The OSI Security Architecture

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

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

Security service: Security services refer to the different services available for maintaining the security and safety of an organization.

Security Attacks

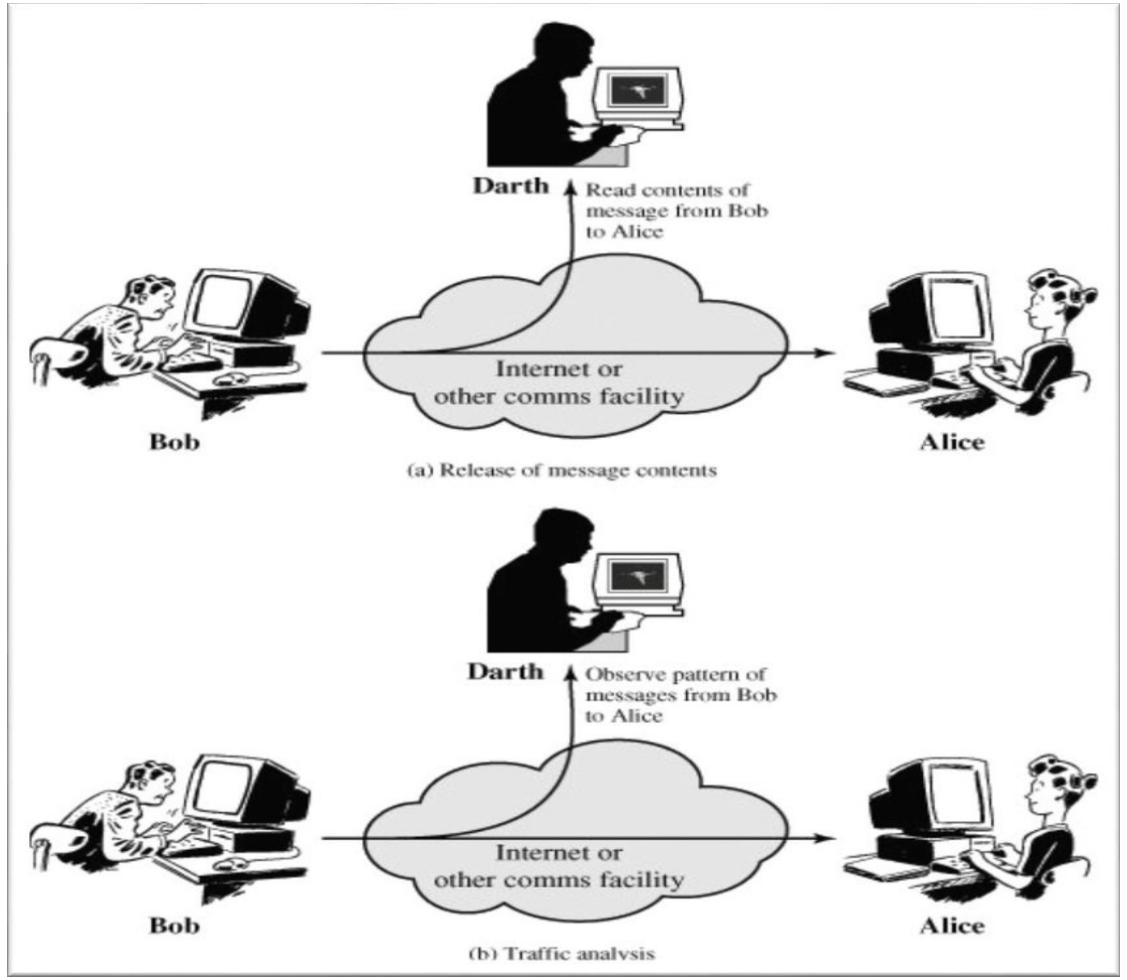
- Passive Attacks
- Active Attacks

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

- Release of message contents
- Traffic analysis

Passive Attacks

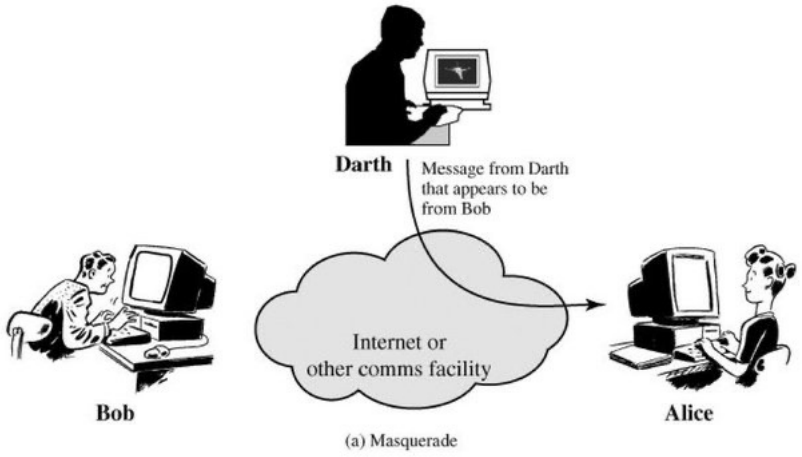


Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream

- **Masquerade**
- **Replay**
- **Modification of Message**
- **Denial of service** (DoS)

