Department of CSE

COURSE NAME: DBMS
COURSE CODE:23AD2102R

Topic: Security Considerations in DBMS, Access Control, Encryption, Intrusion Detection Systems(IDS)

Session – 6

AIM OF THE SESSION

To familiarize students with the basic concepts of Security considerations of DBMS

INSTRUCTIONAL OBJECTIVES

This Session is designed to: discuss and study the concepts of Security considerations of DBMS

LEARNING OUTCOMES

At the end of this session, you should be able to: understand Security considerations of DBMS

ENCRYPTION AND INTRUSION DETECTION

- **Data encryption** is the process of converting readable data, known as **plaintext**, into an encoded form, known as **ciphertext**.
- This transformation makes data unintelligible to unauthorized individuals, **protecting sensitive information from unauthorized access or disclosure.**

Key Objective of Encryption Data

- **Confidentiality:** Encryption ensures that only authorized parties can get access to data and recognize the information.
- **Data Integrity:** Encryption can also provide data integrity by making sure that the encrypted data remains unchanged during transmission. Any unauthorized changes to the encrypted information will render it undecipherable or will fail integrity checks.
- **Authentication:** Encryption may be used as part of authentication mechanisms to verify the identification of the communication party.
- **Non-Repudiation:** Through encryption, events can make sure that they cannot deny their involvement in growing or sending a selected piece of data.

Importance of Data Encryption

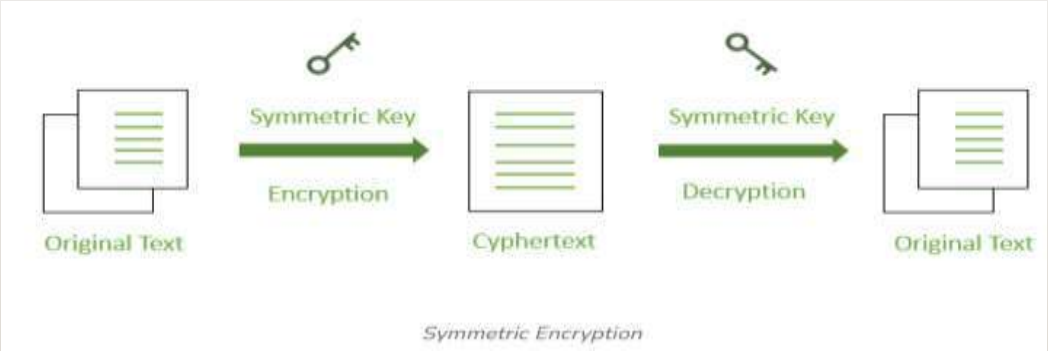
The significance of encryption cannot be overstated in any way. Even though your data is stored in a standard infrastructure, it is still possible for it to be hacked. There's always the chance that data will be compromised, but with data encryption, your information will be much more secure. Consider it this way for a moment. If your data is stored in a secure system, encrypting it before sending it out will keep it safe. Sanctioned systems do not provide the same level of protection.

So, how do you think this would play out in real life?

Suppose the user has access to sensitive information while at work. The user may put the information on a portable disc and move it anywhere they choose without any encryption. If the encryptions are set in place ahead of time, the user can still copy the information, but the data will be unintelligible when they try to see it someplace else. These are the benefits of data encryption that demonstrate its genuine value.

Types of Data Encryption

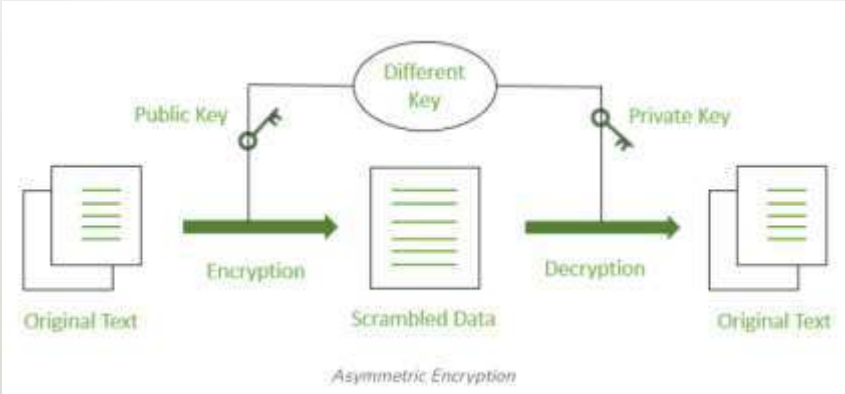
1. **Symmetric Encryption**: Uses a single key for both encryption and decryption. It is fast and suitable for encrypting large volumes of data but requires secure key distribution.
    - **Examples**: AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple DES).



Symmetric Encryption

2. **Asymmetric Encryption**: Uses a pair of keys — a public key for encryption and a private key for decryption. It is slower but provides a more secure way to share keys.

   - **Examples**: RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography).



Asymmetric Encryption

States of Data Encryption

1. **Data at Rest**: Data stored on devices such as hard drives, databases, and mobile devices. This data can be encrypted to protect it from unauthorized access if the device is stolen or compromised.
2. **Data in Transit**: Data moving between locations, such as across the internet or a network. Encryption is used to protect this data from interception and eavesdropping during transmission.
3. **Data in Use**: Data actively being processed by applications. Encrypting data in use is more complex, but techniques like homomorphic encryption can enable processing without decryption.

