



**A.V.C COLLEGE OF ENGINEERING**  
**DEPARTMENT OF COMPUTER APPLICATIONS**  
(A Recognized as a Research centre  
Approved by Anna University , Chennai)



***"CAS Newsletter"***

**Volume:09**

**Month: Dec'18**

**Issue:8**

*I Congratulate the students those who got Anna University Rank and very good CGPA in University examinations. I wish 10 Final MCA students who got Government project internship from Sub Collector @ SPANSYS, Kumbakonam. I wishing them to all success in future endeavors.*

**Dr. S.SELVAMUTHUKUMARAN.**

## LEARNER → WRITER

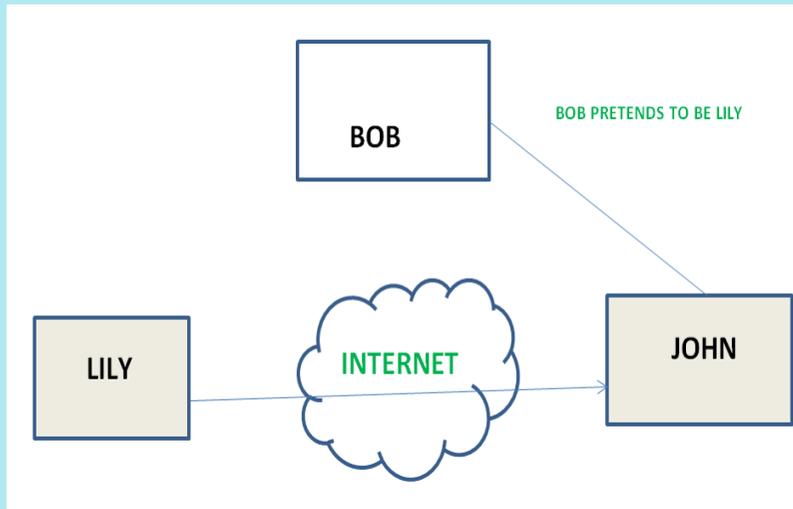
### Types of Security attacks / Active and Passive attacks

M. Mumtaj Farajana - III MCA

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

#### 1. Masquerade

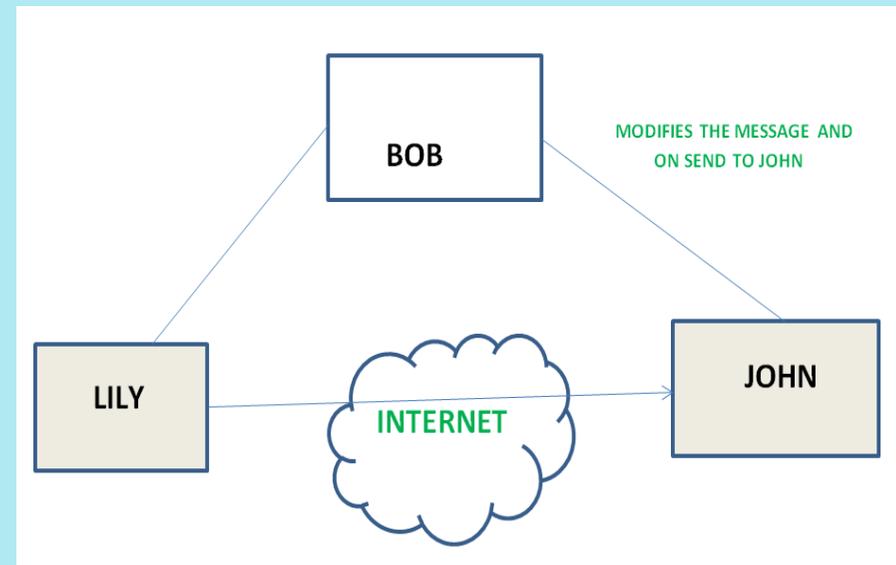
Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active



attacks.

