Complex

Experiential Learning (site visits)

Forum Theater

Jigsaw Discussion

Inquiry Learning

Role Playing

Active Review Sessions (Games or Simulations)

Interactive Lecture

Hands-on Technology

Case Studies

Brainstorming

Groups Evaluations

Peer Review

Informal Groups

Triad Groups

Large Group Discussion

Think-Pair-Share

Writing (Minute Paper)

Self-assessment

Pause for reflection

Simple

Department of CSE

NETWORK PROTOCOLS & SECURITY 23EC2210 R/A/E

Topic:

Introduction to Security

Session - 33

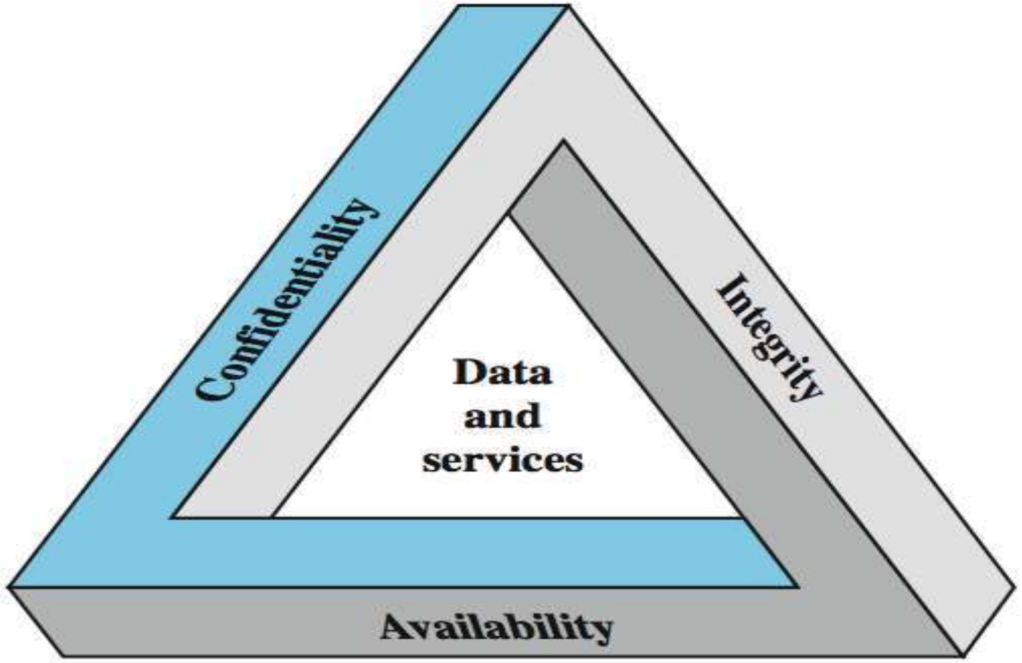
Introduction to Security

Security:

Ensuring the (secrecy) confidentiality, data integrity and availability of components of computer system.

1. **Network security** – measures to protect data during their transmission
2. **Internet security** - measures to protect data during their transmission over a collection of interconnected networks
3. **Computer security** – Computer security, also called cybersecurity, is the protection of computer systems and information from harm, theft, and unauthorized use.

