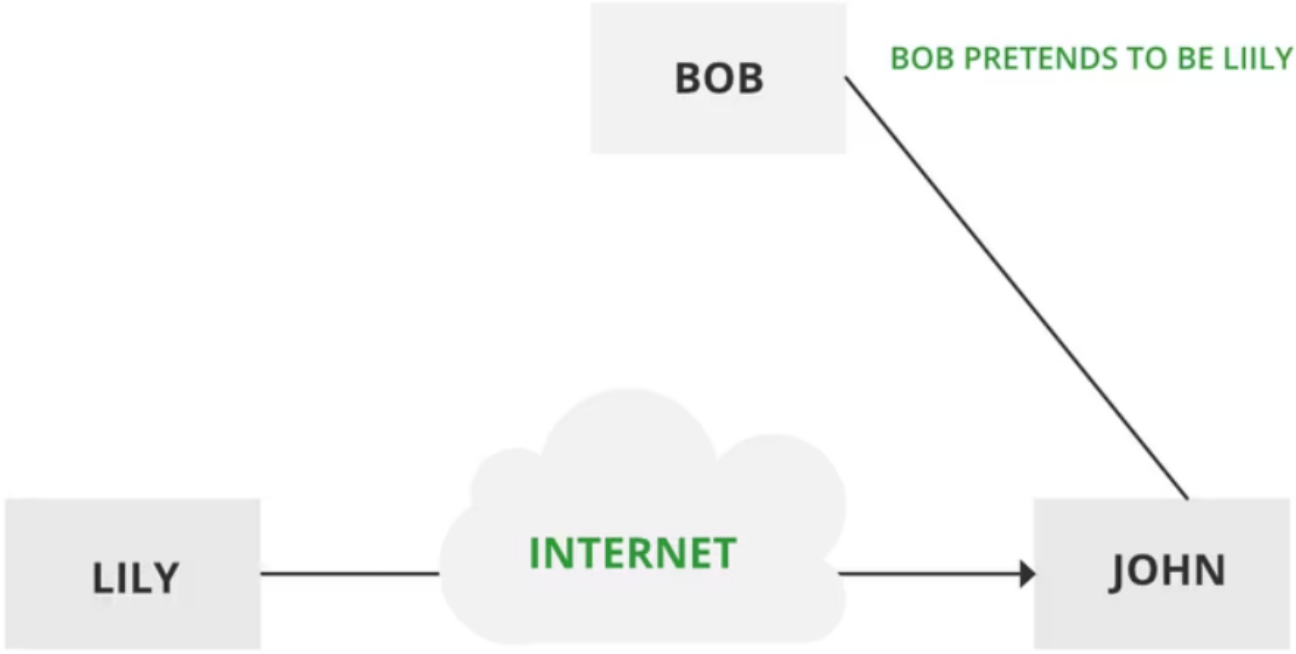
What Is a Network Attack?

A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity. There are two main types of network attacks:

- **Passive:** Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.
- **Active:** Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.

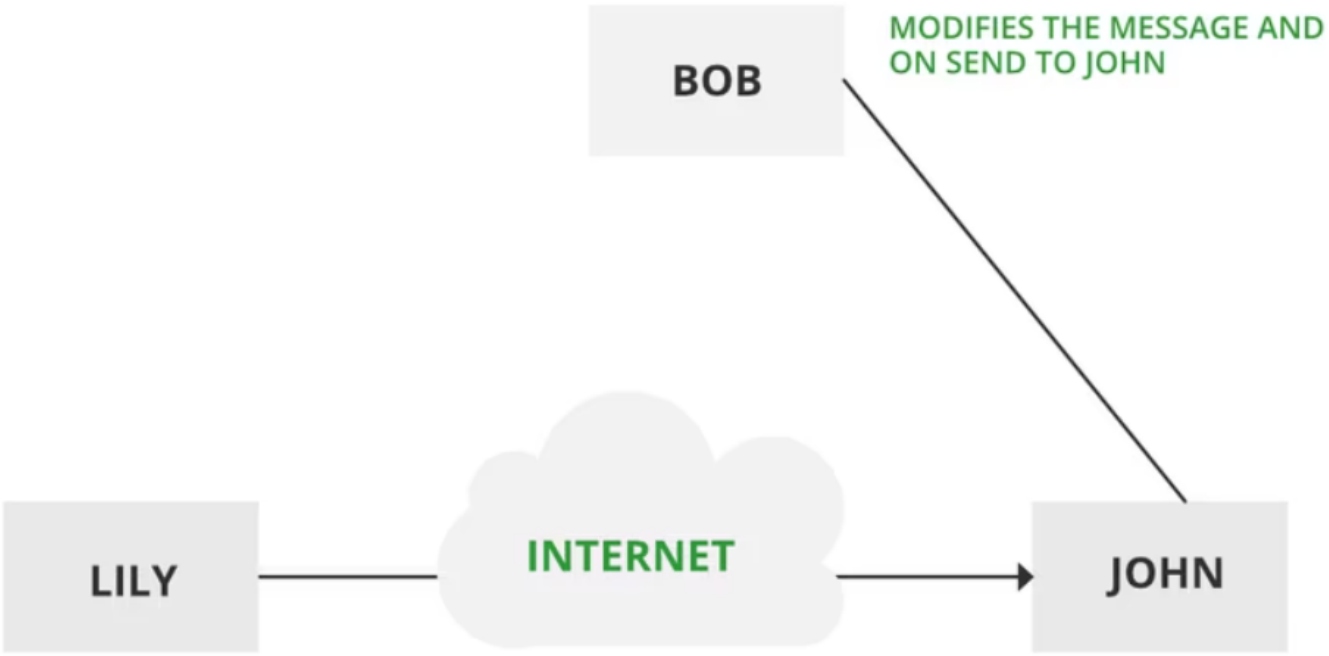
Active attacks: An Active attack attempts to alter system resources or affect their operations. The active attack involves some modification of the data stream or creation of false statement. Types of active attacks are as following:

1. **Masquerade –**
   Masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks.



Masquerade Attack

2. **Modification of messages –**
   It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.



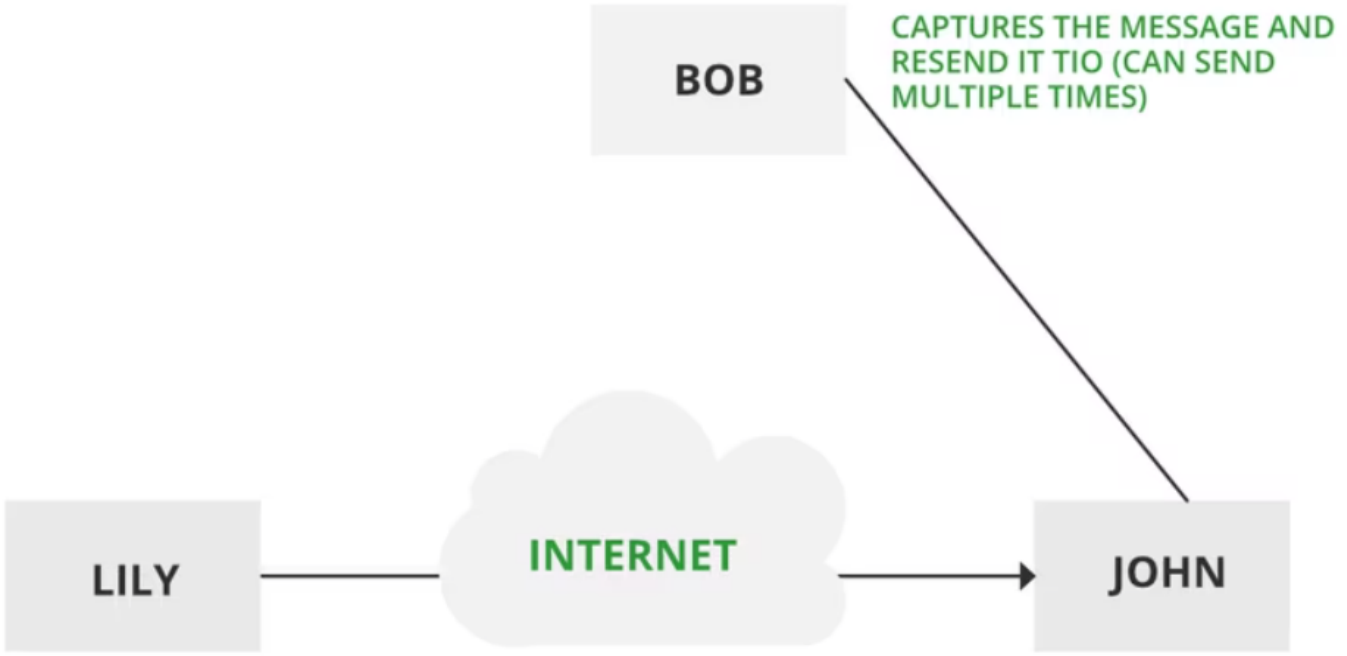
Modification of messages

3. **Repudiation –**

   This attack is done by either the sender or receiver. The sender or receiver can deny later that he/she has sent or receive a message. For example, the customer asks his Bank “To transfer an amount to someone” and later on the sender(customer) deny that he had made such a request. This is repudiation.