#### 2. Modification of messages

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

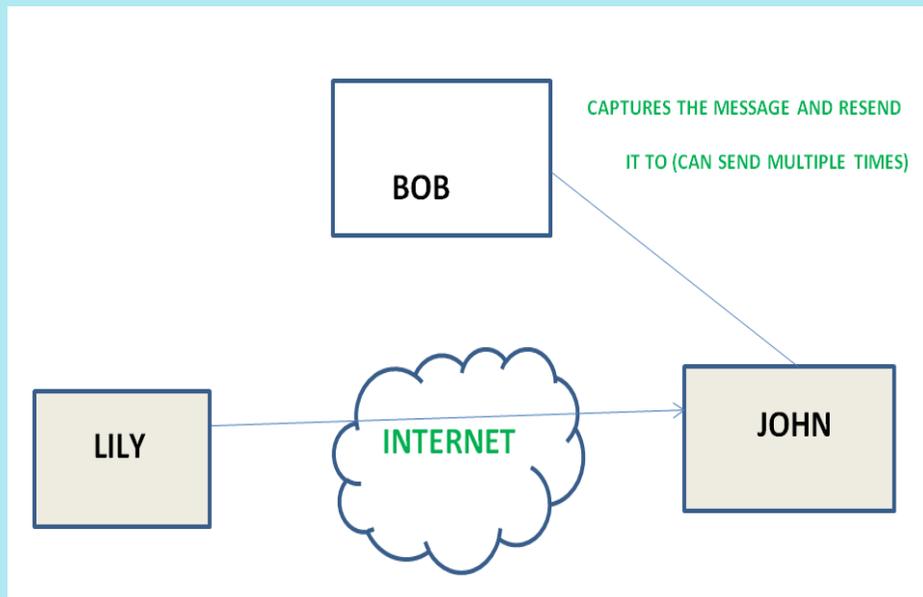


### 3. Repudiation

This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask 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.

### 4. Replay

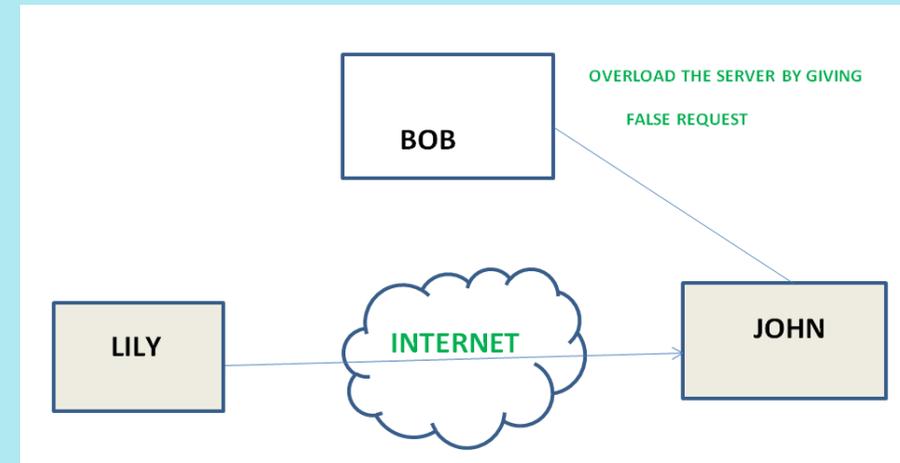
It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.



### 5. Denial of Service

It prevents 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 wither by disabling the network or by overloading it by messages so as to degrade performance.