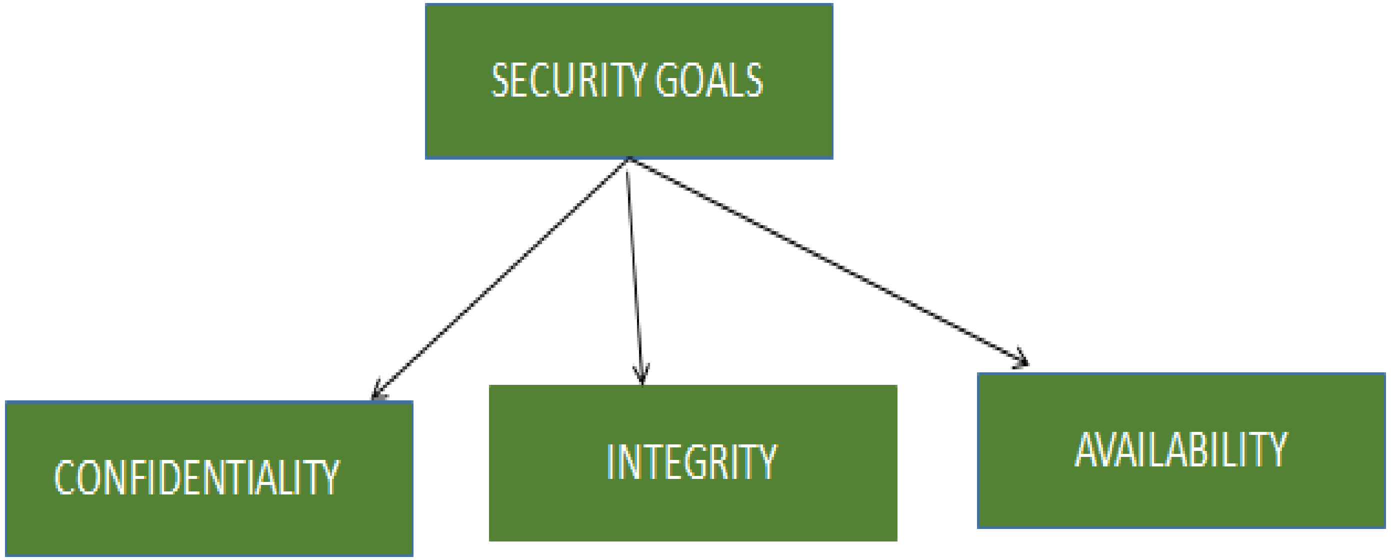
Key Security Concepts



Authentication
Non-repudiation

Security Goals

- Confidentiality, data integrity and availability are the Security goals to protect computer assets from human errors, natural disasters, physical and electronic maliciousness.



SECURITY GOALS

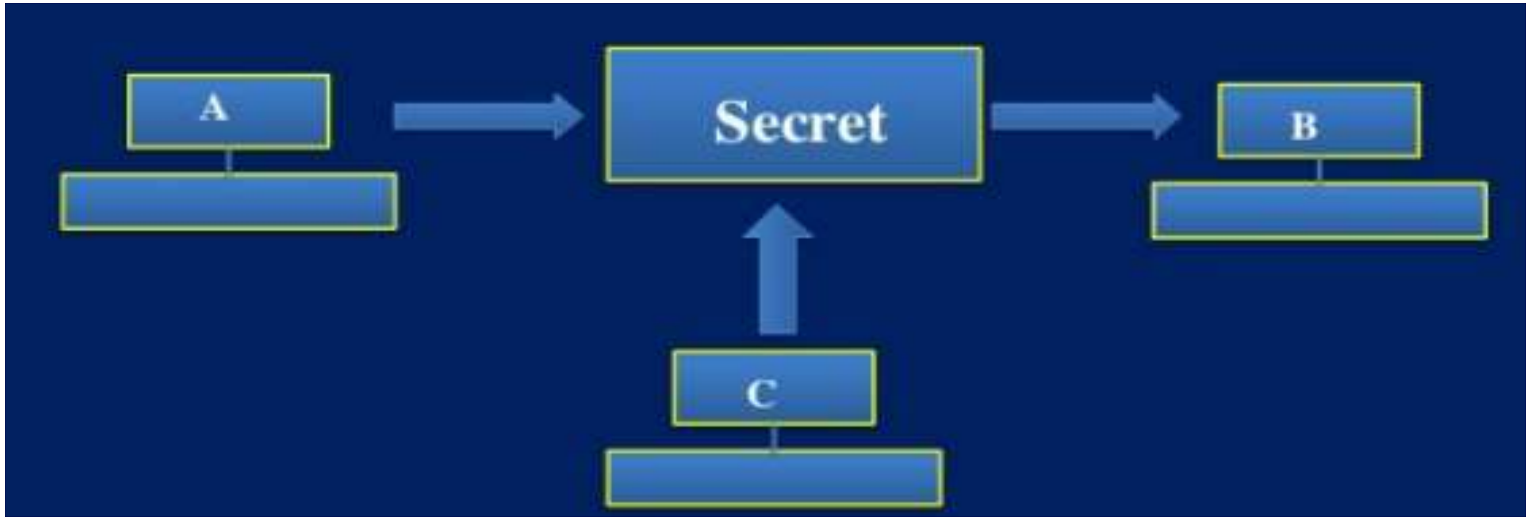
CONFIDENTIALITY

INTEGRITY

AVAILABILITY

Confidentiality

- Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Specifies that only the sender and the intended recipient(s) should be able to access the contents of a message.
- Another user C gets access to this message, which is not desired and therefore, defeats the purpose of confidentiality.



