RESEARCH ARTICLE OPEN ACCESS

An Overview of the Man-In-The-Middle Attack

Sonia Rachel[1], Subhashkar S[2]
1(Department of Computer Science, St. Joseph's College (Autonomous), Bangalore)
2(Department of Computer Science, St. Joseph's College (Autonomous), Bangalore)

Abstract:

The 'Man-In-The-Middle' (MITM) attack is one of the most well-known attacks in computer network security, illustrating one of the biggest concerns for security professionals. MITM attacks target the actual data that flows between endpoints, the confidentiality and the integrity of the data itself. The MITM attack makes it hard for the clients to comprehend on whether or not they are associated with a unique and a secured connection. As the certificate which is passed during the course of the connection set up is unreliable, the attacker can manipulate its information effortlessly. The approval of the certificate is left to the client. Since numerous clients are not well aware of the locations of such fake certificates and their equivalent attacks, they acknowledge the certificates which pave the way for attackers to actualize the attack. This paper emphasizes on the different types of MITM attacks.

Keywords —**ARP, DNS, eavesdropping, HTTP, HTTPS, IP, MITM, spoofing**

I. INTRODUCTION

The name 'man-in-the-middle' comes from the game of basketball wherein the ball is grabbed by another player while two other players are passing the ball to each other. A man-in-the-middle attack is a cyber attack in which the attacker interferes in a conversation between two parties, mirrors both parties and gains access to the information which was being shared by both the parties. The attacker is able to intercept, send and receive information which is meant to be sent to someone else, or not to be sent at all in the first place. Both the parties of the conversation are not aware of the attacker and his actions. [9]

The term 'man-in-the-middle' is usually abbreviated as 'MITM' and hence the attacks coming under this category are known as 'MITM attacks'. The MITM attack is also better known by the following names - 'Bucket-brigade attack', 'Fire brigade attack', 'Monkey-in-the-middle attack', 'Session hijacking', 'TCP hijacking', 'TCP session hijacking'.

II. HISTORY

Leslie Lamport is apparently the first person to talk about the 'man-in-the-middle analysis' in terms of communication security. His work related to communication security was published in 1981 in an article titled "Password authentication with insecure communication" for the magazine named "Communications of the ACM", but there are evidences of his thoughts regarding this matter as early as in 1979. [1], [12], [13]

MITM attacks have evolved over time. These attacks work on a simple concept, that is, an unauthorized third-party with vested interests, taps a wired or a wireless connection. Although the concept of MITM is not so new, attackers are constantly trying new approaches to make such attacks relevant to current times. The following are some of the evolved versions of the MITM attack:

A. MITC (Man-In-The-Cloud)

This is an MITM-based attack which occurs in cloud-based storage services. The attacker exploits the session management and steals data.

B. MITB (Man-In-The-Browser)

This is an MITM-based attack which occurs in a browser. The attacker tricks the user in such a way so as to download a Trojan virus.

C. MITMO (Man-In-The-Mobile)

This is an MITM-based attack which occurs during the usage of a mobile phone for financial transactions. The attacker intercepts SMS traffic and then captures the codes.

D. MITA (Man-In-The-App)

This is an MITM-based attack which takes place via a software application. The attacker inserts a fake certificate and starts communicating with the application.

E. MIT-IoT (Man-In-The-Internet of Things)

This is an MITM-based attack which takes place in an IoT (Internet of Things) network. The attacker simply exploits poor validation of certificates and can steal the user's credential data. [2]

III. LITERATURE SURVEY

A. "The Password Reset MitM Attack" by Nethanel Gelernter, Senia Kalma, Bar Magnezi, and Hen Porcilan - According to this paper, it is said that an attacker can exploit a user during the registration and password reset processes on a website, by launching a PRMiTM (Password Reset Man-in-The-Middle) attack. Popular websites and mobile applications are found to be vulnerable to this attack. The findings in this paper indicate that the two-step authentication process is better and less vulnerable to such security attacks when compared to the one-step authentication process. The paper also suggests some rules and recommendations for better and easy auditing in order to improve the password reset process with respect to the vulnerable websites and applications. [18]

B. "Spinner: Semi-Automatic Detection of Pinning without Hostname Verification" by Chris McMahon Stone, Tom Chothia, and Flavio D. Garcia - According to this paper, it is said that the lack of certificate hostname verification leads to MITM attacks. It has been found that the apps of two of the largest banks in the world and VPN apps are vulnerable to such attacks. Trading and cryptocurrency apps are also some of the other vulnerable apps. Certificate pinning is an effective method to hide this vulnerability. This paper suggests a new tool called the 'Spinner' which dynamically detects this vulnerability and thereby purchasing of certificates is not required. [19]

C. "Prevention of MITM Attacks in Cloud Computing by Lock Box Approach Using Digital Signature" by Suman Yadav and Anoop Jaysawal - According to this paper, MITM attacks targeted on cloud data can be prevented by the usage of a lock box which is secured by a digital signature to protect the keys. The paper suggests that this is a better method in comparison to securing the original data which is encrypted. [20]

IV. TYPES OF MITM ATTACKS

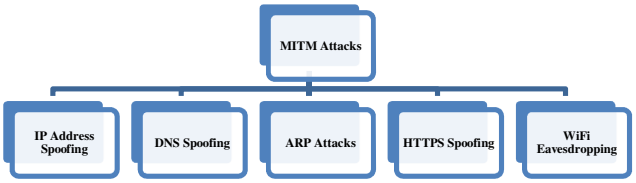

Fig. 1 Schematic representation of the types of MITM attacks.

A. IP Address Spoofing

1) Overview of IP address: Internet Protocol (IP) is a method which provides a set of rules to send or receive data over the Internet, which is present at layer 3 of the OSI model. Information is transferred in the form of IP datagrams which are also known as packets. The IP packets contain IP headers and data which have to be transmitted. The IP header contains the IP source address and the IP destination address. [16], [17]

2) Working of IP address: It is a unique identification number having 32 bits. Example: 146.82.101.132. It has four parts which consist of

eight binary digits each. These parts are known are 'octets'. This number is then converted into its decimal equivalent separated by three dots. IP addresses can range from 0.0.0.0 to 255.255.255.255. IP addresses are divided into five classes, namely from A to E. [16]

As the IP address contains the source address and the destination address, the packets are transferred to their destination by routing process. Based on the IP address, the routers will know where exactly the packets have to be transferred to. It works using the Transmission Control Protocol (TCP). [17]

3) Attack mechanism of IP address spoofing: It is also called as Internet Protocol (IP) spoofing. In this type of attack the attacker will create an IP packet and sends it from a forged IP source address, so that he/she can hide the true identity of the sender. The attacker tries to overload the network of the legitimate user by two methods.

In the first method, the attacker will send numerous data packets from the forged or spoofed address. This makes the target's network to overload since it cannot handle such a large amount of data.

In the second method, the attacker will spoof the victim's IP address and then sends packets to other receivers. When the receivers receive these packets, they respond to it by transmitting the packets to the victim's IP address. The packets from many different receivers will overload the victim's network.

In this type of attack, the hacker will change or modify the IP source address and makes it look like a legitimate source address and then starts to communicate. Hackers use this attack mostly to crash the victim's entire network by overloading the network with massive amounts of data. They also use this attack to hide the sender's identity. [3]

B. DNS Spoofing

1) Overview of DNS: Domain Name System (DNS) is used to resolve human readable hostnames like www.sjc.ac.in into their corresponding IP addresses like 204.14.298.115. The devices that connect to the internet rely on the DNS for this purpose.

2) Working of DNS: When the user requests for information about something either by typing in the URL or by clicking on a particular link, the computer checks in its own local cache to find the answer. If it does not get the answer, it performs a DNS query with the help of the Internet Service Provider's recursive DNS server and returns the information, even after this if it is not able to find the answer; it uses the nameserver which will direct the user's query to the place where it should be found. It does so by just reading the first part of the user's request from right to left and sends it to the Top Level Domain (TLD), which in turn helps us to navigate to that particular server which contains the user's information. Then the next part of the user's request is checked and the corresponding DNS record is retrieved which contains the complete information about a specific domain and stores that record in its local cache for the next use. Now this information is passed to the browser which then displays it to the user. [5]

3) Attack mechanism of DNS spoofing: In this type of attack, the attacker may change the DNS server so that it redirects a particular domain name to a different IP address. Now the victim is forced to use the fake website which looks like the legitimate one. The attacker then steals data from the victim. [3] These are the two methods of DNS Spoofing:

- ***DNS cache poisoning:*** In this type of spoofing the local DNS server will be replaced with DNS server which contains the tailor-made entries of the authentic website. When the user sends his/her request to the local DNS server, the user will be forced to visit the fake website which was created by the attacker. [6]

- ***DNS ID spoofing:*** When a client sends a resolve request, the packet ID and the IP information is generated. In this type of spoofing, the resolve request information is duplicated with fake content and stored.

