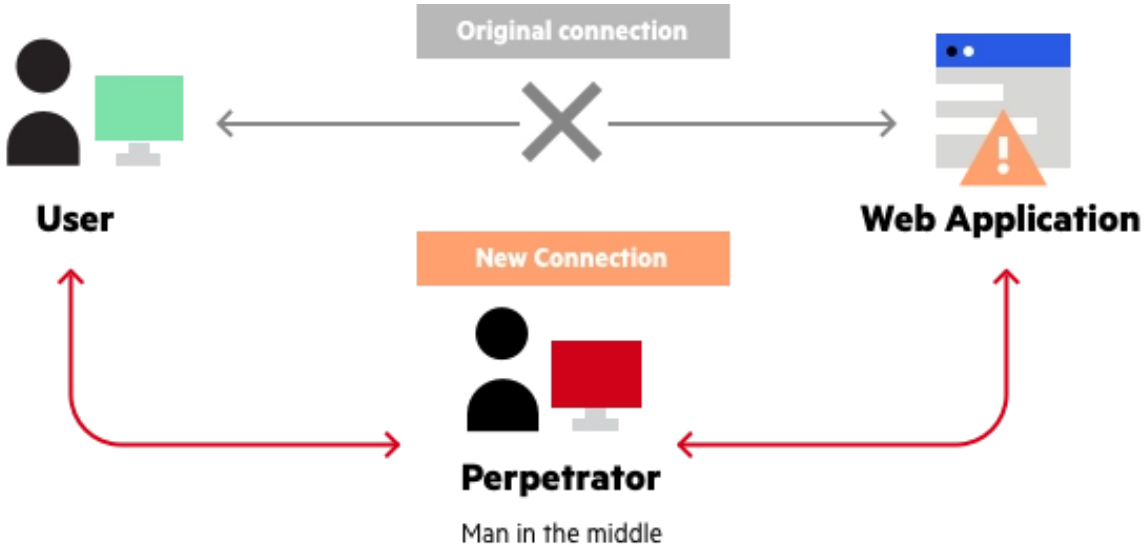
ITEC442 IOT & Cyber Security

Week 6-7 – MITH Attack

What is a man in the middle attack?

A man-in-the-middle (MITM) attack is a type of cyber attack where an attacker intercepts communication between two parties and pretends to be one of them to the other. This allows the attacker to see and potentially modify the communication, as well as trick the parties into thinking they are communicating directly with each other. There are various ways that an attacker can perform an MITM attack, but one common method is to use a device that is connected between the two parties, such as a router or network switch, and to configure it to forward traffic between them while also allowing the attacker to see and potentially modify the traffic.

To prevent MITM attacks, it is important to use secure protocols for communication, such as HTTPS, which encrypts the communication and makes it difficult for an attacker to read or modify the traffic. Other measures that can be taken include using strong passwords and two-factor authentication, and being cautious about connecting to unknown networks or devices. It is also a good idea to use a firewall and antivirus software to protect against malware and other types of attacks.



MITM attack progression

Successful MITM execution has two distinct phases: interception and decryption.

Interception

The first step intercepts user traffic through the attacker's network before it reaches its intended destination.

The most common (and simplest) way of doing this is a passive attack in which an attacker makes free, malicious WiFi hotspots available to the public. Typically named in a way that corresponds to their location, they aren't password protected. Once a victim connects to such a hotspot, the attacker gains full visibility to any online data exchange.

Attackers wishing to take a more active approach to interception may launch one of the following attacks:

- **IP spoofing** involves an attacker disguising himself as an application by altering packet headers in an IP address. As a result, users attempting to access a URL connected to the application are sent to the attacker's website.
- **ARP spoofing** is the process of linking an attacker's MAC address with the IP address of a legitimate user on a local area network using fake ARP messages. As a result, data sent by the user to the host IP address is instead transmitted to the attacker.
- **DNS spoofing**, also known as DNS cache poisoning, involves infiltrating a DNS server and altering a website's address record. As a result, users attempting to access the site are sent by the altered DNS record to the attacker's site.

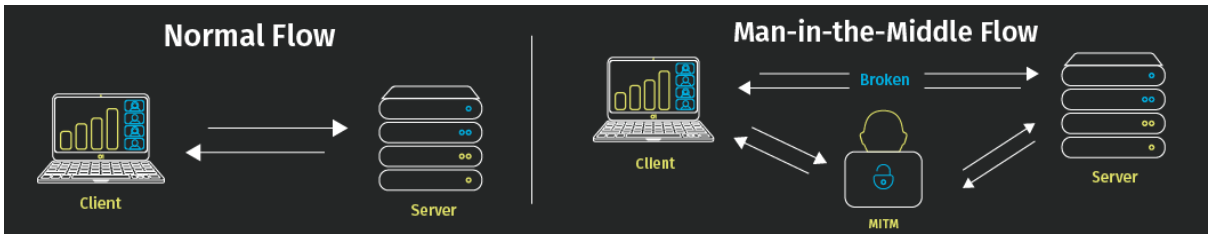
Decryption

After interception, any two-way SSL traffic needs to be decrypted without alerting the user or application. A number of methods exist to achieve this:

