Al-Mustaqbal University
College of Sciences
Intelligent Medical System Department

جامـــــعة المـــــستـقبـل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قســـم الانظمة الطبية الذكية

Lecture: (1)

Information Security in Healthcare

Subject: Introduction to Computer Security
Level: Fourth
Lecturer: Prof. Dr. Mehdi Ebady Manaa

1. Computer Security is Critical in Healthcare

Modern hospitals are cyber-physical systems, very similar to Industrial Control Systems (ICS) used in power plants and factories. Healthcare depends on real-time digital systems that directly affect human life.

2. A Definition of Computer Security

COMPUTER SECURITY: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).

3. The CIA Triad

This definition introduces three key objectives that are at the heart of computer security:

1. **Confidentiality:** This term covers two related concepts:
    - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
    - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
2. **Integrity:** This term covers two related concepts:
    - **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
    - **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
3. **Availability:** Assures that systems work promptly and service is not denied to authorized users.

- These three concepts form what is often referred to as the **CIA triad** (Figure 1.1).

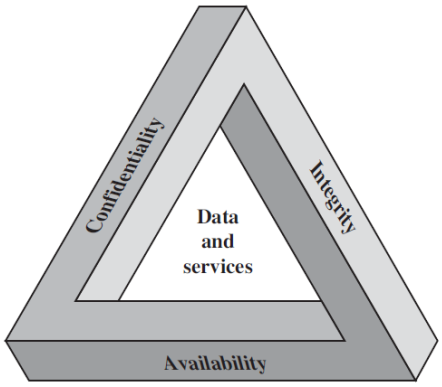


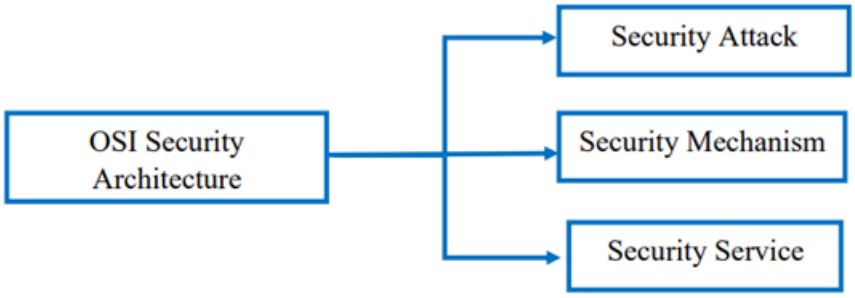
Figure 1.1 The Security Requirements Triad

Although the CIA triad defines the core of security, two additional goals are important:

- **Authenticity** – ensuring that users and messages are real and come from trusted sources.
- **Accountability** – ensuring that every action can be traced to a specific user, supporting auditing, investigation, and legal responsibility.

4. The OSI Security Architecture

ITU-T (International Telecommunication Union, Telecommunication Standardization Sector) X.800 Security Architecture for OSI. It provides a systematic way of defining and providing security requirement.



➢ **Security attack:** Any action that compromises the security of information owned by an organization.

➢ **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

➢ **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an

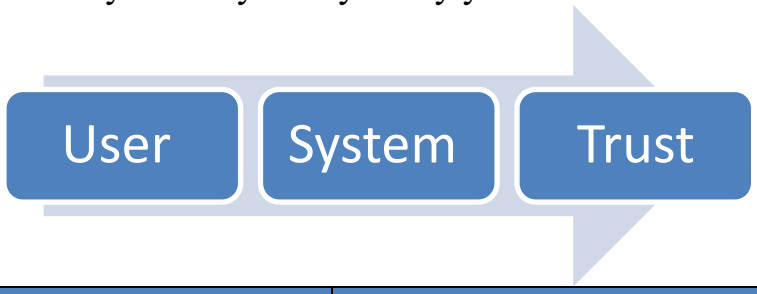
organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

1. Security Services (X.800 Model)

➢ A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. Security services are divided into 6 categories 14 specific services:

1. Authentication

➢ Are you really who you say you are?



Type	What it means	Healthcare Example
Peer Entity Authentication	Verifies the identity of connected users	Doctor logging into hospital system
Data-Origin Authentication	Verifies who sent the data	Lab system sending test results

2. Access Control

- Prevents unauthorized use of systems, files, or devices
- Defines what users are allowed to view, change, or use

User ⟶ [Access Rules] ⟶ Resource

Example: A nurse can view records but cannot change diagnoses.

3. Data Confidentiality

Who can see the data?

Patient Data ⟶ [Encryption] ⟶ Safe Transmission

Type	What it protects
Connection Confidentiality	All data on a session

Connectionless Confidentiality	One message or data block
Selective-Field Confidentiality	Only sensitive fields (e.g., diagnosis)
Traffic-Flow Confidentiality	Hides communication patterns

- *Example:* Encrypting patient records sent to a specialist.

4. Data Integrity

Has the data been changed?

Original Data ──► Network ──► Verified Data

Type	What it checks
Connection Integrity with Recovery	Detects & fixes errors
Connection Integrity without Recovery	Detects errors only
Selective-Field Integrity	Checks specific data fields
Connectionless Integrity	Checks a single message

- *Example:* Ensuring lab results were not altered.

5. Nonrepudiation

No one can deny their actions

Sender ──► Message ──► Receiver

└──── Proof & Logs ────┘

Type	What it proves
Origin	Who sent the message
Destination	Who received it

- ***Example:* Proving which doctor approved a treatment.**

2. Security Mechanisms

Table 1 lists the security mechanisms defined in X.800. As can be seen the mechanisms are divided into those that are implemented in a specific protocol layer. X.800 distinguishes between reversible encipherment mechanisms and irreversible encipherment mechanisms. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

Table 1: Security Mechanisms (X.800)

Specific Security Mechanisms May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).
Access Control A variety of mechanisms that enforce access rights to resources.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.
Traffic Padding The insertion of 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 breach of security is suspected.
Notarization The use of a trusted third party to assure certain properties of a data exchange