمتنصت.....الخ.

الهاكر Hacker : هو عبارة عن شخص له إلمام واسع في الحاسوب و/أو شبكات ألحاسوب والذي يحاول إيجاد ثغرات أمنية في ألبرنامج أو ألنظام.

ألفيروس Virus : هو عبارة عن برنامج عند تنفيذه يمكنه أن يكرر نفسه وتضمينها داخل برنامج أخر. بالرغم من وجود فيروسات غير مؤذية ولكن معظمها يكون هدفها هو تدمير ألنظام ألمضيف والبيانات المتراسلة وخاصة في ألشبكات.

ألدودة Worm : هي عبارة عن برنامج مستقل يحاول الحصول على وصول إلى النظام من خلال شبكة الحاسوب. مثلا يجرب أنواع مختلفة من كلمات المرور. تسمى ألدودة بأشباه ألفيروس لأنها تقوم بنفس ألعمل لكنها تتميز بصفة وحيدة وهي عدم تكرار نفسها.

حصان طروادة Trojan Horse: هو عبارة عن برنامج صحيح وقانوني لإجراء عمل مفيد لكن ضمنه تنفذ شفرة مخفية والتي قد تكون فيروس يسمح بوصول غير مخول إلى الحاسوب لتدمير الملفات والبيانات.

Introduction to Cryptography

- **Cryptography** is the science of protecting information by transforming it into a secure format so that only authorized users can read or use it. It is widely used in computer networks, banking systems, secure communications, and data storage.
- The main goal of cryptography is to ensure **data security** by protecting information from unauthorized access, modification, or theft.

Data Security

- **Data security** refers to protecting digital information from unauthorized access, corruption, or theft.

It ensures that data remains:

- **Confidential** – Only authorized users can access it.
- **Integrity** – Data cannot be altered without detection.
- **Availability** – Authorized users can access the data when needed.
- Example:
  When you log into a banking website, encryption protects your username and password from hackers.

Security Attacks

- A **security attack** is any attempt to violate the security of information or systems.

Security attacks try to:

- Steal information
- Modify data
- Interrupt communication
- Gain unauthorized access

Security attacks are generally divided into **two main types**:

- Passive attacks
- Active attacks

Security Services

- **Security services** are mechanisms that protect data and systems from attacks.

Common security services include:

- **Confidentiality**
  Ensures that information is accessible only to authorized users.
- **Integrity**
  Ensures that data is not modified or altered during transmission.
- **Authentication**
  Verifies the identity of users or systems.
- **Non-repudiation**
  Prevents someone from denying that they performed an action (such as sending a message).
- **Access Control**
  Restricts unauthorized users from accessing resources.

Passive Attack

- **A passive attack occurs when an attacker secretly monitors or listens to communication without altering the data.**

The goal is to **steal information without being detected**.

Examples of passive attacks:

1.Eavesdropping

Listening to private communication.

1.Traffic Analysis

Observing communication patterns to gather information.

Example:

A hacker intercepts network packets to read messages but does not modify them.

Passive attacks are difficult to detect because the attacker does not change the data.


Message
Sender
Receiver
Observing
the message
Attacker
Passive Attack

Active attack

It is a type of **cybersecurity attack** where the attacker **actively interferes with a system, network, or communication**. Instead of just observing data, the attacker **modifies, disrupts, or injects information** into the system

Key Idea

- **Active attack:** The attacker **changes or disrupts data or operations**.
- This can damage systems, steal information, or stop services.


Sender
Receiver
Message
Modifying
the message
Attacker
Active Attack

Applications of cryptography

Common Examples

1.Data modification

The attacker intercepts data and **changes it before it reaches the receiver**.

2.Man-in-the-Middle (MitM) attack

The attacker secretly sits between two parties and **alters the messages** being exchanged.

3.Denial-of-Service (DoS)

The attacker floods a server with traffic so **legitimate users cannot access the service**.

4.Masquerade attack

The attacker **pretends to be an authorized user** to gain access.

5.Replay attack

The attacker **captures a valid data transmission and sends it again** to trick the system.

Simple Example

Imagine you send a message:

"Transfer $100 to John"

•In an **active attack**, a hacker intercepts it and changes it to:

•"Transfer $10,000 to John"

The attacker **actively changes the data** before it reaches the bank.

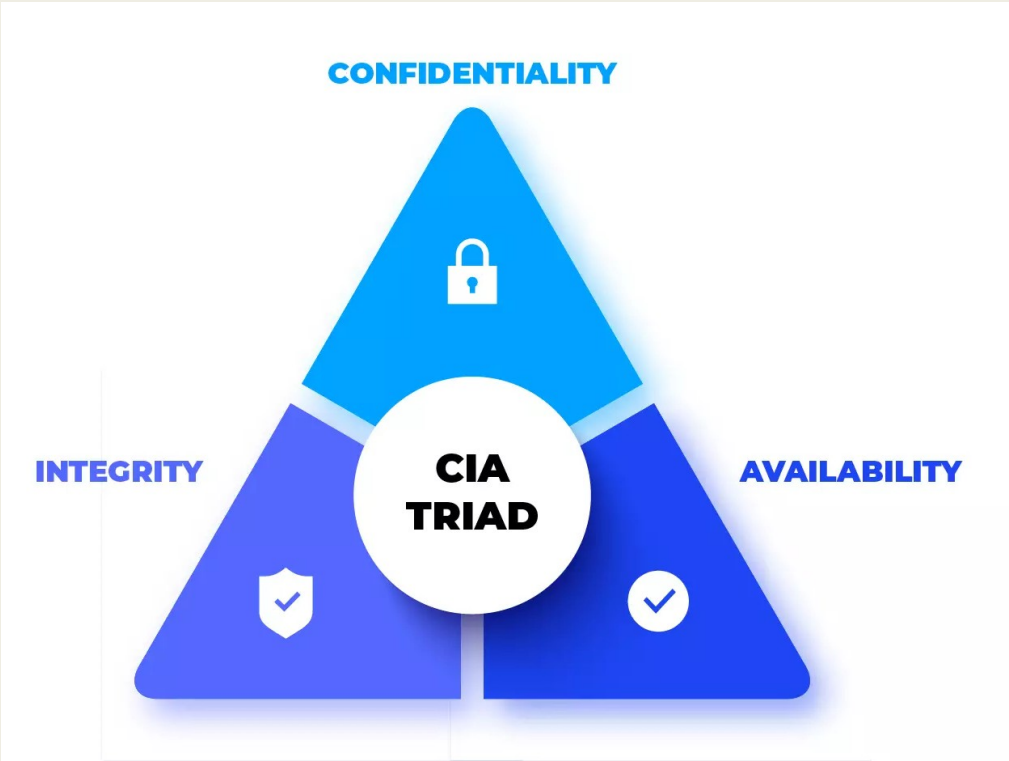
Active Attack vs Passive Attack

Type	What Happens
Active attack	Data is **modified, injected, or disrupted**
Passive attack	Attacker **only listens or monitors** data

Basic Principles of Security

- The **basic principles of information security** are often called the **CIA Triad**:

1. **Confidentiality**
   - Protecting information from unauthorized access.
   - Example: Encryption of emails.
2. **Integrity**
   - Ensuring that data is not changed or tampered with.
   - Example: Hash functions used to verify file integrity.
3. **Availability**
   - Ensuring systems and data are available when needed.
   - Example: Backup systems and server redundancy.




Questions


THANK
YOU