Data Encryption Algorithms

Some widely used encryption algorithms include:

- **AES (Advanced Encryption Standard)**: A symmetric key algorithm commonly used for securing sensitive data.
- **RSA**: An asymmetric encryption algorithm often used for secure data transmission and key exchange.
- **Blowfish**: A fast symmetric encryption algorithm known for its efficiency and flexibility.
- **Elliptic Curve Cryptography (ECC)**: Uses shorter keys for encryption, providing equivalent security with less computational power than RSA.
- **Twofish**: A symmetric key algorithm known for its speed and suitability for hardware and software.

Intrusion Detection

Intrusion detection is the process of monitoring and analyzing network or system activities for malicious activities or policy violations. An intrusion detection system (IDS) collects information from various network points to identify possible security breaches, which can include attempts to break into systems, misuse of resources, or attacks on networks.

Example of Intrusion Detection: An IDS may be configured to detect abnormal traffic patterns, such as a large volume of data suddenly being sent from a particular server. For instance, if an attacker tries to gain unauthorized access by brute-forcing login attempts, the IDS can recognize the unusual number of failed login attempts and flag this as suspicious. It can then alert administrators, who can take action to block the IP or further investigate the incident.

Types of Intrusion Detection Systems (IDS)

There are two primary types of IDS:

1. **Network-based IDS (NIDS)**: Monitors and analyzes network traffic for signs of suspicious activities by inspecting data packets. NIDS often sit at strategic points within the network, such as routers or switches, to provide visibility into the entire network's traffic.
2. **Host-based IDS (HIDS)**: Monitors activities on individual devices or hosts, including user activities, file modifications, and system logs. HIDS is installed on specific systems and provides a detailed view of potential threats on that particular device.

There are several types of intrusion detection systems (IDS), including:

Host-based IDS (HIDS)

Scans a single system for changes to system files and unusual behavior

Network-based IDS (NIDS)

Scans an entire network for malicious packets and changes in regular traffic

Signature-based IDS

Compares incoming traffic to signatures of known threats in a database of known malware

Anomaly-based IDS

Uses machine learning to identify anomalies and improve the accuracy of detecting security attacks

Hybrid IDS

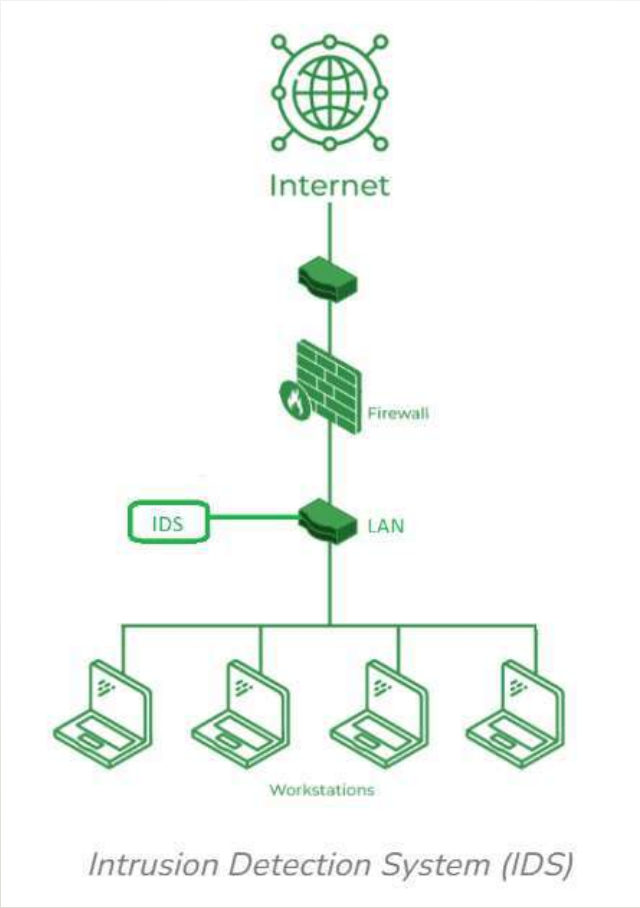
Combines two or more intrusion detection approaches to provide a comprehensive view of the network system

Protocol-based IDS (PIDS)

Interprets the protocols between the server and the user to monitor the HTTPS server

SIEM

Analyzes events and identifies suspicious events, sending an automated report to security officials



Intrusion Detection System (IDS)

Methods of Intrusion Detection

1. **Signature-based Detection**: Relies on known patterns of malicious activity, known as signatures, to detect intrusions. It is effective at identifying known threats but may fail to detect novel or unknown attacks.
2. **Anomaly-based Detection**: Establishes a baseline of "normal" behavior and flags activities that significantly deviate from this baseline. Anomaly-based IDS can detect unknown threats, but it may produce false positives if normal activities fall outside the established baseline.

Example of Intrusion Detection in Action

Imagine a company network where employees regularly access an internal file server for work. This system typically records user access patterns, such as file reads, edits, and uploads. The organization has set up an IDS to detect unusual activities that deviate from these patterns.

Scenario:

An attacker attempts to infiltrate the network by obtaining the credentials of an employee through a phishing attack. Using these credentials, the attacker logs into the system and attempts to copy a large number of files from the file server to an external IP address.