Replay –

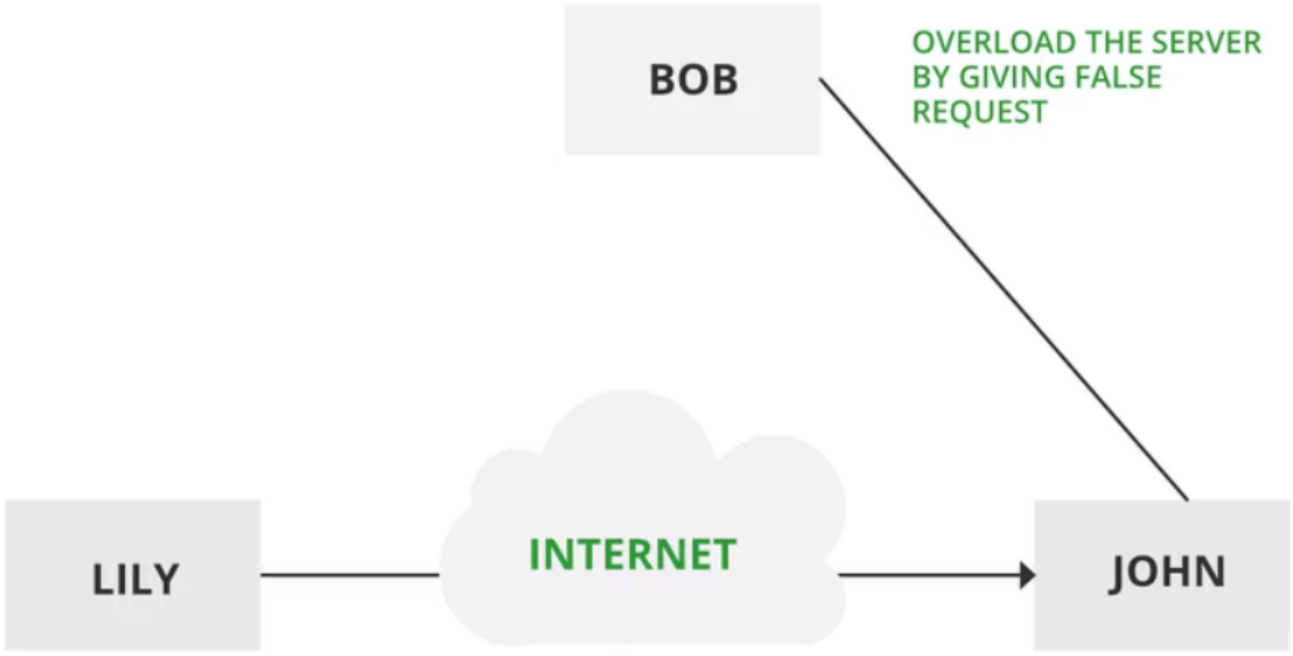
It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.


BOB
CAPTURES THE MESSAGE AND RESEND IT TIO (CAN SEND MULTIPLE TIMES)
LILY
INTERNET
JOHN

Replay

Denial of Service –

It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance.



