

# ***Report on Active and Passive attack***

*Department of Information Technology*

*Indian Institute of Information Technology, Allahabad*

## **Group Members :**

<i>Soumyadeep Basu</i>	<i>(IIT2018001)</i>
<i>Kumar Utkarsh</i>	<i>(IIT2018007)</i>
<i>Rohit Haolader</i>	<i>(IIT2018008)</i>
<i>Raushan Raj</i>	<i>(IIT2018031)</i>
<i>Suryasen Singh</i>	<i>(IIT2018069)</i>

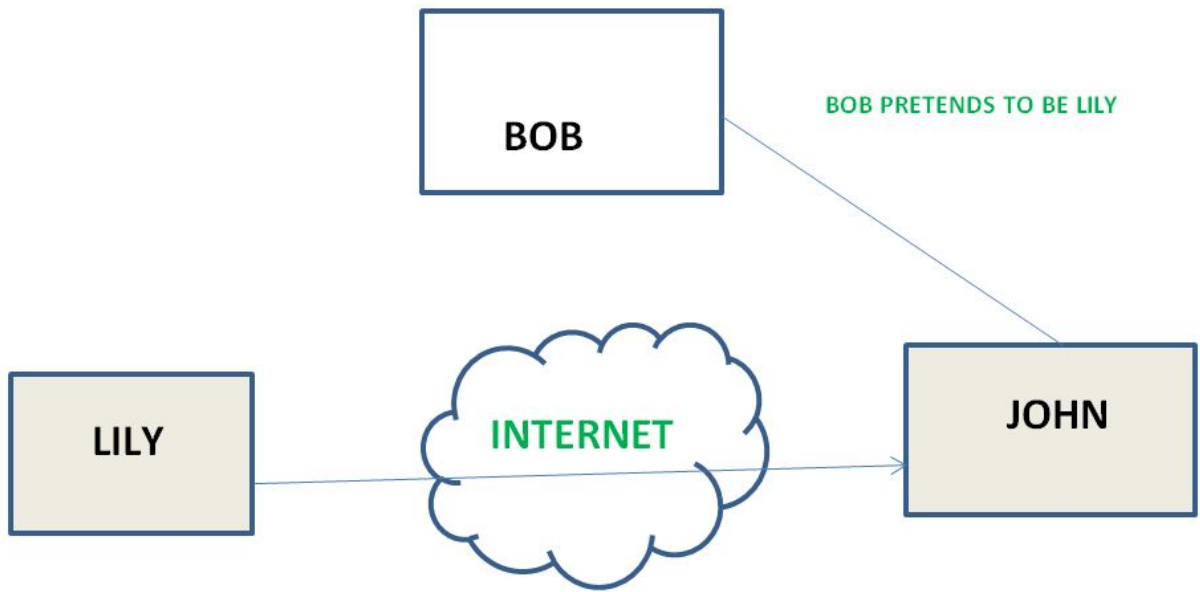
## **1. Active attacks :**

Active attacks try to modify system resources or activate their functionality. Active attacks include some modifications to the data distribution or the creation of a false statement. Active Attack is like a threat for Integrity and availability as well. Because of an active attack, the system is often corrupted/damaged and the system resources can be modified. The most important thing is that, in active attacks, the victim receives information about the attack.

