Final Project: 'Man in The Middle' Attack

Dilnoza Saidova, Abdulrehim Shuba, and Gil Rabara

University of Washington, Tacoma

TCSS483: Secure Coding Principles

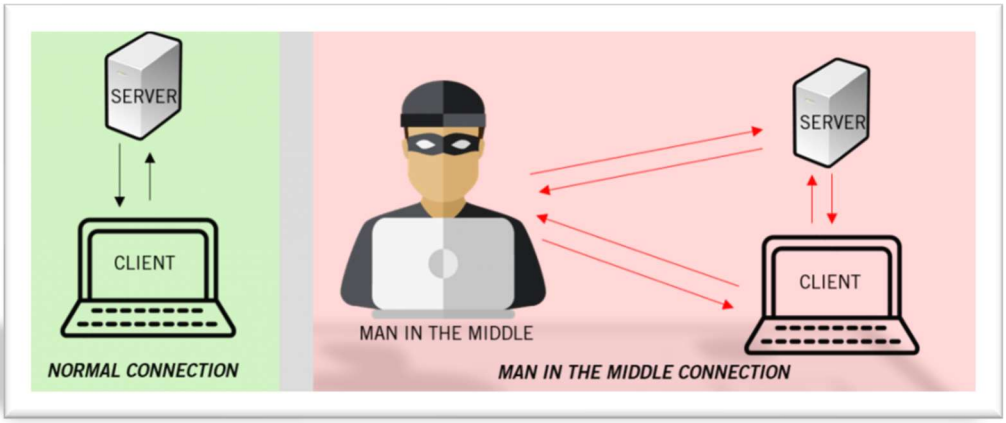
August 19, 2022

Abstract

As computer systems and applications develop and improve so do cyber-attacks directed at them. One of such attacks is Man in the Middle attack (MITM), which can also be referred to as a hijack attack. MITM is one of the most prevalent and well-known cybersecurity attacks where a third party targets a connection between two parties online without their awareness nor permission. In such cases the malware can monitor and change the exchanged only by those two parties, making this cyber-attack an important matter. The purpose of this paper is to introduce and discuss the Man in the Middle attack, its types, and how it can be prevented.

1. Introduction: What is MITM Attack and How Does it Work?

Internet has become one of the most important aspects of life in this age. A lot of people's day-to-day activities are closely tied to their phones and the Internet. Some of the examples of such activities could be sending emails, internet banking, and online shipping, all of which have made people's lives easier through digitalization of data, its storage and exchange. The amount of time and dependence people put in their digital devices and the Internet has opened doors of possibility of cyber-attacks aimed at accessing and/or stealing people's personal data. The first ever-recorded MITM attack was planned and executed by the Royal British Intelligence (MI-6) during WWII for intercepting the German Military's radio communications. In today's day and age, most of the MITM attacks are done through social media such as Twitter, Instagram, messenger aps, emails, etc.



Man-in-the-Middle attack is sometimes referred to as *monster-in-the-middle*, *machine-in-the-middle*, *man-in-the-browser*, and *monkey-in-the-middle*, and can be abbreviated as MIM, Mim, MitM, MITM, or MITMA. This is a type of cyber-attack over a communication channel through a malicious third party where overly personal or confidential information between two parties is targeted. In MITM cyber-attack, the attacker has access to view sensitive information as well as the ability to modify, change, replace, or intercept the information interchange between the two

parties. In addition to that, the attacker leaves no traces of their interception, remaining unnoticed by the victims. To perform a MITM attack, there needs to be a communication channel; Bluetooth, GSM, Long-Term Evolution (LTE), Near Field Communication (NFC), Radio Frequency, UMTS, and Wi-Fi are the most used communication channels of MITM attack.

