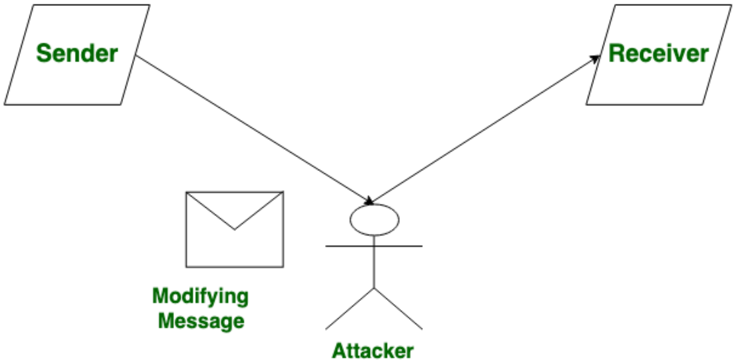
What is a Security attack?

A security attack refers to an attempt to exploit vulnerabilities or weaknesses in a system or network in order to compromise its confidentiality, integrity, or availability. Security attacks can take many forms, such as viruses, malware, phishing, denial-of-service attacks, and unauthorized access to sensitive information. The goal of a security attack can be to steal information, damage or disrupt services, or gain unauthorized access to a system.

What are Active Attacks?

Active attacks are the type of attacks in which, the attacker efforts to change or modify the content of messages. Active Attack is dangerous to Integrity as well as availability. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, In an active attack, Victim gets informed about the attack.



Active Attack

Advantages of Active Attack (during the process by the attacker)

- **Immediate Impact:** By definition, active attacks are also much quicker in that they can immediately and visibly bring about conditions such as system halts, loss of data, and the like.
- **Potential for Data Manipulation:** Hackers may corrupt or compromise data, and data integrity problems may arise that may cause significant and prolonged implications for organizations.
- **Disruption of Services:** Active attacks, again, can be a great threat to services as they intend to attack key systems or networks.

Disadvantages of Active Attack

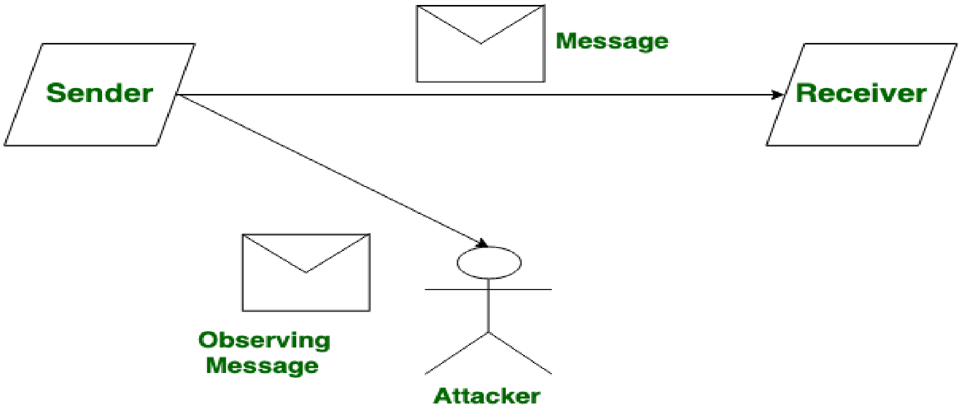
- **Higher Risk of Detection:** Based on the fact that active attacks imply wavelength or disruption, it is easier for them to be identified by security systems and administrators.

- **Legal Consequences:** There is only passive attack, and it is unlawful and if the attacker is apprehended, he will face legal repercussions.

- **Resource Intensive:** An active attack is normally more resourceful, technical and needs more tools and skills than those typical of passive attacks.

What are Passive Attacks?

Passive Attacks are the type of attacks in which, The attacker observes the content of messages or copies the content of messages. Passive Attack is a danger to Confidentiality. Due to passive attack, there is no harm to the system. The most important thing is that In a passive attack, Victim does not get informed about the attack.



Passive Attack

Advantages of Passive Attack (from the attacker's perspective)

- Low Risk of Detection: Passive attacks are hidden in the sense that they do not attempt to modify or destroy the data or the systems and as such, they are more difficult to recognize.

- Information Gathering: Such attacks make it possible for the attackers to obtain useful information which can be useful in future active attacks or other vices.