Intrusion Detection Process:

1. **Baseline of Normal Behavior**: The IDS already has a baseline of normal employee access patterns, including the usual login times, locations, and the typical number of files accessed.

2. **Anomalous Activity Detected**: The IDS notices that the employee's account is accessing the file server outside of usual work hours. Additionally, the account is downloading a significantly larger number of files than usual and attempting to send them to an unfamiliar IP address.

3. **Alert and Action**: Recognizing this as suspicious activity, the IDS triggers an alert to notify the network administrator. The IDS logs detail the time of the anomaly, the files accessed, and the IP address to which the data was being sent. This information can assist the administrator in verifying whether this was a legitimate user or an unauthorized intrusion attempt.
4. **Response**: Upon investigation, the administrator confirms that this activity is indeed an intrusion. The administrator can then take actions such as blocking the IP address, revoking the compromised user credentials, and launching a deeper investigation to prevent further data loss.

Conclusion

Intrusion Detection System (IDS) is a powerful tool that can help businesses in detecting and prevent unauthorized access to their network. By analyzing network traffic patterns, IDS can identify any suspicious activities and alert the system administrator. IDS can be a valuable addition to any organization's security infrastructure, providing insights and improving network performance.

CYBER ATTACK

- A **cyber attack** occurs **when hackers try to penetrate computer systems or networks with a personal agenda** or **some purpose to damage or steal information by gaining unauthorized access to computer systems**. It can occur to anyone, either companies or government agencies, which can then have stolen data and financial losses.

Attack:-Gaining the access of data by unauthorized user

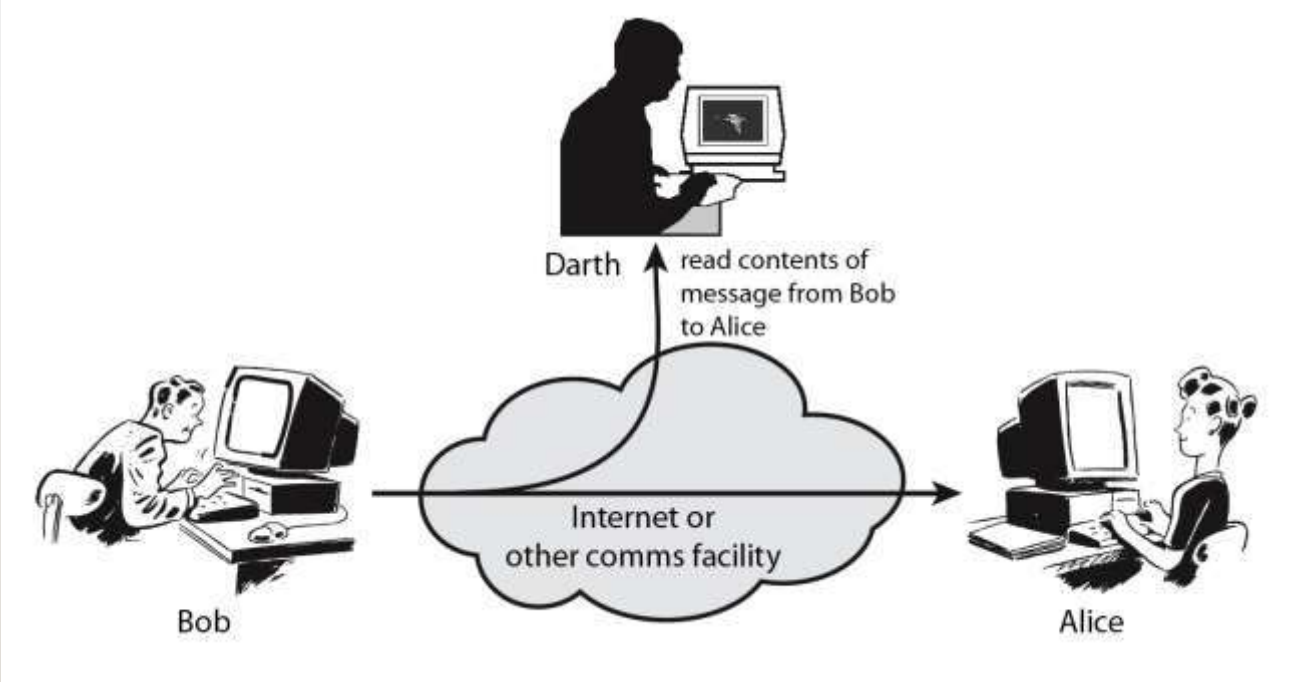
Passive Attacks

- A **Passive Attack** in cryptography and network security is a type of attack where an **unauthorized person intercepts or monitors communications without altering the data**.
- The **primary goal** of passive attacks is to gather information rather than to disrupt communication or harm systems. Because passive attacks don't change data, they are often harder to detect than active attacks.