C. ARP Attacks

1) Overview of ARP: Address Resolution Protocol (ARP) is a protocol which is used to map an IP address to a MAC (Medium Access Control) address, that is, the physical address of the computer system belonging to a specific network.

The different types of ARP messages which can be sent using the ARP protocol are:
(a) ARP (Address Resolution Protocol) request
(b) ARP (Address Resolution Protocol) reply
(c) RARP (Reverse Address Resolution Protocol) request
(d) RARP (Reverse Address Resolution Protocol) reply [4]

2) Working of ARP: The request message would look like - "My IP address is xx.xx.xx.xx and my MAC address is xx.xx.xx.xx.xx.xx. I want to transmit data to the IP address yy.yy.yy.yy, but I don't know the MAC address." The system with this IP address will respond in the ARP reply packet saying "I am the device you are looking for with the IP address yy.yy.yy.yy and my MAC address is yy.yy.yy.yy.yy.yy". This is a unicast message. After this, both the parties can start off with their communication.

3) Attack mechanism of ARP attacks: In an ARP attack, the malevolent party broadcasts the forged/spoofed ARP message requests to all the systems which are connected in the same network in order to link the attacker's physical machine address i.e. the MAC address, with the IP address of the legitimate system. Since it is a broadcast message, every system will receive this message. When the system with that particular MAC address responds to the attacker's request, the attacker can then receive any data that is intended for that legitimate IP address. The attacker can modify or even stop data during transmission. [3]

D. HTTPS Spoofing

1) Overview of HTTPS: In earlier days people used only the HTTP protocol i.e. Hyper Text Transfer Protocol to transfer data. When people realized that their sensitive data like credential data is being used to log in into different websites, they felt the need to secure their data and so they came up with the idea of HTTPS.

HTTPS - HTTP Secure deals with security threats by encrypting the data which is exchanged between the client and the website. Even if the hacker manages to break into your connection, he/she would still not be able to get your credential data, as it is encrypted and it is not easy to decrypt that. [6]

2) Working of HTTPS: It uses either of the two protocols viz., SSL (Secure Socket Layer) and TLS (Transport Layer Security) for encrypting a communication. These protocols make use of a system known as the Public Key Infrastructure (PKI). The PKI is asymmetric in nature, that is, it makes use of two different keys namely, the public key and the private key for the process of data encryption and/or decryption. Public key can be shared with everyone, but the private key should not be disclosed to anyone. One key can be used to encrypt while other keys can be used to decrypt. Then, when you request for an HTTPS connection, the website will initially send an SSL digital certificate, an 'SSL handshake' is initiated and then a secure connection is set up between the website and the user. [6]

3) Attack mechanism of HTTPS Spoofing: When the user requests for an HTTPS connection by typing in the URL or by clicking on any link of a website, instead of sending the legitimate website certificate, it is replaced by the fake certificate which was created by the attacker which seems like the legitimate one and it is difficult to identify that it is fake. Then the attacker creates his 'thumbprint' which is checked against certificate authorities. This makes the user believe that the website is trusted and his/her data will be encrypted and is hence secured. [8]

E. WiFi Eavesdropping

1) Overview of WiFi: WiFi is the standard wireless technology which is used for wireless local area

networking. It allows computers and other devices term WiFi is not the short form for 'Wireless Fidelity', it is just a name chosen by the Wi-Fi Alliance. [14], [15]

2) Working of WiFi hotspot: WiFi hotspot allows us to use a wireless network. One can also create his/her own hotspot. Once your computer detects the WiFi connection, you have the option to accept or reject the connection. If you accept, it allows you to use the wireless network and also allows you to move your computer from one place to another without any reinstallation or disconnecting of wires. [7], [11]

3) Attack mechanism of WiFi attacks: These attacks mostly happen when there are poor or weak passwords set to your WiFi. When people use public WiFi hotspots or fake WiFi nodes, the attacker can get into the user's computer and can then collect all the credential data which is being transferred over the Internet or the attacker can also create his own WiFi connection which looks more or less like the original WiFi connection and then steals your personal information. [10]

V. CONCLUSION

The 'man-in-the-middle' attack is very dangerous because it breaks the trust of the user, as the user feels that he/she is communicating over a secured network with the intended recipient. The attacker can steal, modify and/or misuse private information for personal gain. Therefore, this paper emphasizes on the different types of MITM attacks and the modus operandi of such attacks. Thus, the objective of this paper is to create a sense of awareness among the general public who are not well informed/educated about security threats/attacks like these and how they can easily fall prey to such malicious attacks unknowingly.

