Sountra et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 4 Issue 1, Jan, - March 2020

Man in the Middle - Hacker's Playground

[1]Shariq Malik, [2]Muhammad Shairoze Malik
[1]Shariqmalik@lgu.edu.pk, [2]Shairozemalik@lgu.edu.pk
Lahore Garrison University

Abstract

There has been an increase in potential sources of threats to the security of information systems and data of governments, companies and individuals in the present day, due to the growing number of information systems types and devices, the expanding availability of freely-downloadable open source tools, the degree of interconnectivity made possible by the internet, and the concentration of more self-help power in the hands of individual end users. A numerically-insignificant number of the total population of information systems end users is made up of black hat users who have caused significant economic losses and reputational damages for organizations and governments through exploitation of security vulnerabilities. One of the most common and widespread security threats is that of Man-in-the-Middle (MitM), which has remained a major source of concern to security professionals for many years, and continues to pose a threat to information security as the focus of attack continues to be data, and the black hat users continue to look for new ways to circumvent security safeguards implemented for existing technologies and countermeasures planned for new and emerging technologies. Many papers have been written about Man-in-the-Middle attack, that have described different kinds of such attacks and explained solutions to the attacks but not illustrated how the attack can be carried out and showed how the risks arising from such attacks can be mitigated. This paper presents a step-by-step account of one way in which MitM attack can be realized and how the confidentiality and integrity of data can be prevented from being compromised through use of PKI (Public Key Infrastructure).

Keywords: MitM (Man-in-the-Middle), Attack, Defense, PKI (Public Key Infrastructure), Security.

1. Introduction

Man in the Middle (MitM) attack refers to a security scenario in which the direct communication of information between two systems is intercepted by a third party who can then secretly passively read, relay and or maliciously modify the data that is being sent between the two communicating systems. The name Man-in-the-Middle is believed to have been coined from a pattern of play in the sport of Basket Ball, whereby two players are in the process of passing a ball to one another while a player between them attempts to seize the ball. It is also referred to as bucket (or fire) brigade attack, which is a name derived from the fire brigade process of putting out fires by passing buckets of water around different persons between the source of the water and the fire. MitM attack is also known as TCP Session Hijacking.

In this report, based on our demonstration of a MitM attack and defense, and limited review of a few relevant research publications, we:

i. Discuss some techniques used in MitM attacks
ii. Present complete instructions to demonstrate a MitM attack.
iii. Present complete instructions to demonstrate a Public Key Infrastructure (PKI) defense against a MitM attack.
iv. Present a conclusion from our observations.

2. Some Techniques used in MitM Attacks

One common feature of all types of MitM attacks is that the attacker forces a connection to be established with each of the two communicating systems, without the two communicating systems knowing that they are each connected directly with the Man-in-the-Middle and not with each other, as shown in Fig. 1.

2.1 ARP Spoofing

ARP Spoofing is a security attack in which an attacker sends falsified ARP (Address Resolution Protocol) messages across a LAN (Local Area Network), resulting in the mapping of the attacker's MAC address to the IP address of a system or server on the network. It is also known as ARP Cache Poisoning. After the attacker's MAC address has been successfully mapped to an IP address, any data addressed to the IP address will be received by the attacker.
To effectively become a Man-in-the-Middle between any two systems via ARP Spoofing, the attacker will map the IP addresses of the two systems to its system's MAC address.
ARP Spoofing is possible only in LANs that use ARP.

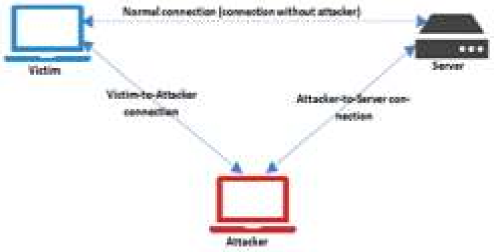
2.2 DNS Spoofing

DNS Spoofing is a security attack in which falsified Domain Name System (DNS) data is injected into the cache of the DNS resolver, causing the DNS to serve the false or fake IP address in response to DNS queries for the affected domain name. It is also known as DNS Cache Poisoning.

The fake address can quite easily spread from one DNS server to several other DNS servers, as other DNS servers query the corrupt DNS cache for the corrupt domain name entry and update their own caches in turn with the falsified mapping.

2.3 Host File Modification

Host File Modification is a security attack in which the attacker successfully fraudulently inserts an entry in the hosts file of the victim's system to map attacker's IP address to a domain name, so that every request sent by the victim to the domain name will be directed to the attacker's system.


Normal connection (connection without attacker)
Victim
Server
Victim-to-Attacker connection
Attacker-to-Server con-nection
Attacker

(Fig. 1: Man-in-the-Middle Attack)

The attacker can then, in addition to other actions, modify the message's source IP to attacker's IP address and destination IP to the server's IP before sending the message to the server. The server will then send the response back to the attacker, who can then read and or modify the payload and change the source and destination IP addresses to the attacker's and victim's IP addresses respectively before sending the message to the victim.

3. MitM Demonstration

3.1 Demonstration Environment and Tools
The demonstration environment and tools include the following components:
i. Oracle Virtual Box
ii. Three Ubuntu 16.04 LTS 32-bit Linux VMs, namely Server VM, Victim VM, Attacker VM

3.2 Setup and Execution

i. Create three (3) VMs, namely Server, Victim, Attacker
a. Configure Network as Host Only, so that the VMs can communicate with each other but not with the internet
ii. Start the VMs
a. Notice that the VMs have internal IPs in the same network subnet

3.3 Demonstrate Normal Connection (Connection Without Attacker)

3. Do the following in Server's VM:
a. Create directory, TestServer, in user's home directory:mkdir ~/TestServer

b. Change directory to TestServer:
cd ~/TestServer

c. Create a file inside TestServer directory, called Mitm.html, that contains just the words "Hi from Server":

```
echo "Hi from Server" > Mitm.html
```

d. Run the following command while in ~TestServer; this command starts a Python HTTP server listening on port 8000

```
python -m SimpleHTTPServer
```

4. Do the following in Victim's VM:

a. Enter the following line inside Victim's /etc/hosts file, to help in resolving www.lgu.edu.pk to the server's IP (replace Red entry below with the server's IP):

```
<Server_IP> www.lgu.edu.pk
```

b. Launch a browser

c. Type the following in Victim's browser and observe that the resulting web page displays the words "Hi from Server":

```
http://www.lgu.edu.pk:8000/TestServer/Mitm.html
```

3.4 Demonstrate Victim-To-Attacker Connection

5. Run the following in Victim's VM, to forward all outbound traffic with destination ports 80, 443, 8000, to Attacker's IP (replace Red entry below with the attacker's IP):

```
sudo iptables -t nat -A OUTPUT -p tcp --dport 80 -j DNAT --to-destination <Attacker_IP>
sudo iptables -t nat -A OUTPUT -p tcp --dport 443 -j DNAT --to-destination <Attacker_IP>
sudo iptables -t nat -A OUTPUT -p tcp --dport 8000 -j DNAT --to-destination <Attacker_IP>
```

6. Do the following in Attacker's VM:

a. Create directory, TestServer, under user's home directory:

```
mkdir ~/TestServer
```

b. Change directory to TestServer:

```
cd ~/TestServer
```

c. Create a file inside TestServer directory, called Mitm.html, that contains just the words "Hi from Attacker":

```
echo "Hi from Attacker" > Mitm.html
```

d. Run the following command while in ~TestServer; this command starts a Python HTTP server listening on port 8000

```
python -m SimpleHTTPServer
```

7. Refresh the browser session on Victim's VM and observe the displayed content change to "Hi from Attacker". This is because in Victim's VM, we are now forwarding all outbound traffic going to port 8000 to Attacker VM.

3.4 Demonstrate Attacker-To-Server Connection

8. Run the following in Attacker's VM, to forward all incoming traffic with destination ports 80, 443, 8000, to server's IP (replace Red entry below with the server's IP):

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination <Server_IP>
sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination <Server_IP>
sudo iptables -t nat -A PREROUTING -p tcp --dport 8000 -j DNAT --to-destination <Server_IP>
sudo iptables -t nat -A POSTROUTING -j MASQUERADE
```

9. Refresh the browser session on Victim's VM and observe the displayed content is "Hi from Server". However, the traffic between Victim and Server is now being routed through the Attacker.
10. Open Wireshark in Attacker VM to inspect traffic flow between Victim and Server. The words "Hi from Server" were displayed in plain text.

3.5 Demonstrate PKI Certificates Implementation - A Defense Against MitM Attack

Do the following on Server VM:

11. Copy this file, /etc/ssl/openssl.cnf, to your home directory on Server VM:

```
cd
cp /etc/ssl/openssl.cnf .
```

12. Create files and directories under your home directory for openssl, as follows:

```
mkdir demoCA
mkdir demoCA/certs
mkdir demoCA/crl
touch demoCA/index.txt
mkdir demoCA/newcerts
echo 1000 > demoCA/serial
```

13. Run the following command to create create CA certificates. You will be prompted for the items shown below following the command:

```
openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
```

PEM passphrase: <Enter a phrase of your choice, but you must remember it>

Country Name: <Enter:- CA>

Province: <Enter:- Ontario>

Locality Name: <Optional, press Enter to continue>

Organization Name: <Enter:- Group4 6100G Project>

Organizational Unit Name: <Optional, press Enter to continue>

Common Name: <Enter:-www.grp4_6100g_project_uoit.edu>

Email Address: <Optional, press Enter to continue>

14. Run the following command to generate public/private key pair. You will be prompted for the items shown below following the command:

```
openssl genrsa -aes128 -out server.key 1024
```

passphrase for server.key: <Enter a phrase of your choice, but you must remember it>

15. Run the following to create a CSR. You will be prompted for the items shown below following the command:

```
openssl req -new -key server.key -out server.csr -config openssl.cnf
```

passphrase for server.key: <Enter the same phrase you entered when generating public/private key pair above. e.g. fessam>

Country Name: <Enter:- CA>

Province Name: <Enter:- Ontario>

Locality Name: <Optional, press Enter to continue>

Organization Name: <Enter:- Group4 6100G Project>

Organizational Unit Name: <Optional, press Enter to continue>

Common Name: <Enter:-www.grp4_6100g_project_uoit.edu>

Email Address: <Optional, press Enter to continue>

A challenge password: <Optional, press Enter to continue>

An optional company name: <Optional, press Enter to continue>

16. Run the following command to generate signed certificate. Respond to the prompts shown below following the command:

```
openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
```

Sign the certificate? [y/n]: <Enter y>

1 out of 1 certificate requests certified, commit? [y/n] <Enter y>

17. Put both the secret key and the certificate in a .pem file

```
cat server.key > server.pem
cat server.crt >> server.pem
```

18. Create and save a script file in user's home directory, named server.py, with the following contents:

```
#!/usr/bin/python

import BaseHTTPServer, SimpleHTTPServer
import ssl

httpd = BaseHTTPServer.HTTPServer(('<Server_IP>', 8000), SimpleHTTPServer.SimpleHTTPRequestHandler)
httpd.socket = ssl.wrap_socket (httpd.socket, certfile='server.pem', server_side=True)
httpd.serve_forever()
```

19. Start Python's secure web server, as follows. Enter the same PEM passphrase as chosen earlier above:

```
python server.py
```

20. Enter the following line inside Victim's /etc/hosts file if not already done, to help in resolving www.lgu.edu.pk to the server's IP (replace Red entry below with the server's IP):

```
<Server_IP>        www.lgu.edu.pk
```

21. Launch a broswer on Victim's VM and enter the following as URL. Note that this URL is now using secure HTTP, i.e. HTTPS:

    https://www.lgu.edu.pk:8000/TestServer/Mitm.html

22. If the browser displays error, import the self-signed CA certificate (ca.crt) into the browser, as follows if using Firefox Web Browser (follow the appropriate procedure if using a different web browser), then click Import button:

    Edit -> Preference -> Privacy & Security -> View Certificates

23. Repeat step #21 above, if you did step # 22.

24. Open Wireshark in Attacker VM to inspect traffic flow between Victim and Server.

The words "Hi from Server" were no longer displayed. This is because the contents of the conversation between the victim and the server have now been encrypted and can therefore neither be seen in plain text nor identifiable in Wireshark.

4. Results

From the above demonstration we can take a look at how easy it is for hackers to perform a Man in the Middle attack on a given target and go through the target's sensitive information. In article two types of attacks were demonstrated. One where the traffic between victim and internet in unencrypted while the other in which the said traffic in encrypted. In both cases MitM attack was performed but due to encryption in second attack the sniffed data was not compromised.

5. Conclusion

Man in the Middle attack is just one of the recipes in a hacker's playbook and we can see just how much effective it is in different environments. We can see that without the proper secure certificates implemented on the websites, all the data that goes through them is at risked to be taken. The implementation of PKI certificates effectively protected the integrity and confidentiality of the information exchanged between the victim and the server.

6. References

[1] Mauro Conti, Senior Member, IEEE, Nicola Dragoni, and Viktor Lesyk "A Survey of Man In The Middle Attacks"
IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, THIRD QUARTER 2016

[2] Mayank Agarwal, Santosh Biswas, and Sukumar Nandi "Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks"
IEEE COMMUNICATIONS LETTERS, VOL. 19, NO. 4, APRIL 2015

[3] Matthew Johnson, Peter Lutz, and Daryl Johnson, Rochester Institute of Technology "Covert Channel using Man-In-The-Middle over HTTPS"
International Conference on Computational Science and Computational Intelligence, Year: 2016, Pages: 917 - 922

[4] Enrique de la Hoz, Rafael Paez-Reyes, Gary Cochrane, Ivan Marsa-Maestre, Jose Manuel Moreira-Lemus, Bernardo Alarcos "Detecting and Defeating Advanced Man-In-The-Middle Attacks against TLS"
2014 6th International Conference on Cyber Conflict, Pages: 209 - 221

[5] Prerna Arote and Karam Veer Arya (ABV-Indian Institute of Information Technology and Managament, Gwalior, India) "Detection and Prevention against ARP Poisoning Attack using Modified ICMP and Voting"
International Conference on Computational Intelligence & Networks, 2015, Pages 136 - 141

[6] Peng Zhou (1School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, People's Republic of China), Xiaojing Gu (2School of Information Science and Engineering, East China University of Science and Technology, Shanghai, People's

Republic of China) "HTTPAS: active authentication against HTTPS man-in-the-middle attacks"
IET Journals, 2016, ISSN 1751-8628

[7] Parth Patni, Kartik Iyer, Rohan Sarode, Amit Mali, Anant Nimkar (Department of Computer Engineering, Sardar Patel Institute of Technology, University of Mumbai, Mumbai, India - 400053) "Man-in-the-Middle Attack in HTTP/2"
International Conference on Intelligent Computing and Control (I2C2), 2017

[8] Shaun Stricot-Tarboton, Sivadon Chaisiri, Ryan K L Ko (Cyber Security Lab, University of Waikato) "Taxonomy of Man-in-the-Middle Attacks on HTTPS" 2016 IEEE TrustCom/BigDataSE/ISPA, Pages: 527 - 534

[9] Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. Int. Arab J. e-Technol., 1(2), 26-36.

[10] Altunbasak, H., Krasser, S., Owen, H., Sokol, J., & Grimminger, J. (2004, November). Addressing the weak link between layer 2 and layer 3 in the Internet architecture. In Local Computer Networks, 2004. 29th Annual IEEE International Conference on (pp. 417-418). IEEE.

[11] Anagreh, M. F., Hilal, A. M., & Ahmed, T. M. (2018). Encrypted Fingerprint into VoIP Systems using Crypto-graphic Key Generated by Minutiae Points. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCI-ENCE AND APPLICATIONS, 9(1), 151-154.

[12] Andersen, D. G., Balakrishnan, H., Feamster, N., Koponen, T., Moon, D., & Shenker, S. (2008, August). Account-able internet protocol (aip). In ACM SIGCOMM Computer Communication Review (Vol. 38, No. 4, pp. 339-350). ACM.

[13] Hossain, M. S., Paul, A., Islam, M. H., & Atiquzzaman, M. (2018). Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks. Network Protocols and Algorithms, 10(1), 83-108.

[14] Hudaib, A. A. Z. (2014). Comprehensive Social Media Security Analysis & XKeyscore Espionage Technol-ogy. International Journal of Computer Science and Security (IJCSS), 8(4), 97

[15] Li, X., Li, S., Hao, J., Feng, Z., & An, B. (2017, February). Optimal Personalized Defense Strategy Against Man-In-The-Middle Attack. In AAAI (pp. 593-599).

[16] 'man-in-the-middle-attack" (Rapid Web Ser.), Blog Post, 2017, Retrieved from: https://www.thess-lstore.com/blog/man-in-the-middle-attack/

[17] 'man-in-the-middle-attack-mitm' (Techpedia), 2018, Retrieved from: https://www.techopedia.com/defini-tion/4018/man-in-the-middle-attack-mitm

[18] 'man-middle-attack' (CA Tech.), 2018, Retrieved from: https://www.veracode.com/security/man-middle-attack