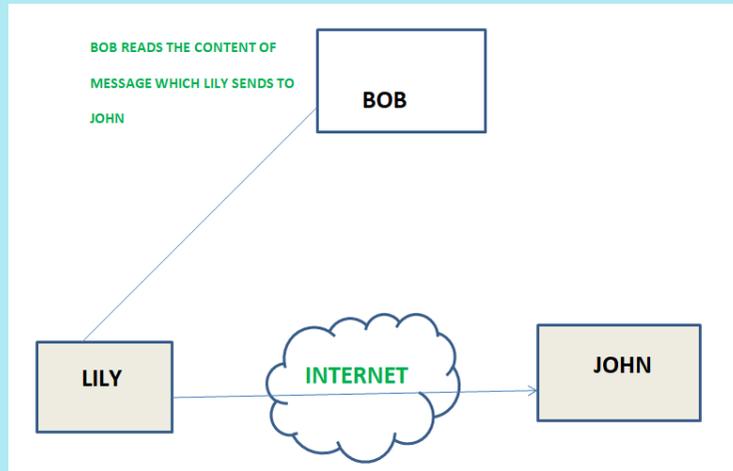


### Passive attacks

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

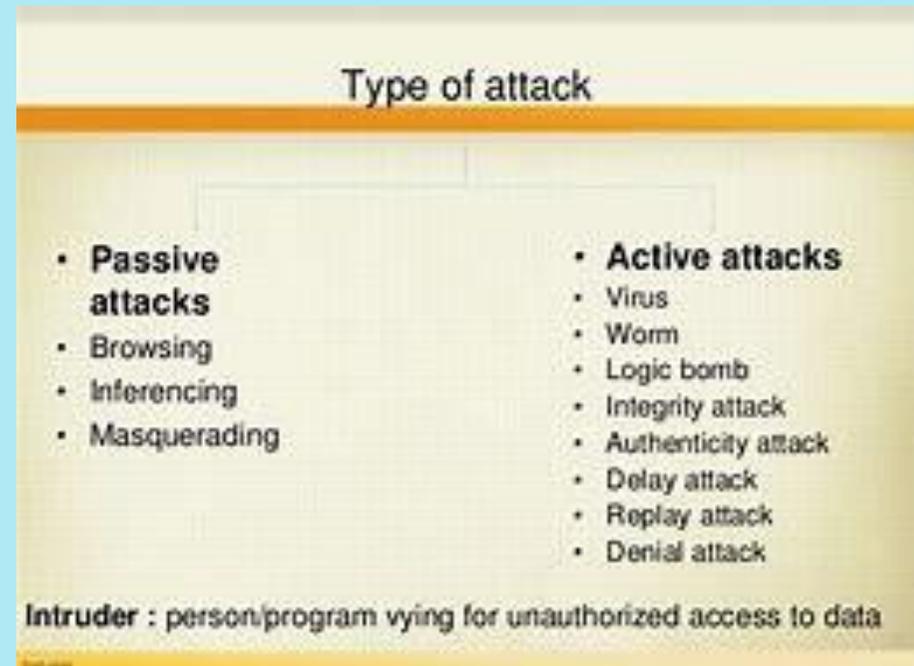
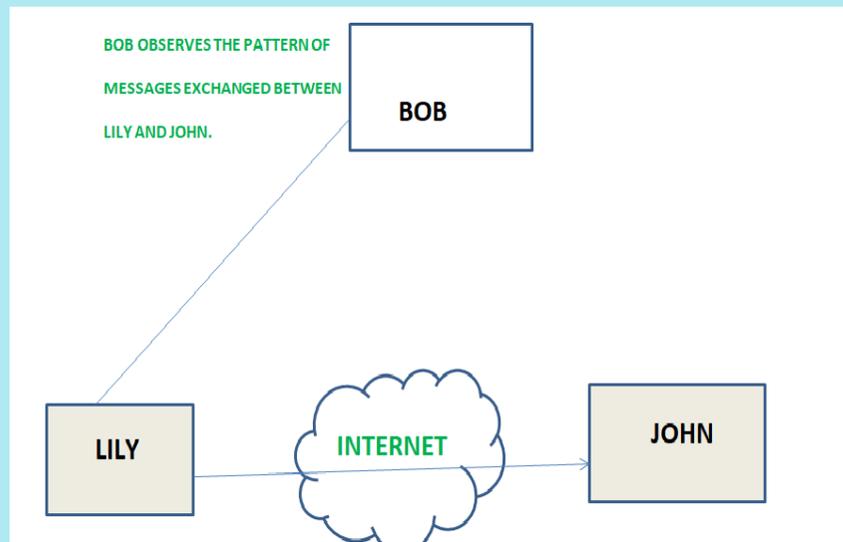
Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



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

## 2. Traffic analysis



guessing the nature of the communication that was taking place.

***Editorial dusk.....***

***Top 10 Antivirus Software for Windows 2018.....***

- ✓ Norton Antivirus
- ✓ Panda
- ✓ BullGuard
- ✓ Bitdefender
- ✓ MacKeeper
- ✓ Avira
- ✓ McAfee
- ✓ Kaspersky
- ✓ Trend Micro
- ✓ Intrusta

*Rush your ideas to*

**M. ASHOKVEL MCA.,M.Phil,M.Tech.,**

**Assistant Professor / CA**

**Editor – CAS**

**Mail-Id: [editor.cas@gmail.com](mailto:editor.cas@gmail.com), mashokvel@gmail.com**