- **Types of Active attack :**

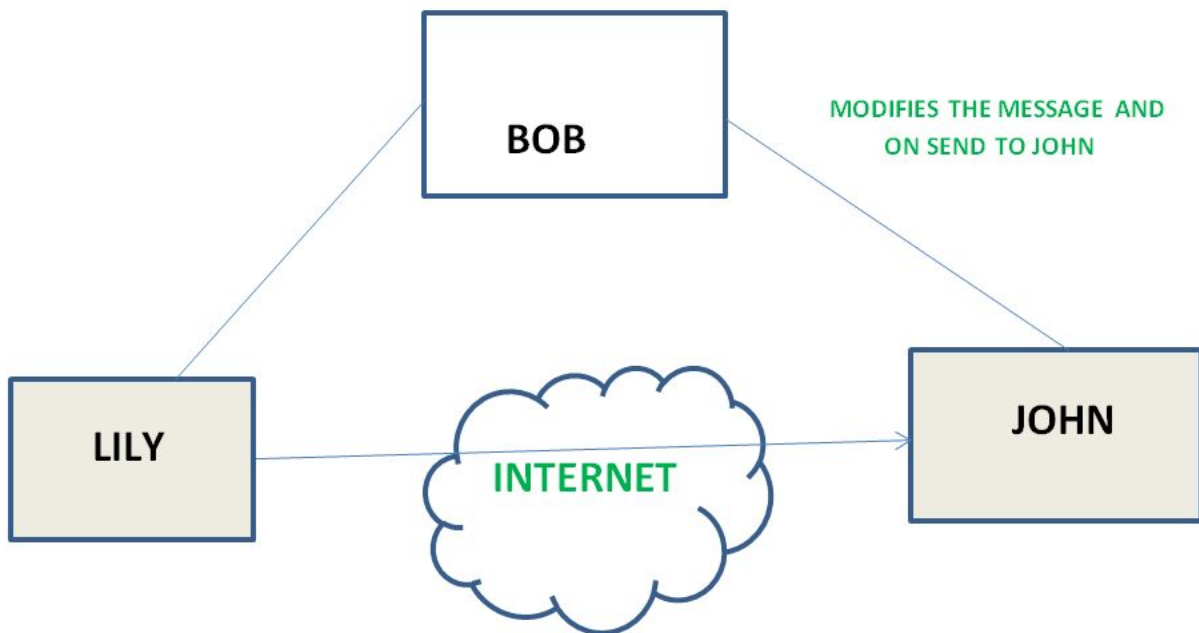
### **a) Masquerade :**

Masquerade attacks occur when one business pretends to be a different business. Masquerade attacks include another type of active attack.



**b) Modification of messages :**

It means that a part of a message is being changed or that message is delayed or rearranged to produce an unauthorized result. For example, the message "Let JOHN read secret X" is translated as "Let Smith read secret file X".

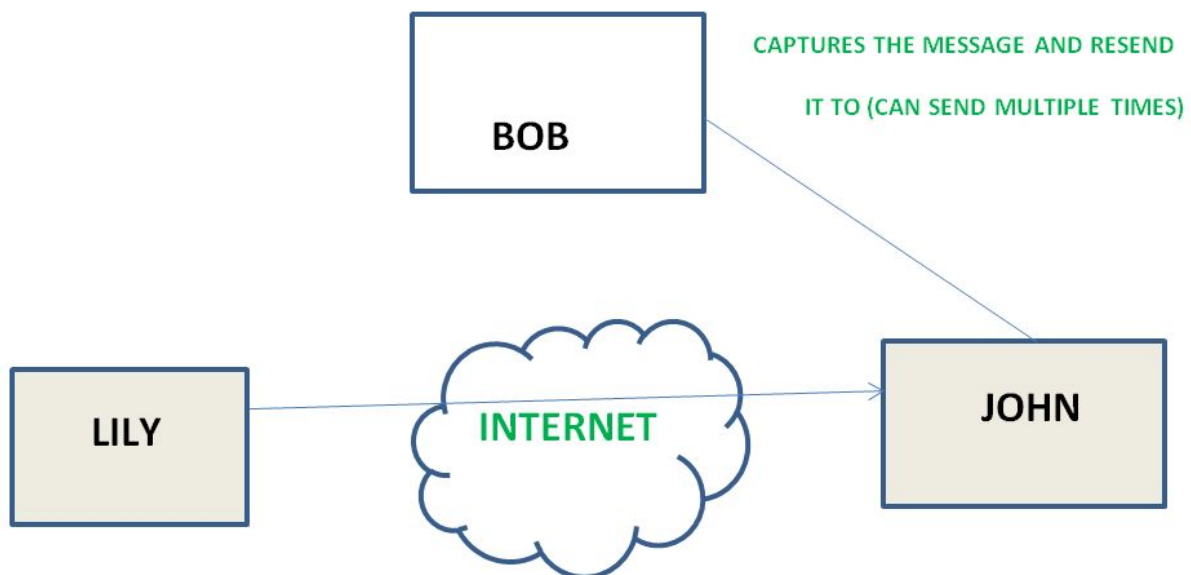


**c) Repudiation :**

These attacks are caused by the sender or receiver. The sender or recipient may later deny that you sent or received the message. For example, a customer asks his Bank to “transfer the amount to a person” and later to the sender (customer) deny that he has made such a request. This is a waste.

