SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19EC402- WIRELESS ADHOC AND SENSOR NETWORKS

IV ECE / VII SEMESTER

UNIT 5 – SECURITY ISSUES IN AD HOC / SENSOR NETWORK

TOPIC 1 – Introduction Need for Security

ACTIVE AND PASSIVE ATTACKS IN INFORMATION SECURITY

- In Cybersecurity, there are several kinds of cyber threats you need to know these days, that can relate to computer security, network security, and information security. There are basically two forms of threats: active and passive attacks. An active attack is an attack in which attackers directly harm your computer systems .

- They can create several problems, such as crashing files, stealing data, etc. On the other hand, a Passive attack refers to an attack in which the attackers quietly watch and collect the information without your knowledge.

ACTIVE AND PASSIVE ATTACKS IN INFORMATION SECURITY

- They do not modify or destroy the data but collect the data secretly. Therefore, having adequate knowledge about these threats will enable us to protect our personal information and computers safely.

- Sometimes, there is an integration of both types of attacks. In addition, technology is not the only means for attackers, some get your private information using tricky methods, such as manipulating someone to give them your password. In this article we will see Active and Passive attacks, how they take place, what kind of problems they cause, and how you may prevent such attacks from reaching your accounts.

WHAT IS 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.

- 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.

WHAT IS CYBER ATTACK?

- 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. This may include the injection of hostile code into communications, alteration of data, and masquerading as another person to get unauthorized access.

ACTIVE ATTACKS TYPES

Types of active attacks are as follows:

- Masquerade Attack
- Modification of Messages
- Repudiation
- Replay Attack
- Denial of Service (DoS) Attack

1. Masquerade Attack

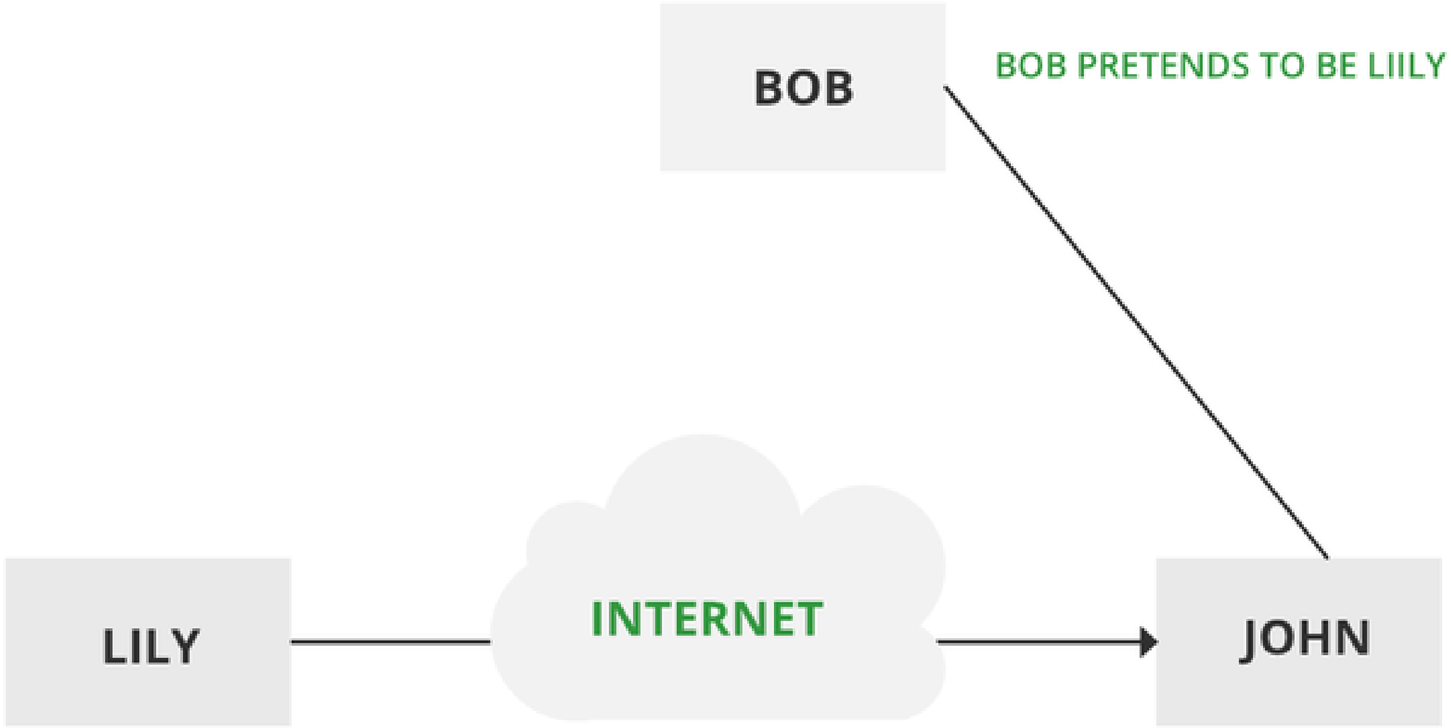
Username and Password Masquerade: In this masquerade attack, a person uses either stolen or even forged credentials to authenticate themselves as a valid user while gaining access to the system or application.

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.

