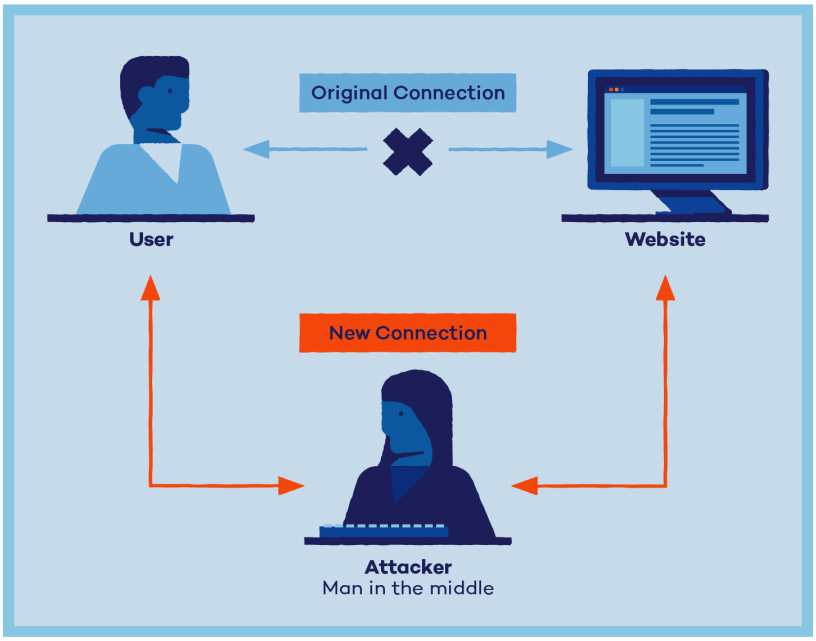
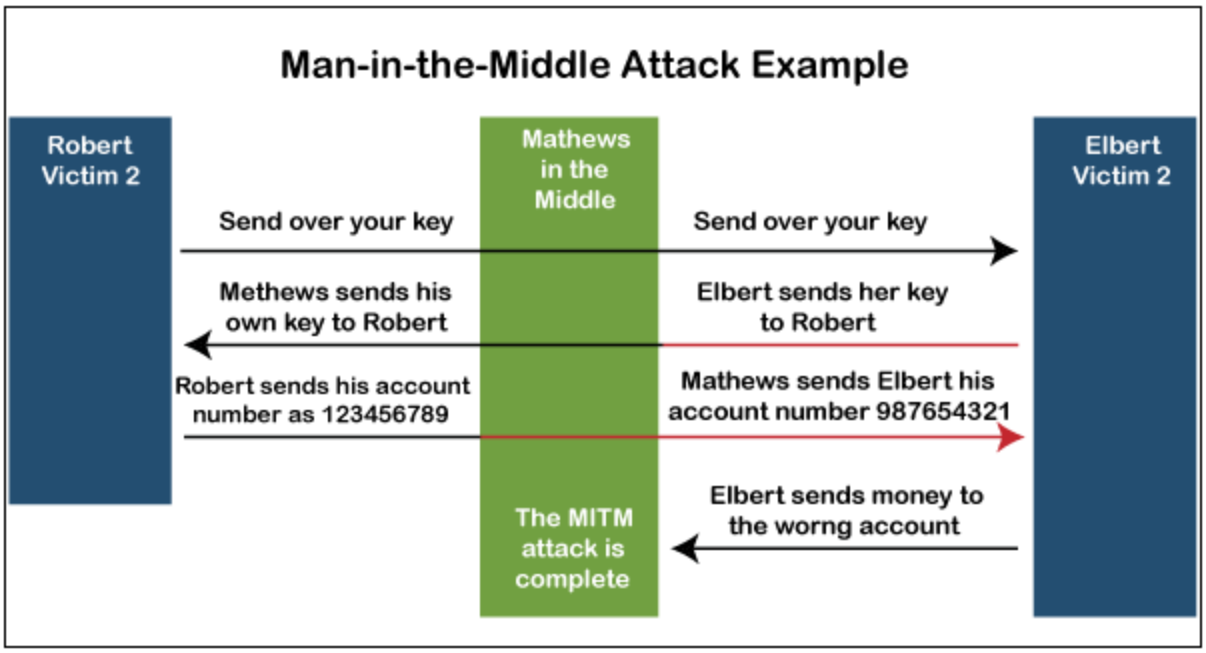
Module:- SECURITY CONCEPT
(MITM Attack)
Name:-Prithviraj Nikam

Lab Assignments:

Man-in-the-middle attacks (MITM):- Man-in-the-middle attacks (MITM) are a common type of cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen to, hence the name “man-in-the-middle.”

For example:-In order to intercept financial login credentials, a fraudulent banking website can be used. Between the user and the real bank webpage, the fake site lies "in the middle."





Types of MITM Attack

1. Interception

Interception involves the attacker interfering with a victim's legitimate network by intercepting it with a fake network before it can reach its intended destination. The interception phase is essentially how the attacker inserts themselves as the "man in the middle."

Wi-fi Eavesdropping

- You may have seen a notification that suggests, "This connection is not safe," if you've used a device in a cafe. Public wi-fi typically offers "as-is," without any promises of service quality.
- The unencrypted wi-fi networks are easy to watch. Although, it's just like having a debate in a public place-anybody can join in. You can limit your access by setting your computer to "public," which disables Network Discovery. This avoids other users on the network from exploiting the system.
- Some other Wi-Fi snooping attack occurs when an attacker establishes his own "Evil Twin" wi-fi hotspot. Attackers make the link, through the network Address and passwords, appear identical to the real ones. Users will link to

the "evil twin" unintentionally or automatically, enabling the attacker to intrude about their actions.

DNS Spoofing

- The Site operates with numeric IP addresses like **192.168.3.131** is one of Google's addresses.
- For example, a server is used by several sites to interpret the address to a recognizable title: google.com. A DNS server, or DNS, is the server that transforms 192.156.65.118 to google.com.
- A fraudulent Web server can be developed by an attacker. The fraudulent server transports a specific web address to a unique IP address, which is termed as "spoofing."

IP Spoofing

- Many devices connected to the same network contains an IP address, as we all know. Each device is equipped with its IP address in several enterprise internal web networks. In IP spoofing, the attackers imitate an approved console's IP address. For a network, it appears just as the system is authorized.
- It might be causing a network to be exploited by unauthorized access. They must stay quiet and track the actions, or a Denial of Service (DoS) attack may also be released. In a Middle-in-the-man attack, IP spoofing may also be used by placing between two devices.
- For Example, Device A and device B assume that they communicate with each other, but both are intercepted and communicated to the attacker.
  Device A= = = = Attacker= = = = Device B

ARP Spoofing

- ARP refers to the Protocol on Address Resolution.
- An ARP request is sent out by a client, and an attacker produces a fraudulent response. The attacker is like a computer modem in this situation, which enables the attacker to access the traffic flow. Usually, this is restricted to local area networks (LAN) that use the ARP protocol.

2. Decryption

A MITM attack doesn’t stop at interception. After the attacker gains access to the victim’s encrypted data, it must be decrypted in order for the attacker to be able to read and use it. A number of methods might be used to decrypt the victim’s data without alerting the user or application:

E-mail Hacking

- An attacker exploits the email system of a user in a such a kind of cybersecurity intrusion. The intruder also watches quietly, collecting data and eavesdropping on the discussion via email. The Attackers may have a scan pattern that searches for targeted keywords, such as "financial" or "hidden Democratic policies."
- Through Social Engineering, email hacking operates perfectly. To imitate an online friend, the attackers might use relevant data from some kind of hijacked email address. Spear-phishing can also be used to trick a user into downloading malicious apps.

Session Hijacking

- Usually, this form of MITM attack is often used to hack social media platforms. The webpage contains a "session browser cookie" on the victim's machine for most social media platforms. If the person steps off, this cookie is disproved. But when the session is running, the cookie offers identity, exposure, and monitoring data.
- A Session Hijack happens when a configuration cookie is stolen by an intruder. Unless the victim's account is hacked with malware or application attackers, it can arise. It can occur if a user exploits an XSS cross-scripting intrusion, in which the hacker injects malicious script into a site that is commonly visited.

SSL Stripping

- SSL refers to Secure Socket Layer. SSL is the security standard used if you see https:/ next to a website address, not http:/. The attacker accesses and routes data packets from a user using SSL Stripping:
- User = = = = Encrypted website User = = = = Authenticated website
- The user tries to link to a website that is secured. In the account of the client, the attacker encrypts and links to the secured website. Usually, a fake design is developed by the attacker to present it to the customer. The victim thinks that they have signed on to the normal website, but actually they signed in to

a hacker's website. The attacker does have the SSL certificate "stripped" from the data connection of the victim.

MITB attack

- This is a form of attack that leverages internet browser security flaws.
- The malicious attacks will be trojans, desktop worms, Java vulnerabilities, SQL injection attacks, and web browsing add-ons. These are commonly used to collect financial information.
- Malware steals their passwords as the user signs in to their bank account. In certain instances, malware scripts may move money and then alter the receipt of the transaction to conceal the transaction.

HTTPS Spoofing

- Duplicating an HTTPS webpage is not currently possible.
- A theoretical approach for circumventing HTTPS, however, has been illustrated by cybersecurity experts. The attacker creates an authoritative address.
- It uses letters of international alphabets rather than standard scripts. This acts as phishing emails with unusual characters that you might have used. Rolex may be written Rólex, for example.

Detection of Man-in-the-middle attack

- It is harder to identify a MITM attack without taking the appropriate measures. A Man-in-the-middle assault will theoretically proceed unchecked till it's too late when you do not consciously need to evaluate if your interactions have been monitored. Usually, the main technique for identifying a potential-attacks are always searching for adequate page authorization and introducing some kind of temper authentication; however, these approaches may need further forensic investigation after-the-fact.
- Instead of trying to identify attacks when they are operational, it is necessary to manage precautionary measures to avoid MITM attacks whenever they occur. To sustain a safe environment, being mindful of your surfing habits and identifying possibly hazardous environments can be important.

Prevention and How to Prepare

- **Avoid Wi-Fi networks** that aren't password-protected, and never use a public Wi-Fi network for sensitive transactions that require your personal information.
- **Use a Virtual Private Network (VPN) —** especially when connecting to the internet in a public place. VPNs encrypt your online activity and prevent an attacker from being able to read your private data, like passwords or bank account information.
- **Log out of sensitive websites** (like an online banking website) as soon as you're finished to avoid session hijacking.
- **Maintain proper password habits,** such as never reusing passwords for different accounts, and use a password manager to ensure your passwords are as strong as possible.
- **Use multi-factor authentication** for all of your passwords.
- **Use a firewall** to ensure safe internet connections.
- **Use antivirus software** to protect your devices from malware.