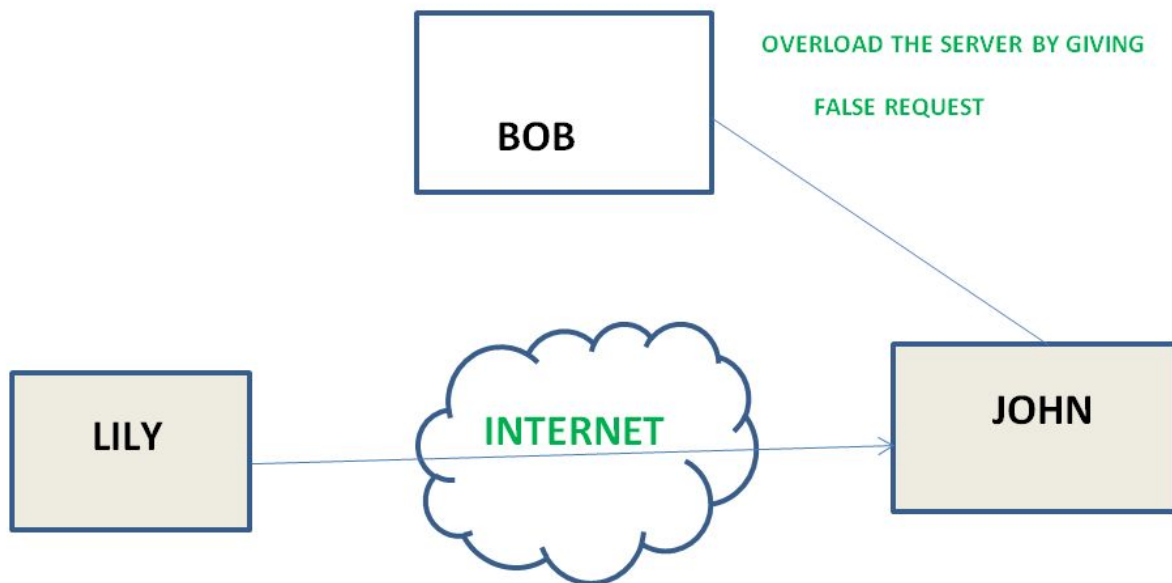
**d) Replay:**

It involves the capturing of the message that took place and its subsequent transmission to produce an authorized result.



**e) Denial of Service:**

Prevents normal use of social media. This attack can have a certain gate. For example, a business may compress all messages directed to a specific location. Another way to reject service is to disrupt the entire network to wither by disabling the network or overloading it with messages to ruin performance.



**Prevention:**

Active attacks can be prevented by using Firewalls and IPS (Intrusion Prevention Systems).

