IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-4, Special Issue-7, Dec 2016 ISSN: 2347-2693

A Survey on Man in the Middle Attack: Classification, Defense Mechanisms and Challenges

Manjula Kalita[1], Sukanya Dutta[2] and Ayesha Yesmin[3]

[1, 2, 3] Department of Computer Science & Engineering, GIMT
Azara, Guwahati-781017, Assam, India
(Email: manjula_kalita05@yahoo.com, sukanyadutta111.sd@gmail.com, ayeshayesmin27@yahoo.com)

Available online at: www.ijcseonline.org

Abstract- **This paper presents a survey of man-in-the-middle attacks in communication networks and methods of protection against them. Man in the middle attack allows the attacker to gain unauthorized entry into the connection between two devices and listen to the network traffic. This paper focuses on the areas where man-in-the-middle attack can occur and the different methods with which we can defense against the attack.**

Keywords: Man-in-the-middle attack, attacker, victim, ARP Cache Poisoning, DNS spoofing, Session Hijacking

I. Introduction

Security is kept at the topmost priority when it comes in the field of networking and communications. Man-in-the-Middle (MITM) attack makes the task of keeping data secure and private particularly challenging since attacks can be mounted from remote computers with fake addresses. The MIM attack takes advantage of the weakness in the authentication protocols (an agreement between the sender and the receiver) being used by the communicating parties. In this attack, attacker listens to the network traffic between two devices [2]. In this attack the victims have no idea that they are communicating with the attacker. The end result is the attacker not only alter the sensitive data , but can also inject and manipulate a data stream to gain further control over its victim[1].

II. Working Principles of MITM Attack

Man-in-the-Middle Attack works in such a manner that users are unaware of the fact that if they are connected to a secured network or to a similar non-secured connection. At the beginning of the communication, the user tries to establish a connection, the user first sends packet which include the details of the user's device to the necessary network. The network creates a digital certificate which includes the encrypted connection key and the address of the user's device. Since the certificate that is been passed during the connection initialization is insecure, the attacker can easily access to the digital certificate and alter the information in the certificate for his approval of entry into the connection. Many users don't compromises their time on checking the duplicate certificates and the attacks corresponding to them, thus they accept the certificate and attacker gets the approval to be a part of the connection in the middle and find its way to implement the attack [3].

III. Types of Web Attacks

A. Sniffing

Sniffing is the easiest attack to happen between the communicating parties, where the attacker itself transits the packets between them as a middle person[4].

Content sniffing attack is the way of altering the content and is also known as Media Type Sniffing. Such files are generally presented or introduced by the attackers to the host computer which contains malicious content. The victim simply downloads such malicious file for his use unknowingly [6].

B. Hijacking

It is a type of network security attack where the attackers take over the control on a established connection while it is in progress. The attacker uses a program that appears to be the server to the client and client to the server and then the attacker gain the control over the communication and access to the messages and sensitive data and modify them before transmitting[5].

C. SQL Injecting

There are many web attacks and SQL injection is one of them where the hacker tries to steal data from database. SQL injection refers to a class of code-injecting attack in which data provided by the user is included in a SQL query in such a way that part of the user input is treated as SQL code [15].

IV. MITM Attack: An Example, Types and its Defenses

An example of an offline Man-In-The-Middle is an interception of a letter by the mailman who either just reads it's content or even replaces its content. Another example for online attack is accessing a public Wi-Fi in a mall or station that has a wireless router with malicious software installed in it. If a person opens his bank account from that open network, he will lose all his bank credentials easily [2].There are mainly three types of MITM Attack:

A. ARP Cache Poisoning [1].
B. DNS Spoofing [1].
C. Session Hijacking [1].

A. ARP Cache Poisoning

In the normal ARP communications, the sender will send a packet that contains 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 mentioned IP address will only send the ARP reply with its MAC address in it and then communication takes place. This is not a secured protocol [2].

This is the initial step of MITM attack. In this attack , the attacker sends modified ARP packets on a LAN such that the attacker's MAC address gets associated with the IP address of the another host. This causes all the traffic to go to the attacker first and then to the original receiver. In this way the intruder can extract or alter the acquired information [1].

Defenses ARP Cache Spoofing:

Secured LAN: Since this type of attack can only takes place in LAN, therefore to prevent the attack we need to secure the LAN so that any local user with malicious intent would be stopped from doing so [1].

Hard Coded ARP Cache: Static entries could be made in the ARP cache on Windows hosts. ARP cache on a Windows host can be viewed by typing the command 'arp' in the command prompt [1].

Third Party program to monitor ARP traffic: This is the last and final approach to stop this type of attack. In this method we use intrusion detection system or some freely available downloadable utilities which are designed specifically for this purpose [1].