Denial of Service

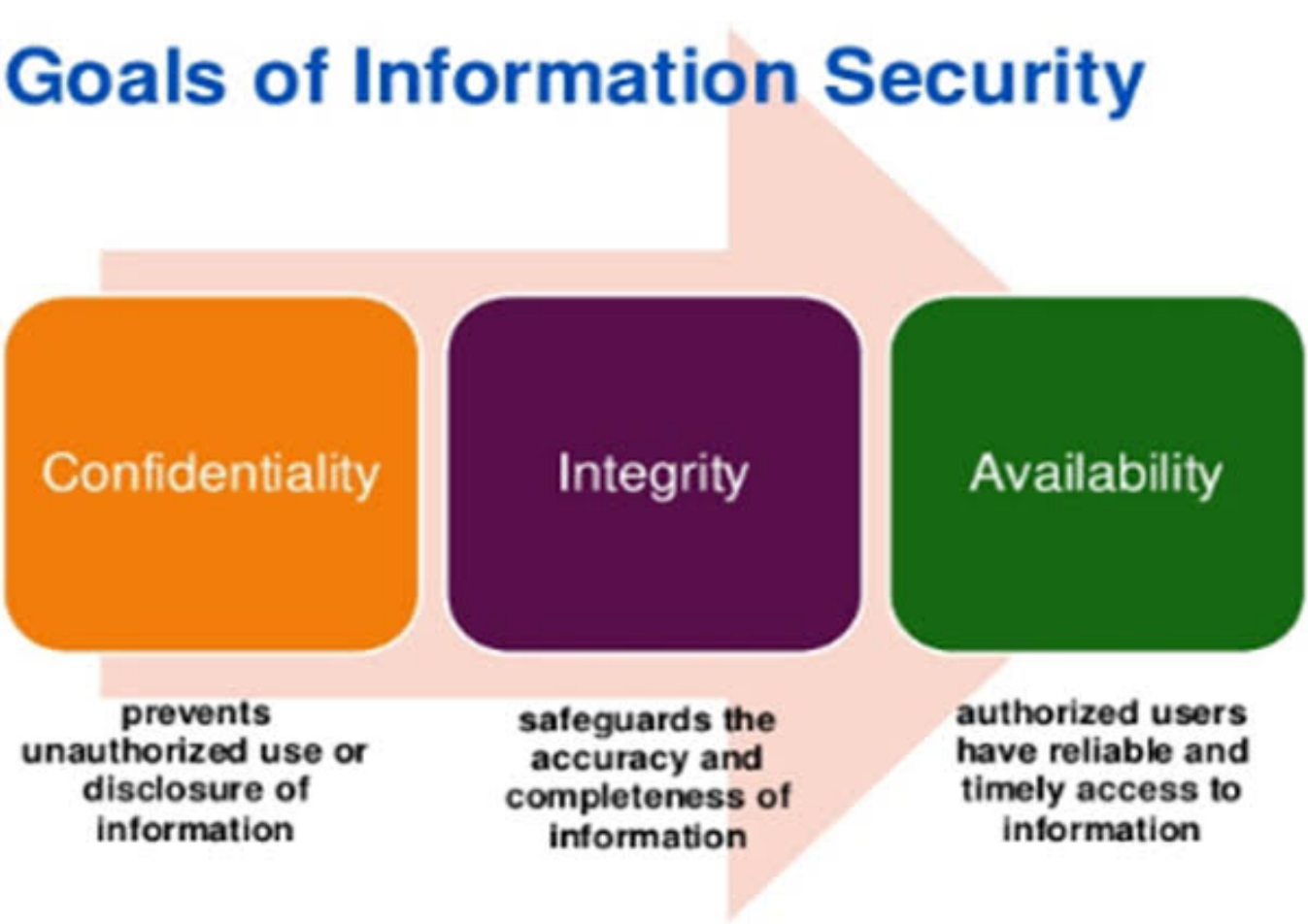
Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. **The release of message content –**
   Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

2. **Traffic analysis –**

   Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message. The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Goals of Information Security



SECURITY

What is the CIA Triad?

The CIA Triad is a security model developed to ensure the 3 goals of cybersecurity, which are Confidentiality, Integrity, and Availability of data and the network.

1. Confidentiality

Keeping the sensitive data private and accessible to only authorized users.

2. Integrity

Designed to protect the data from unauthorized access and ensure its reliability, completeness and correctness.

3. Availability

Authorized users can have access to system resources and data as and when they need it.

Methods to ensure Confidentiality are :

1. Encryption of raw data
2. Using biometrics for authentication

Methods to ensure Integrity are :

1. Making use of user access control to restrict unauthorized modification of files.
2. Setting up backups to restore data during any system failure.

Methods to ensure Availability are :

1. Installing firewalls, proxy servers during downtime.
2. Locating backups at geographically isolated locations.


Data Flair
Encryption
Access Control
Tools for Confidentiality
Authentication
Authorisation
TOOLS FOR ACHIEVING CIA GOALS
Physical protection
Computational Redundancy
Tools for Availability
Tools for Integrity
Backups
Checksums
Error-correcting codes