Decoding a MITM attacks takes a longer time to process and can be done in three ways. First way is based on imitating cyber decoding methods, or simply decoding the attack. Second way is based on telecommunication addressing techniques through the IP address of the attacker. The third way of decoding a MITM attack is based on locating the attacker and victims through GPS and tracking down attacker's location. On the other hand, two main approaches that are taken to set up a MITM attack are creating fake networks controlled by the attacker or the connection tampering between an authenticated network and the victim. The first approach is extensively used for attacking individual victims through public Wi-Fi, which could be found in any café, airport, store, institution, and so on. The second approach requires more work and is closely tied to infiltration that comes with non-secured connection between the attacker and the victim, and the secured connection and the legitimate network and the attacker. This is rather difficult to detect if the proper transference and encryption are present. Similarly, depending on the type and sensitivity of information transferred through the unsecured connection between the attacker and the victim, serious consequence may follow. A good example of that can be an online purchase made through such unauthenticated network where the attacker gets banking information of the victim.

2. 'MITM' Attack Types

MITM attack is one of the most common network attacks. It happens when attacker gets in the middle of communication between two parties, the sender and the receiver. By making the

two parties believe they are safely communicating, the attacker tricks the data flow traffic and controls the communication. Oftentimes, the two communicating parties in networks are the client and the server. The client and the server communicate with each other through authorized communication channels: based on the requests sent by the client, the server sends responses to those requests. Through using the MITM attack, the hacker disturbs the legitimate communication channel and creates a different one, controlled by the attacker. Essentially, the clients perceive the attacker as a server and the server takes the attacker as a client, both unaware of the unsecured connection and the 'man in the middle.'

In given situation, when a client sends a request to the server, the attacker receives the request instead of the server, which is then sent to the server by the attacker. Similar case happens when the server sends back the response to the client with attacker receiving the response first. The attacker's position in this communication lets the attacker access to the shared information, which may include such sensitive information as passwords, addresses, social security numbers, login credentials, and so on. The hacker gets the ability to sniff, control, and modify the accessed information.

MITM attacks where the hacker only receives and sends information without modifying it is called a passive MITM attack. The opposite of passive attacks is active MITM attack. In this case, received the packets of data and sends it after making changes to them.

Using the protocol used to perform MITM attacks, there are multiple types of MITM attacks:

- ARP (*Address Resolution Protocol*) Poisoning
- IP (*Internet Protocol)* Spoofing
- DNS (*Domain Name System*) Spoofing
- DHCP Spoofing

- Wi-Fi Eavesdropping
- SSL (*Secure Sockets Layer*) Stripping / Hijacking
- HTTPS (*Hyper Text Transfer Protocol - Secure*) Spoofing

2.1. ARP Poisoning

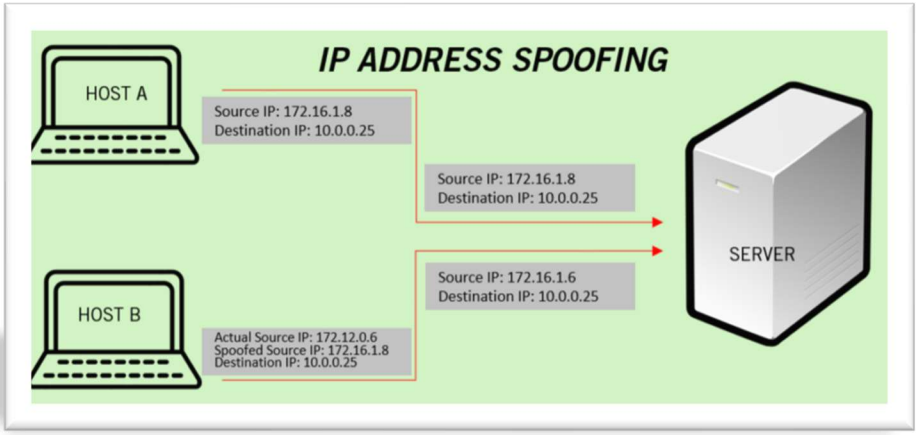
ARP (Address Resolution Protocol) poisoning, also known as ARP spoofing, is one of the common techniques used to perform MITM attacks. ARP is a protocol that enables network communications by translating to the IP (Internet Protocol) addresses to MAC (Media Access Control) address and vice-versa. The communication line consists of two parties, source host and destination host. Both hosts use request/response communication relationship. ARP cache is a table that maps IP addresses with MAC addresses of every host connected to network. The hosts maintain ARP cache to connect to destinations on network. ARP was not designed for security, meaning that it doesn't verify that replies to ARP requestion always come for authorized parties, allowing the hosts accept ARP responses whether the request was sent. This weakness of ARP allows room for ARP spoofing attacks.

