Vulnerabilities, Attacks, and Countermeasures

TCS 591 : UNIT 2

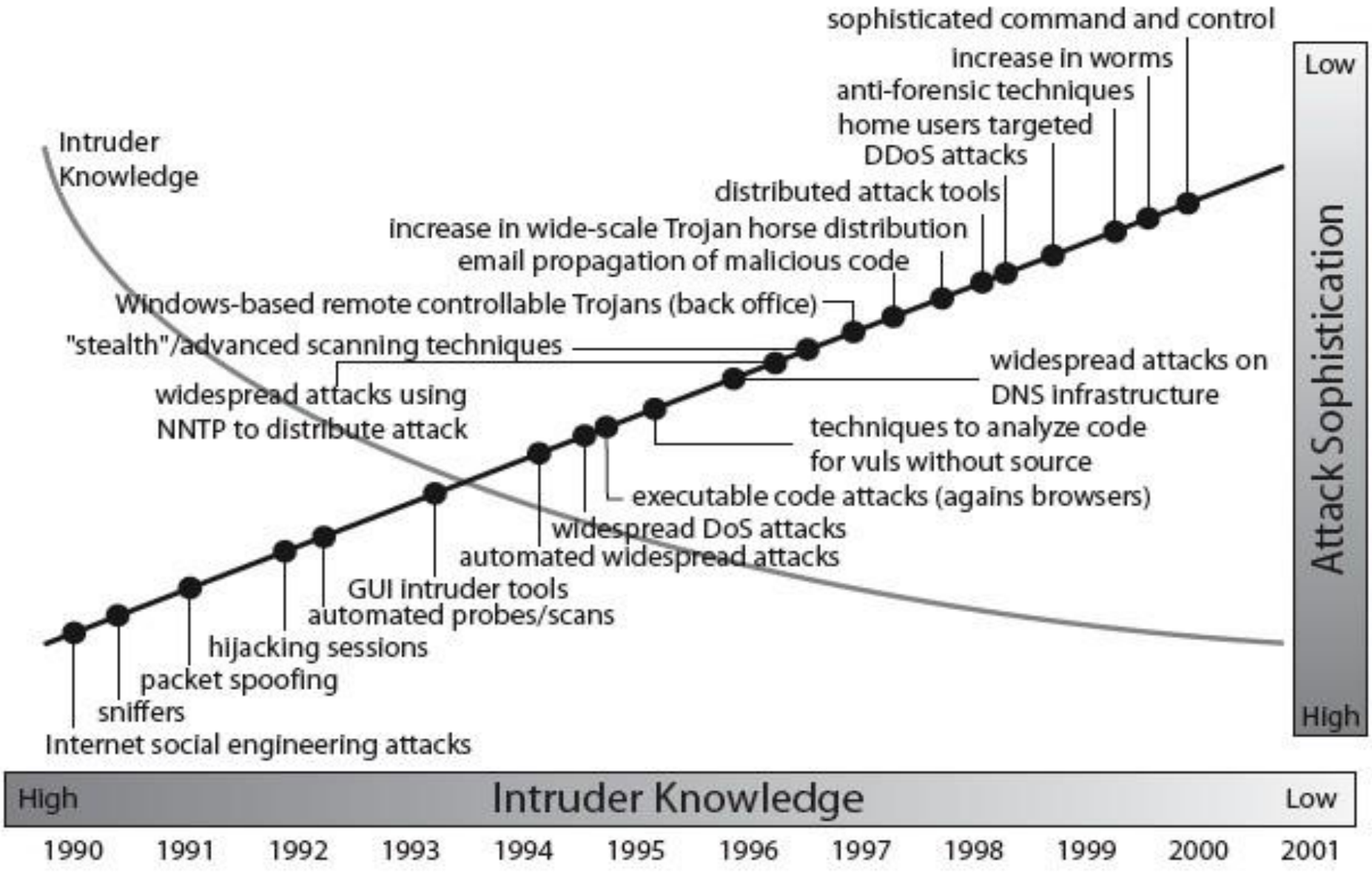
What is Computer System Vulnerability?

- A computer system vulnerability **is a flaw or weakness** in a system or network that could be exploited to cause damage, or allow an attacker to manipulate the system in some way.

Difference Between "Cyber Threat" and "Vulnerability"

- Vulnerability is different from a "cyber threat" in that while a cyber threat may involve an outside element, computer system vulnerabilities exist on the network asset (for example, a computer, database, or even a specific application).
- Vulnerabilities are not usually the result of intentional effort by an attacker—though cybercriminals will leverage these flaws in their attacks.

