A Survey on Man-in-the-Middle Attacks

Umang Chaturvedi, Apoorv Mishra, Prof. Varsha Tyagi
Guide (CSE Dept.)

DEPARTMENT OF COMPUTER SCIENCE
VISHVESHWARYA GROUP OF INSTITUTIONS
DADRI, GHAZIABAD
203207

Abstract- This research paper presents information about Man in the Middle attacks and prevention against them. The most common attack occurs due to ARP poisoning, sniffing, spoofing and hijacking. MITM Attacks are occurring a lot in now a day. Not everyone is technologically literate and thus are being victim and losing their privacy.

1. INTRODUCTION

MITM attacks challenges the data security and privacy since attacks can be performed from remote computers with fake addresses. The MITM attacks takes the advantages of weaknesses in the authentication protocol used in communication. The authentication is usually provided by third parties who provide certificates.

The MITM attacks allows the attacker to sniff on data through backdoor or payload. These payloads are also being used by industries to pry upon their employee or customer and even for advertisements.

Consider two individuals, namely X and Y, communicating with each other. The third- party, Z, is the MITM performer. The communication between X and Y starts after the authentication. If the authentication protocol is not strong, then Z can act as the other communicating party to both X and Y.

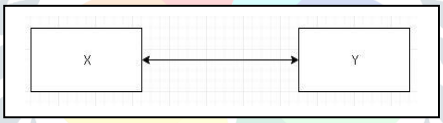

Figure 1: Normal Communication between X and Y

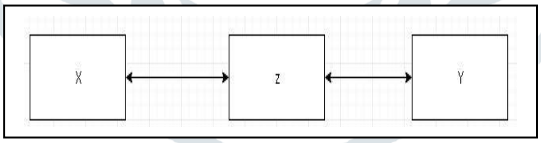

Figure 2: MIM attack performed by Z

In this MIM attack, Z will start communicating with both X and Y. The information between X and Y will go through Z as Z will impersonate X as Y and Y as X. Both X and Y won't know about Z intercepting. Therefore, Z will take advantages of X and Y without their knowledge and obtains vital information.

2. HOW ARE MITM ATTACKS PERFORMED

In a public place that provides free Wi-Fi connection available, if a user visits an unsafe website at that time from phone or laptop, he or she may end up losing important credentials. These attacks can be caused because of the following reasons and techniques: -

2.1 ARP Cache Poisoning
2.2 DNS Spoofing
2.3 Session Hijacking
2.4 Packet Sniffing

2.1 ARP CACHE POISONING

For understanding about ARP Cache Poisoning, one should know about ARP (Address Resolution Protocol).

2.1.1 ADDRESS RESOLUTION PROTOCOL (ARP)

In ARP communication, the host PC will send a packet which has the source and destination IP address inside the packet and will broadcast it to all the devices connected to the network. The device which has the target IP address will only send the ARP reply with its MAC address in it and then communication takes place. The ARP protocol is not a secured protocol and the ARP cache doesn't have a secure mechanism which results in a big risk.

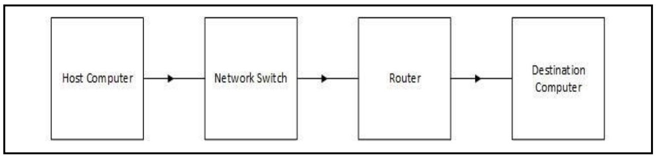

Figure 3: Regular traffic flow between two Computers

Back in ARP Cache Poisoning, the attacker would sniff the network by controlling the network switch to monitor the network traffic and spoof the ARP packets between the host and the destination PC and perform the attack.

The attacker can modify the sequence numbers and keep the connection synchronized while keep injecting packets.

This is how ARP Cache Poisoning takes place using the vulnerabilities of Address Resolution Protocol communication.

2.2 DNS SPOOFING

In DNS Spoofing, the host will be provided with fake information which would lead to loss of information. This attack is a kind of online MIM attack where the attacker creates a fake website, so when you visit it, you will be redirected to the website created by the attacker and then the attacker will gain all your credentials or sensitive information. Whenever we enter a website on our PC, DNS request is sent to the DNS Server and we will get a DNS reply message in the response.

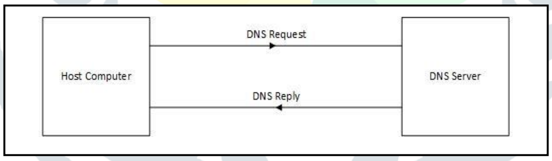

Figure 4: DNS Communication between the host and the DNS Server

This DNS reply and request are mapped together with a unique identification number. If the attacker gets hold of the unique identification number, then by disguising the victim with a corrupt packet containing the identification number, he can launch the attack.

