BOOK CHAPTER | Man-In-The-Middle-Attacks

Man-In-The-Middle-Attacks: Types, Methods, Detection and Preventive Measure.

Akinsanya Seye Emmanuel
Department of Computer Science
Federal University Oye-Ekiti
Ekiti State, Nigeria
E-mail: sedalomo1@gmail.com
Phone: +2348100381619

Abstract

Cyber-attacks are now a significant illegal act, and this has made it a bone of contention, as well as a highly discussed topic. Man-In-The-Middle Attacks are categories of cyberattack in which an unauthorized third party penetrate an internet conversation between two users and remains unnoticed by the two sides. The information which was acquired by the two users is frequently monitored and changed by the malware which is in the middle of the attack. An external individual in the system is susceptible to a man-in-the-middle attack, which allows the external individual to obtain, read, and modify confidential information without leaving any traces of manipulation. This is a serious problem, as most cryptosystems without adequate authentication protection are at risk of being attacked by malware known as 'Man-In-The-Middle-Attack'. This research primarily focuses on recognizing the term 'Man-In-The-Middle-Attacks'; the research is mostly focused on gathering related data/information that may be used as a reference to do additional study related to this research. This research also examines the most cited publications on 'man-in-the-middle-attack' that have been found on 'Google Scholar' and some related the internet The purpose of this research is to assist readers in comprehending and familiarizing themselves with the concept of 'Man-In-The-Middle Attacks'.

Keywords: Cybersecurity, Cyberattack, Malware, Cryptosystems, Eavesdropping, Internet Security, network traffic

Introduction

A man-in-the-middle also known as monster-in-the-middle(Gabbi and Luke, 2019), monkey-in-the-middle, machine-in-the-middle (John, 2019), meddler-in-the-middle or person-in-the-middle (ACSC, 2020) attack is a cyberattack in which the perpetrator discreetly relays and perhaps modifies messages between two users who feel they are speaking directly with each other while the perpetrator has positioned himself between them (Elakrat et al., 2018). A laudable example of mam-in-the-middle-attack is eavesdropping, where the attacker establishes separate connections with the victims and send and receive data between them.

Citation: Akinsanya S.E (2022). Case Study: Assessment of Insider Data Attack.
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

The attacker gives the impression that they are speaking directly with each other over a secure connection when, in reality, the attacker is controlling the entire discussion. The intruder must be able to disrupt and inject any important messages transferred between the victims. In several cases, this is feasible; for instance, an intruder intercepting an unsecured Wi-Fi access point might act as a man-in-the-middle (Tanmay, 2013). An attack can only work if the intruder manipulates each endpoint well enough to match their requirements, as it seeks to evade authentication process. To mitigate Malicious activities, most cryptographic systems also include endpoint authorization. TLS, for instance, can use a mutually recognized certificate authority to validate one or both sides (Callegati et al., 2009).

Categories of Man-In-The-Middle Attack

Man-in-the-middle attacks take advantage of a variety of flaws, including:

- DNS Spoofing: DNS transforms domain names to IP addresses in the same way that ARP converts IP addresses to MAC addresses on a LAN. The intruder tries to introduce faulty DNS cache content to a host in order to visit another host claiming their domain name, such as www.gistfun.com, while utilizing a DNS spoofing attack. As a result, the target sends sensitive data to a malicious server, believing they are communicating with a trusted party.
- Rogue Access Point: Wireless-card-equipped devices will frequently try to connect to the access point that has the strongest signal. Attackers can create their own wireless access point and entice neighboring devices to connect to it. The attacker now has access to all of the target's network traffic. This is harmful since the attacker may not even have to be connect to a trusted network to execute this; what they really need is physical proximity.
- mDNS Spoofing: Multicast DNS is related to DNS, but this is executed on a LAN utilizing broadcast, related to ARP. As a result, it's an appropriate option for spoofing attacks. Users don't need to recognize which addresses their computers should communicate with; instead, they can let the system figure it out. This protocol is used by devices such as televisions, printers, and sound systems because they are often connected to recognized networks.
- ARP Spoofing: The Address Resolution Protocol (ARP) is a protocol for resolving addresses. In a local area network, ARP is used to resolve IP addresses to the physical media access control addresses. Whenever a system needs to communicate with another system with a specific IP address, the ARP cache is used to convert the IP address to the MAC address. If the address is unknown, a request is sent for the device's MAC address along with the IP address. An attacker posing as another host could use its own MAC address to interact with users it shouldn't be responding to. An attacker might sniff the private traffic between different hosts with a few carefully placed packets.