- **HTTPS spoofing** sends a phony certificate to the victim's browser once the initial connection request to a secure site is made. It holds a digital thumbprint associated with the compromised application, which the browser verifies according to an existing list of trusted sites. The attacker is then able to access any data entered by the victim before it's passed to the application.
- **SSL BEAST** (browser exploit against SSL/TLS) targets a TLS version 1.0 vulnerability in SSL. Here, the victim's computer is infected with malicious JavaScript that intercepts encrypted cookies sent by a web application. Then the app's cipher block chaining (CBC) is compromised so as to decrypt its cookies and authentication tokens.
- **SSL hijacking** occurs when an attacker passes forged authentication keys to both the user and application during a TCP handshake. This sets up what appears to be a secure connection when, in fact, the man in the middle controls the entire session.
- **SSL stripping** downgrades a HTTPS connection to HTTP by intercepting the TLS authentication sent from the application to the user. The attacker sends an unencrypted version of the application's site to the user while maintaining the secured session with the application. Meanwhile, the user's entire session is visible to the attacker.

Examples of MITM Attacks

Although the central concept of intercepting an ongoing transfer remains the same, there are several different ways attackers can implement a man-in-the-middle attack.



Scenario 1: Intercepting Data

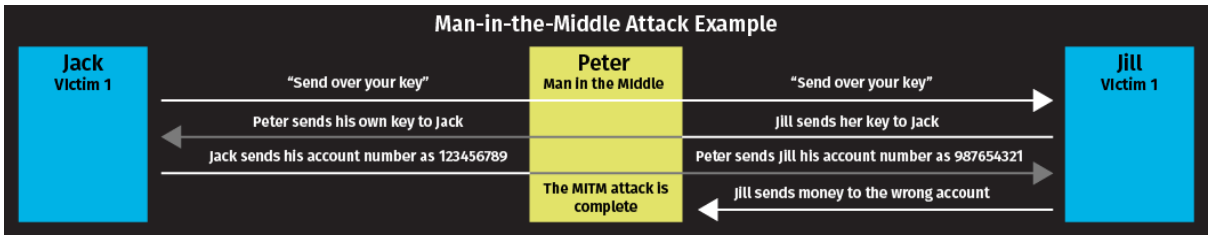
1. The attacker installs a packet sniffer to analyze network traffic for insecure communications.
2. When a user logs in to a site, the attacker retrieves their user information and redirects them to a fake site that mimics the real one.
3. The attacker's fake site gathers data from the user, which the attacker can then use on the real site to access the target's information.

In this scenario, an attacker intercepts a data transfer between a client and server. By tricking the client into believing it is still communicating with the server and the server into believing it is still receiving information from the client, the attacker is able to intercept data from both as well as inject their own false information into any future transfers.

Scenario 2: Gaining Access to Funds

1. The attacker sets up a fake chat service that mimics that of a well-known bank.
2. Using knowledge gained from the data intercepted in the first scenario, the attacker pretends to be the bank and starts a chat with the target.
3. The attacker then starts a chat on the real bank site, pretending to be the target and passing along the needed information to gain access to the target's account.

In this scenario, the attacker intercepts a conversation, passing along parts of the discussion to both legitimate participants.



Real-World MITM Attacks

In 2011, Dutch registrar site DigiNotar was breached, which enabled a threat actor to gain access to 500 certificates for websites like Google, Skype, and others. Access to these certificates allowed the attacker to pose as legitimate websites in a MITM attack, stealing users' data after tricking them into entering passwords on malicious mirror sites. DigiNotar ultimately filed for bankruptcy as a result of the breach.

In 2017, credit score company Equifax removed its apps from Google and Apple after a breach resulted in the leak of personal data. A researcher found that the app did not consistently use HTTPS, allowing attackers to intercept data as users accessed their accounts.

My Reflections from the references and given videos:

A man-in-the-middle (MITM) attack is a type of cyber attack in which an attacker intercepts communication between two parties and pretends to be one of them to the other. This allows the attacker to see and potentially modify the communication, as well as trick the parties into thinking they are communicating directly with each other. MITM attacks can be difficult to detect and prevent, and can have serious consequences if they are successful.

One way to think about MITM attacks is as a kind of "reflection" on the normal process of communication between two parties. In a normal communication, there is a clear sender and a clear receiver, and the message is transmitted directly from the sender to the receiver. In an MITM attack, the attacker reflects the message back to the sender, effectively inserting themselves into the middle of the communication and altering the normal flow of information.

To prevent MITM attacks, it is important to use secure protocols for communication, such as HTTPS, which encrypts the communication and makes it difficult for an attacker to read or modify the traffic. Other measures that can be taken include using strong passwords and

two-factor authentication, and being cautious about connecting to unknown networks or devices. It is also a good idea to use a firewall and antivirus software to protect against malware and other types of attacks.

References:

https://www.youtube.com/watch?v=p4pLVN_hVsU

https://www.youtube.com/watch?v=DgqID9k83oQ

https://www.veracode.com/security/man-middle-attack

https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/