# Common Types of Network Attacks

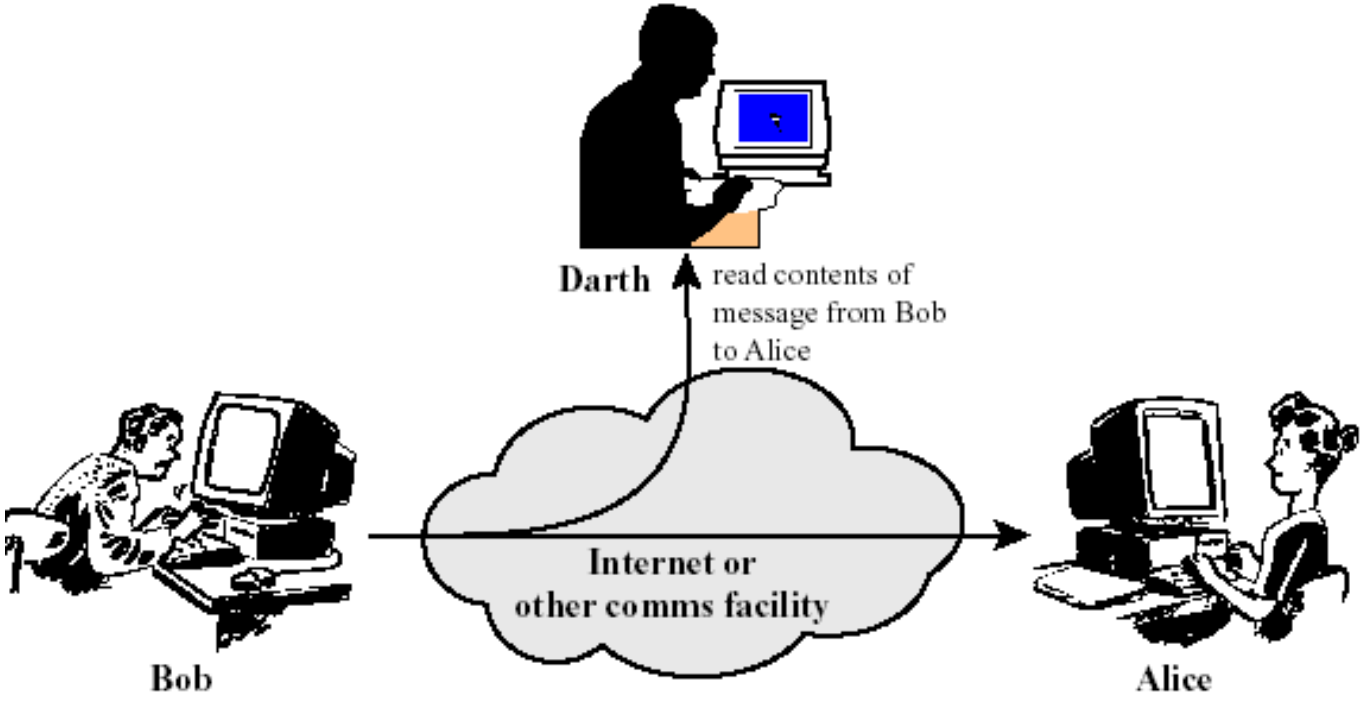
# Common Types of Network Attacks

- Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

# Passive and active attacks

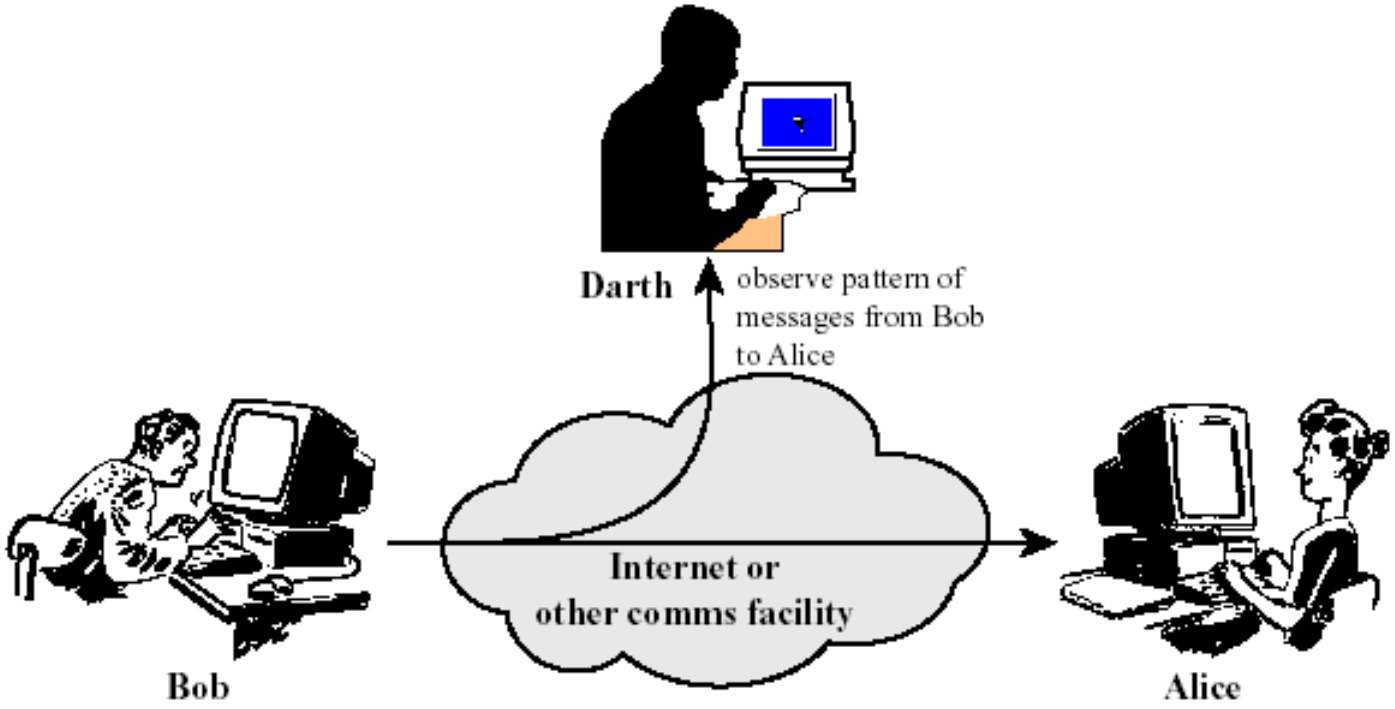
- **Passive attacks**
  - No modification of content or fabrication
  - Eavesdropping to learn contents or other information (transfer patterns, traffic flows etc.)
- **Active attacks**
  - Modification of content and/or participation in communication to
    - Impersonate legitimate parties
    - Modify the content in transit
    - Launch denial of service attacks

