جامعة الحمدانية /كلية التربية
قسم علوم الحاسوب
Fourth Class

Data Security

أستاذ المادة:
م.م. سماح فخري عزيز

Lecture 2

Aspects of Information Security

CONTENTS

* **Aspects of Information Security**
* **Security service**
* **Security attack**
* **Security mechanism**

Aspects of Information Security

- ***The Security Architecture*** **focuses on three aspects of information security:**

  - **Security service**
  - **Security attack**
  - **Security mechanism**

Security Services

- 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.

Security Services

6 security services :

1. **Confidentiality or Secrecy: The concept of *Confidentiality* relate to the protection of information and prevention of unauthorized access or disclosure. The ability to keep data confidential, or secret, is critical to staying competitive in today's business environments.**

Examples of Confidentiality:

- Student grade information is an asset whose confidentiality is considered to be very high
- Student enrollment information: may have moderate confidentiality rating; less damage if enclosed
- Directory information: low confidentiality rating; often available publicly

Security Services

2. Integrity : - deals with prevention of unauthorized modification of intentional or accidental modification.

- **Data integrity:** assures that information and programs are changed only in a specified and authorized manner
- **System integrity:** Assures that a system performs its operations in unimpaired manner

Examples of Integrity

* A hospital patient's allergy information (high integrity data): a doctor should be able to trust that the info is correct and current
* An online newsgroup registration data: moderate level of integrity
* An example of low integrity requirement: anonymous online poll

Security Services

3. Authentication : is the process by which the information system assures that you are who you say you are; how you prove your identity is authentic.

* **Methods of performing authentication are:**

User ID and passwords:

The system compares the given password with a stored password. If the two passwords match then the user is authentic.

Swipe card

which has a magnetic strip embedded, which would already contain your details, so that no physical data entry takes place or just a PIN is entered.

Digital certificate

an encrypted piece of data which contains information about its owner, creator, generation and expiration dates, and other data to uniquely identify a user.

key fob

small electronic devices which generate a new random password synchronized to the main computer

Biometrics

retinal scanners and fingerprint readers. Parts of the body are considered unique enough to allow authentication to computer systems based on their properties.

Security Services

4. Non-Repudiation : - prevents either sender or receiver from denying a transmitted message.

* when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

5. Access Control : The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

Security Services

6. Availability: - assures that the resources that need to be accessed are accessible to authorized parties in the ways they are needed. Availability is a natural result of the other two concepts (confidentiality and integrity).

* **Examples of Availability**
* **A system that provides authentication: high availability requirement**
* **If customers cannot access resources, the loss of services could result in financial loss**
* **A public website for a university: a moderate availably requirement; not critical but causes embarrassment**
* **An online telephone directory lookup: a low availability requirement**

Security attack

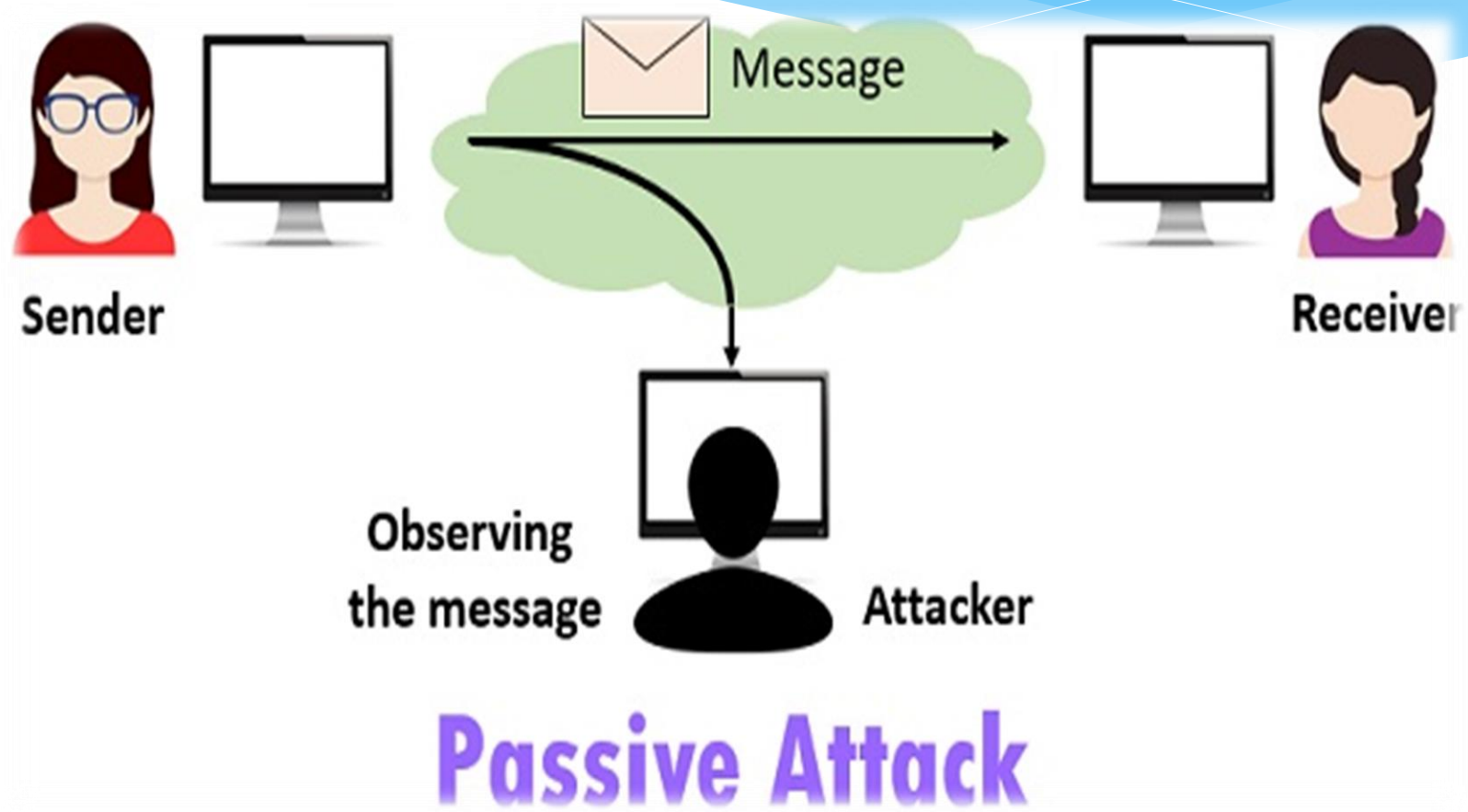
Any action that compromises the security of information owned by an organization.