- Minimal Resources Required: Passive attack types can be accomplished using less means, and less skills, and are therefore available to a larger set of potential attackers.

Disadvantages of Passive Attack (from the attacker's perspective)

- No Immediate Impact: Compared to active attacks passive attacks are not able to directly effect system resources, this may reduce their applicability in some cases.

- Reliance on Future Actions: The information obtained in passive attacks have to be utilized at some point in time to fulfill the attacker’s goals – and this entails additional measures.
- Limited to Information Gathering: Passive attacks do not let the attacker to manipulate or destroy data and is usually confined to the collection of data.

Difference Between Active Attack and Passive Attack

Active Attack	**Passive Attack**
In an active attack, Modification in information takes place.	While in a passive attack, Modification in the information does not take place.
Active Attack is a danger to **Integrity** as well as **availability**.	Passive Attack is a danger to **Confidentiality**.
In an active attack, attention is on prevention.	While in passive attack attention is on detection.
Due to active attacks, the execution system is always damaged.	While due to passive attacks, there is no harm to the system.
In an active attack, Victim gets informed about the attack.	While in a passive attack, Victim does not get informed about the attack.
In an active attack, System resources can be changed.	While in passive attack, System resources are not changing.
Active attack influences the services of the system.	While in a passive attack, information and messages in the system or network are acquired.
In an active attack, information collected through passive attacks is used during execution.	While passive attacks are performed by collecting information such as passwords, and messages by themselves.
An active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibit in comparison to active attack.
Can be easily detected.	Very difficult to detect.
The purpose of an active attack is to harm the ecosystem.	The purpose of a passive attack is to learn about the ecosystem.
In an active attack, the original information is modified.	In passive attack original information is Unaffected.
The duration of an active attack is short.	The duration of a passive attack is long.
The prevention possibility of active attack is High	The prevention possibility of passive attack is low.
Complexity is High	Complexity is low.

What is Cyber/Security 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. Common forms of cyber-attacks include malware, which is harmful software like viruses, ransomware, and phishing, where attackers send emails that appear to be authentic but have malicious intent, to convince other users to share sensitive information with them. Other forms are denial of service, DoS, and MitM attacks, which intercept communications between two parties. It is through this cyber knowledge of the threats that people are protected in the sensitive information secured through digital security by advanced technology these days.

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.

Types of active attacks are as follows:

1. Masquerade Attack
2. Modification of Messages
3. Repudiation
4. Replay Attack
5. Denial of Service (DoS) Attack

1. Masquerade Attack

Masquerade attacks are considered one type of cyber attack in which the attacker disguises himself to pose as some other person and accesses systems or data. It could either be impersonating a legal user or system and demanding other users or systems to provide information with sensitive content or access areas that are not supposed to be accessed normally. This may even include behaving like an actual user or even some component of the system with the intention of manipulating people to give out their private information or allowing them into secured locations.

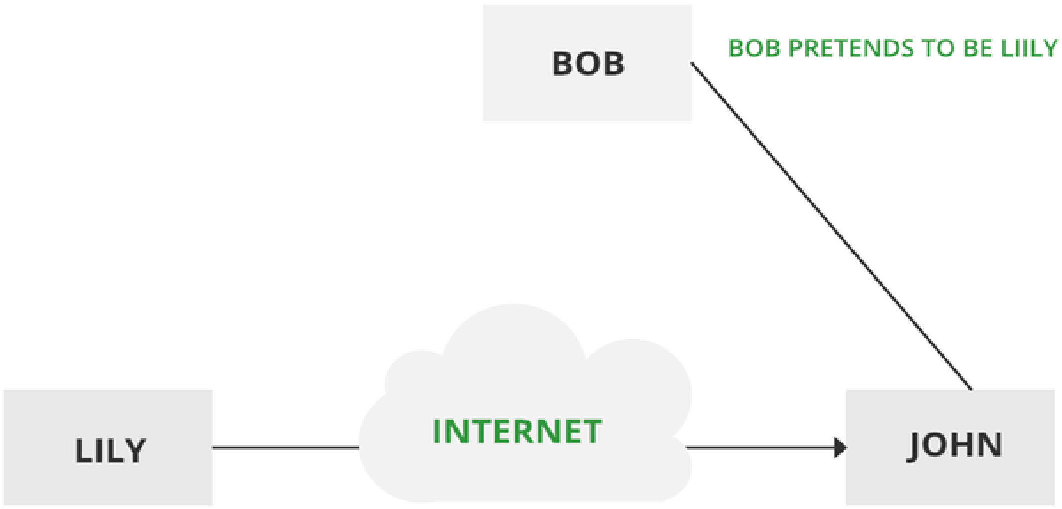
There are several types of masquerading attacks, including:

- **Username and Password Masquerade:** In this masquerade attack, a person uses either stolen or even forged credentials to authenticate themselves as a valid user while gaining access to the system or application.