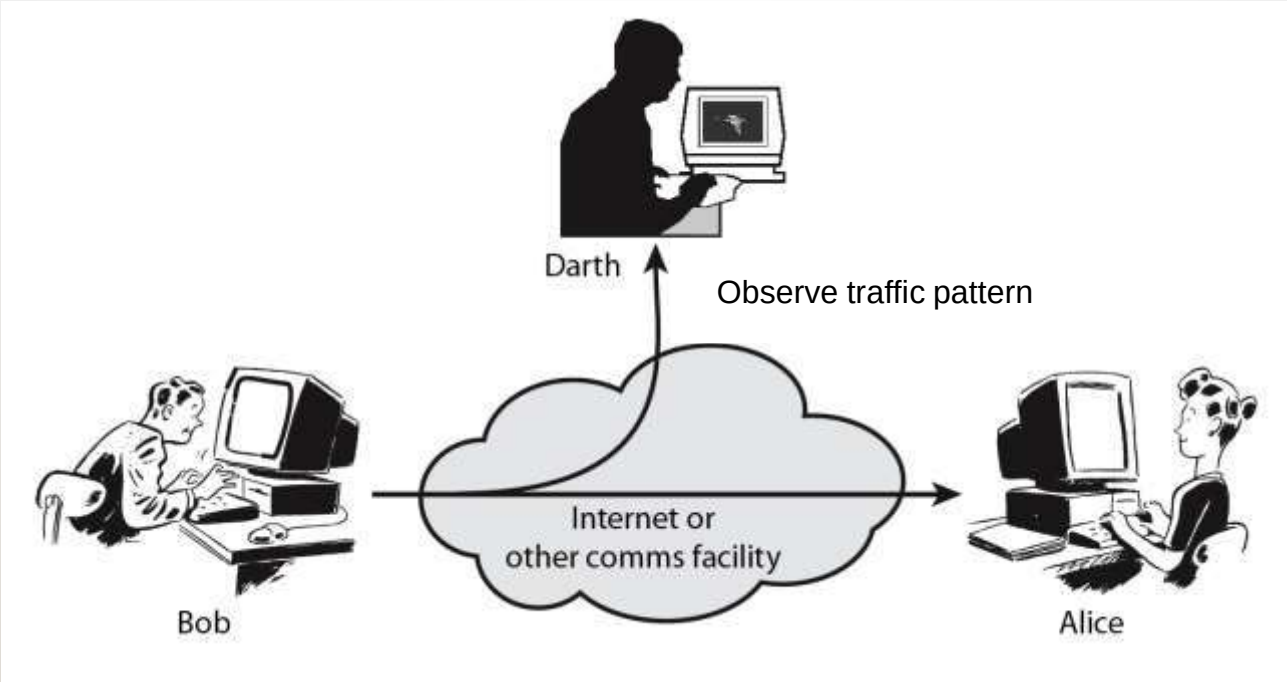
There are two main types of passive attacks:

1. **Eavesdropping or Interception**: The attacker listens in on communication channels to obtain sensitive information.
2. **Traffic Analysis**: The attacker observes the patterns, timings, or frequency of communications, which can reveal valuable information about network activity or organizational structure.

Passive Attack - Interception



Passive Attack: Traffic Analysis



Effects of Passive Attacks

Even though passive attacks don't modify data, they can lead to significant security risks, as the attacker may gather:

- Confidential information (e.g., passwords, messages).
- Organizational or user behavioral patterns, which can be used in later active attacks.

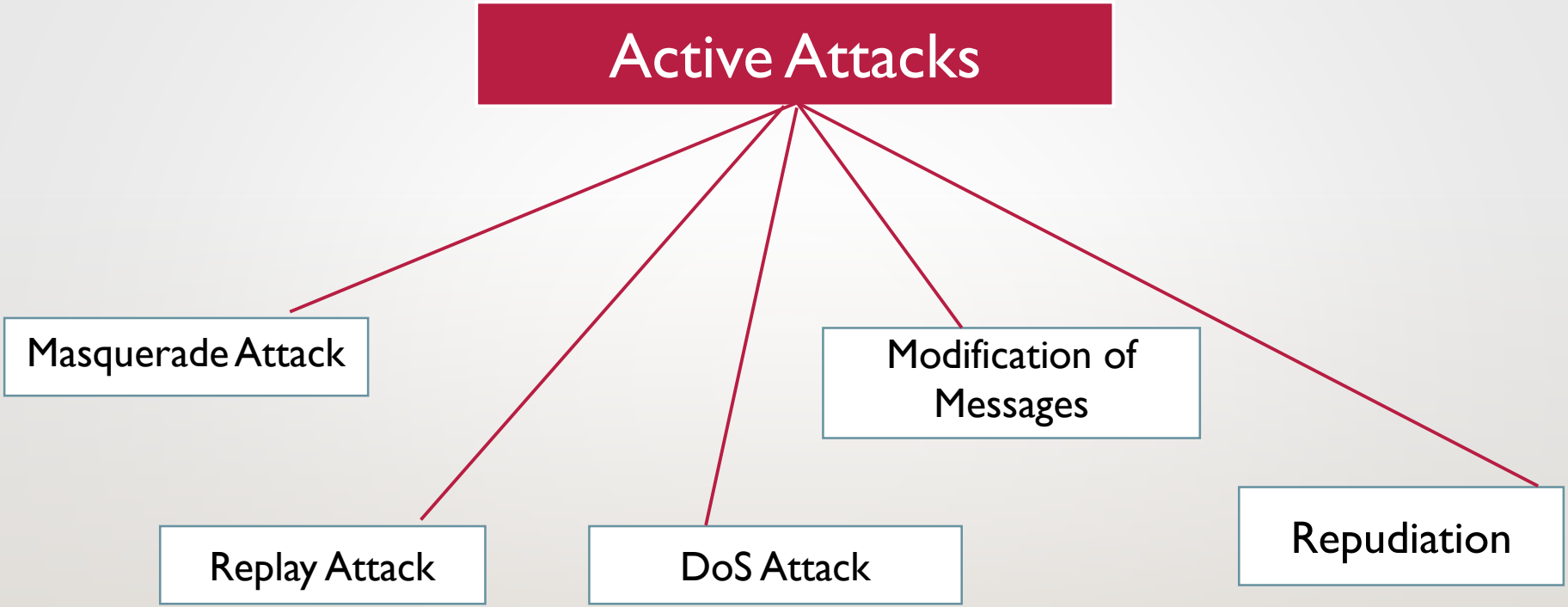
Prevention Measures

To protect against passive attacks, organizations and users can:

- **Use Encryption**: Encrypting data in transit (such as HTTPS for web traffic) makes intercepted data unreadable to attackers.
- **Secure Network Access**: Using secure networks (avoiding open or unencrypted Wi-Fi) and VPNs reduces the chances of data interception.
- **Implement Secure Protocols**: Using secure protocols like SSL/TLS for communication adds a layer of security against interception.

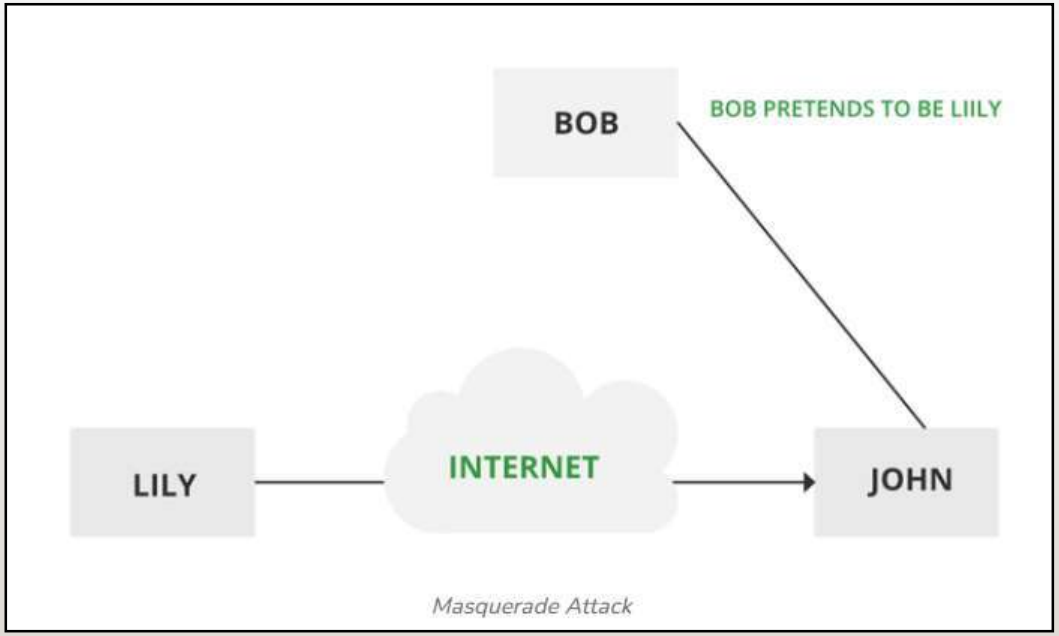
Active Attacks

- **Active attacks** are **unauthorized actions** that **alter the system or data**.
- In an **active attack**, the attacker will **directly interfere with the target** to damage or gain unauthorized access to **computer systems** and networks.
- This is done by **injecting hostile code into communications**, masquerading as another user, or altering data to get unauthorized access.


Active Attacks
Masquerade Attack
Modification of Messages
Replay Attack
DoS Attack
Repudiation

Masquerade Attack

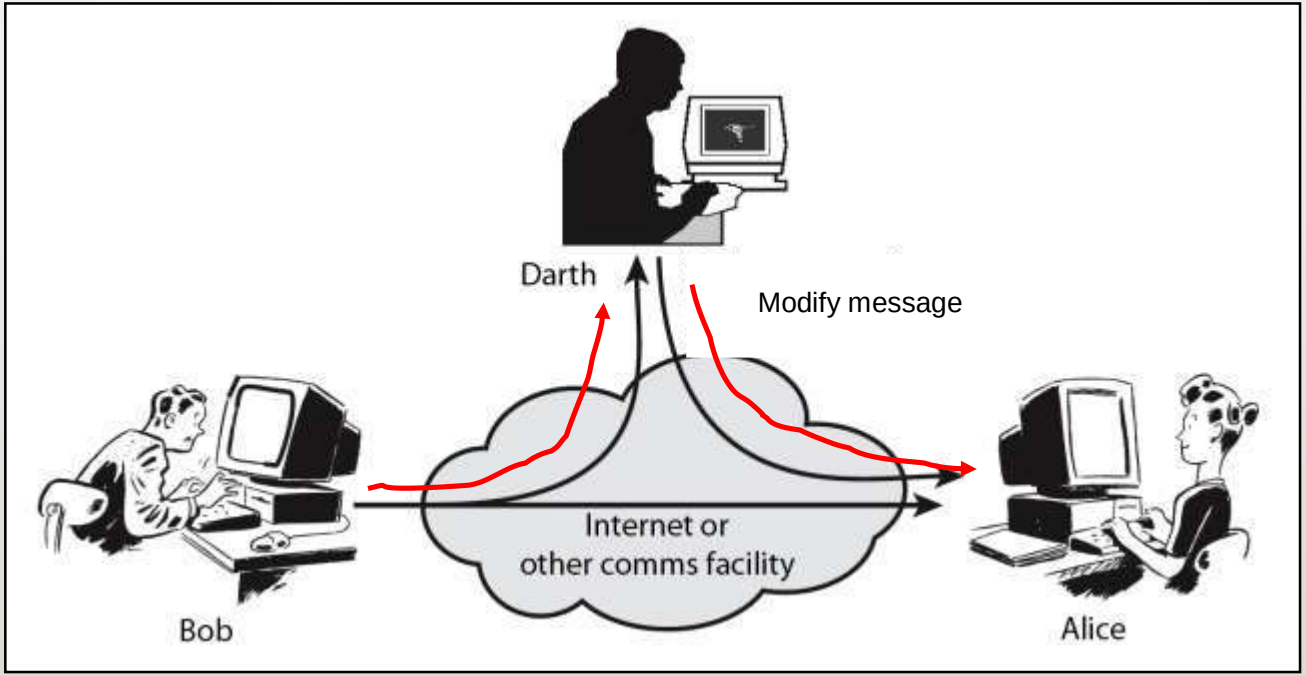
The attacker pretends to be an authorized user