Integrity

Integrity deals with making sure that things are not changed from their true form. Attacks against integrity are those that try and modify something that’s likely going to be depended on later.

Examples include changing prices in an ecommerce database, or changing someone’s pay rate on a spreadsheet.

Availability

- Assures that systems work promptly and service is not denied to authorized users.
- Ensuring that authorized parties are not denied access to information and resources.

Authentication

- Authentication is the process of verifying the identity of user or information.
- User authentication is the process of verifying the identity of user when that user logs into a computer system.
- The main objective of authentication is to allow authorized users to access the computer and to deny access to the unauthorized users.

Non-repudiation

- Non-repudiation is the assurance that someone cannot deny something.

- It does not allow the sender of a message to refuse the claim of not sending that message.

Security Attacks

K L University

u/s 3 of UGC Act. 1956

Koneru Lakshmaiah Education Foundation

Levels of Impact

- We can define 3 levels of impact from a security attack
  - Low - The loss is minor
  - Moderate - The loss is serious
  - High - The loss severe

Security Attacks

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

  - Passive Attack

  - Just to obtain information. Does not Modify or harm the system.

  - Active Attack

  - May Change the Data and harm the system.

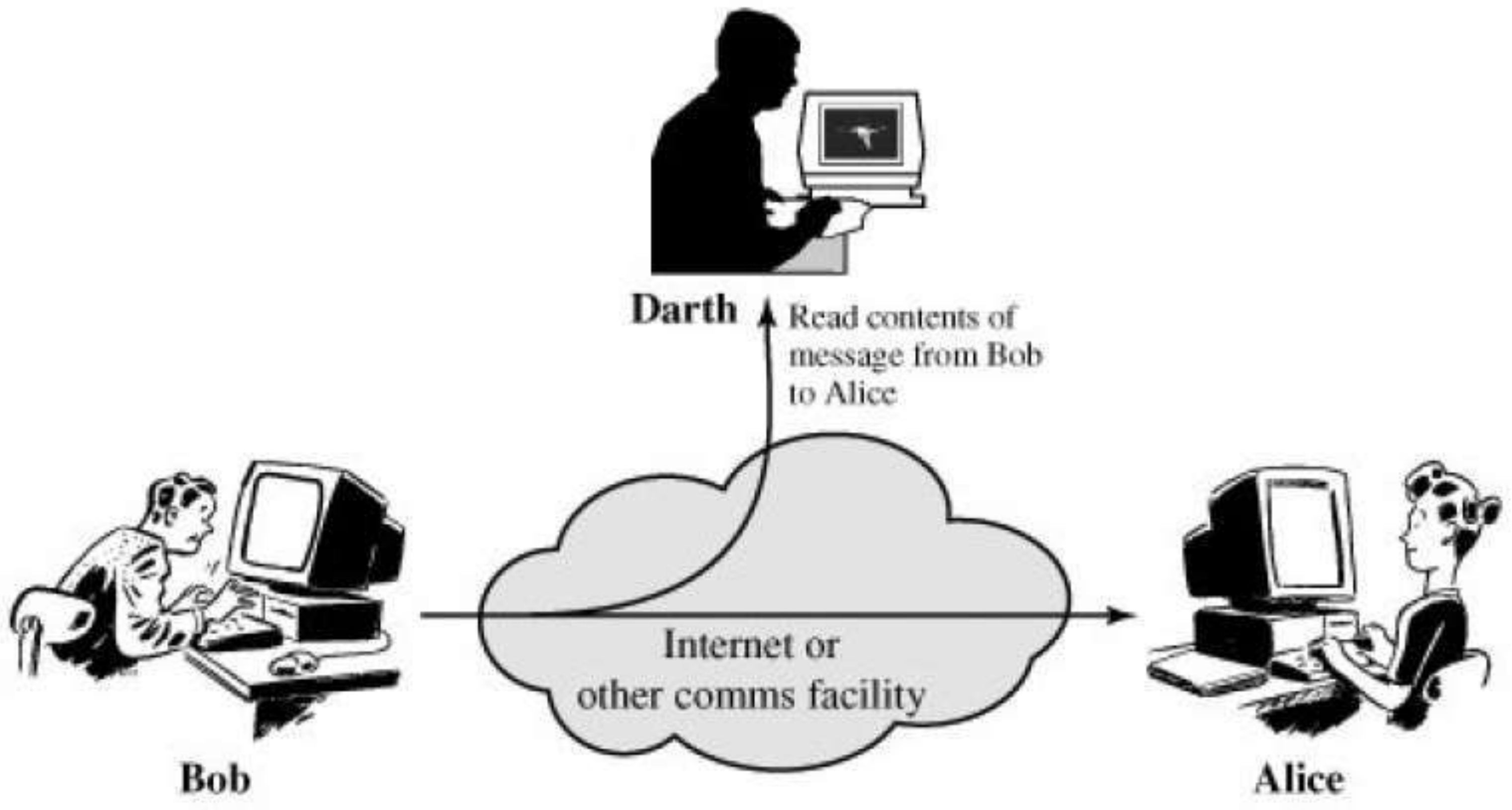
Passive Attacks

- 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.
- Two types of passive attacks

