Analyzing Man in the Middle Attack

Sahil Vashisht

Department of Information Technology & Maharaja Agrasen Institute of Technology

Abstract – Ransacking for just the right article is the foremost preferred and is sort of challenging to look out supported the current requirements. With the advancement in technology day by day, the occurrence of hacking is increasing very often. In these modern times, the area of cybersecurity is in desperate need of prevention from hacking. Gone are those days when firewalls were handy to protect your data. We require to try to do this individually to prevent cybercrime. In keeping with Kaspersky Labs, the standard cost of a cyber-breach is $1.23 million. This paper's main task is to give the simplest possible ways to assist and help make secure websites. Security of a Web application has become the most vital challenge nowadays because of some common vulnerabilities. Web Security is a crucial step to persuade through a number of your queries for an explanation [9]. Once you know that your website is safe, you will be less stressed. There are loads of attacks that can be used to hack a website like CSRF, XSS, MITM, Session Hijacking and many more. I have thoroughly researched the most general vulnerabilities, and during this paper, I have discussed one vulnerability (MITM). I have discussed in detail what Man in the Middle is? Its types, preventions and how it is performed.

Key Words: Hacking, Cyber Security, Web Security, MITM (Man in the Middle)

1. Introduction

What is MITM?

A man-in-the-middle (MITM) attack is when an attacker intercepts transmissions between two teams either to secretly eavesdrop or alter traffic transiting between the two.

[1]The objective of an attack is to seize private data, such as login credentials, account details and credit card numbers. Victims are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Data obtained during an attack could be utilized for numerous goals, comprising identity larceny, unapproved fund transfers or an illicit password change. Broadly speaking, a MITM attack is the equivalent of a mailman unlocking your bank statement, documenting your account details and then resealing the envelope and transmitting it to your door.

As it aims to evade reciprocal authentication, a MITM attack can achieve just when the attacker impersonates each end point adequately well to fulfill their expectations. Most cryptographic procedures comprise some aspect of endpoint authentication specifically to prevent MITM attacks. For example, TLS can verify one or both parties utilizing a mutually trusted certificate permission.

During this paper, my mission is to assist everyone who is working over the internet to learning about cybersecurity. This paper has been divide into many sections. Previous section was abstract. Section I is that the introduction of the subject. Chapter 2 is about the methodology of how attack is performed. Chapter 3 is about the prevention of the attack. This is the most important part of this research paper. Chapter 4 deals with the popular csrf vulnerabilities. Section 3 is conclusion on my research. In the end are the References.

2. Body of paper

Chapter 2: METHODOLOGY

How the attack takes place?

The man in middle attack (MITM) thwarts a communication between two systems. For example, in an http agreement the victim is the TCP connection between client and server. [2]Using various methods, the attacker divides the actual TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server, Once the TCP connection is stopped, the attacker behaves as a representative, being able to browse, inject and amend the data in the intercepted transmission.

The MITM attack is fairly beneficial because of the essence of the http protocol and data transfer which are all ASCII based. In this means, it’s feasible to view and conference within the http protocol and also in the data transferred. So, for example, it’s possible to catch a session cookie reading the http header, but it’s also possible to alter a quantity of money transaction inside the application context. The MITM attack could also be done over an https connection by utilizing the similar technique; the only disparity comprises in the establishment of two autonomous SSL sessions, one over each TCP connection. The browser sets a SSL connection with the attacker and the attacker ascertains another SSL connection with the web server. SSL scripting is further discussed in the paper below. In general the browser notifies the user that the digital certificate utilized is not legal, but the user may reject the notification because they don’t comprehend the threat. In
some particular contexts it’s reasonable that the indication doesn’t occur, as for example, when the Server certificate is jeopardized by the attacker or when the attacker certificate is signed by a counted CA and the CN is the similar of the actual web site.

MITM is not only an assault procedure, but is also usually utilized during the advancement step of a web application or is still used for Web Vulnerability assessments.

2.1 Working principle of attack

Presume A wants to communicate with B. Meanwhile, C wants to thwart the dialogue to overhear and optionally to transmit an inaccurate message to B.

First, A inquires B for his public key. If B delivers his public key to A, but C is eligible to thwart it, an MITM attack can begin. C delivers A, a forged message that seems to arise from B, but rather includes C's public key.

A, speculating this public key to be B’s, encrypts her message with C’s key and delivers the enciphered message back to B. C then blocks, deciphers the message utilizing its private key, possibly alters it if it wants, and re-enciphers it using the public key it stopped from B when it initially attempted to send it to A. When B receives the newly enciphered message, it thinks it came from A.