B. DNS Spoofing

This is a kind of online MIM attack, where the user will unknowingly enter into the fake website created by the attacker. For example, an attacker has created a fake website of user's bank, and when user visit to that website, it would be redirected to the website created by the attacker and the attacker will gain all the credentials. Whenever we enter a website in our PC, DNS request is sent to the DNS server and we get a DNS reply message in the response [2]. This shown with figure :

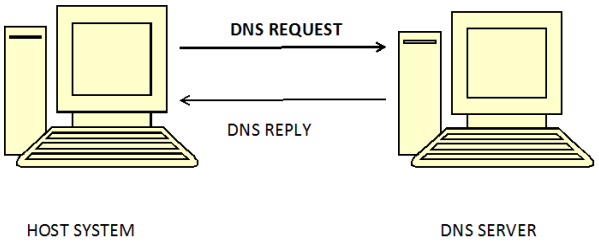

Fig1. DNS Communication with host and DNS Server [2]

In this method fake DNS information is sent to the host. This is done by changing the information in the DNS resolver cache, which causes the server to reply to attacker's IP address.

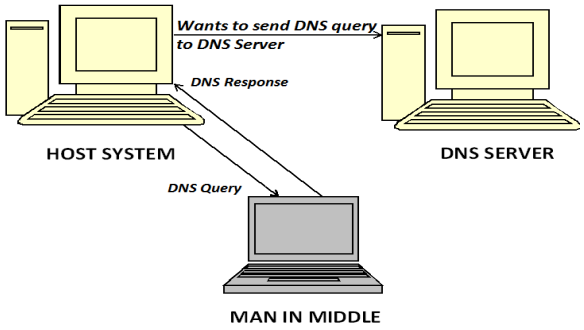

Fig2. The attacker performs MITM attack using DNS Spoofing.

The host computer wants to connect to a website so it will send a DNS query to the DNS Server, but unknowingly to the host computer the DNS query visits to the attacker and the attacker send a fake DNS response to the host computer. Since the host computer is unaware of the fake response of the attacker and so communication will takes place with the malicious website of the attacker which causes data breaches [2].

Defense against DNS Spoofing:

Internal Security: This type of attacks takes place within the same network. So it is important to maintain security of devices on the same network. This reduces the computer to become the victim of the attacker [1].

Less Reliance on DNS for secure system: It is the best practice not to rely on DNS for highly sensitive and secure system [1].

Use of intrusion detection system: Perfectly configured IDS can detect many forms of DNS spoofing and ARP Cache poisoning [1].

DNSSEC (The Domain Name System Security Extension): This is digitally signed DNS which ensures validity of a request or a response. DNS resolver's cache checks for this digital signature and then decides if the packet is original, modified, or coming from an unknown source [1].

C. Session Hijacking

Session is started when there is a connection between client and server[1]. Transmission Control Protocol (TCP) is referred as a session since it first establishes a connection, then transfers the data, and then finally terminates the connection. One of the proper session hijackings is done by stealing cookies with the help of Hyper Text Transfer Protocol (HTTP)[2].

In any interactive websites, there is a login session where the user provides it username and password and establishes a session. Once the session is established, unless and until the user logs out the session is not terminated. The credentials will be remaining in the cookie and the attacker can obtain certain parts of the session establishment by capturing the cookies that were used for the session establishment [2].

Defense against Session Hijacking:

This kind of attacks can be performed by various techniques and many different forms, and according to those techniques different defenses are introduced. This is attack is very difficult to detect and almost impossible to defend against. We would never come to know about this attack unless the attacker performs some obvious activity[2]. But there are few things we can take in concern to prevent session hijacking:

- Using SSL for the better security of connection channel [1].
- Logout should be done by the user after his/her works ends for the session termination [1].
- Authentication cookies must be cleared after the session termination [1].

V. MITM Attack: Handling Techniques

Man in the Middle attack is usually happen on router or server-side. As it is described earlier the user will have no control over security. Instead, we can use strong encryption between server and the client. In this case server authenticates the client's requests by presenting a digital certificate and then only connection is established.

Another method is not to connect to the open Wi-Fi networks which is generally available at all public points nowadays. And if the user is willing to connect to any open Wi-Fi network, it is suggested to use it through a browser plug-in such as HTTPs everywhere or ForceTLS [13]. The 's' is HTTPs refers that the browser is secured and safe to use. This will help to establish a secure connection.

When communicating over HTTPS, the browser uses certificates to verify the identity of the servers you are connecting to. These certificates are verified by reputable third party authority companies like VeriSign [11].