1. Masquerade Attack

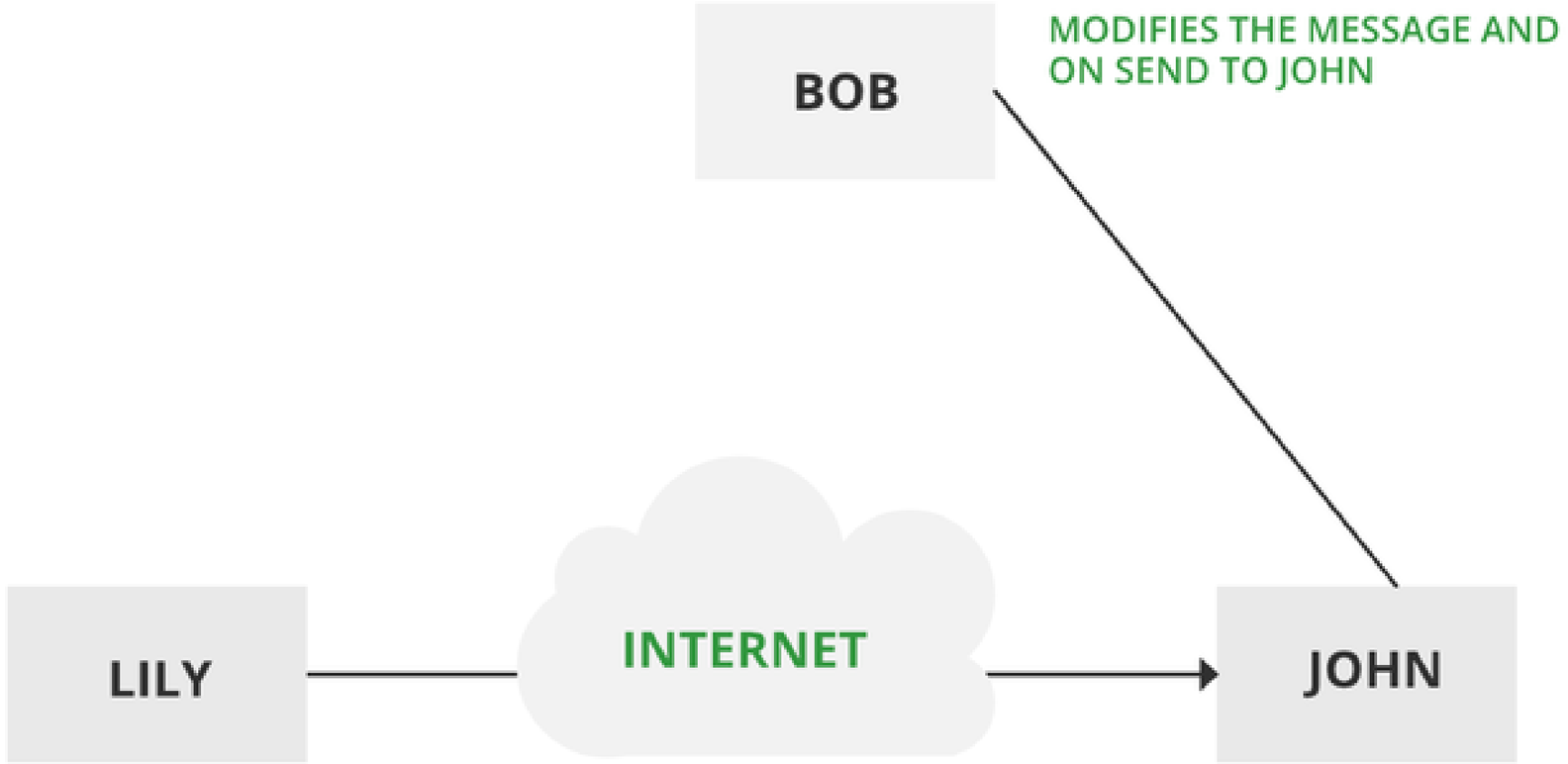


2. Modification of Messages

- 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”.

2. Modification of Messages



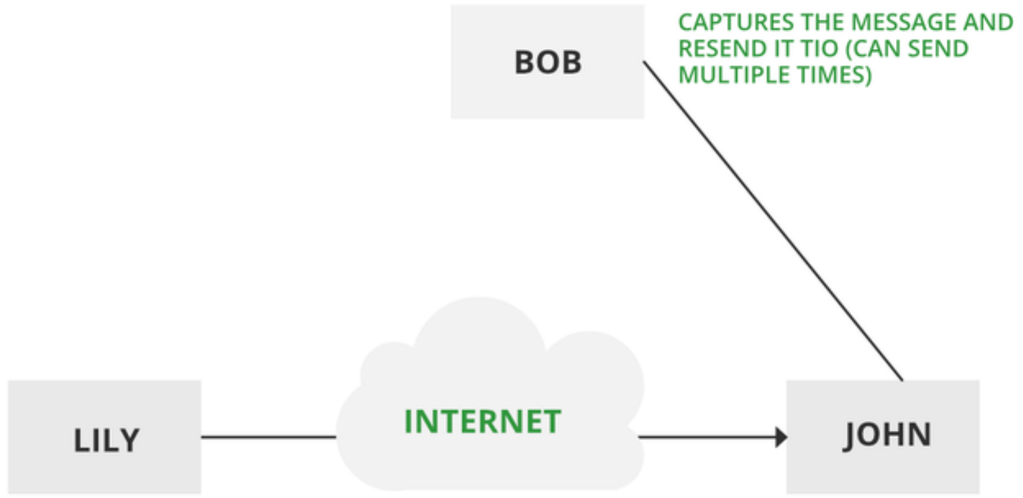
3. Repudiation

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.

3. 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.



THANK YOU