Security Trends



Source: CERT

Three Aspects of Information Security

- **Security Attack**
  - Any action that compromises the security of information.
- **Security Mechanism**
  - A mechanism that is designed to detect, prevent, or
  - recover from a security attack.
- **Security Service**
  - A service that enhances the security of data processing systems and information transfers.
    - Makes use of one or more security mechanisms.

Types of Attacks

- Active Attack
- Passive Attack

Passive Attack

- A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities.
- The purpose is solely to gain information about the target and no data is changed on the target.

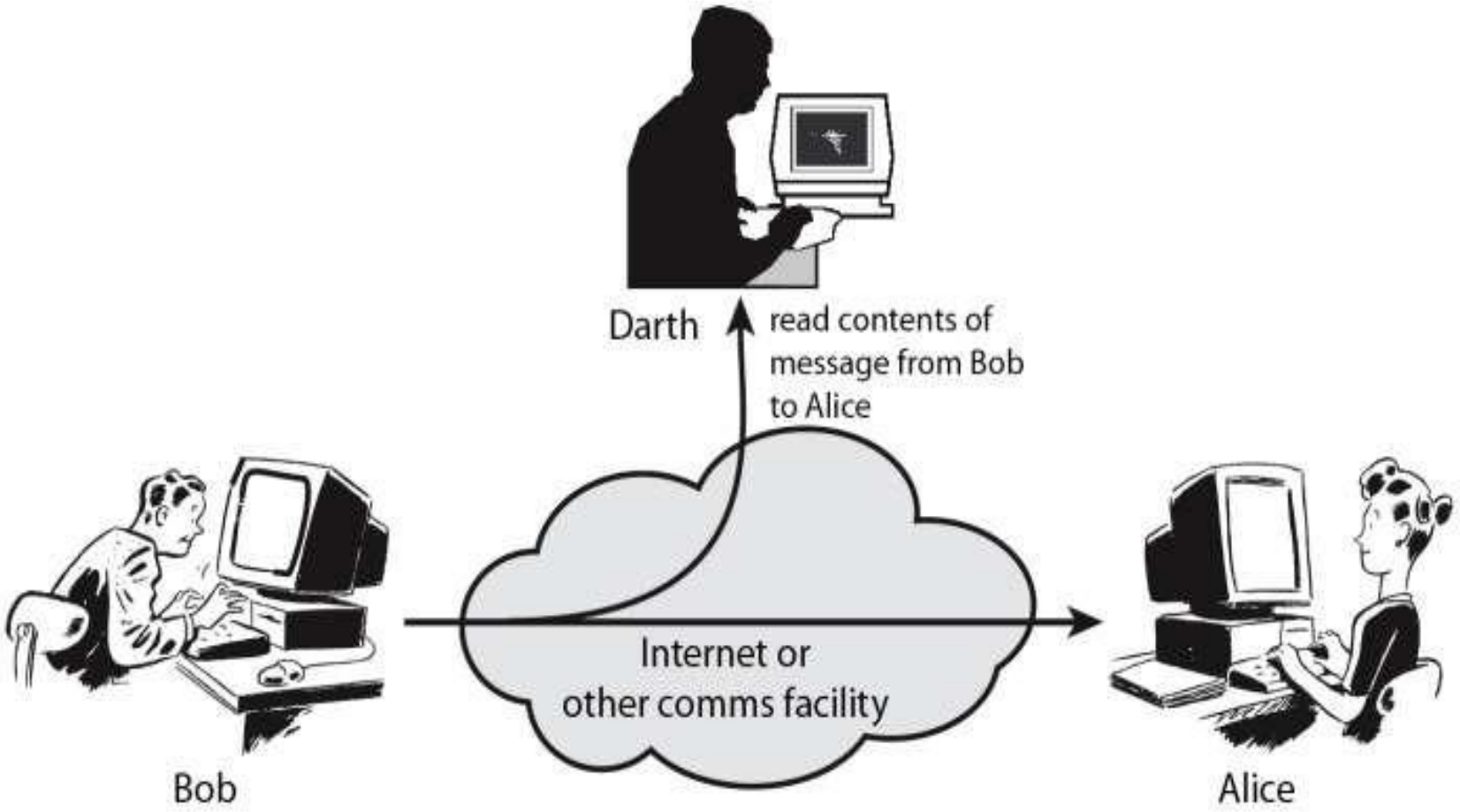
Active & Passive Reconnaissance

- In passive reconnaissance, an intruder monitors systems for vulnerabilities without interaction, through methods like session capture.
- In active reconnaissance, the intruder engages with the target system through methods like port scans.