  - release of message contents

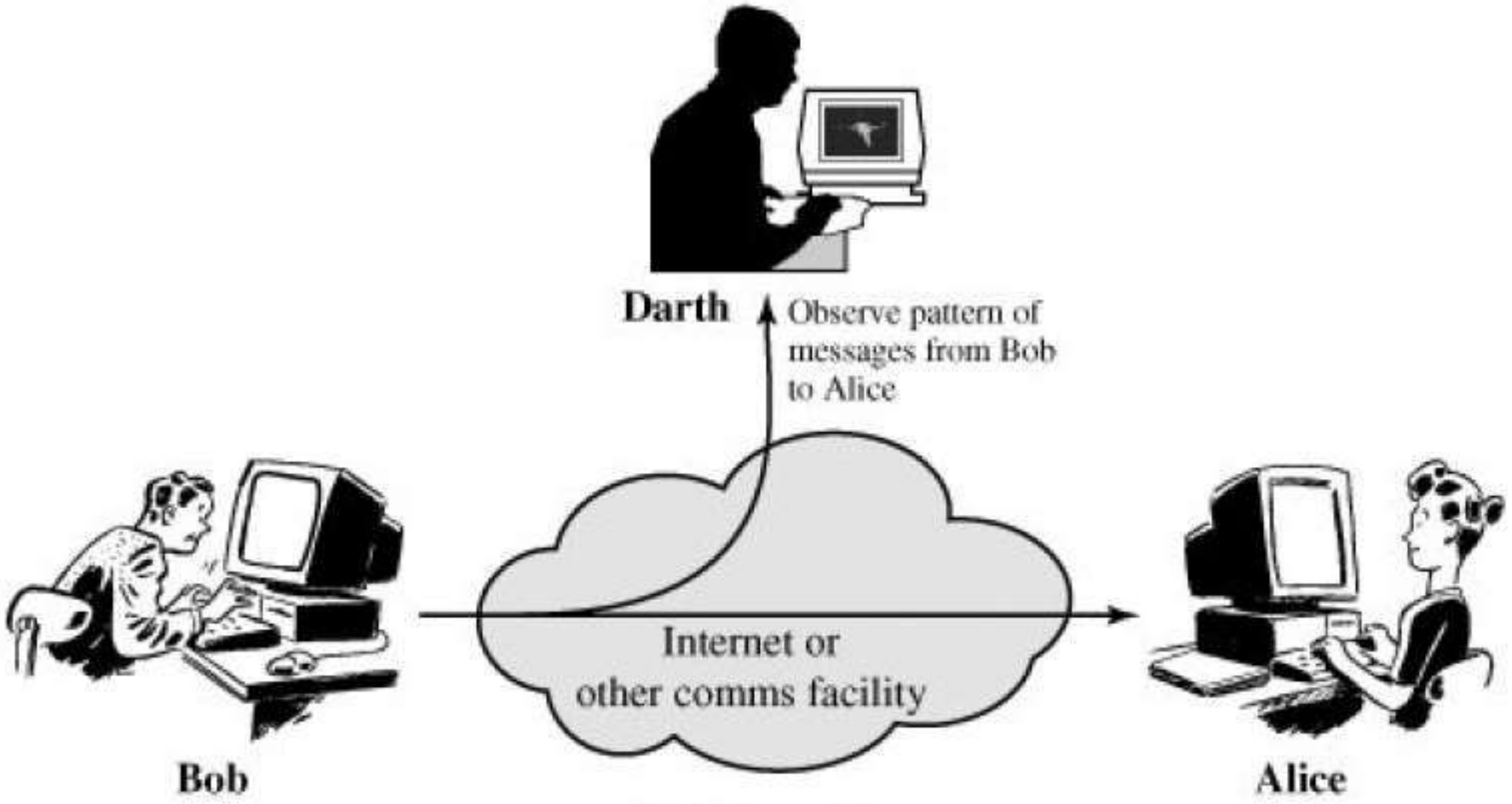
  - traffic analysis

Passive Attack (a) Release of message Contents


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

This attacker happens when confidential user data are released publicly over the network.

Passive Attack (b) Traffic analysis


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