- **IP address masquerade:** This is an attack where the IP address of a malicious user is spoofed or forged such that the source from which the system or the application is accessed appears to be trusted.

- **Website masquerade:** A hacker creates a fake website that resembles as a legitimate one in order to gain user information or even download malware.

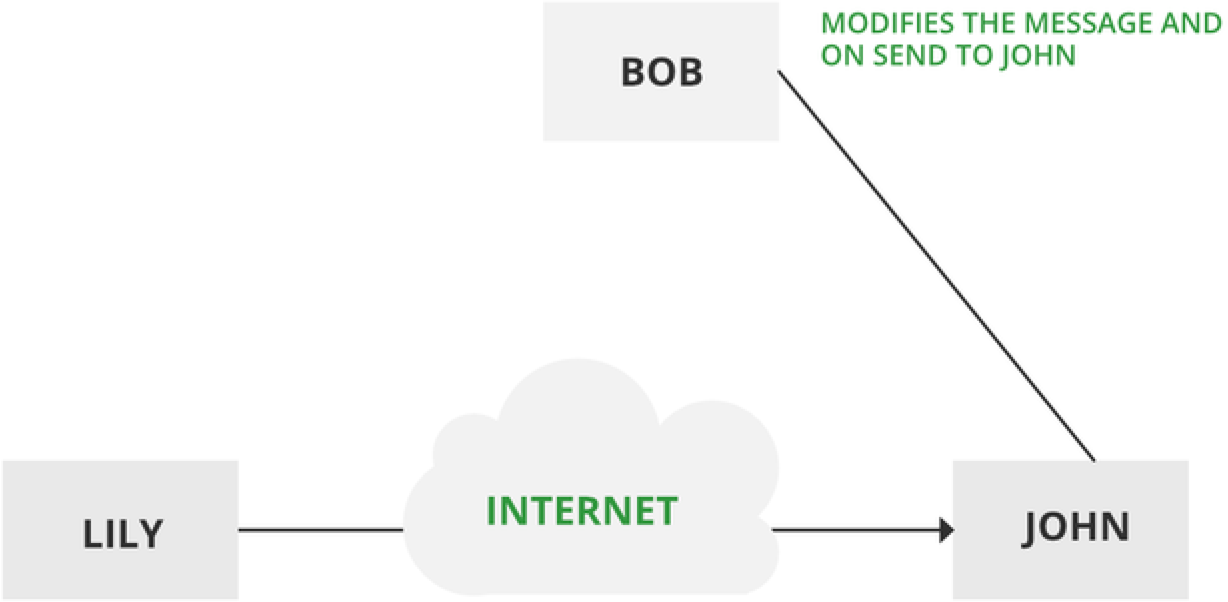
- **Email masquerade:** This is an e-mail masquerade attack through which an attacker sends an apparently trusted source email so that the recipient can mistakely share sensitive information or download malware.



Masquerade Attack

2. Modification of Messages

This is when someone changes parts of a message without permission, or mixes up the order of messages, to cause trouble. Imagine someone secretly changing a letter you sent, making it say something different. This kind of attack breaks the trust in the information being sent. 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