Masquerade Attack

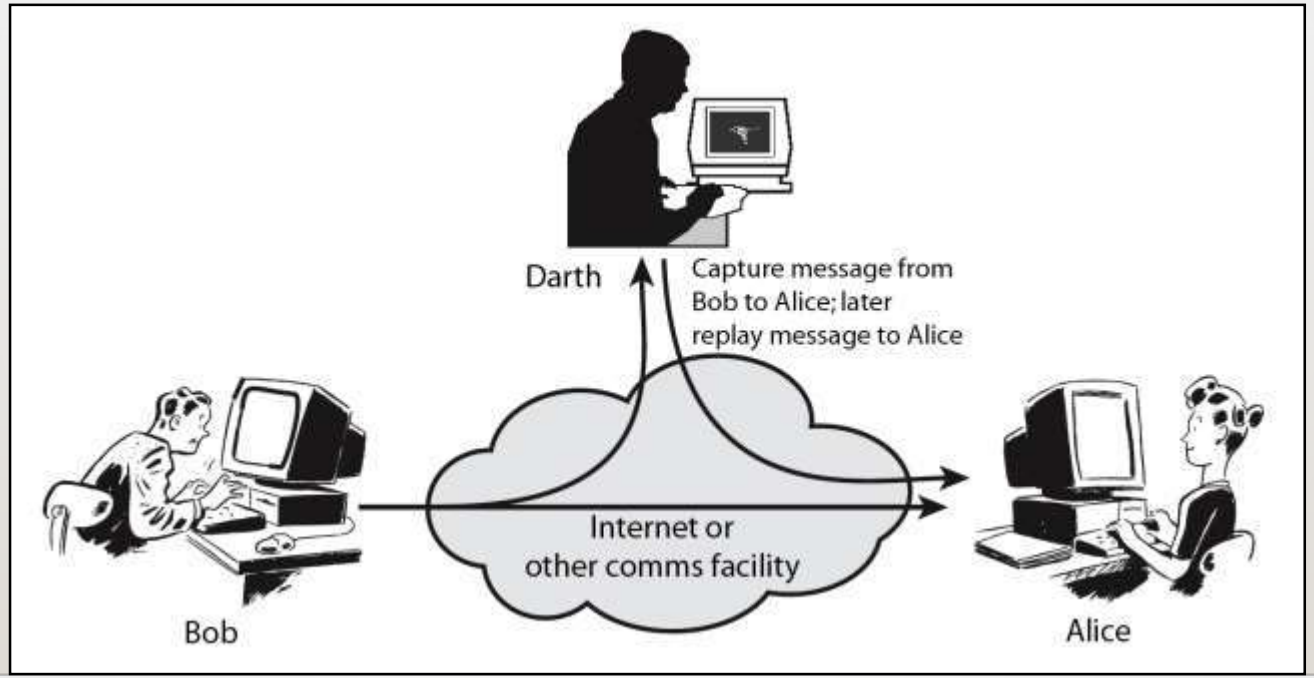
Active Attack: Modification

The attacker alters the contents of a message being sent over a network.

