Man In The Middle Attack

Introduction

We all have been using computers and alike devices on a daily basis for a long time now. And with its constant and ongoing evolution, new techniques are getting built so as to ease the pressure of manually doing a certain task or to make the process work much faster. This all is being possible because of the computers and technology advancements. But as the verse goes, “A coin has two sides”, not everything is very secure and it causes data theft and probable wrong uses of the same. Man In The Middle Attack is of such type.

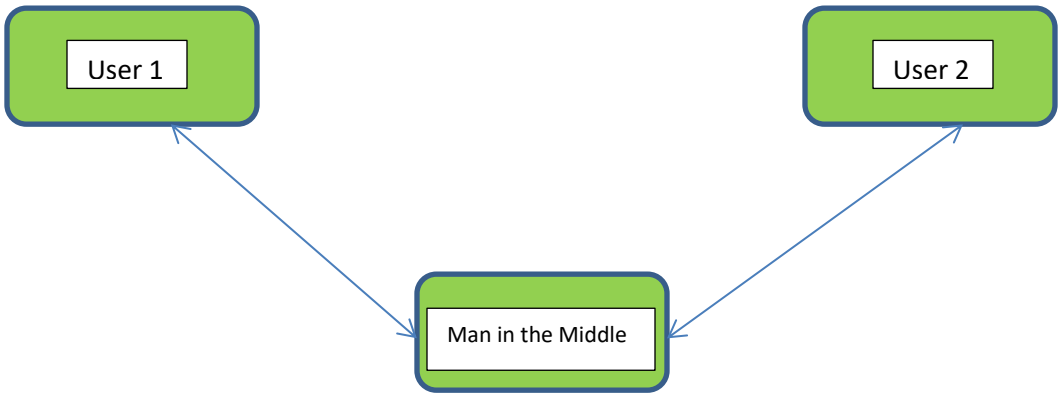
What is Man In The Middle Attack:

When two users are communicating with each other and another third unknown entity enters into the conversation to eavesdrop so as to attain the data from the conversation. This third unknown entity is totally unknown to the recipient and sender of the communications (users). E.g.: You are chatting with someone online. There’s a third unknown entity present in the communication, which is totally unknown to both of you. This third person might chat individually with both in a way that both will keep thinking that the other is sending messages. Or the third entity can intercept the messages and add new content to it. This all will be done so discreetly that both the users will remain totally un-notified.

Following diagrams depicts how a MITM happens:

1. **Original / Valid Communication:**

2. **Invalid / MITM Attacked Conversation :**



As depicted in the Figure 1: this is the regular route or the channel through which the communication should take place.

Figure 2: The communication is taking place through the altered channel and Man in the Middle has attacked the systems /users.

In simple words, Main in the Middle Attack is same to the person who eavesdrops in the conversation and uses the information for his / her benefit.

Types of Man in the Middle Attack:

a. **Session Hacks:**

   We often get notifications when we browse about cookies and sessions. So these cookies and sessions store the information which is our personal. It might contain login ids and passwords. So what MITM attackers do is, they get the hold of these session cookies and once they have it, all the sensitive data is accessible to them and then the data theft happens. Generally, all the sites have auto-fill up forms, and ask users to enter the passwords and verify, etc, this is where the get peoples data.

b. **Email Hacks:**
   MITM attackers access the interception of messages between two users. First user sends some sensitive information over the net to the second user. So, it works exactly like the figure 2. The attacker sends the email the either parties, which is masked, that means, either one doesn't figure it out that it is fake and demands some sensitive information or account details and then the hacking takes place.

c. **Wi-Fi Hacks:**
   Generally, this happens when users connect to a free Wi-Fi source and hackers can easily target such users. Free Wi-Fi sources are very crucial mediums of connections, as very low level of security is made available through it. Another Wi-Fi hack is, the attackers develop a very similar network to what the users are currently working on.

Purpose & Motive of Man in the Middle Attack:

Man in the Middle attackers; generally target the users who are naïve with the network controls. Easy targets. But, it doesn't mean that complex systems cannot be hacked. These attackers gather this information and then use it like a normal user uses it. It is mainly targeted to get sensitive information of / from the users like account details, bank PINs. This information helps them to enter into the system and use it or even sell the information. This has been seen recently many times, that due to the attacker, system data has been published online or sensitive data has been leaked.

How does Man in the Middle Attack happen:

There are two main steps with the help of which MITM attackers hacks into the systems;viz:

1. **Interception:**
   The attacker makes an dummy network which can be used by users for free. And when the users enters the data, it is first transferred to the attackers files and then towards the real location. This is the passive and most easy of attacking the systems. Attackers might use one of the following ways too:
   a. **IP Spoofing:** All the devices have IP addresses. When the user enters the data over a network, it gets transferred to the receivers IP address. But in between, the attackers create some IP addresses which are very similar to the recipients IP address. So, instead of sending data to the real destination, it gets transferred to the attackers IP address.
   b. **ARP Spoofing:** In this, MAC addresses of the attackers are attached alongwith the IP address of the user. So data gets transferred to the attackers IP address as soon as it is sent.
   c. **DNS Spoofing:** DNS means Domain Name System. Attackers, change the cache records of the browsers. So when the user enters the given site, instead of going to the correct URL / website, it is sent to some dummy site which has been created by the attacker.

2. **Decryption:**
   a. **HTTPS Spoofing:** Generally all the users see the “https” as secure. But in this attacker,puts in manually a certificate, which looks like secure and trusted to be used. So, all the data is routed through it. But as it looks similar to secure site, browser sends the key to read the data and attacker gains access to the information.
   b. **SSL Beast:** Attacker infects the user’s computer with some false cookies and CBC is compromised, so the data is easily decrypted.
   c. **SSL hijacking:** As mentioned earlier, HTTPS stands for secure. But, just before the browser connects to the HTTPS from HTTP, it is routed to the attacker’s browser.
   d. SSL Stripping: Attacker brings down the website security to a level, where all it is in between HTTPS and HTTP. So all the data is available in non-encrypted textual format.

What to do after Man in the Middle Attack and How to prevent it

There are certain ways / steps which can be followed to prevent the attack after it has taken place, viz:

1. Check the security levels of the networks, to which you are connected with.

2. Never connect to the Free Wi-Fi source unless it is from a known source.

3. Stay alerted of potential fraudulent emails and unknown links,which might lead to other unknown websites.

4. Stay connected to the websites, which are connected with HTTPS protocols, they have more level of security over HTTP.

5. Use VPN’s while on a network, so the data which is being used or transferred securely. All the data is fetched and saved using VPN is encrypted.

6. Use anti-malware softwares which detect and eliminate the malwares.

Conclusion:

While using data on network, always stay connected to the secure sites and avoids clicking on the links which might lead to some unknown sources.