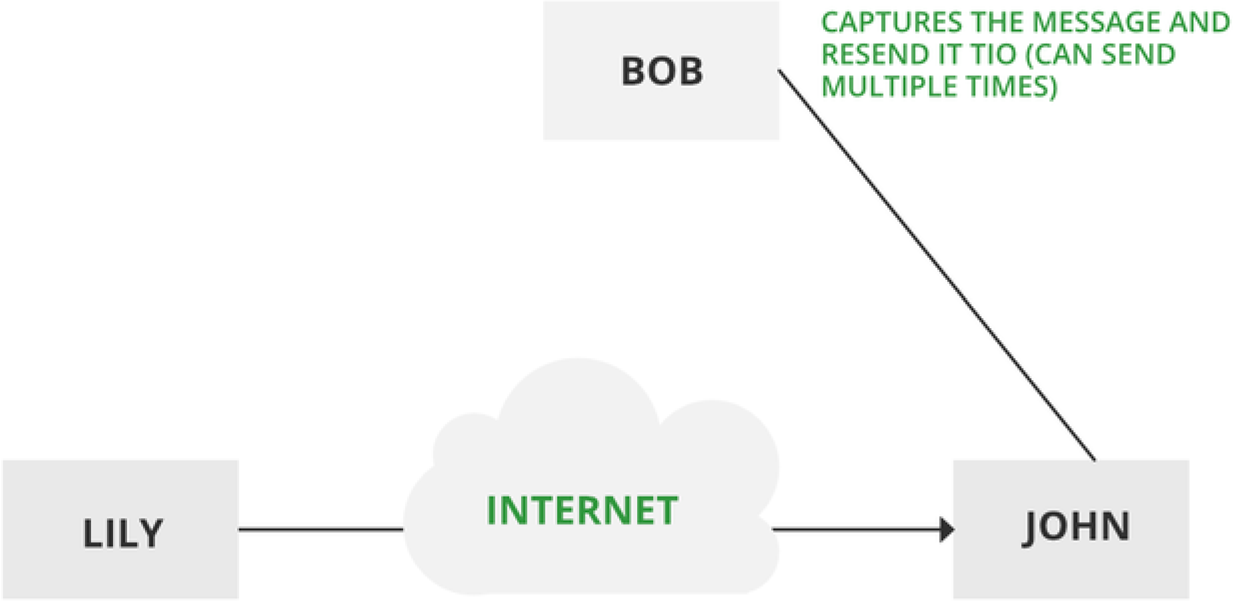
Repudiation attacks are a type of cyber attack wherein some person does something damaging online, such as a financial transaction or sends a message one does not want to send, then denies having done it. Such attacks can seriously hinder the ability to trace down the origin of the attack or to identify who is responsible for a given action, making it tricky to hold responsible the right person.

There are several types of repudiation attacks, including:

- **Message repudiation attacks:** In this attack, a message has been sent by an attacker, but the attacker later denies the sending of the message. This can be achieved either through spoofed or modified headers or even by exploiting vulnerabilities in the messaging system.
- **Transaction repudiation attacks:** Here, in this type of attack, a transaction-for example, monetary transaction-is made, and at after some time when the evidence regarding the same is being asked to be give then the attacker denies ever performing that particular transaction. This can be executed either by taking advantage of the vulnerability in the transaction processing system or by the use of stolen and forged credentials.
- **Data repudiation attacks:** In a data repudiation attack, data is changed or deleted. Then an attacker will later pretend he has never done this. This can be done by exploiting vulnerabilities in the data storage system or by using stolen or falsified credentials.

4. Replay

It is a passive capturing of a message with an objective to transmit it for the production of an authorized effect. Thus, in this type of attack, the main objective of an attacker is saving a copy of the data that was originally present on that particular network and later on uses it for personal uses. Once the data gets corrupted or leaked it becomes an insecure and unsafe tool for its users.


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

Replay

5. Denial of Service (DoS) Attack

Denial of Service (DoS) is a form of cybersecurity attack that involves denying the intended users of the system or network access by flooding traffic or requests. In this 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.

There are several types of DoS attacks, including:

- **Flood attacks:** Here, an attacker sends such a large number of packets or requests to a system or network that it cannot handle them all and the system gets crashed.

- **Amplification attacks:** In this category, the attacker increases the power of an attack by utilizing another system or network to increase traffic then directs it all into the target to boost the strength of the attack.

