Cryptography and Network Security

By Dr. Upma Jain

Taxonomy of attacks with relation to security goals

- **Attacks threatening confidentiality**
- **Attacks threatening Integrity**
- **Attacks Threatening availability**

Taxonomy of attacks with relation to security goals

- **Attacks threatening confidentiality**
  - Snooping (unauthorized access can be avoided by using encryption)
  - Traffic analysis (monitoring online data to guess the nature of transaction between sender and receiver)

Taxonomy of attacks with relation to security goals

- **Attacks threatening Integrity**
  - Modification (After accessing attacker modifies information for own benefit)
  - Masquerading (Attacker impersonate someone else)
  - Replaying (obtains a copy of message and tries to reply it)
  - Repudiation (Denial of sender or receiver)

Taxonomy of attacks with relation to security goals

- **Attacks Threatening availability**
  - Denial of service (may slow down or totally interrupt the service of a system)

Security Mechanism

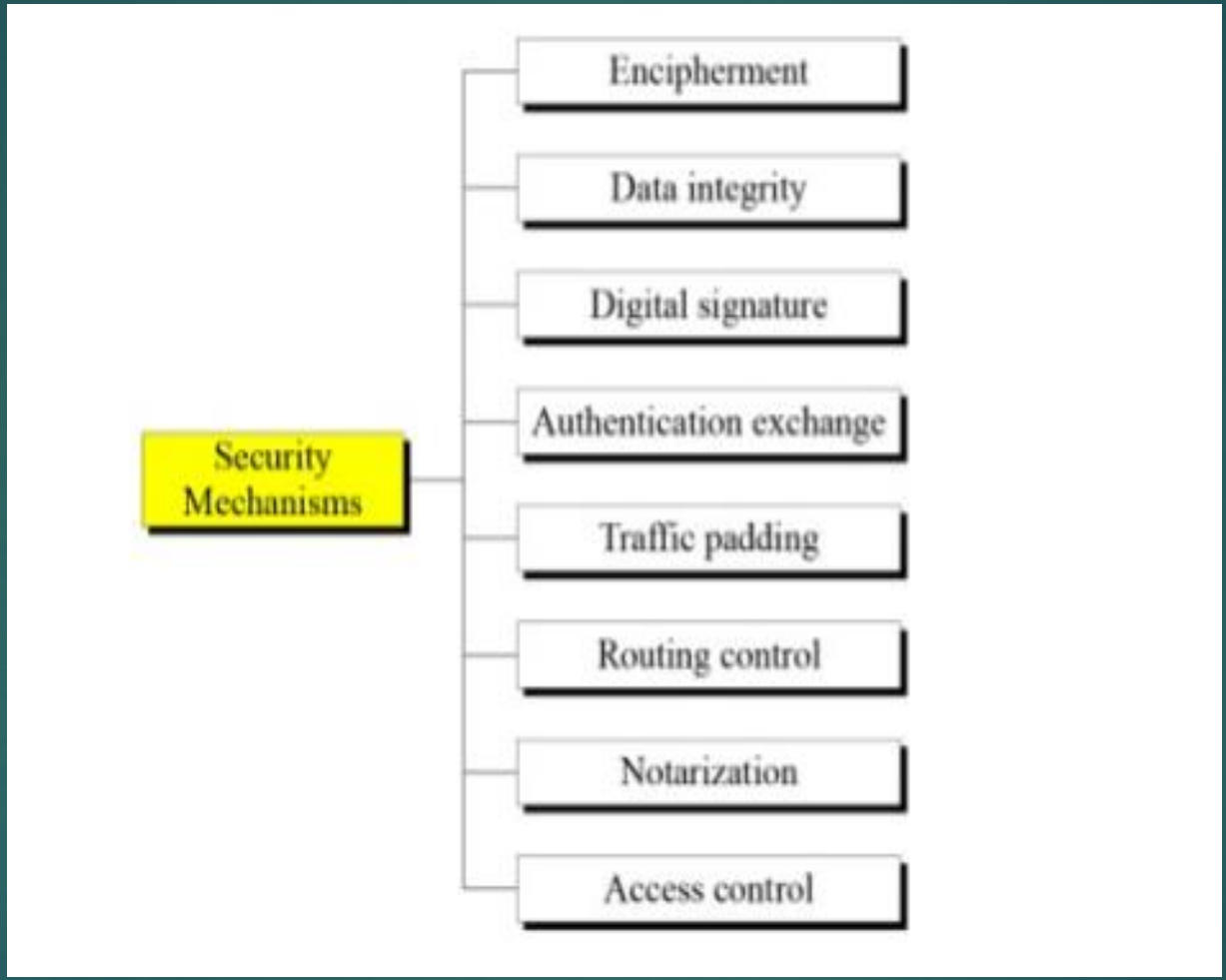

Fig. 1 [Cryptography and network security (B.A. Forouzan)]

Encipherment

- Encipherment is hiding or covering data and to provide confidentiality.
- It makes use of mathematical algorithms to transform data into a form that is not readily intelligible.
- Cryptographyand Steganography techniques are used for enciphering.

Data integrity

- The data integrity mechanism appends a short check value to the data which is created by a specific process from the data itself.
- The receiver receives the data and the check value. The receiver then creates a new check value from the received data and compares the newly created check value with the one received. If the two check values match, the integrity of data is being preserved.

Digital Signature

- A digital signature is a way by which the sender can electronically sign the data and the receiver can electronically verify it.
- The sender uses a process in which the sender owns a private key related to the public key that he or she has announced publicly.
- The receiver uses the sender's public key to prove the message is indeed signed by the sender who claims to have sent the message.

Authentication exchange

- A mechanism intended to ensure the identity of an entity by means of information exchange.
- The two entities exchange some messages to prove their identity to each other. For example the three-way handshake in TCP.

Routing control

- Enables selection of particular physically secure routes for certain data and allows routing changes which means selecting and continuously changing different available routes between the sender and the receiver to prevent the attacker from traffic analysis on a particular route.

Notarization

- The use of a trusted third party to control the communication between the two parties.
- It prevents repudiation.
- The receiver involves a trusted third party to store the request to prevent the sender from later denying that he or she has made such a request.

Access Control

- A variety of mechanisms are used to enforce access rights to resources/data owned by a system, for example, PINS, and passwords.

Thank you