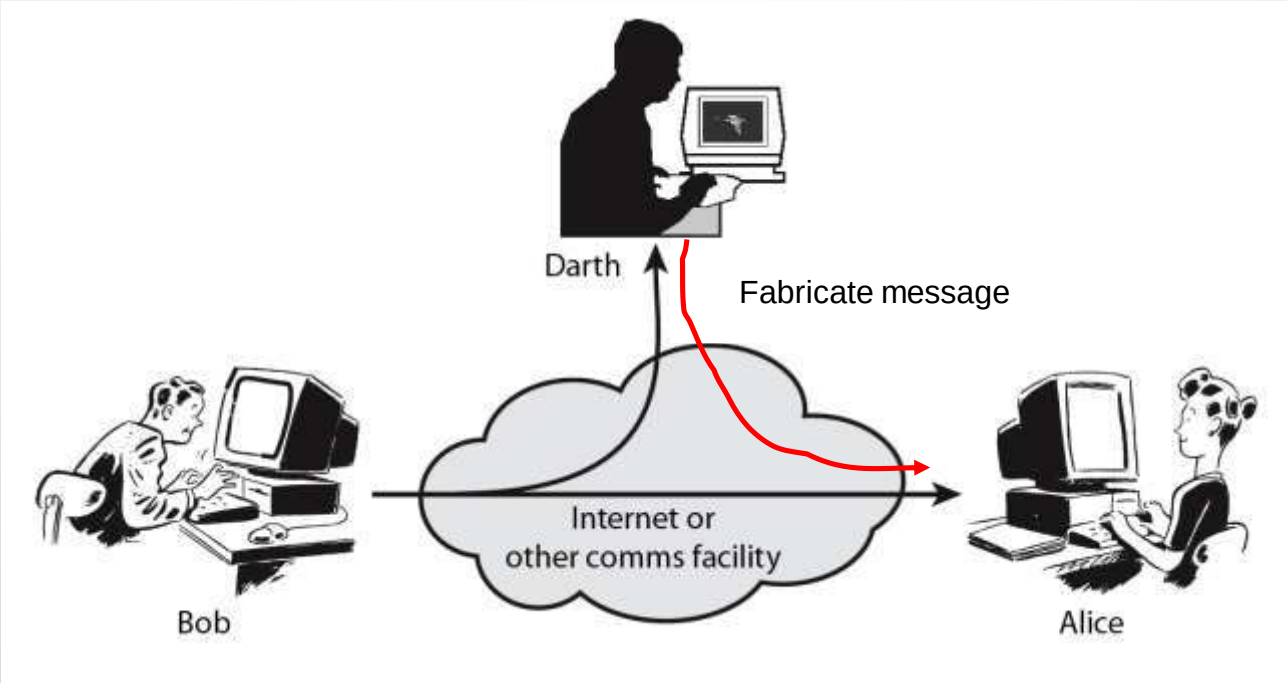


Active Attack: Replay

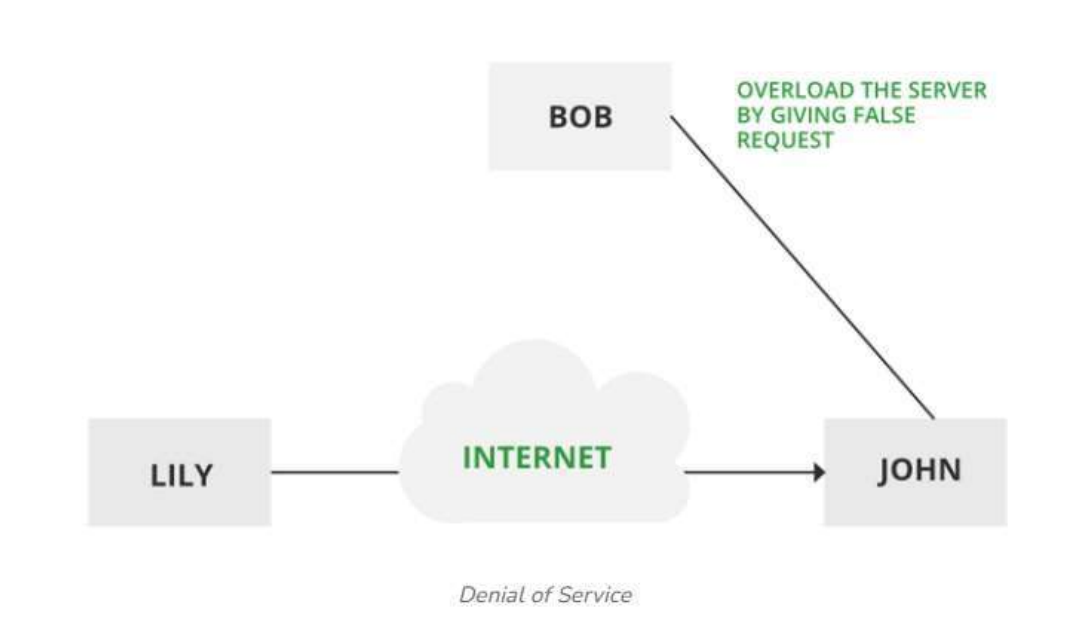
Replay Attack: The attacker intercepts a message and later replays it to trick the receiver into believing it's a new message



Active Attack: Fabrication



Denial of Service (DoS Attack)



The attacker floods a target system or network with traffic or requests in order to consume the available resources such as bandwidth, CPU cycles, or memory and prevent legitimate users from accessing them

Man-in-the-Middle (MitM) Attack

A **Man-in-the-Middle (MitM) Attack** is a type of active attack where an attacker secretly intercepts and manipulates the communication between two parties who believe they are communicating directly with each other. In this scenario, the attacker can eavesdrop on the communication, modify it, or impersonate one of the parties, potentially gaining access to sensitive data.