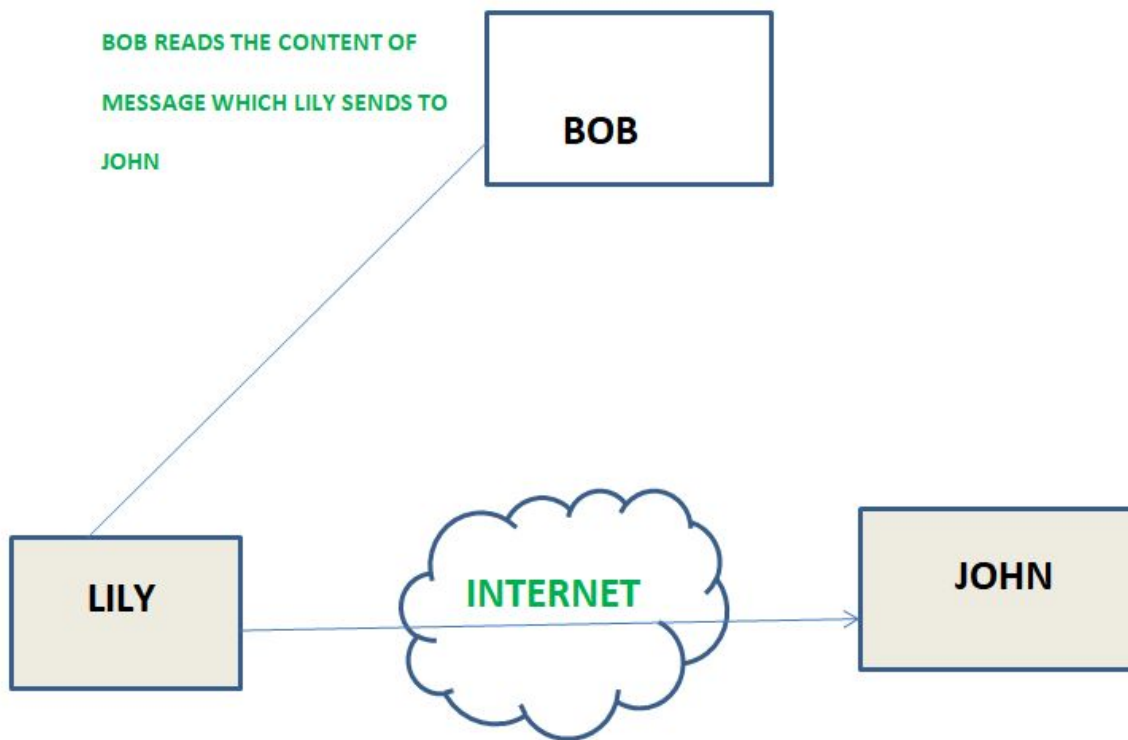
**2. Passive Attack :**

Passive Attack attempts to read or use information from the system but does not affect system resources. Passive Attacks are in the form of mental retrieval or visual recognition. The object of the opponent's intent to obtain the information is transferred. Passive attack types are as follows:

- **Types of Passive attack :**

**a) The release of message content -**

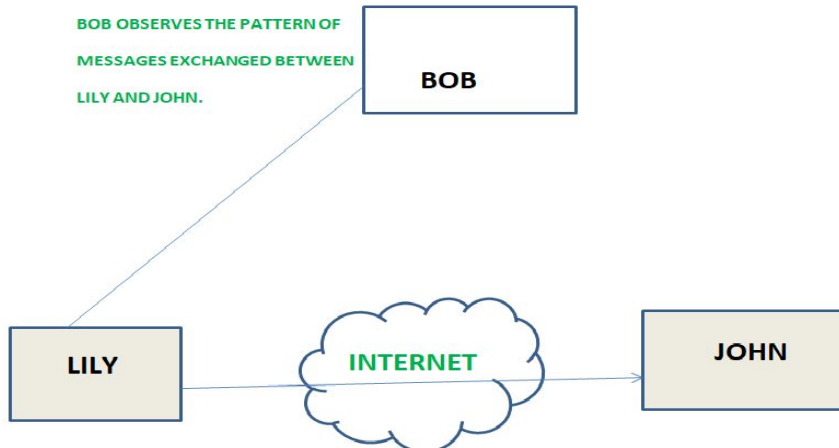
Phone chat, email message or forwarded file may contain sensitive or confidential information. We'd like to prevent the opponent from reading the content of this post.



## **b) Traffic Analysis -**

Suppose we have a way of encrypting (encrypting) information, so that the attacker or the photographer can extract any information from the message.

The opponent can specify the location and identity of the contact area and can see the frequency and length of the exchange messages. This information may be helpful in guessing the type of communication that is taking place.



### Prevention:

Potential threats from Passive attacks can be eliminated by implementing good network encryption.

- **Difference between Active and Passive attack :**

Active attack	Passive attack
1. Active attack is a threat to integrity and availability.	1. Passive attack is a threat to confidentiality.
2. Because of an active attack , the system always gets harmed.	2. Because of a passive attack , the system doesn't get harmed in any way.
3. In active attack , victim receives the information about the attack	3. In passive attack, the victim doesn't receive the information about the attack.
4. In active attack, system resources can be modified.	4. In passive attack, system resources can't be modified.However it can be monitored.
5. Active attack pays attention to detection of an attack.	5. Passive attack pays attention to the prevention from an attack.
6.Active attack is easily detected.	6.Passive attack can't be detected easily .

References : Tutorials Point Website(<https://www.tutorialspoint.com>)  
ShodhGanga  
(<https://shodhganga.inflibnet.ac.in/bitstream/10603/111166/6/05chapter3.pdf>)

**--- The End ---**