Attacks types:-

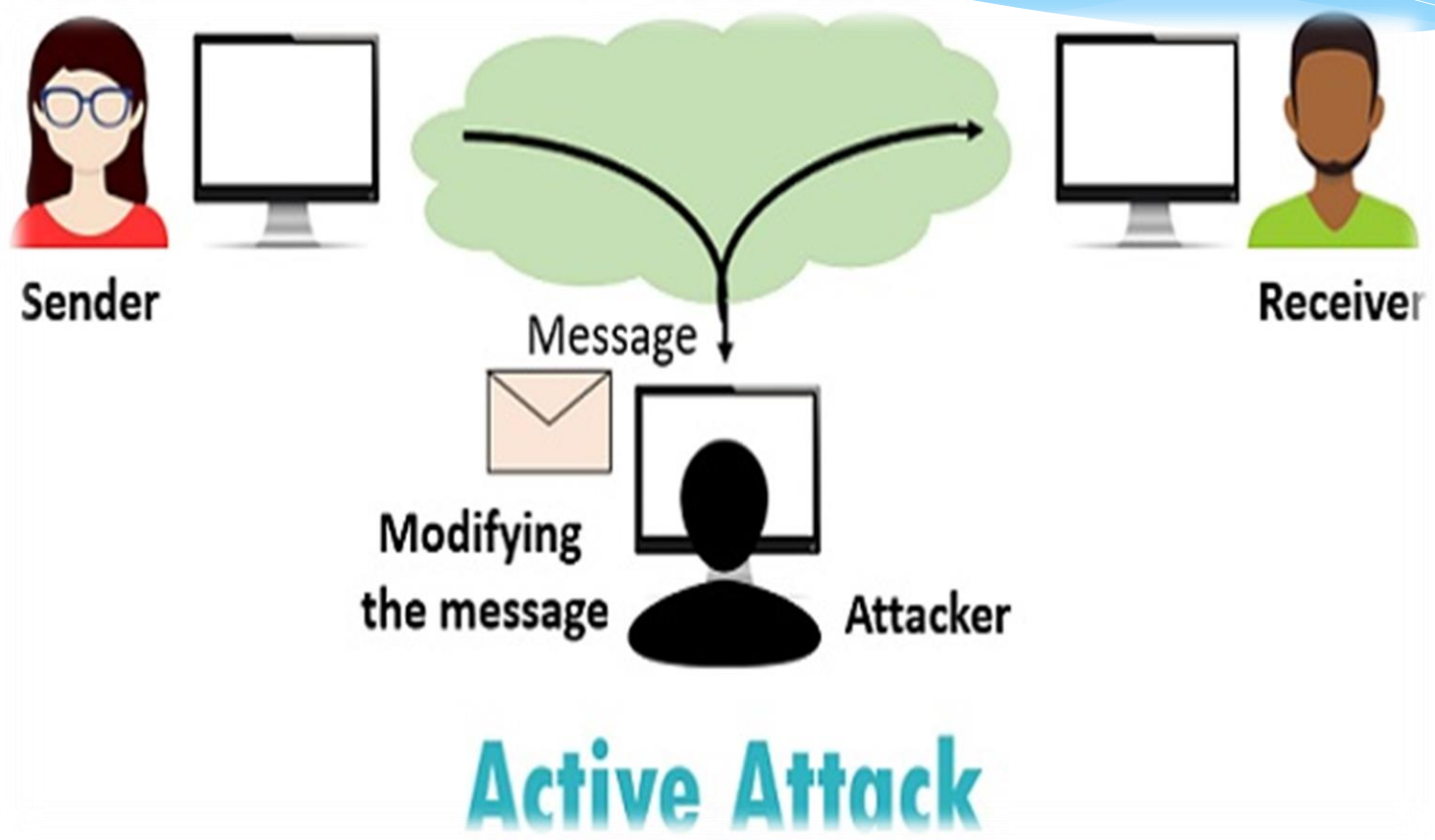
* Passive Attack:- **does not affect the system, just take the wanted data and information.**

* Active Attack:- **affect the system in addition to have the wanted data and information.**

Passive Attack



Active Attack



- **Next lecture**

  Computer Crimes

شكرا لاصغاءكم