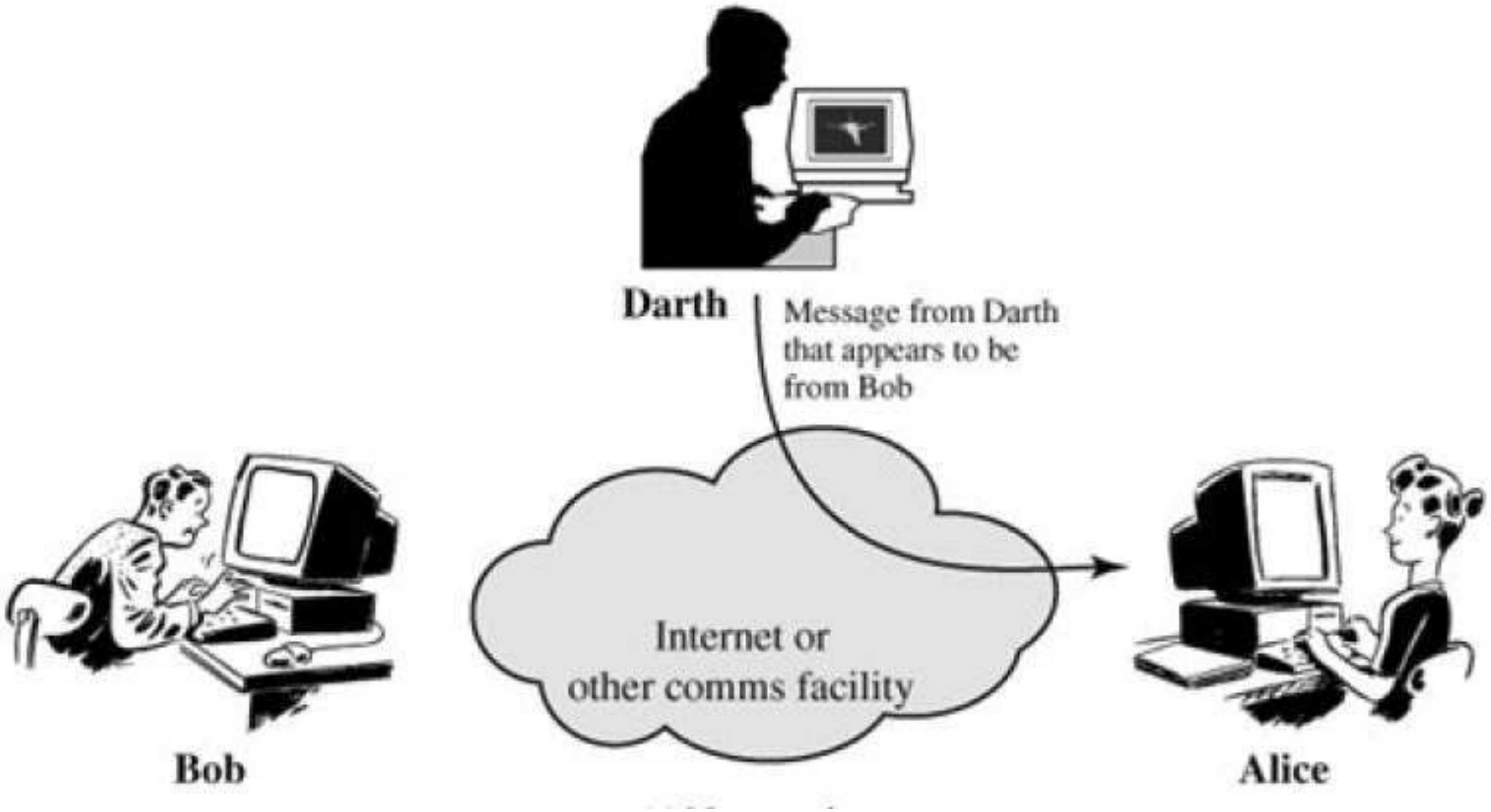
Take SSH(*Secure Socket Shell)*, for example. Every time you press a key on your keyboard, SSH sends a separate IP packet. By analyzing these packets, an attacker can distinguish the timing between key presses. They can then use this information then, for example, **to guess users' password lengths**.