A delivers a message to B, which is thwarted by C:
Alice "Hi B, its A. Provide me your key." \(\rightarrow\) C B

C transmits this message to B; B cannot tell it is not certainly from A:
A \(\rightarrow\) C "Hi B, its A. Lend me your key." \(\rightarrow\) B

B responds with his encryption key:
A \(\leftarrow\) [B’s key] B

C reinstates B’s key with its own, and transmits this to A, contending that it is B's key:
A \(\leftarrow\) [C’s key] C B

A encrypts a message with what it understands to be B’s key, believing that only B can read it:
A "Meet me at coffee shop!" [Encrypted with C’s key] \(\rightarrow\) C B

Nonetheless, because it was certainly encrypted with C's key, C can decrypt it, read it, modify it (if desired), re-encrypt with B’s key, and forward it to B:
A \(\rightarrow\) C "Meet me by the dominos!" [Encrypted with B’s key] \(\rightarrow\) B

B believes that this message is a secure communication from A.

This indicates the need for A and B to have some way to guarantee that they are truly each using each other's public keys, rather than the public key of an attacker. Otherwise, such attacks are normally feasible, in principle, against any message sent using public-key technology. A variation of procedures can help protect against MITM attacks.

2.2 Scenario 1: Intercepting Data

The attacker introduces a packet sniffer to assess network traffic for unsafe communications. When a user logs in to a site, the attacker procures their user data and changes course them to a fraud site that parrots the actual one.

The attacker's bogus site packets data from the user, which the attacker can then employ on the actual site to access the target's information.

In this scenario, an attacker blocks a data transfer between a client and server. By cheating the client into speculating it is still articulating with the server and the server into thinking it is still obtaining information from the client, the attacker is able to thwart data from both as well as inject their own incorrect data into any future transfers.

Scenario 2: Gaining Access to Funds

The attacker sets up a fake chat service that pantomimes that of a well-known bank.

Utilizing information attained from the data intercepted in the first method, the attacker bluffs to be the bank and commences a chat with the victim.

The attacker then commences a chat on the real bank site, feigning to be the victim and authorizing along the crucial information to attain admission to the target's account.

In this scenario, the attacker thwarts a conversation, passing along portions of the discussion to both valid participants.

2.3 Types of man-in-the-middle attacks [4]

Cybercriminals can use MITM attacks to gain control of devices in a variety of ways.

Types of MITM attacks

1. IP spoofing

All device eligible of attaching to the internet has an internet protocol (IP) address, which is comparable to the street address for your home. By spoofing an IP address, an attacker
can trick you into believing you’re interacting with a website or somebody you’re not, possibly bestowing the attacker entry to information you’d oppositely not share.

2. DNS spoofing

Domain Name Server, or DNS, spoofing is a method that compels a user to a phony website somewhat than the actual one the user plans to tour. If you are a victim of DNS spoofing, you may think you’re touring a safe, trusted website when you’re actually interacting with a fraudulent. The perpetrator’s objective is to fluctuate traffic from the actual site or capture user login credentials.

3. HTTPS spoofing

When doing business on the internet, seeing “HTTPS” in the URL, rather than “HTTP” is a sign that the website is secure and can be trusted. In fact, the “S” exists for “secure.” An attacker can trick your browser into thinking its touring a believed website when it’s not. By pivoting your browser to an unsecure website, the attacker can survey your interactions with that website and probably steal private information you’re sharing.

4. SSL hijacking

When your device connects to an unsecure server — indicated by “HTTP” — the server can frequently automatically redirect you to the secure version of the server, indicated by “HTTPS.” A connection to a secure server implies basic security protocols are in spot, insuring the data you share with that server. SSL stands for Secure Sockets Layer, a protocol that ascertains encrypted links between your browser and the web server.

In an SSL hijacking, the attacker utilizes another computer and secure server and thwarts all the information enacting between the server and the user’s computer.

5. Email hijacking

Cybercriminals occasionally target email accounts of banks and different financial institutions. Once they gain admission, they can survey transactions between the institution and its clients. The attackers can then imitate the bank’s email address and send their own teachings to customers. This assures the customer to follow the attackers’ teachings rather than the banks. As an outcome, an unwitting client may end up laying money in the attackers’ hands.