If the browser does not recognize the authority of the certificate sent from a particular server, it will display a message indicating that "the server's certificate is not trusted" , which means it may be coming from a man-in-the-middle-attacker. In this situation you should not proceed with the HTTPs session [14].

There are 3 different ways by which we can defend against MITM attack. Although, the efforts to defend the MITM attack have not given surety about 100% secureness, but the awareness can be taken by following these methods:

Method 1: VPN

VPN is an abbreviated form of Virtual Private network which is primarily used for secured network. A VPN extends a private network into a public network e.g., the Internet. A point to point connection through the use of dedicated connection a VPN can be created[11].

To proceed for the connection of VPN, you should have a remote VPN server set up & configured, you can do it yourself or just employ some reliable VPN service such as 'HideMyAss', and once have it, you can follow the steps below to establish a safe point-to-point connection with it. All data transmission is encrypted so that even if being intercepted, the attacker will have no idea about the content of the traffic [11].

Step1. Click to "Control Panel" in the startup menu.
Step2. In Control Panel, select to "Network and Internet".
Step3. Click "Network and Sharing Center".
Step4. Click "Setup a new connection or network".
Step5. In the "Setup a new connection or network" dialog, select "Connect to a workplace" and then press "Next".

Step6. In the "Connect to a Workplace" dialog, click "Use my Internet connection (VPN)".
Step7. Input the IP address of the VPN server and press "Next".
Step8. Input your username and password, then press "Create".
Step9. Click "Connect Now" [11].

Method 2: Proxy Server with Data Encryption

It encrypts the transmission between user and the proxy and so it can be achieved by having some software like "HideMyIp" which provides proxy servers and option of encryption [11].
Step1. Download and install HideMyIP in your PC and double click on it to launch the program.
Step2. In the main interface, click on the "Advanced Settings".
Step3. After clicking to "Advanced Settings", a dialog box will open, where you need to check on "Encrypt my Connection with SSL", which ensures that the data to the sites you are visiting will be kept encrypted, like a https connection. Step4. Select a server you want to connect and then finally, press to "Hide My IP" [11].

Method 3: Secure Shell Tunneling.

Secure Shell (SSH) is a network protocol for remote administration of UNIX/LINUX hosts. SSH are supports tunneling, forwards TCP ports and X11 connections. An SSH tunnel is used to transfer an unencrypted traffic over a network through an encrypted channel [11].

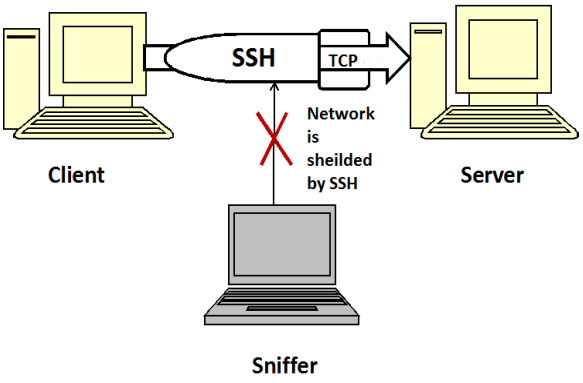

Fig3. SST technique [11].

Step1. Download and install "Bitvise SSH Client" and double-click to launch the program.

Step2. Select the "Services" tab in the main interface, in the SOCKS/HTTP Proxy Forwarding Section, check to Enable forwarding feature, then fill in the IP address of Listen Interface, 127.0.0.1, which means the local host. Listen Port could be an arbitrary number ranging from 1 to 65535, but to avoid conflicts with the well-known port, a port number between 1024 and 65535 is suggested here.

Step3. Switch to the "Login" tab to Login.

Step4. When connect to a server for the first time, a dialog containing the MD5 fingerprint of the remote server will pop up, you should check the fingerprint carefully to authenticate the real identity of the SSH server. You can get the real MD5 fingerpirnt of the server from your host administrator or using Linux command ssh-keygen -lf file.

Step5. Open a browser (e. g Firefox), open menu, then click "Options".

Step6. Select "Advanced" in "Options" Dialog, click "Network" tab, then click "Settings…".

Step7. In the "Connection Settings" dialog, select "Manual Proxy Configuration" option, choose the proxy type "SOCKS v5", and fill in the IP address and port number of the proxy server, then press "OK". Since we are running SOCKS proxy forwarding using Bitvise SSH client in the same computer, the IP address should be 127.0.0.1 or localhost, and the port number must be the same as we set in step 2 [11].

VI. MITM Attack: Challenges

One of the challenges of MITM attacks is active eavesdropping. Eavesdropping means silently and secretly listening to the conversation of client and server or the users. In this attack, the attacker gets the independent connection with the victims (i.e., the sender and the receiver) and alter messages between them. Here, the victims will think that they are directly having conversation with each other.