The Basic Methods of Man-In-The-Middle Attacks

The basic methods employed by an attacker to lunch man-in-the-middle attacks are highlighted below:

- Packet Injection: Attackers can use the monitoring mode on their device to inject malicious packets into data transmission streams. The malicious packets might mix with legitimate data transmission streams, giving the impression that they are part of the conversation but are actually harmful. Sniffing is usually the initial step to identify how and when to build and deliver packets in packet injection.
- Sniffing: Packet capture methods are used by attackers to inspect packets at a low rate. An attacker can observe packets that are not meant for it to see, such as packets addressed to other hosts, by using specified wireless devices that are authorized to be set into monitoring mode.

- Secure Socket Layer (SSL) Striping: HTTPS is a typical defense against DNS or ARP spoofing, intruders capture packets and redirect HTTPS-based address entries to their own HTTP equivalent destination, compelling the host to make unsecured requests to the server.
- Session Hijacking: In order to prevent the user from typing a password at every page, several web applications utilize a login method that creates a temporary session id that may be used for subsequent requests. Someone that wanted to launch an attack can sniff vital traffic to find a user's session id and then use it to request access in the user's name. As soon as the attacker get the session id, he won't need to spoof again.

Detection of Man-In-The-Middle Attacks

Unless necessary precautions are taking, identifying a Man-in-the-Middle attack may be very difficult. Man-in-the-Middle attack might go unreported until it was far too late if you're not constantly looking to see whether your communications have in one way or the other been intercepted. The major approaches for detecting a prospective attack include often checking for correct page authentication and adopting some type of tamper detection, however these procedures may necessitate additional forensic investigation after the fact. Instead of attempting to identify MITM attacks while they are ongoing, it is critical to take preventative measures to avoid them before they occur. Ensuring a secure network requires being conscious of your browsing habits and detecting potentially dangerous sites. Some basic preventive measure will be highlighted in the next section.

Preventive measures against Man-In-The-Middle-Attack

Man-in-the-middle-attack can be mitigated by implementing the following measures:

- Make sure your wireless access point has strong encryption. The more robust the encryption, the safer it is.
- Your router login details must be strong and well secure. Once an attacker discovers the login details of your router, they can redirect your DNS requests to their own malicious servers. Or, probably, install malicious files on your router.
- You can make use of a Virtual Private Network (VPN) to provide a secure important data while using a local area network. VPN construct a secure communication subnet by using key-based encryption. In the process of a shared network, if an attacker gain access he won't be able to decrypt the data in the VPN
- To have a secure communication over the HTTP, HTTPS can be adopted by utilizing public-private key exchange. This will stop an attacker from using the information he is sniffing.
- Make use of pair based public key authentication such as RSA which can be used at multiple stages of the network to confirm that what you are connecting with are the right channel you want to communicate with.

Conclusion

This research focuses on the basic analysis of man-in-the-middle attacks, a comprehensive categories, methods, detection and preventive measure of man-in-the-middle-attack was presented. Even though the research did not elaborate on a detailed analysis of anticipated MITM research directions, it did provide a good knowledge of MITM and the basic MITM prevention measures.

References

1. Gabbi, F. & Luke V. (2019, March). "Monsters in the Middleboxes: Introducing Two New Tools for Detecting HTTPS Interception" (https://blog.cloudflare.com/monsters-in-the-middleboxes/).
2. Matthias, F. (2018, April). "Usable Authentication Ceremonies in Secure Instant Messaging" (http://www.ifs.tuwien.ac.at/~weippl/Thesis/2018/Matthias%20Fassl%20%20Usable%20Authentication%20Cer emonies%20in%20Secure%20Instant%20Messaging.pdf) (PDF).
3. John, R. R. (2019, November). "Monkey In The Middle" (https://sites.psu.edu/hacking/2017/02/2 4/monkey-in-the-middle/).
4. ACSC (2020, May). "Person-in-the-middle" (https://www.cyber.gov.au/acsc/view-all content/glossary/person-middle).
5. Elakrat, M. A., & Jung, J. C. (2018). Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network. *Nuclear Engineering and Technology*, *50*(5), 780-787.
6. Tanmay P., (2013, November). "How to defend yourself against MITM or Man-in-the-middle attack" (https://web.archive.org/web/20131124235452/http://hackerspace.lifehacker.com/how-to-defen d-yourself-against-mitm-or-man-in-the-middl-1461796382). Archived from the original (https://hackersp ace.lifehacker.com/how-to-defend-yourself-against-mitm-or-man-in-the-middl-1461796382) on November 24, 2013. Retrieved November 25, 2014.
7. Callegati, F., Cerroni, W., Ramilli, M., (2009). "Man-in-the-Middle Attack to the HTTPS Protocol". IEEE Security & Privacy Magazine. 7: 78–81. doi:10.1109/MSP.2009.12 (https://doi.org/10.110 9%2FMSP.2009.12) . S2CID 32996015 (https://api.semanticscholar.org/CorpusID:32996015).