VI. FUTURE SCOPE

This paper gives only an overview of the MITM attack and its types. The security measures and the comparison of different preventive measures against MITM attacks have to be discussed further.

to exchange information over a wireless signal. The

ACKNOWLEDGMENT

We would like to express our heartfelt thanks and gratitude to Ms. Mrinmoyee Bhattacharya, Assistant Professor of the Department of Computer Science of St. Joseph's College, Bangalore for her invaluable guidance and constant support throughout the course of this research work.

REFERENCES

[1]. Ayoma Gayan Wijethunga, "Man in the middle attack - lab setup with VirtualBox", May 2016. *Available: http://www.ayomaonline.com/security/man-in-the-middle-attack-lab-setup-with-virtualbox/*

[2]. Michael Gregg, "How new technologies are reshaping MiTM attacks", December 2015. *Available: http://searchnetworking.techtarget.com/tip/How-new-technologies-are-reshaping-MiTM-attacks*

[3]. Neil DuPaul, "Spoofing attack: IP, DNS & ARP", February 2014. *Available: https://www.veracode.com/security/spoofing-attack*

[4]. Godred Fairhurst, "Address Resolution Protocol (arp)", December 2005. *Available: http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html*

[5]. Chris Gonyea, "DNS: Why it's important & how it works", August 2010. *Available: https://dyn.com/blog/dns-why-its-important-how-it-works/*

[6]. "What is HTTPS?" *Available: https://www.instantssl.com/ssl-certificate-products/https.html*

[7]. Marshall Brain, Tracy V. Wilson, and Bernadette Johnson, "How WiFi works", April 2001. *Available: https://computer.howstuffworks.com/wireless-network.htm*

[8]. Arun Kumar, "HTTPS security and spoofing - who is that man in the middle?", August 2014. *Available: http://www.thewindowsclub.com/https-security-spoofing-man-in-the-middle*

[9]. "What is a man in the middle attack?" *Available: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html*

[10]. Ricky Jay Publico, "What is a man-in-the-middle attack and how can you prevent it?", March 2017. *Available: https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack/*

[11]. Marshall Brain, Tracy V. Wilson, and Bernadette Johnson, "How WiFi works" - "WiFi hotspots", April 2001. *Available: https://computer.howstuffworks.com/wireless-network2.htm*

[12]. "Origins of the man-in-the-middle analysis", January 2015. *Available: https://security.stackexchange.com/questions/78843/origins-of-the-man-in-the-middle-analysis*

[13]. Leslie Lamport, "Password authentication with insecure communication", Communications of the ACM, Volume 24 Issue 11, November 1981. *Available: https://dl.acm.org/citation.cfm?id=358797#*

[14]. Vangie Beal, "Wi-Fi (wireless networking)". *Available: https://www.webopedia.com/TERM/W/Wi_Fi.html*

[15]. Christensson, "Wi-Fi", March 2014. *Available: https://techterms.com/definition/wi-fi*

[16]. "Understanding TCP/IP addressing and subnetting basics", January, 2017. *Available: https://support.microsoft.com/en-in/help/164015/understanding-tcp-ip-addressing-and-subnetting-basics*

[17]. Nadeem Unuth, "How IP routing works", June 2017. *Available: https://www.lifewire.com/ip-routing-3426716*

[18]. Nethanel Gelernter, Senia Kalma, Bar Magnezi, and Hen Porcilan, "The Password Reset MitM Attack", IEEE Symposium on Security and Privacy (SP), 2017. *Available: https://www.ieee-security.org/TC/SP2017/papers/207.pdf*

[19]. Chris McMahon Stone, Tom Chothia, and Flavio D. Garcia, "Spinner: Semi-Automatic Detection of Pinning without Hostname Verification", 2017 Annual Computer Security Applications Conference (ACSAC), December 4-8, 2017. *Available: https://www.cs.bham.ac.uk/~garciaf/publications/spinner.pdf*

[20]. Suman Yadav and Anoop Jaysawal, "Prevention of MITM Attacks in Cloud Computing by Lock Box Approach Using Digital Signature", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 7, Issue 5, May 2017. *Available: https://ijarcsse.com/docs/papers/Volume_7/5_May2017/SV7I5-0276.pdf*