# Passive Attacks



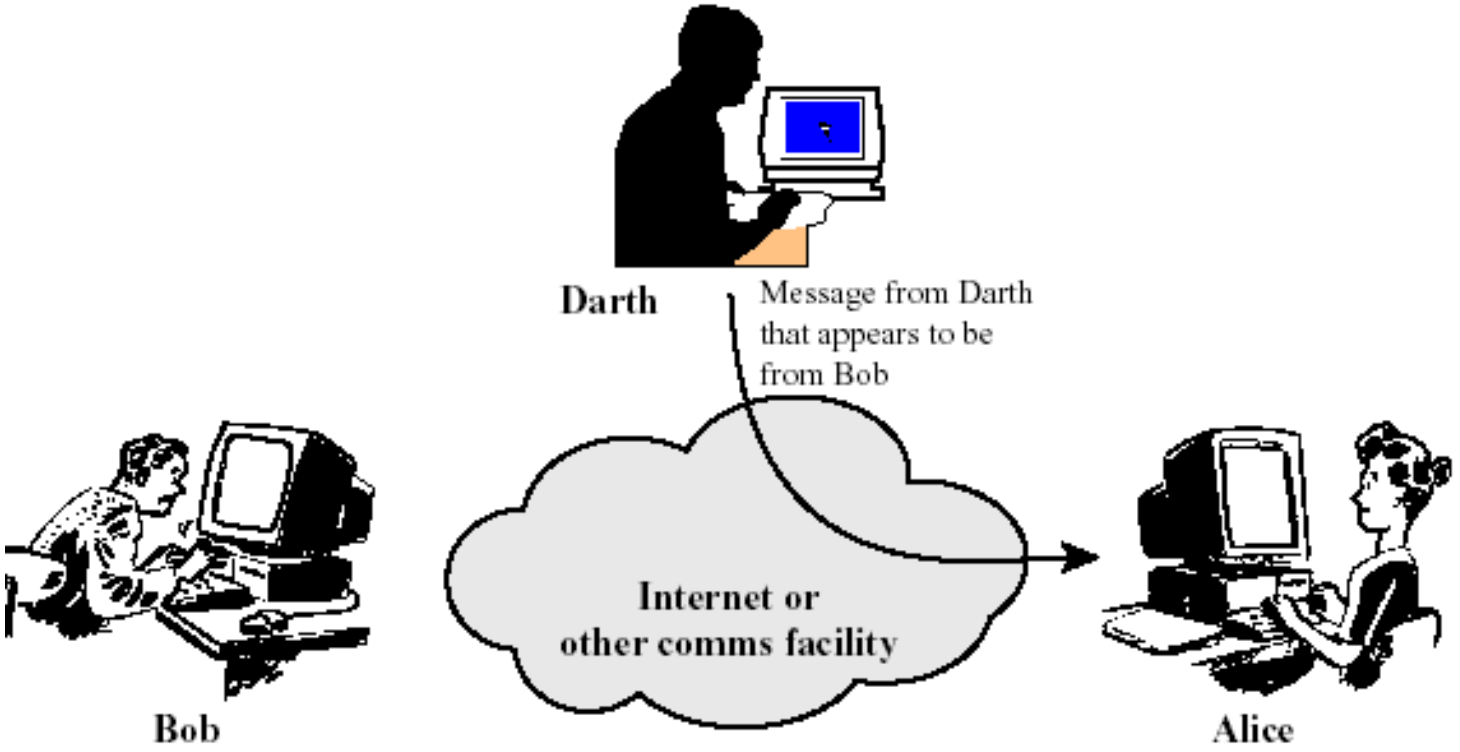

(a) Release of message contents

# Passive Attacks



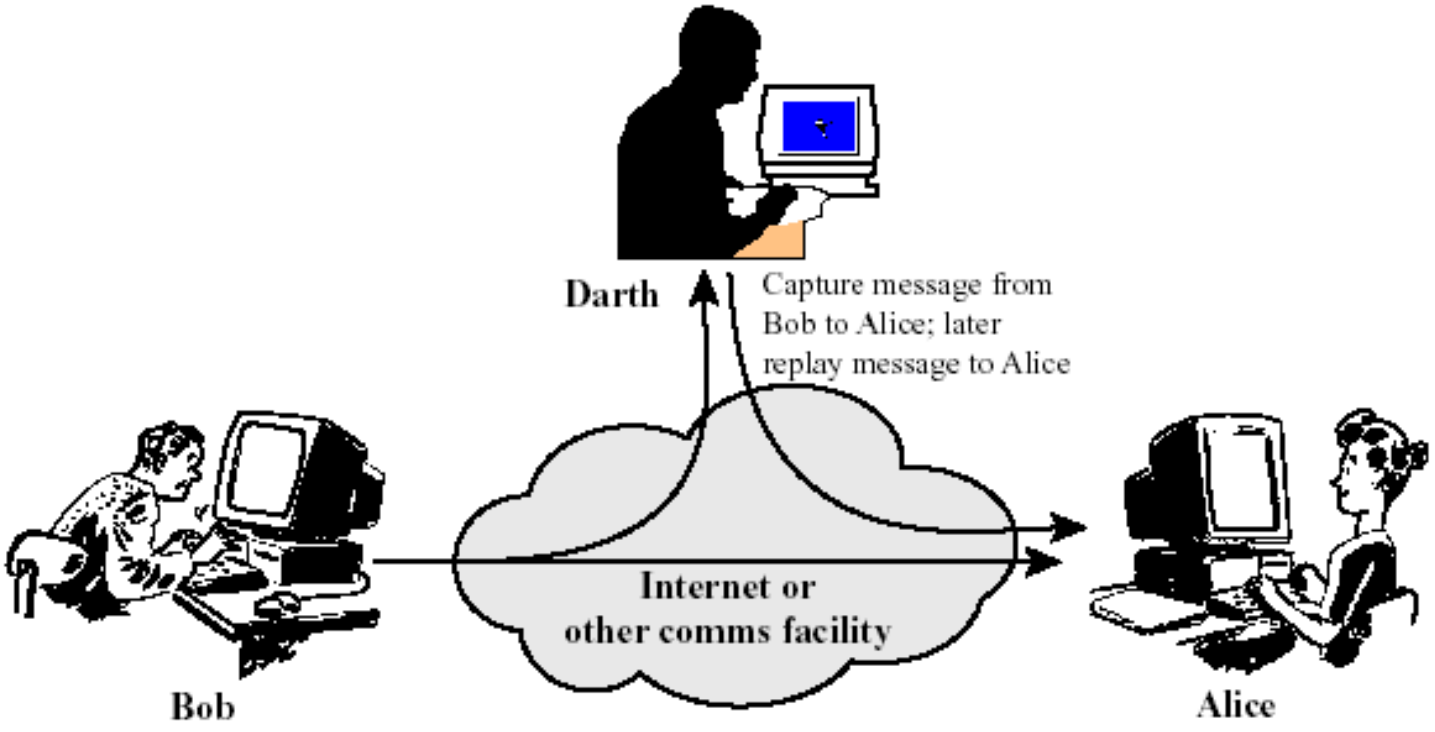

(b) Traffic analysis

# Active Attacks




(a) Masquerade

# Active Attacks




(b) Replay

Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

- Eavesdropping
- Majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic.
- When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

# Common Types of Network Attacks (Continue…)

- Data Modification
- After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver.

# Common Types of Network Attacks (Continue…)

- Identity Spoofing (IP Address Spoofing)
- Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing.
- After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data.

# Common Types of Network Attacks (Continue…)

- Password-Based Attacks
- A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.
- If an attacker gain/guess your password, then?

# Common Types of Network Attacks (Continue…)

- Denial-of-Service Attack
- denial-of-service attack prevents normal use of your computer or network by valid users.
- After gaining access to your network, the attacker can do any of the following:
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

# Common Types of Network Attacks (Continue…)

- Man-in-the-Middle Attack
- As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange.
- Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information.

# Common Attacks on Encrypted Schemes

- cipher text only
- known plain text //compromise Key
- chosen plain text //compromise key