ARP poisoning is attack that allows attackers to intercept the communication between network devices, making it a MITM attack. ARP's vulnerability is in its non-state protocol where the hosts always accept requests even if they didn't request any. Therefore, they update their ARP cache every time they get an ARP response. Taking advantage of this vulnerability, the attacker sends a reply using a copied MAC address, attacking two parts of the communication line. To attack the source host, the attacker sends ARP reply deceiving the source host to think that the IP address of destination host maps the MAC address of the destination, while in fact it belongs to attacker. Similarly, the destination host is not aware the attacker is the source. As a

result, the information exchanged between the two hosts first passes through the attacker, which is the forwarded to the hosts.

2.2. IP Spoofing

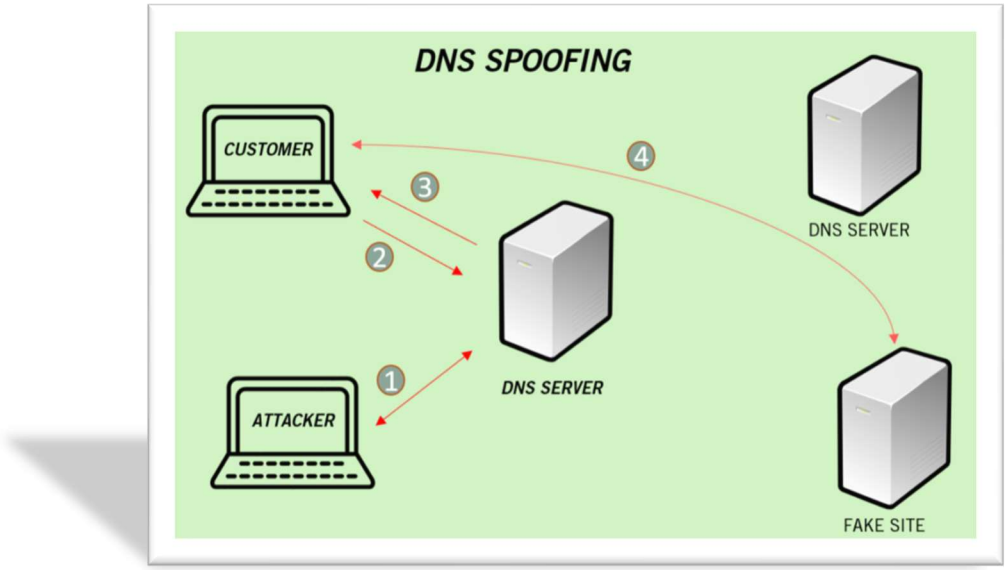
IP Spoofing involves a technique for intercepting traffic by modifying the IP packets to imitate another computer system. It is like APR spoofing, but in IP spoofing the attacker sends a package to the user with the different return address. It this attack, the communication between legitimate parties is captured and regulated, meaning the victims don't have the information on the real endpoint addresses.



2.3. DNS Spoofing

DNS (Domain Name System) spoofing, also known as DNS cache poisoning, is an attack where the website's address record is altered to redirect online traffic to a different, fraudulent website. This result in the users being sent to attacker's site when they try to access a legitimate one. DNS is an unencrypted protocol and DNS servers don't validate the IP addresses of where the traffic is redirected; this makes it easy to intercept traffic with spoofing. In a DNS spoofing attack, the resulting threat mimics a legitimate server's destination and redirects the domain's traffic. The ultimate goal of this attack is making the user end up on malicious websites controlled by the attacker.

To perform a DNS spoofing attack, the attacker must control the local DNS access, making the victim use the attacker's server. This spoofing attack is used to locate the cache, and usually involves two steps: insertion of malicious DNS into the fraudulent network and sending the fake DNS response before sending the legitimate one.



