Chapter 3
Computer Network Security

I) Definitions

1) Computer Security

A broad term for tools and technologies designed to safeguard data and prevent unauthorized access or actions by hackers ..

2) Network Security

Techniques and measures to ensure data is protected while being transmitted across a specific network

3) Internet Security

Specialized measures to protect data during transmission over interconnected networks, such as the global Internet

II) What is Network Security

. Network Security encompasses the measures and technologies used to protect data during transmission and to ensure the integrity, confidentiality, and availability of the network

Key Components:

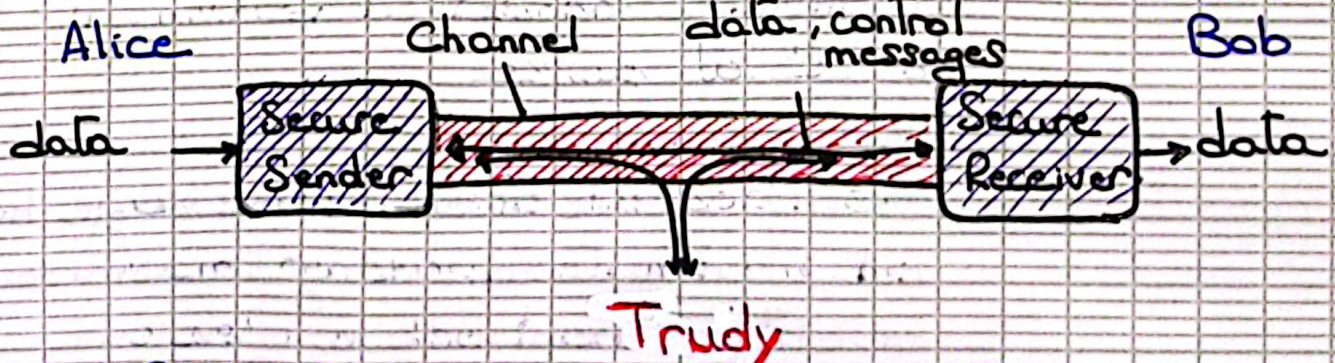
1) Confidentiality:
   - Goal: Ensure that only the sender and intended receiver can understand the message contents
   - How It's Achieved?
     - The sender encrypts the message, making it unreadable to unauthorized parties
     - The receiver decrypts the message to restore it to its original form

2) Authentication:
   - Goal: Confirm the identities of the sender and receiver
   - How It's Achieved?
     Both parties verify each other's identity through passwords, certificates, or other authentication methods

3) Message Integrity
   - Goal: Ensure that the message has not been altered during transmission or after receipt
   - How It's Achieved
     Use of checksums, hashing, and digital signatures to detect any changes in the message.

4) Access and Availability
- Goal: Ensure that network services are accessible and available to authorized users when needed
- How It's Achieved?
  Implementing proper access controls, network monitoring, and protection against denial-of-service (DoS) attacks

III) Friends and Enemies in Network Security
- Alice, Bob, and Trudy
  - These names are commonly used in network security scenarios to represent participants and potential intruders in communication
  - Alice and Bob: Secure sender and receiver, want to communicate "securely"
  - Trudy: Intruder (Attacker), may intercept, delete, add messages.



- Real-Life Examples of Alice and Bob
  - Web Browser / Server: for secure communication such as online purchases or transactions
  - DNS Servers: Secure communication between DNS servers, which resolve domain names into IP addresses

→ Online Banking Client / Server: Secure communication between users and banking services
→ Routers: Routers exchanging secure routing table updates to ensure data finds the best path through the network.

What can a "Bad Guy" (Truly) do in Network Security?

1) Eavesdropping:
Intercept and read messages passing over the network
2) Message Insertion:
Actively insert malicious or unauthorized messages into an ongoing communication, disrupting the flow
3) Impersonation (Spoofing):
Fake (spoof) the source address or other fields in a packet to appear as though the message is comming from a trusted source
4) Hijacking:
Take over an active connection by removing the legitimate sender or receiver and inserting themselves into the communication
5) Denial of Service (DoS)
Overload system resources (like a server or network link) to make the service unavailable to legitimate users.

IV. Types of Security Violations

1) Capture :
- A sensitive file (F) is captured by an unauthorized party (C) while in transit between A and B

2) Intercept - Update
- A message from A to B instructing an update to file F is intercepted by C.
- C alters the message (e.g. adding their own name) before forwarding it to B, resulting in unauthorized modification of F

3) Substitude
- C impersonates A by sending a message to B to update F with C's name, bypassing A's intended instructions

4) Intercept - Preempt
- A sends a message to B to stop C's read / write access.
- C intercepts the message and prevents it from reaching B, maintaining unauthorized access to the resource

5) Denial
- C sends a message to B
- Later, B queries C about the message
- C denied having sent it to B, leading to a denial of service or failur to authenticate the sender's action

V - OSI Security Architecture

The OSI Security Architecture provides a structured approach for managing and implementing security in network systems. It focus on identifying security attacks, defining mechanisms to counter them, and providing services to protect information.

1) Security Attack:

- Any action that compromises the security of information owned by an organization
  - ↳ Ex: Unauthorized data access, data modification, caves dropping, etc.

2) Security Mechanism:

- A process or tool designed to detect, prevent or recover from a security attack
- It protects messages and communications from unauthorized entities
  - ↳ Ex: Encryption, authentication methods, firewalls, intrusion detection systems

3) Security Services

- The services that implement security policies and are realized through Security mechanisms
- It Ensure confidentiality, integrity, availability, and other security aspects for data and communication