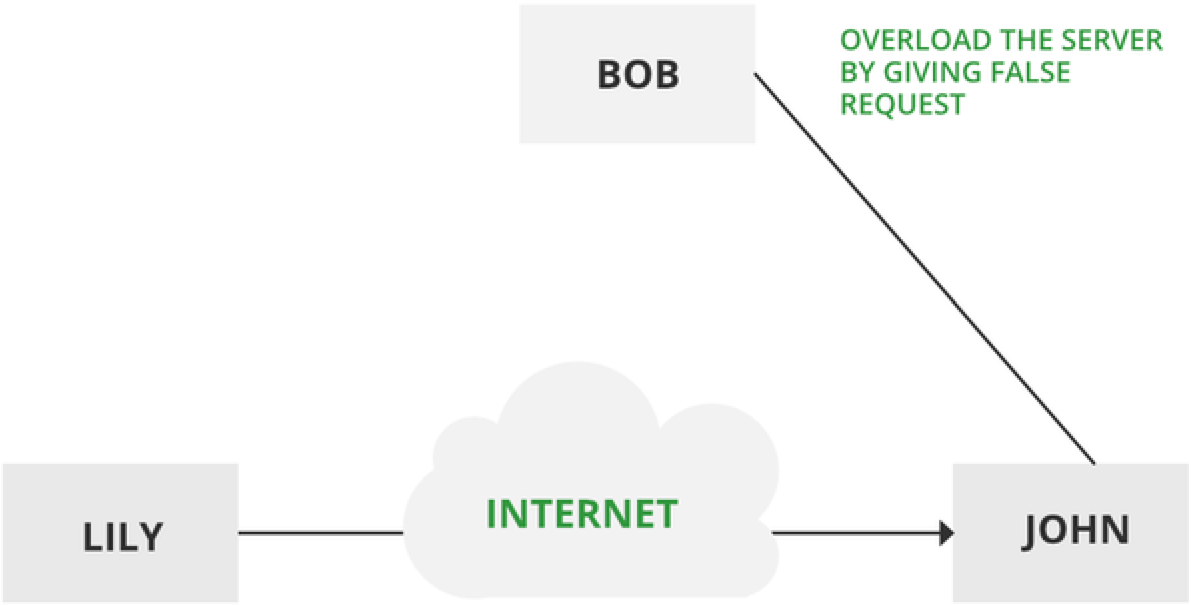
To Prevent DoS attacks, organizations can implement several measures, such as:

1. Using firewalls and intrusion detection systems to monitor network traffic and block suspicious activity.

2. Limiting the number of requests or connections that can be made to a system or network.

3. Using load balancers and distributed systems to distribute traffic across multiple servers or networks.

4. Implementing network segmentation and access controls to limit the impact of a DoS attack.



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 transmission. The goal of the opponent is to obtain information that is being transmitted. Passive attacks involve an attacker passively monitoring or collecting data without altering or destroying it. Examples of passive attacks include eavesdropping, where an attacker listens in on network traffic to collect sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information.

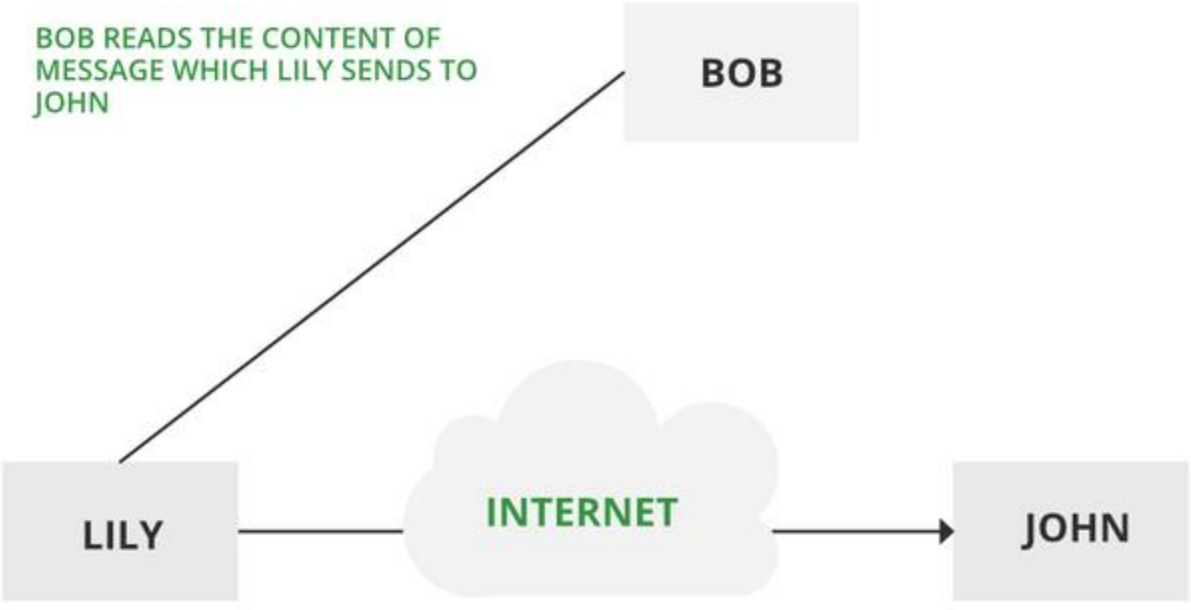
Types of Passive attacks are as follows:

