INTRODUCTION

— Computer data often **travels from one computer to another, leaving the safety of its protected physical surroundings**.

— Once the data is out of hand, **people with bad intention could modify or forge your data**, either for amusement or for their own benefit.

— **Cryptography can reformat and transform our data**, making it safer on its trip between computers.

—The **technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways**.

- **Computer Security** - generic name for the **collection of tools designed to protect data** and to thwart hackers
- **Network Security** - measures to **protect data during their transmission**
- **Internet Security** - measures to **protect data during their transmission over a collection of interconnected networks**

Security Attacks, Services and Mechanisms

— To assess the security needs of an organization effectively, the manager responsible for **security needs** some systematic way of **defining the requirements for security and characterization of approaches to satisfy those requirements**.

— One approach is to consider three aspects of information security:

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

Security mechanism – A **mechanism that is designed to detect, prevent or recover** from a security attack.

Security service – 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

The classification of security services are as follows:

- **Confidentiality:** Ensures that the information in a computer system and transmitted information are **accessible only for reading by authorized parties.**

  E.g. Printing, displaying and other forms of disclosure.

- **Authentication:** Ensures that the **origin of a message or electronic document is correctly identified**, with an assurance that the identity is not false.
- **Integrity:** Ensures that **only authorized parties are able to modify computer system assets and transmitted information**. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
- **Non repudiation**: Requires that neither the **sender nor the receiver of a message be able to deny the transmission.**
- **Access control**: Requires that access to information resources may be controlled by or the target system.
- **Availability**: Requires that computer system assets be available to authorized parties when needed.

SECURITY MECHANISMS

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. **.**

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

1. **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.
2. **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).
3. **Access Control:** A variety of mechanisms that enforce access rights to resources.
4. **Data Integrity:** A variety of mechanisms used to assure the integrity of a

   data unit or stream of data units.

5. Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

6. Traffic Padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

7. Routing Control: Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

8. Notarization: The use of a trusted third party to assure certain properties of a data exchange.

protocol layer in order to provide some of the OSI

B. PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

1. Trusted Functionality: That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

2. Security Label: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

3. Event Detection: Detection of security-relevant events.

4. Security Audit Trail: Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

5. Security Recovery: Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions