International Journal of Engineering Innovation & Research
Volume 1, Issue 5, ISSN : 2277 – 5668

A Simplified Defense Mechanism Against Man-In-The-Middle Attacks

Alok Pandey
Sr. Systems Manager
Department of Computer Science Engineering, Birla Institute of Technology Mesra, Jaipur Campus, Rajasthan, INDIA
E-mail : alokpandey1965@yahoo.co.in

Dr. Jatinderkumar R. Saini
Director (I/C) & Associate Professor
Narmada College of Computer Application, Bharuch, Gujarat, INDIA
E-mail : saini_expert@yahoo.com

Abstract **- Using the Man-In-The-Middle attack the attacker tries to intercept / modify / change or replace the data being exchanged with false information. At times the attacker tries to inject commands and even force the victims system to downgrade some of the running services so that the target system can be easily exploited using different techniques. The basic concept behind "Man-in-the-middle attack" (MITM attack) is to intrude into the existing communication between the endpoints on a network and intercept the data transferred between them and change the actual contents or inject false information.**

The purpose of this document is to spread the awareness about the MITM attacks that are seen in the real time scenario. The initial sections discuss the different types of attacks that can be launched under the MITM category. It also gives a general idea of how the attackers can launch different types of downgrading of services attacks on the victim machine so that further exploitation of the victim becomes easier. Some of the commonly used techniques and tools that are used by the attackers are also mentioned here-in.

Finally the document discusses some of the different countermeasures that are being used to avoid the MITM attacks. Although several technologies employing different levels of complexity are used these days, we hereby suggest some simple and effective measures that can be used to simplify the user authentication process and assure the identity of the communicating partners using simple basic individual identifiers.

Keywords **- Command Injection, Downgrade Attack, Intercepting Public Key, Man-in-the-Middle (MITM) attack, Malicious Code Injection.**

I. INTRODUCTION

By using Man-In-The-Middle attack the attacker tries to intercept the data being exchanged and modify or change or replace it with false information. The kind of techniques involved in carrying out such kind of an attack involve eavesdropping and intruding into a connection, intercepting the messages and modifying the data. Some other popular names for this kind of attack are :-

- Monkey-in-the-middle attack
- Session hijacking
- TCP hijacking
- TCP session hijacking

The basic concept behind "Man-in-the-middle attack" to intrude into the existing communication between the endpoints on a network and intercept the data transferred between them change the actual contents or inject false information. [1]

The MITM attack can be visualized as an active eavesdropping in which the attacker establishes separate connections with the victims and relays messages between them. But actually the entire conversation between the victims is now being controlled by the attacker. [2]. We can say that an unwanted user gets between the sender and receiver of information and sniffs the information being exchanged. [3]. In other words the intruder in such attacks actually infiltrates unnoticed into the communication channel between two genuine partners and thus is able to access or modify the data being exchanged. [4]

The MITM attacks are also sometimes called as "session hijacking attacks", wherein the intruder aims to gain access to a legitimate user's session and to tamper it. Such attack is usually initiated by sniffing and eavesdropping leading to alter, forge or reroute the intercepted data. Main objectives of MITM attack are as follows:-

1. To gain access to the information being exchanged and use it later for alteration and retransmitting such modified versions to the actual receiving end.
2. To mislead the communicating partners at the client or server end,
3. To intercept the individual identity, address details, password combinations, bank account related information or other forms of personal, confidential or financial information for malicious purposes.
4. For manipulating the transactions.

The Hackers usually select this kind of attack against public-key cryptosystems. The intruder may substitute the intercepted public key with a forged public key. The victims are made to believe that they are safely communicating with each other. [1].

Another common MITM attack scenario may involve the attacker gaining access into the communication between a client and a server and violate the security while the client and the server feel that they are safely communicating with each other. The attacker may use such a program which appears like a server to the client or vice versa.

In some cases, the attacker initially tries to get in between target network endpoints and remain transparent to all the communication between them. Once established, the attacker may launch different attacks including sniffing the passing packets or hijacking already authenticated sessions or even injecting packets or commands into the server, and sending the forged responses to the victim client.

II. USAGE of M.I.T.M. ATTACKS

The application of the MITM attacks is commonly seen in the following areas:-

1. False Commands & Malicious Code are injected by the attacker.
2. Intercepting Secrete Key & other sensitive personal & financial information being exchanged during a web based e-commerce transaction
3. Downgrading of services Attacks.

2.1For Injection of Commands and Malicious Codes

Command may be injected and executed by the attackers to hijack sessions on the server and emulate fake replies to the clients during the MITM attacks [6]
Attacks like SQL injection, HTML / Script injection, modifying the binary files etc. being downloaded to implant victim clients with malicious codes, Trojans etc. to change the execution process of the downloaded programs are carried out using MITM attacks. [6]

2.2. Intercepting Secrete Key & other sensitive personal& financial information during e-commerce transactions:

Gaining access to e-commerce transactions and other web-based financial transaction systems, including online banking, insurance, credit card payments, and other forms of e-business websites are some prominent areas where MITM is used which may result in identity thefts and financial frauds.

For doing so the attackers intercept the communication while the public key is being exchanged between the client and the server, and change the original public keys for a malicious reasons. The relevant encrypted messages and replies are also intercepted by the attackers who may then use the correct public keys to decrypt and re-crypt the messages so as to avoid any suspicion. Such attacks pose high risks on the insecure networks. [5]

2.3. Downgrading of Services Attacks

Attackers may manage to change the parameters being exchanged between the endpoints at the start of their connection itself [6] and force the victims to use the lower security features, functions or protocols which remain supported for backward-compatibility reasons. An attacker may "force the client to initialize a SSH1 connection instead of SSH2".

The network protocol SSH supports command-line access capabilities. SSH ver. 1 had some security holes which were improved in the SSH ver. 2. Although SSH ver. 2 is preferred by hosts, yet SSH ver.1 is still being supported for backward compatibility reasons. During the downgrade attacks, a MITM attacker can force the victims to use the SSH ver.1 protocol and play havoc. [9].

During an MITM the attacker may manipulate the messages being exchanged so that the victims may be tricked into thinking that IPSEC is not supported on the remote communication partner and hence cannot start the IPSEC session. Even worse, if the victim hosts are configured in rollback mode, they may initiate clear text transmission over the connection which might not be noticed by the victims.

In some cases MITM attackers may force the victims to use the less secure PAP authentication, MSCHAP ver.1 instead of MSCHAP ver.2, or communication without encryption by manipulating the parameters during the initial information exchanged during the protocol handshaking phase of the PPTP session. It is also possible to steal passwords. PPTP is a protocol for VPN implementation. The Microsoft MSCHAP-V2 or EAP-TLS is used for authentication of PPTP connections. The Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) is a safer security option for PPTP than MSCHAP-V2 since it is certificate based.[10]

III. TECHNIQUES USED FOR CARRYING OUT MITM ATTACKS

Some of the techniques used for MITM attacks can be summarized as follows:

1. ARP spoofing
2. IP address spoofing
3. DHCP spoofing
4. DNS spoofing
5. Gateway spoofing
6. ICMP redirection
7. Stealing of Ports

3.1. ARP spoofing:-

The attacker sometimes uses “ARP spoofing” to sniff data frames on LAN and to modify the packets being transmitted on the LAN. “ARP spoofing” is also called as "ARP Poisoning". Using this technique the attacker may corrupt the ARP caches of the victims that are directly connected and take over their IP address.

3.2. IP address spoofing:-

For hiding the identity of the sender or impersonating another computer the attacker creates IP packets with forged source IP address. Such types of attacks are normally aimed to exploit the trust relationship between victim endpoints. Hping is one of the commonly used tool.

3.3. DHCP Spoofing:-

DHCP spoofing is an attack on a DHCP server where the attacker attempts to fool the server into obtaining the IP address by using Spoofed DHCP messages to obtain access into the server resources.

3.4. DNS spoofing:-

The attacker sniffs the ID of the DNS request and sends forged replies to the victim before the genuine DNS Server. Sometimes the records of DNS server are forged by the attacker to divert the traffic to its servers.

3.5. Gateway Spoofing:-

The idea is to cheat the gateway which is an internal network PC. The attacker sends a series of wrong router MAC address within the network continuously to the gateway so that the real users can not update the address information stored in the router, this results in the router sending data to the wrong MAC address, causing the normal PCs not to receive the genuine communication

messages. Using forged gateway the idea is to create false gateway, so as to cheat gateway PC to send false data, rather than through the normal way to access the router

3.6. ICMP Redirection:-

ICMP is used by the IP layer to send one-way informational messages to a host. Since ICMP does not support authentication it leads may lead to attacks that result in denial of services or allowing the attacker to intercept packets. The ICMP "Redirect" message is commonly used by gateways when a host assumes that the destination is not on the local network.

During ICMP packet magnification an attacker sends forged ICMP echo packets to networks' broadcast addresses. All the systems on such networks send ICMP echo replies to victim, consuming the bandwidth and creating a denial of service to genuine traffic.

3.7.Stealing of Ports:-

In this technique the attacker spoofs the switch forwarding database and manipulates the switch port on L 2 switched victim networks for sniffing of the packets. Such kind of attacks are initiated by flooding the switch with the forged ARP packets containing the same source MAC address as that of the victim host and the destination MAC address of the attacking host.

As a result the switch will repeatedly alter the MAC address binding to either of these two ports. The switch will be receiving genuine packets from the victim host connected to one port and forged packets from the attacker on other port. If the rate at which attacker's packets arrive is faster then the switch will send the packets intended for the victim host to the attacker. In the process the attacker sniffs the received packet, stops flooding and sends an ARP request for the victim's IP address. The victim host sends the ARP reply, which the attacker uses to forward the forged packets to the victim. [11].

IV. Tools Used for Carrying out MITM Attacks

Details of the commonly used tools for launching the MITM attacks in different environments are as under :-

4.1 Parasit - URL:
http://packetstormsecurity.org/groups/thc/parasite-1.2.tar.gz

Parasite is a tool with the ability to perform ARP spoofing, MAC flooding and MAC duplicating. When operating in spoofing mode, the chance that the ARP spoofing attack will be successful are increased.

4.2 ARPoison - URL: http://arpoison.sourceforge.net

Arpoison is a program that sends out a custom ARP REPLY packet. Since ARP is a stateless protocol, most operating systems will gladly update their ARP cache with any information you send them in your hand-crafted packet.

4.3 Zodiac - URL :
http://packetfactory.openwall.net/projects/zodiac/index.html

Zodiac is a DNS protocol analysis and exploitation program. This sturdy tool is used to explore the DNS protocol. It has the support for DNS packet construction and disassembling.

4.4 ADM DNS spoofing tools - URL :
http://packetstormsecurity.org/groups/ADM/ADM-DNS-SPOOF/

ADM DNS spoofing tools - Uses a variety of active and passive methods to spoof DNS packets.

4.5. Ettercap [7] - URL: ettercap.sourceforge.net

Ettercap is multipurpose LAN-based hacking tool for which is used for sniffing, intercepting and logging. It supports detailed analysis of many protocols. It even supports network and host analysis. Hackers use Ettercap to launch an MITM attack using ARP poisoning or port stealing techniques.

4.6. Dsniff [8]- URL:
http://www.monkey.org/~dugsong/dsniff

Dsniff tool suite was primarily developed for network auditing & penetration testing. The attackers use it conducting for SSL MITM attacks. It supports passive monitoring of network for sensitive data like e-mail, files and passwords etc. Some of its components like "ARPSPOOF", "DNSSPOOF" etc. allow the interception of network packets. While using the other components like "SSHMITM" and "WEBMITM" the attackers can launch active man-in-the-middle attacks.

4.7. Yersinia - URL: http://www.yersinia.net/

Yersinia can be used to exploit the network protocols like STP, DHCP, VTP etc. This robust tool can support combinations of multithreading & multiple attacks per user. Yersinia works in command line mode, network client mode and GUI mode. It is used to listen the network traffic, sniff packets, intercept network data, analyze, edit, modify and / or replay the captured packets after modifications.

V. Defenses Against the MITM Attacks

Majority of the defense mechanisms that are being used against MITM attacks are authentication based techniques which might be based upon the following [2]:

- Passwords
- Secret questions
- Public key infrastructures
- Voice recognition
- Biometrics (Figure printing and Retina scan)
- Off-the-Record Messaging for instant messaging
- Off-the channel verification

A large number of newer techniques that have evolved in the recent time to provide stronger authentication at login to users are :-

1. Use multi-factor authentication to protect logins.
2. Time-synchronized, one-time password authenticators.
3. Software toolbars.
4. Site-to-user Authentication.
5. Multi-factor Authentication to Protect Logins.

5.1. Use multi-factor authentication to protect logins

Just by the mere provision of username and password is not enough to protect sensitive data with the advanced nature of security threats in the current times. Besides, many countries have imposed security regulations requiring organizations to provide strong authentication mechanisms [12].

5.2. Time-synchronized, one-time password authenticators.

In this technique a time-synchronized, one-time password authenticator device offers a unique Symmetric key which is combined with an algorithm to generate a new one-time password (OTP) every 60 seconds. This handheld O.T.P. authentication device is synchronized with a security server that checks the validity of the password for that 60-second window. The hardware device used for this purpose could be as small as a key-chain. The user can use such devices for accessing the Internet from different locations, for performing high-value and high-risk transactions.

5.3. Software toolbars.

Similar to the hardware devices, software toolbars are available which act as a one-time password authenticator which gets embedded within a standard Internet browser such as Internet Explorer or Mozilla Firefox. The software toolbars generate a new one-time password (OTP) every 60 seconds.

5.4. Site-to-user Authentication.

In this technique a visible security reminder is given to users at each login so that the user is assured that he is transacting with a legitimate website. These security reminders include a personal security image and caption that were pre-selected by the user during the enrolment sessions at the previous login. Once the web site has proven its authenticity then only the user must enter their password for further processing.

5.5. Multi-factor Authentication to Protect Logins

Majority of the one-time password (OTP) authentication solution are based on something that is you know to the user only like a PIN or something that is available only with the user (an authenticator). The authenticator generates a new code every 60 second making it difficult for anyone other than the genuine user to input the correct token code at any given time. For gaining the access the users simply combines the secret Personal identification Number (PIN) with the token code that appears on the display of the authenticator devices at that given time. This results in a unique, one-time password combination that can confidently assure a user's identity.

IV. OUR SUGGESTIONS

For simplification of the process & at the same time hardening of the mechanism and vouching for the authenticity of the user a combinations of the following may be used along with the OTP scheme :-

To generate a specific code number the following confidential information pertaining to an individual which uniquely identify him can be used :-

1. A 10 digit Bank Account Number
2. A 10 digit Mobile Phone Number
3. Social Security Number of the user issued by the Government based / nominated agencies

6.1. Procedure to Generate the secret key(In the Indian context) :-

Assuming the persons individual details are as mentioned below, the users secrete key can be generated as explained

10 digit user bank account – 10 02 02 12 34
10 digit mobile number - 98 25 01 23 45
12 digit Aadhar social security no. – ABCD EFGH IJKL

Picking the character at odd places in the 1st set of information we get - 0,2,2,2,4
Picking the character at even places in the 2nd set of information we get - 8,2,0,2,4
Picking the character at every third places in the3ed set of information we get - C,F,I,L,

Adding a character in the last place in the third set of information to represent the social id type. In this case it is character A representing the Aadhar unique id is added. finally we have a matrix of 5 x 3

0,2,2,2,4
8,2,0,2,4
C,F,I,LA

Interchanging the rows and columns of the matrix for first time we get

0,8,C
2,2,F
2,0,I
2,2,L
4,4,A

The secrete key can be written like 08C,22F,20I,22L,44A. Dropping the commas we get a 15 digit unique code like –

08C22F20I22L44A

Now this uniquely generated secrete key can be used for encrypting the message being sent. At the receiving end the encrypted message can be decrypted using this secret key. The secrete key should be transmitted to the receiver by offline communication like s.m.s. on the cell phone of the user. The above mechanism would satisfy the following dimensions of security:-

1. Confidentiality of the message is maintained as it is an encrypted communication.
2. The credentials of the sending party are frozen so that the sender is genuinely identified as the genuine sender and not any unauthorized person or hacker.
3. Since the identifications used for generating the secrete key are vouched by third parties which are genuine authenticators of the user hence it satisfies the Authentication and Integrity conditions for the sender.

4. As the transmission of the secrete key from the sender to the receiver is in the offline mode using the mobile phone which can be considered as the second form factor and is available only with the receiver it can be treated the foolproof transfer of the secrete key to the receiver. Thus using the above mechanism the communication can be secured and the integrity of the message is retained.

6.2. Combination with other commonly available user parameters

In addition to the above, tracking mechanism for recording the other parameters which the legitimate user generally uses for accessing the internet and conducting transactions like :-

1. The combination of IP address and the MAC address.
2. The operating system and browser combination normally used.
3. The user's location.

Any deviations in the above behavioral pattern may be processed accordingly to differentiate between legitimate users and MITM attacks. So based upon the above we can simplify the process of securing the communication and easily identify any unauthorized persons playing the MITM attacks.

VII. CONCLUSIONS

We acknowledge the ongoing efforts in this area by various individuals and research based organizations. .Although a lot of work is being done in this area yet there is always a scope for newer ideas which may prove to be successful in the longer runs.

Our approach primarily aims at simplify the process of generating the secrete key that is used for the encryption and decryption process being used for proving the identity of the communicating partners. Since the unique individual parameters that are being used in the process have already been established and vouched by third parties which are in the public domain or government based / approved agencies, hence they can be treated as genuine and as such counter verification of the user details can be avoided making the process faster.

In addition we have tried to minimize the chances of leakage of the information to the unauthorized persons, while it is in transit, by using the sophistications of the "offline mode of communication" through S.M.S. and implementing two factor authentication mechanism. Going one step further we have tried to incorporate the concept of multifactor authentication by recording and analyzing the combinations of IP address, MAC address, Operating System, Browser type and checking the location of the user.

We feel that the above suggested simplifications will not only seed-up the overall procedure for implementing security in communication but also provide flexibility of operation as the scheme allows to select and change to a different set of input parameters like Income Tax Account details or Passport number or Driving License Number etc. of the communicating partners based upon the specific requirements. However the actual implementations could be vary depending upon the country specific requirements and the prevailing laws.

REFERENCES

[1] Whatis.com | SearchSecurity.com Definitions: What is man in the middle attack?
[2] Wikipedia: Man-in-the-middle attack
[3] Javvin Technologies: Network Security Dictionary.
[4] Melani | Information Assurance Reporting and Analysis Center: Semi-Annual Report 2005 Issue 2
[5] Wikipedia: Public-key cryptography
[6] Alberto Ornaghi, Marco Valleri, "Man In The Middle Attacks," BlackHat Conference Europe 2003
[7] Sourceforge.net | Ettercap: Short Description
[8] Monkey.org | Dug Song: dsniffx Frequently Asked Questions
[9] Wikipedia: Secure Shell
[10] Wikipedia: Extensible Authentication Protocol - EAP-TLS
[11] Packetwatch Research | Ryan Spangler 2003: Packet Sniffing on Layer 2 Switched Local Area Networks
[12] RSA Security Incorporated – www.rsa.com

AUTHOR'S PROFILE

Alok Pandey

is Senior Systems manager and faculty member at B.I.T.(MESRA), Jaipur Campus. His qualifications include B.E.(EEE) ,MBA. He is also done MCSE, RHCE, CCNA, IBM Certified E-Commerce and diploma in Cyber law. He has a rich industrial working experience of more than 17 years and also a teaching experience of about 7 years in the areas of Data Communication and Computer Networks, Information Security, E-Commerce, Systems Management , ERP etc. He is also a member of CSI, IAENG and ISOC. His research interests include Computer Networks and Network Security.

Dr. Jatinderkumar R. Saini

is Ph.D. from Veer Narmad South Gujarat University, Surat, Gujarat, India. He secured first rank in all three years of MCA in college and has been awarded gold medals for this. He is also a recipient of silver medal for B.Sc. (Computer Science). He is an IBM Certified Database Associate-DB2 as well as IBM Certified Associate Developer-RAD. He has presented 14 papers in international and national conferences supported by agencies like IEEE, AICTE, IETE, ISTE, INNS etc. One of his papers has also won the 'Best Paper Award'. 11 of his papers have been accepted for publication at international level and 13 papers have been accepted for national level publication. He is a chairman of many academic committees. He is also a member of numerous national and international professional bodies and scientific research academies and organizations.