MITM also exploits session management. In cloud computing services, it is easy to transfer and store large amount of data. Some examples of this are: Dropbox, OneDrive and GoogleDrive. These services typically don't need to log in every time to use. Instead, it saves a session token in the local system after authentication. If any attacker gets that access to the token, they would have full control to the account. It may lead to the stealing of the data, altering files, or uploading malware in the users system to infect the computer [14].

VII. Conclusion

MITM attack is very difficult to be prevented and cannot be eliminated completely but we can minimize the possibility of these attacks onto the network. However some of the actions can be undertaken to provide shield to the existing network system which include client side infrastructure security i.e., new updated operating systems must be used on a network, security of network should be at

primary concern while designing it. In this way we try to implement primary methods so that any user doesn't become the victim of MITM attack [1].

MITM attack applies to quantum cryptographic system [6]-[8]. ARP poisoning can also be prevented by using shell script at the backend that can be helpful in keeping the track on ARP cache table (maps IP address and MAC address). [9],[10]. But this is not the perfect solution since there will be a lot of updating in ARP request, which could lead to traffic inside the network and shell script will run only on Linux, not in Windows.

VIII. Acknowledgment

Authors of this paper gratefully acknowledge the help of each and every author of the referenced papers from where ideas have been borrowed to complete this survey paper.

References

[1] Kapil M Jain & Manoj V Jain, International Journal of Science Technology and Engineering, Man in the Middle Attack survey, March 2016.

[2] Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani and Kamal Bunkar, "An Overview & Study of Security Issues in Mobile Ado Networks", International Journal of Computer Science and Information Security, Vol-9, No.4, pp (106-111), April 2011.ISSN: 1947-5500,

[3] Pushpendra Kumar Pateriya, Analysis on Man in the Middle attack on SSL, International Journal Of Computer Application, 23 May 2012.

[4] Animesh Dubey, Ravindra Gupta, Gajendra Singh, Survey and Analysis of Client Side Detection of Content Sniffing Attack, March,2013

[5] Margaret Rouse, Hijacking, 2012.

[6] Shivlal Mewada, Pradeep Sharma, S.S Gautam, "Exploration of Efficient Symmetric AES Algorithm", 2016 Symposium on Colossal Data Analysis and Networking (CDAN), pp(1-5), Mar, 2016. Doi: 10.1109/CDAN.2016.7570921,

[7] S. Kak, Quantum information and entropy, 2007.

[8] G. N. Nayak and S. G. Samaddar, different flavours of man-in-the-middle-attack, consequences and feasible solutions, 2010.

[9] B. Issac, Secure ARP and secure DHCP protocols to Mitigate Security Attacks. International Journal of network security 8, 2009.

[10] Tanmay Patange, How to defend yourself against MITM or Man-in-the-Middle attack, October 2013.

[11] http://destroyadware.com/articles/security/3-effective-ways-defend-man-middle-attack-mitm/, 3 effective ways to defend against a Man-in-the-Middle Attack (MITM)

[12] Rachna Jain, Sushila Madan and Bindu Garg, "Analyzing Various Existing Security Techniques to Secure Data Access in Cloud Environment", International Journal of Computer Sciences and Engineering, Volume-03, Issue-01, Page No (130-135), Jan -2015,

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

[14] Michael Gregg, How new technologies are reshaping MITM attacks, 23 July 2013.

[15] Dinu P S, Deepa S Kumar, Dr. M Abdul Rehman, Preventing SQL injection Attacks Using Cryptography Methods, 5 May 2015.

Author(s) Profile

Manjula Kalita is an assistant professor in the Department of Computer Science and Engineering at Girijananda Chowdhury Institute of Management and Technology, Azara, Guwahati-781017, Assam, India. She received her M. Tech in Information Technology from Tezpur University in 2008. Her research areas include data and web mining, cloud security, computer and network security. She has presented one papers in International conference ADCOM in Chennai and that paper is published in IEEE Xplore Digital Library. She has presented another one paper in a national conference in Tezpur University and that one was published in conference proceeding.

Sukanya Dutta is a 7th semester B. Tech student in the department of Computer Science and Engineering from Girijananda Chowdhury Institute of Management and Technology under Assam Science and Technology University, Assam India. She is working for the securities in the network to establish a safe connection and avoid intruders to take participate in data transit in today's telecommunication network for her upcoming project.

Ayesha Yesmin is a B. Tech student in the Department of Computer Science and Engineering from Girijananda Chowdhury Institute of Management and Technology under Assam Science and Technology, Assam, India as well. She is working with the author Sukanya Dutta as mentioned above for the same section i.e., for the security in the networking level.