Types of Passive Attack

- Interception Attack
- Traffic Analysis Attack

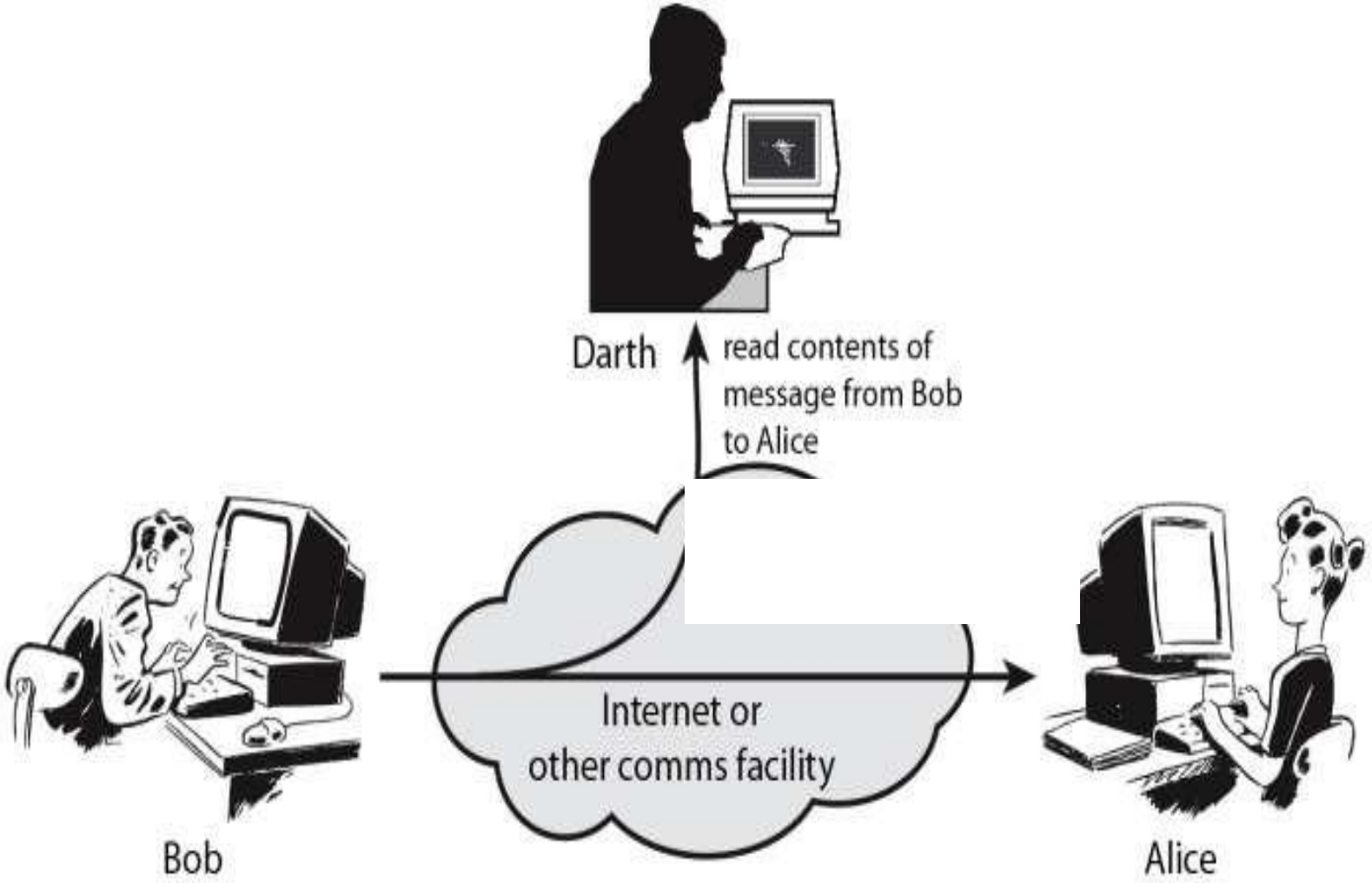
Interception Passive Attack



Interception Passive Attack

- The data or message which is sent by the sender is intercepted by an unauthorized individual where the message will be changed to the different form or it will be used by the individual for his malicious process.
- So the confidentiality of the message is lost in this type of attack.
- It is also known as “Release of message contents”.

Traffic Analysis



Traffic Analysis Passive Attack

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security.

Active Attacks

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en-route to the target.