2.4. DHCP Spoofing

DHCP protocol provides parameters for network arrangement of the new hosts, which includes a subnet mask, the DNS server, default gateway, and the IP address. The DHCP protocol provides a client-server structure for data packets exchange between the server and the host. The DHCP is important to network managements as it has great security standards. Nonetheless, in addition to no source authentication, the DHCP messages are mostly set in unmodified text forms.

The attacker may perform a DoS attack on the DHCP server or conduct a DHCP starvation attack. Therefore, there is no assurance of DHCP server always communicating with the real clients. Overall, the two above mentioned attacks lead to the allocation of the IP address by the DHCP server, not letting the new devices get the IP address.

2.5. Wi-Fi Eavesdropping

Wi-Fi eavesdropping attack focuses on creating fake AP (Access Point) and making users connect to it. A good example of that could be the AP that lacks a password. Gaining the full control of the AP, the attacker can sniff all traffic flow as well as perform SSL stripping and HTTPS spoofing attacks. Wi-Fi eavesdropping can also be performed through ARP spoofing. Lastly, it's the easier to perform this attack on the users connected to public, unsecured Wi-Fi connections.

2.6. SSL Stripping

SSL (Secure Socket Layer) stripping attack is the result of removing the SSL encryption in a data segment between the source and the destination host addresses. This is a serious threat to the confidentiality of the victims. Common cause of SSL stripping is the result of weak algorithms on SSL, which leaves room for cyber-attacks.

To perform SSL stripping, the attacker needs to set up a HTTP connection and redirect it to HTTPS. Then, when a user sends a request to connect, the attacker changes the data and sets up HTTPS connection between the server, and sets ups an unsecured HTTP connection between the users. The attacker can be considered as a bridge between the server and the user.

2.7. HTTPS Spoofing

HTTPS (Hyper Text Transfer Protocol Secure) spoofing can be described as a website with a fake digital certificate. HTTPS was considered safe, until the interception of data packets in the communication was made by making users believe their connection was encrypted. In this attack, the attacker successfully spoofs the certificate and checks the fake certificate against the ones trusted by the user's device, adding the fake certificate to that list. The attacker receives the data (i.e., usernames, passwords, addresses, etc.) and decrypts it, sending the modified copy of the data to the legitimate server.

3. 'MITM' Defense: Detection and Prevention

One way of detecting an MITM attack is Latency examination. It works by calculating multiple transactions that will make transactions and take similar time, then check if one of these transactions is taking too long to respond which indicates there is a third party that is manipulating the transaction and transfer. The other way we can detect MITM attacks is DPI (Deep Packet Inspection) and DFI (Deep Flow Inspection) during the network. Attackers utilize network traffic to find insecure communication in order to intercept data flow, so we can use DPI and DFI to identify anomalous network traffic.

3.1. Best practices to prevent MITM attacks

Most of the cyber-attacks are human-behavior initiated, so educating technology users and training company employees on the possible dangers and consequences of MITM attacks can proactively protect their sensitive information and data. This also includes educating them how to detect malicious email and brining awareness of the best security practices against MITM attacks such as avoiding using unauthenticated Wi-Fi, implementing VPN, not opening

suspicious links, etc. Following subsections will go over some of the way MITM attacks could be prevented.

3.1.1. Secure Connections

First line of defense against MITM attacks is using secure connections. HTTPS (Hypertext Transfer Protocol) can be used for secure communications over HTTP through exchange of public/private keys. This would prevent attackers from using any data they might be sniffing.

It is also crucial to use authenticated Wi-Fi connections and avoid public, unsecured ones, because they are more vulnerable to network interception and MITM attacks. Therefore, many organizations nowadays reenforce two-factor or multifactor authentications across their businesses, adding extra layer of security and protection of cyberattacks.

3.1.2. Virtual Private Network Encryption

VPNs (Virtual Private Network) can be used withing local area networks to provide secure environment for sensitive data. VPNs use key-based encryption to provide secure communication through creating a subnet (or subnetwork) – a smaller part of large network divided into two or more networks. Through using VPNs, attackers wouldn't be able to decipher the traffic within the VPN regardless of his success in get into the shared network.