6. Wi-Fi eavesdropping

Cybercriminals can set up Wi-Fi connections with very valid sounding names, identical to an available business. Once a user connects to the fraudster’s Wi-Fi, the attacker will be able to regulate the user’s online action and be able to stop login credentials, payment card information, and more. This is just one of many risks related with using public Wi-Fi.

Additional form of man-in-the-middle attack occurs when a hacker manages to direct an SSL stripping scheme against the victim. As I spoke of previously, hackers can’t crack into valid HTTPS traffic between a client and a server even if they manage to block and transmit the communications.

In the case of SSL stripping, the attackers weaken the communications between the client and server into an unencrypted layout to be eligible to direct a MITM attack.

When a victim expects to connect to a server, the attacker thwarts the request and builds an autonomous, valid connection to the server through HTTPS protocol. When attackers receive the server’s acknowledgment, they transmit it to the victim in an unencrypted configuration, presenting as the server. Believing they’re conveying with the rightful party, the victim will proceed to send information to the attacker, who will then transmit it to the server in HTTPS.

Sceptical users will see that they’ve been targeted by an SSL stripping attack if they peek in their browser’s address bar and see that they’re attached through the unencrypted HTTP protocol. You can also install HTTPS Everywhere, a browser extension that implements HTTPS communication wherever feasible. HTTPS Everywhere will stave off an unasked party from downgrading your communications to HTTP.

Chapter 3: PREVENTIONS


1. Across-the-board, reasonable cybersecurity hygiene will assist safeguard you from MITM attacks.

2. Just connect to ensured Wi-Fi routers or use your wireless carrier’s encrypted connection. Connect to routers that use WPA2 insurance. It’s not entirely infallible, but it’s much reasonable than zero.

3. Add a VPN to encrypt traffic between end-points and the VPN server (either on the enterprise network or on the internet). If traffic is encrypted, it’s tougher for a MITM to snatch or alter it.

4. Utilize end-to-end encryption for your emails, chat, and video communication (Zoom, Teams, etc.)

5. Maintain the system patched and malware revamped

6. Utilize a password manager to insure your passwords and prevent reuse of passwords

7. Just connect to HTTPS connections, use a browser plugin to carry out this rule

8. Utilize multi-factor authentication wherever accessible

9. Utilize DNS over HTTPS, which is a recent technology that safeguards you from DNS hijacking by encrypting your DNS invitations
10. Attend the zero-trust principles to assemble inner boundaries around admission to data, which preclude infiltrators from striding willingly throughout the system if they were to get inside.

11. Regulate activity on the network to detect information (malicious network connections or unusual user manner) of a settlement or MITM techniques in use

**Chapter 4: POPULAR MITM ATTACKS**

1.) Researchers uncovers “ultimate man-in-the-middle attack” that utilized a detailed spoofing crusade to cheat a Chinese VC firm and burglarize an arising business. (May, 2021)

2.) In 2013, information was seeped about the Quantum/FoxAcid MITM system utilized by NSA to thwart TOR connections.

3.) In 2014, Lenovo installed MITM (SSL Hijacking) adware called Superfish on their Windows PCs [7].

4.) In 2015, a British couple (the Luptons) lost £340,000 in an email eavesdropping/email hijacking MITM attack [7].

5.) In 2011, Dutch registrar site DigiNotar was breached, which enabled a threat actor to attain entry to 500 certificates for websites like Google, Skype, and others. Entry to these certificates authorized the attacker to present as lawful websites in a MITM attack, kidnaping users' data after fooling them into entering passwords on malicious mirror sites. DigiNotar ultimately filed for bankruptcy as an outcome of the breach.

6.) In 2017, credit score company Equifax eliminated its apps from Google and Apple after a breach arose 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.

**3. CONCLUSION**

The MITM is a highly vulnerable insidious attack which has resulted in mass loss of data over the years from its prevalence. Being a network attack it majorly attacks the networks such as the Wi-Fi through routers, network nodes of ad hoc via malicious nodes in the middle or through proxy servers. With the advent of new SSL scripting initially the https sites which were thought to be protected via encryptions are also in grave danger as it can also be now brought down via SSL scripting. MITM has been revolutionised again and again and adapted itself with the new upgrading technology. Being highly insidious the victim doesn't even realise what has hit him. The most serious threat is that MITM can be used as both active as well as passive attacks.

Proper precautions while maintaining the network is a must to check the prevalence of MITM. Regular pentesting is important, setting up highly secure routers is the best possible solution. People also use honeypots to protect the actual servers.

**REFERENCES**