Active Attacks

- Active attacks involve some modification of the data stream or the creation of a false stream
- It can be subdivided into four categories:

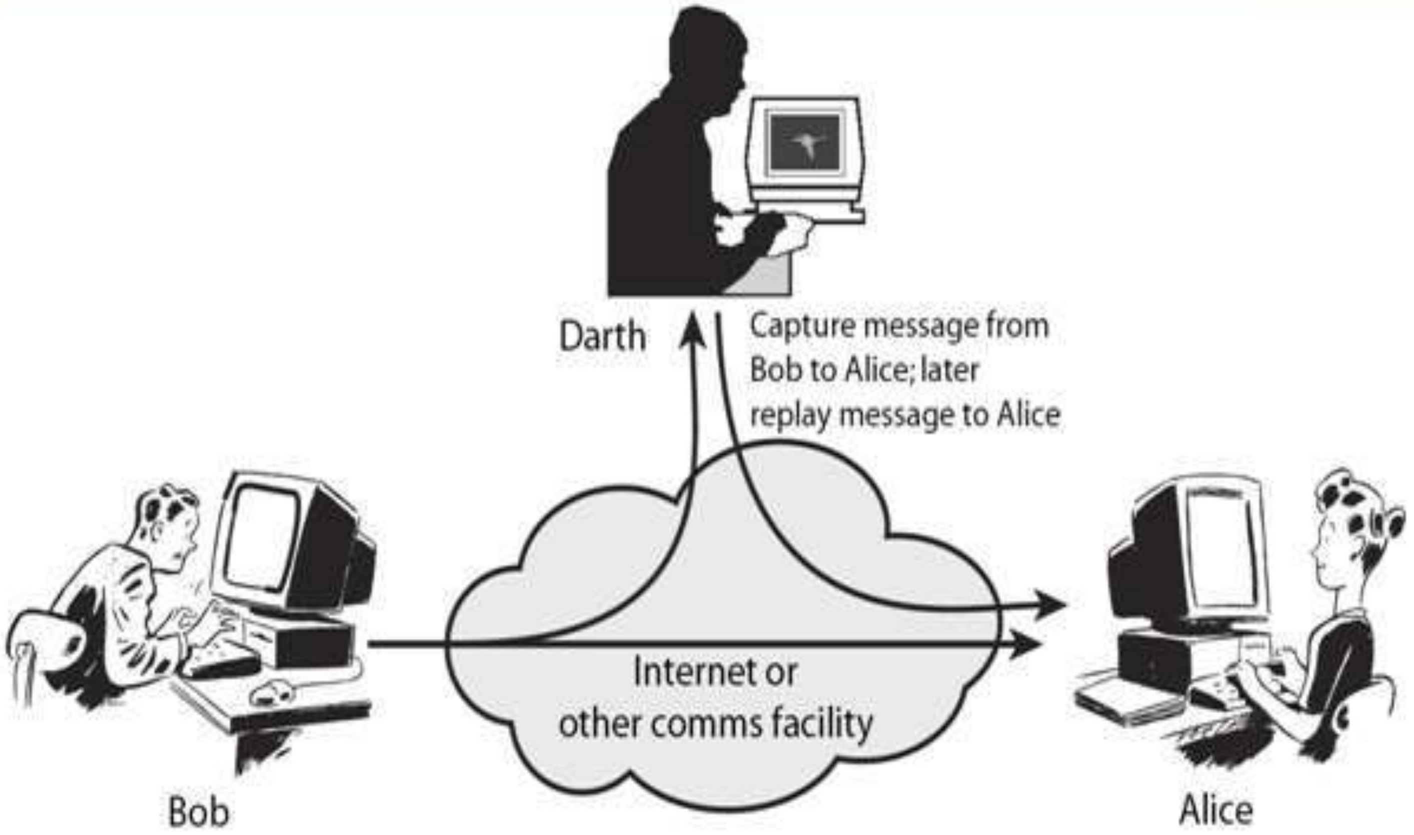
  - masquerade
  - replay
  - modification of messages
  - denial of service.

Active Attacks (a) Masquerade

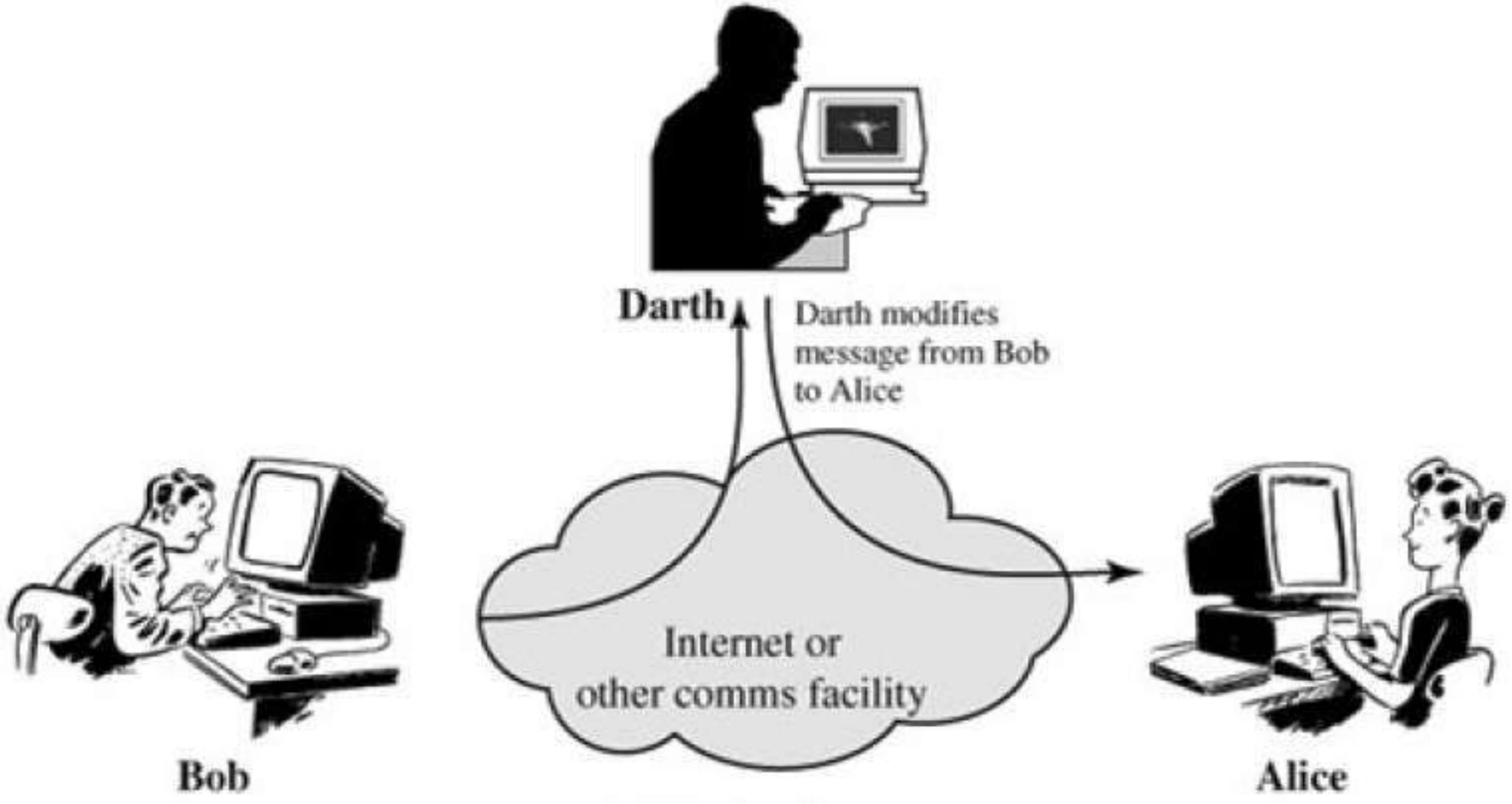

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

A masquerade attack is an online attack in which the attacker masquerades as a legitimate user to gain access to a device.

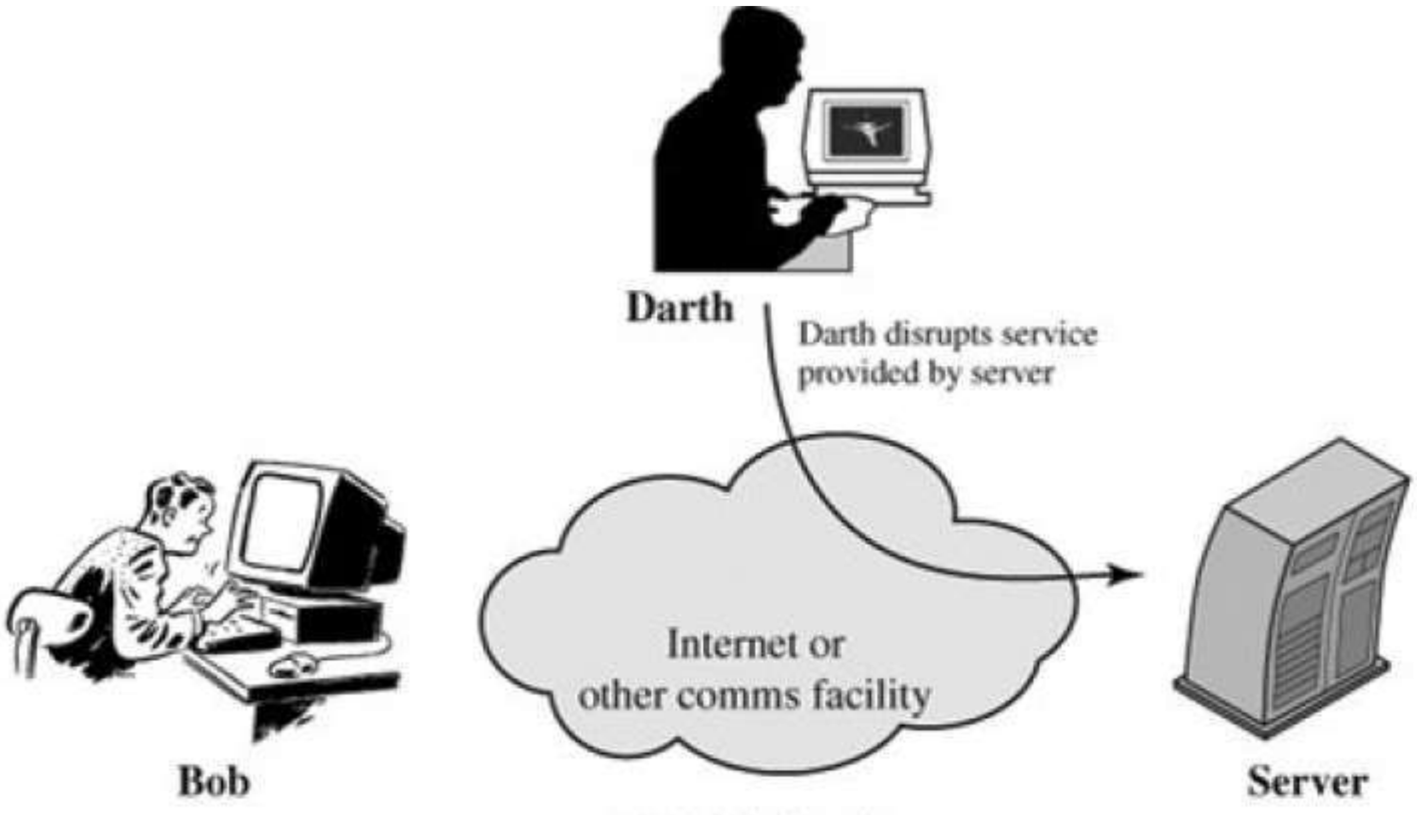
Active Attacks (b) Replay


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

Active Attacks (c) Modification of messages


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Active Attacks (d) Denial of service


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.