1. The Release of Message Content

2. Traffic Analysis

1. The Release of Message Content

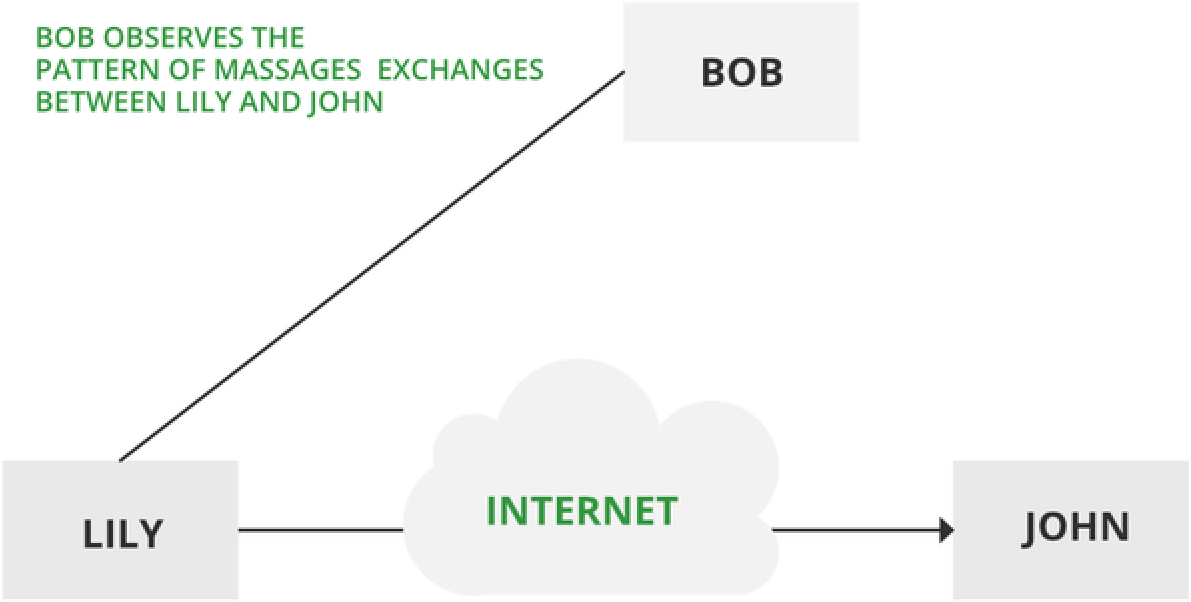
Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



Passive attack

2. Traffic Analysis

Suppose that we had a way of masking (encryption) 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.
The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.



BOB OBSERVES THE
PATTERN OF MASSAGES EXCHANGES
BETWEEN LILY AND JOHN

On the basis of	Active Attacks	Passive Attacks
Modification	Modification of information occurs during an active attack.	Modifying the information does not happen during a passive attack.
Threat	Active attack poses a threat to integrity and availability.	Confidentiality is at risk from passive attacks.
Focus	During an active attack, the focus is on detection.	During a passive attack, the focus is on avoiding harm.
Harm	The system is permanently harmed due to an active attack.	There is no harm to the system due to the passive attack.
Victim	In an active attack, the victim is notified of the attack.	The victim is unaware of the attack while under passive attack.
System Resources	System resources can be modified during an active attack.	System resources do not alter when in the passive attack.
Impact	Active attacks have an impact on the system's services.	Information and communications in the system or network are collected during a passive attack.
Information	During the execution of active attacks, information gathered from passive attacks is utilised.	Passive attacks are carried out by gathering information such as passwords and messages on their own.
Prevention	An active attack is brutal to restrict from entering systems or networks.	In comparison to an active attack, the passive attack is much easier to prevent.