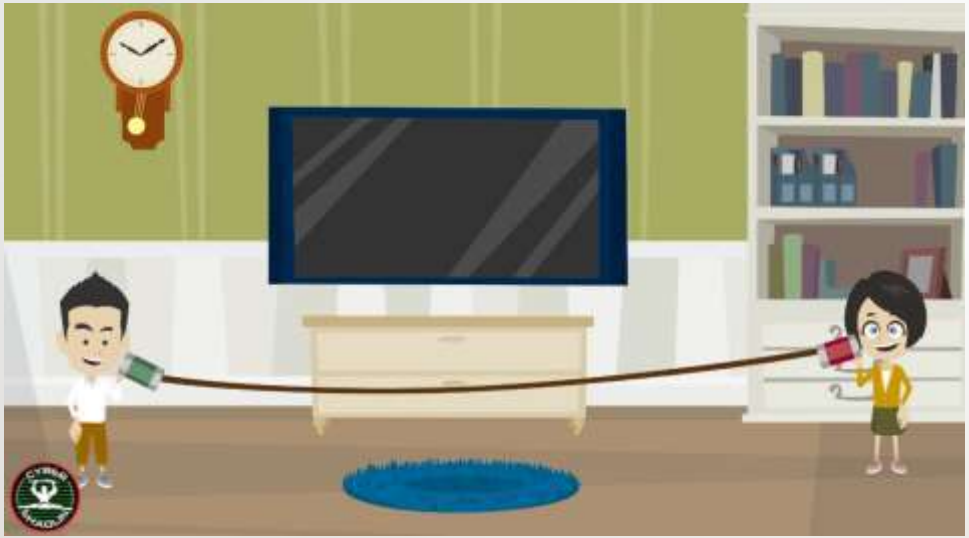
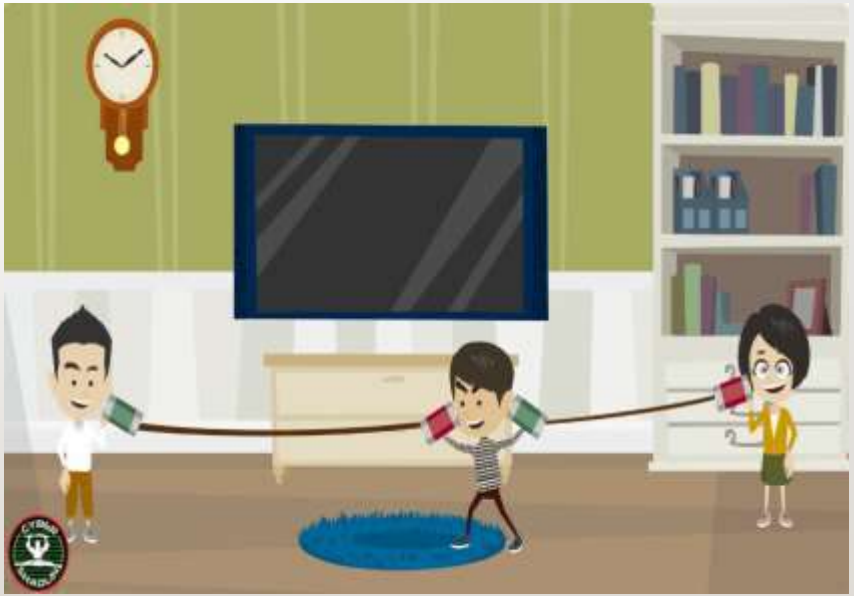


Fig1

Fig2



Key Terms

Cryptography

- **Definition**: Cryptography is the science and art of creating techniques to secure information and communications from unauthorized access. It involves transforming plaintext (readable data) into ciphertext (unreadable data) so that only authorized parties can access the information.
- **Purpose**: To ensure confidentiality, integrity, authenticity, and non-repudiation of information.

Cryptanalysis

- **Definition**: Cryptanalysis is the practice of analyzing cryptographic systems to break or bypass their security measures without having the key. It's essentially the study of techniques used to decode or compromise encrypted information.
- **Purpose**: Cryptanalysts study ciphers and look for weaknesses in encryption algorithms to help improve security or, in some cases, to break it for intelligence purposes.

Cryptology

- **Definition**: Cryptology is the overarching field that includes both **cryptography** (creating secure codes) and **cryptanalysis** (breaking secure codes).
- **Purpose**: To study and develop secure communication techniques, including both the creation and breaking of ciphers.

Cryptanalyst

- **Definition**: A cryptanalyst is a person who specializes in cryptanalysis, aiming to find weaknesses in encryption systems or to decode encrypted information without access to the encryption key.
- **Role**: Cryptanalysts work in areas like cybersecurity, intelligence, and academic research to assess and improve encryption methods or, in some cases, to intercept secure communications.

Plaintext

- **Definition**: Plaintext is the original, unencrypted data or message that is easily readable by humans or computers.
- **Example**: A simple message like "Hello, World!" is plaintext before encryption.

Ciphertext

- **Definition**: Ciphertext is the result of encrypting plaintext; it's an unreadable, scrambled version of the original message. Only someone with the appropriate key can decrypt it back to plaintext.
- **Example**: Encrypting "Hello, World!" might yield a ciphertext like "8zE%p1Fw$!k".

Encryption

- **Definition**: Encryption is the process of converting plaintext into ciphertext using a cryptographic algorithm and an encryption key. This process ensures that only those with the decryption key can access the original information.
- **Purpose**: To protect sensitive information during transmission or storage, making it unreadable to unauthorized parties.

Decryption

- **Definition**: Decryption is the process of converting ciphertext back into plaintext using a decryption key. It's the reverse of encryption, making the information accessible in its original, readable form.
- **Purpose**: To allow authorized parties to read the encrypted data by reversing the encryption process.