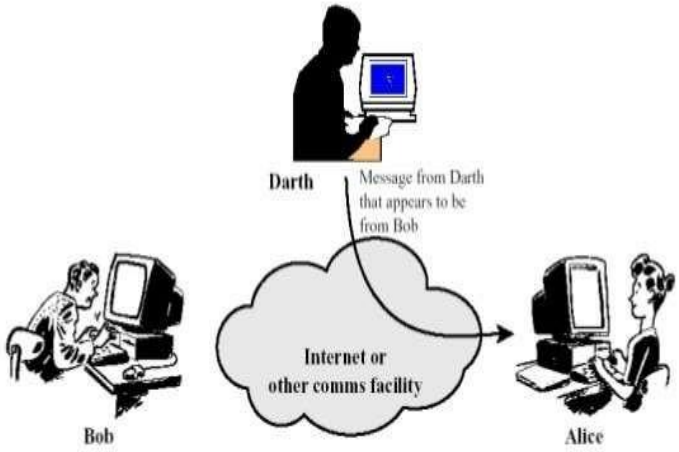
Types of Active Attacks

- **Masquerade Attack**
- **Interruption Attack**
- **Fabrication Attack**
- **Session Replay Attack**
- **Modification Attack**
- **Denial of Service (DOS) Attack**

Masquerade

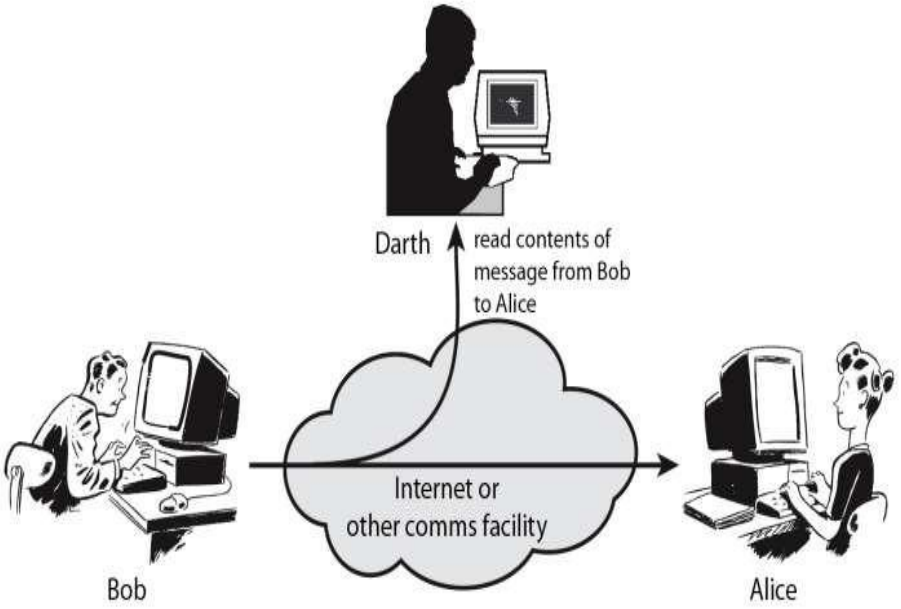
- In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for.

A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.



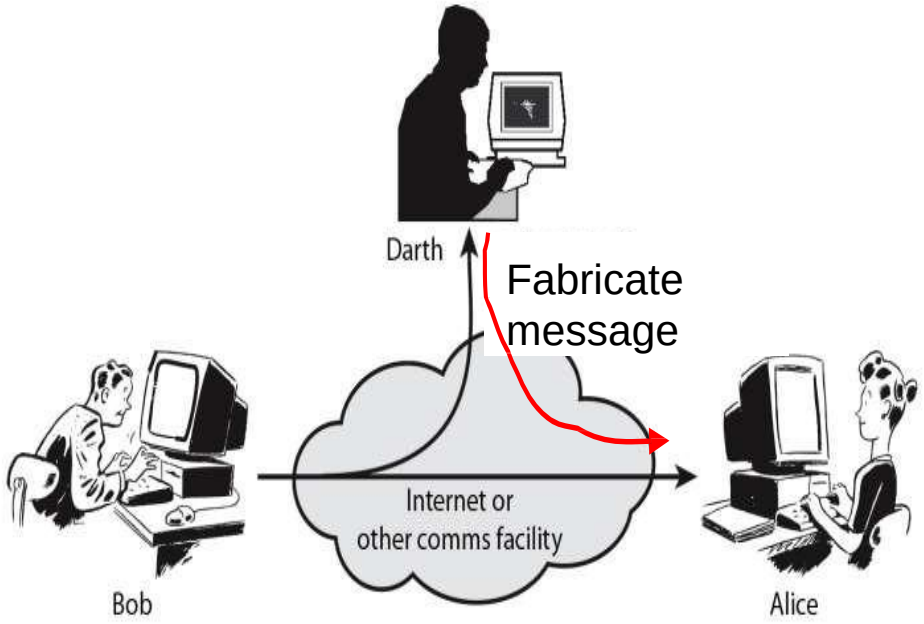
Interruption

- This type of attack is due to the obstruction of any kind during the communication process between one or more systems. So the systems which are used become unusable after this attack by the unauthorized users which results in the wastage of systems.