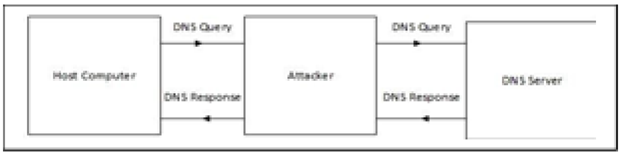

Figure 5: The attacker performs MIM attack using DNS Spoofing

The host computer will send a DNS query request to the DNS server but due to the MIM attack the attacker will intercept this DNS query and send a fake DNS reply to the host PC. The host PC wouldn’t come to know whether the response is legitimate or not and it will start communicating with the malicious website of the attacker

2.3 SESSION HIJACKING

A session is formed when client is connected to the server. Transmission Control Protocol is referred as a session since it first establishes a connection, then transfers the data and finally terminates the connection. This is known as the 3-way handshake process which shows how a proper session looks like.

Session hijackings is thus further done by stealing cookies with the help of Hyper Text Transfer Protocol (HTTP) or other protocols like TELNET etc.

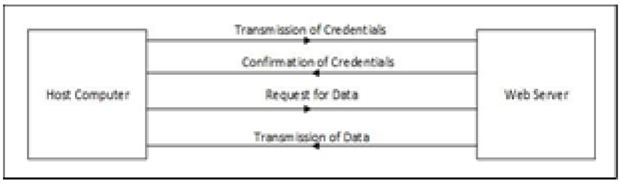

Figure 6: Session Establishment between the host PC and Web Server

2.4 PACKET SNIFFING

Whenever any type of data has to be transferred over the computer network from the sender's end, it is divided into smaller units which are called data packets and reassembled at receiver's end in original format. It is the smallest unit of communication over a computer network. The act of capturing data packet across the computer network is called packet sniffing.

The packet sniffing is performed by tools called Packet Sniffers. It can either be filtered or unfiltered. Filtered is used when only specific data packets have to be captured and unfiltered one is used when all the packets have to be captured. WireShark, EtterCap are examples of packet sniffing tools.

3. PREVENTIONS AGAINST MITM ATTACKS

MITM Attacks can be prevented by following ways: -

- Using Secure Socket Layers (SSL) which provides secure communication by using encryption methodology i.e. using https.
- Refrain from connecting to public Wi-Fi hotspots that are not password protected. And if connected to one, it is always advisable not to perform any sensitive and financial transactions.
- Pay close attention to any alerts or warning messages related to insecurity of websites.
- Log out of any application when not in use and always keep your system updates and protected by antiviruses.
- Never give your device in strangers' or suspicious people. Etc.

CONCLUSION

Since we cannot prevent MITM Attacks completely, we can always try to minimize the possibilities of such attacks by taking some security measures as stated above. Ultimately, MIM attack will remain an attack of choice not only for bad people but also for surveillance groups and for industries since anything can either be used in positive or negative ways. The choice is always yours.

***Acknowledgement**: -* This research was supported by Prof. Varsha Tyagi (CSE Dept.). We thank her as she provided insight and expertise that greatly assisted the research.

REFERENCES

[1] Subodh Gangan, A Review of Man-in-the-Middle Attacks, 2015.

[2] G. Nath Nayak, S. G. Samaddar, "Different flavours of man-in-the-middle attack consequences and feasible solutions", Proc. 3rd IEEE Int. Conf. Computer Sci. Inf. Technol. (ICCSIT), vol. 5, pp. 491-495, 2010.

[3] S. M. Bellovin, M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks", Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy, pp. 72-84, 1992.

[4] R. Demillo, M. Merritt, "Protocols for data security", Computer, vol. 2, no. 16, pp. 39-51, 1983.

[5] W. Baker et al., "Data breach investigations report", Methodology, vol. 36, pp. 1-63, 2011.

[6] S. Frankel, B. Eydt, L. Owens, K. Scarfone, "Establishing wireless robust security networks: A guide to IEEE 802.11i", 2007.

[7] Capec-94: Man in the Middle Attack, 2014.

[8] R. Wagner, "Address resolution protocol spoofing and man-in-the-middle attacks" in Bethesda, Maryland, USA, 2001.

[9] Trend Micro, What is the Man-In-The-Middle attack and how can I protect myself from them?, 28th November 2012.