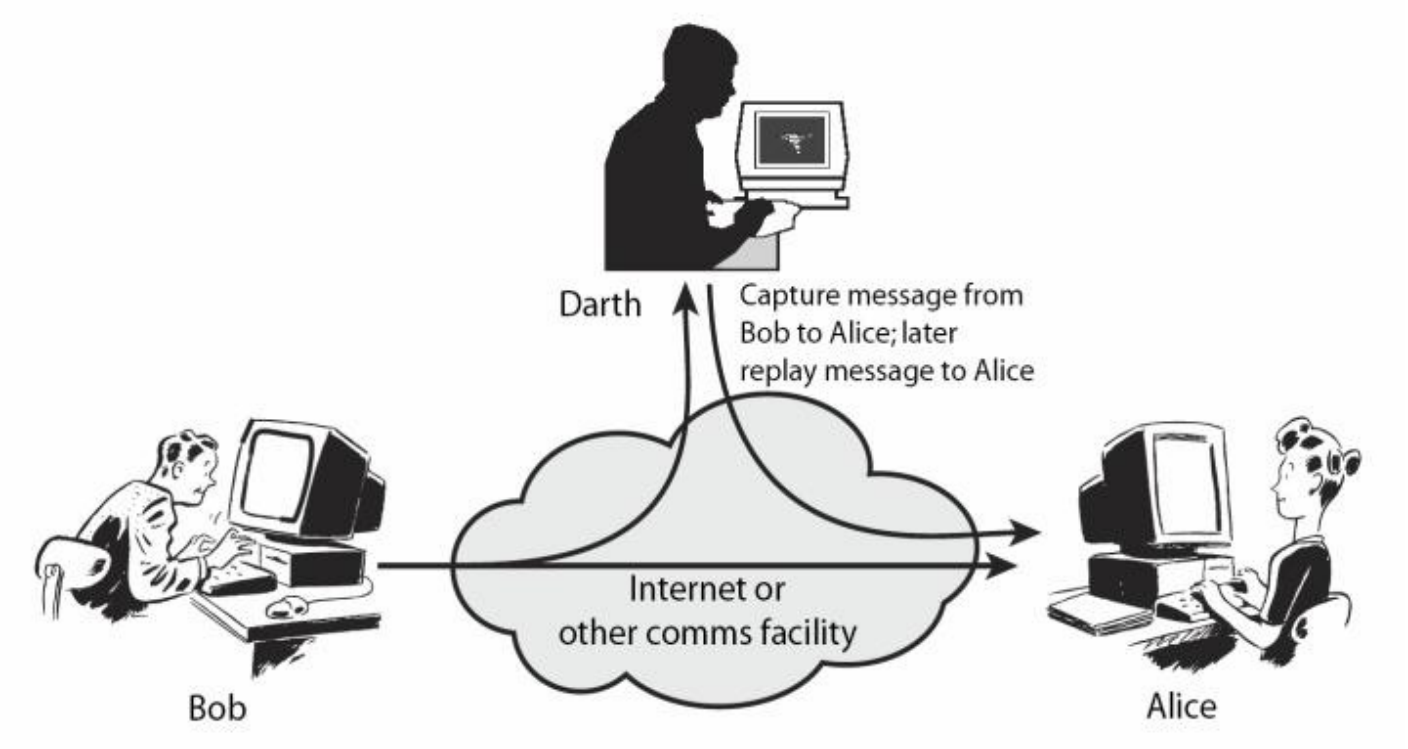
Masquerade



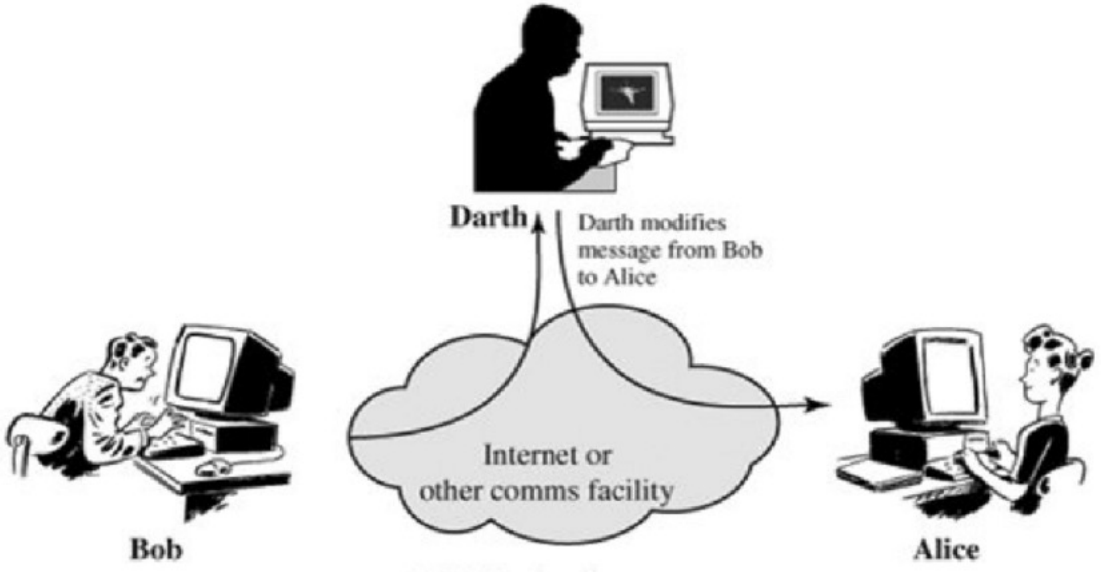
(a) Masquerade

Active Attack – Masquerade

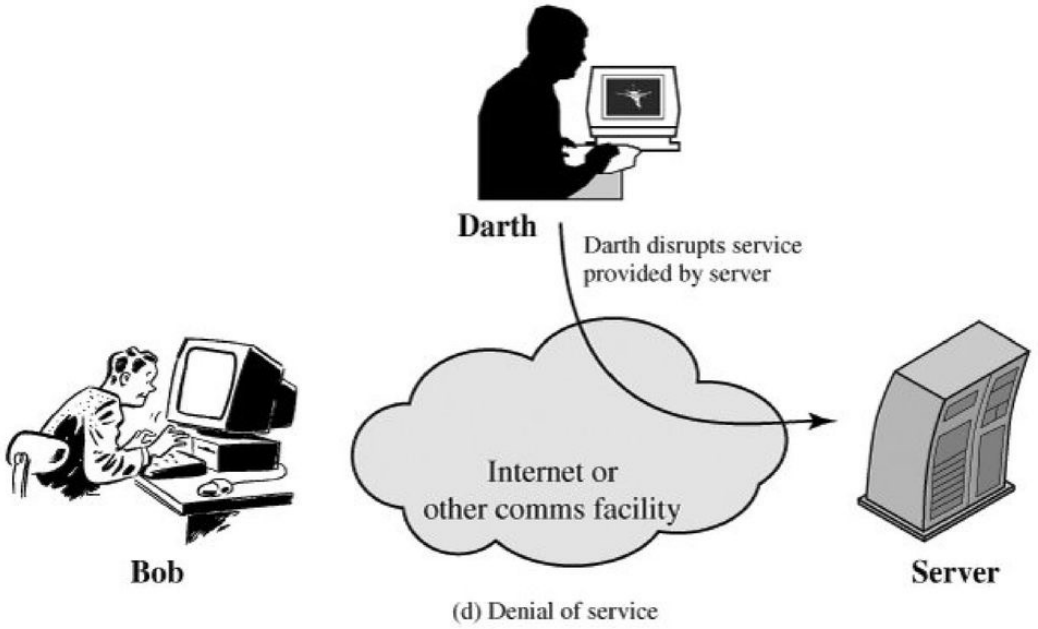
Replay


Darth
Capture message from
Bob to Alice; later
replay message to Alice
Internet or
other comms facility
Bob
Alice

Modification of message



Denial of Service(Dos)



(d) Denial of service

Active Attack –Denial of Service (DoS)

Security Services

Security services refer to the different services available for maintaining the security and safety of an organization.

- **Authentication** is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.
- **Access control** involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- **Data Confidentiality** is responsible for the protection of information from being accessed or disclosed to unauthorized parties.

- **Data integrity** is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.
- **Non- repudiation** involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message. protection against denial by one of the parties in a communication

Security Mechanisms

Encipherment (Encryption) The use of mathematical algorithms to transform data into a form that is not readily intelligible.

Digital signature is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.

Traffic padding is a technique used to add extra data to a network traffic stream in an attempt to obscure the true content of the traffic and make it more difficult to analyze.

Routing control allows the selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap in security is suspected.