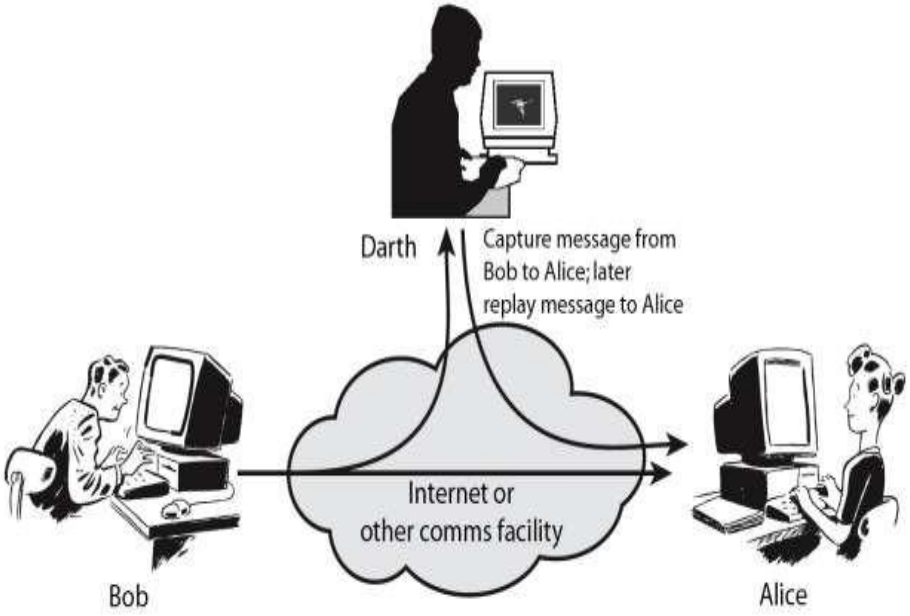
Fabrication

- In this type of attack a fake message is inserted into the network by an unauthorized user as if it is a valid user. This results in the loss of confidentiality, authenticity and integrity of the message.



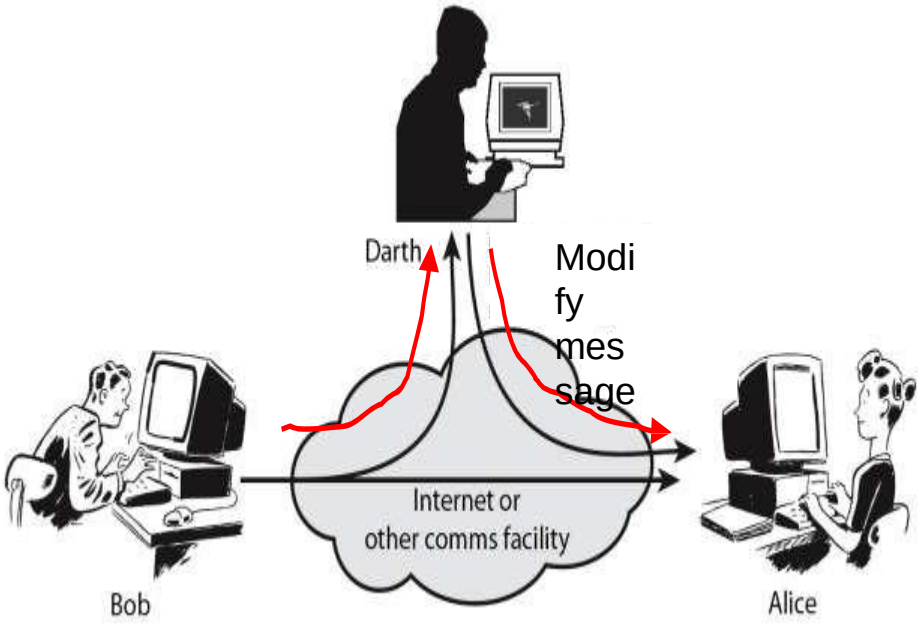
Session Replay

- In a session replay attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.



Modification

- In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.



Denial of Service (DOS)

- In a denial of service (DoS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.