3.1.3. Avoid Phishing Emails

Purposely-crafted phishing emails are often used to trick users into opening them. They may look like safe emails coming form legit sources (i.e., financial institutions, schools, banks, etc.), deceiving users into clicking them. Clicking on such suspicious emails should be avoided, because they might redirect users to sketchy websites or force-download malware on their devices.

4. Examples of MITM Attacks

Example 1: Data Interception

Attacker installs a packet sniffer (a sniffer program targeting packets of data transmitted through the Internet) to find insecure communications in a network traffic. Attacker then can get a user's information when they log in to a website, redirecting the user to a fake website that may look legitimate. Information retrieved by attacker may then be used to log in to legitimate websites to access the victim's information.

Example 2: Active Eavesdropping

Attacker gets user's login credentials for hacking their social media accounts or stealing their credit card information when they are connected to public Wi-Fi networks such as those available in airports or cafés.

4.1. Real-World MITM Attacks

DigiNotar Hack

In 2011, DigiNotar – a Dutch registrar site of digital security certificates – detected an intrusion into its Certificate Authority infrastructures. DigiNotar was breached enabling an attacker to gain access to 500 certificates for well-known websites such as Google and Skype. Digital certificates, enabling browsers to authenticate servers, include the information about the key, identity of the key owner, and digital signature of the entity that verified the contents of the certificate. The attack performed by the hacker used the tactics of MITM attack, which tricked the users into entering their passwords on fake websites that mimicked legitimate ones and stole their information. On September 20, 2011, as a result of this data breach, DigiNotar filed for voluntary bankruptcy.

Equifax Data Breach

On July 29, 2017, Equifax – one of the largest credit reporting agencies – discovered it's been hacked. The company suffered a massive data breach with more than 145.5 million Equifax customers having their financial information leaked. The hack was worldwide with 400 thousand UK, 200 thousand US, and 100 thousand Canadian Equifax customers affected. The cause of this data breach was the company's failure to patch up a known vulnerability in its security system. In addition to that, the company also discovered that it's mobile apps didn't consistently use HTTPS. This allowed the hackers to intercept and gain access to Equifax users' sensitive data, such as addresses, social security numbers, and credit card numbers, when they logged in to their accounts.

References

Chivers, Kyle. “What Is a Man-in-the-Middle Attack?” Norton. NortonLifeLock. Accessed August 19, 2022. https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html.

Javeed, Danish. “Man in the Middle Attacks: Analysis, Motivation and Prevention.” ResearchGate. ResearchGate, July 2020. https://www.researchgate.net/publication/347006863_Man_in_the_Middle_Attacks_Analysis_Motivation_and_Prevention.

Mallik, Avijit, Abid Ahsan, Mhia Shahadat, and Jia-Chi Tsou. “Man-in-the-Middle-Attack: Understanding in Simple Words - Researchgate.” ResearchGate. ResearchGate, January 2019. https://www.researchgate.net/publication/330249434_Man-in-the-middle-attack_Understanding_in_simple_words.

Mallik, Avijit. “Man-In-The-Middle-Attack: Understanding in Simple Words.” Jurnal Pendidikan Teknologi Informasi. Department of Mechanical Engineering, Rajshahi University of Engineering & Technology, October 2018. https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/download/3453/2707.

“Man in the Middle (MITM) Attacks: Types, Techniques, and Prevention.” Rapid7. Rapid7. Accessed August 19, 2022. https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/.

"Subnetwork." Wikipedia. Wikimedia Foundation, July 2, 2022. https://en.wikipedia.org/wiki/Subnetwork.

"What Is ARP Spoofing: Arp Cache Poisoning Attack Explained: Imperva." Imperva. Imperva, May 6, 2020. https://www.imperva.com/learn/application-security/arp-spoofing/.

"What Is DNS Cache Poisoning and DNS Spoofing?" Kaspersky. Kaspersky Lab, January 13, 2021. https://usa.kaspersky.com/resource-center/definitions/dns.

Yasar, Kinza, and Michael Cobb. "Man-in-the-Middle Attack (MITM)." IoT Agenda. TechTarget, April 28, 2022. https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM.