Volume 4, No. 2, February 2013

Journal of Global Research in Computer Science

REVIEW ARTICLE

Available Online at www.jgrcs.info

ISSN-2229-371X

ANALYSIS OF MITM ATTACK IN SECURE SIMPLE PAIRING

Praveen Kumar Mishra
Research scholar, Dept. of computer, ideal institute of technology, Ghaziabad, Utter Pradesh, India,
amanpraveen@gmail.com

Abstract: This paper explain on different types of MITM attacks, their consequences, techniques and solutions under different circumstances giving users options to choose one from various solutions. Man-In-The-Middle (MITM) attack is one of the primary techniques in computer based hacking. MITM attack can successfully invoke attacks such as Denial of service, DNS spoofing and Port stealing. MITM attack of every kind has lot of surprising consequences in store for users such as, stealing online account user id, password, stealing of local ftp id, or telnet session etc. Man-in-the-middle attack is used wildly as a method of attacking the network. To discover how this type of attack works, this paper describes a method of man-in-the-middle attack based on ARP spoofing, and proposes a method of preventing such attacks. a new method is proposed in this paper to secure the exchange of public keys in SSP. By adopting the proposed technique, the exchange of public key becomes more secure and consequently, the process of SSP will be secure, reliable and provide protection against Man-In-The-Middle (MITM) attacks.

Keyword – MITM, DNS .Denial of services, Spoofing, telnet, SSP, Public key

INTRODUCTION

A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. In the process, the two original parties appear to communicate normally. The message sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting to the receiver. Thus, the attacker controls the entire communication. [2]

This term is also known as a janus attack or a fire brigade attack.

Active man-in-the-middle is an attack method that allows an intruder to access sensitive information by intercepting and altering communications between the user of a public network and any requested website. Avoiding logging in to sensitive sites from public locations can protect the user from conventional man-in-the-middle attacks. However, in an active MITM attack, the perpetrator manipulates communications in such a way that they can steal information for sites accessed at other times [1]

An active MITM may be conducted in a number of ways. Here's one method:

a. The attacker listens to communications transmitted over a public network.
b. The victim accesses the Internet over the network and browses to an innocuous website, such as a mainstream news site.
c. The website server processes the request and responds to it.
d. The attacker intercepts the response sent from the server and interjects an I Frame object targeting their chosen site.
e. When the user's browser receives the compromised response, it invisibly requests that website along with the cookie storing user credentials for the site.
f. This response allows the attacker to log in to the site and interact in any way that the valid user can.

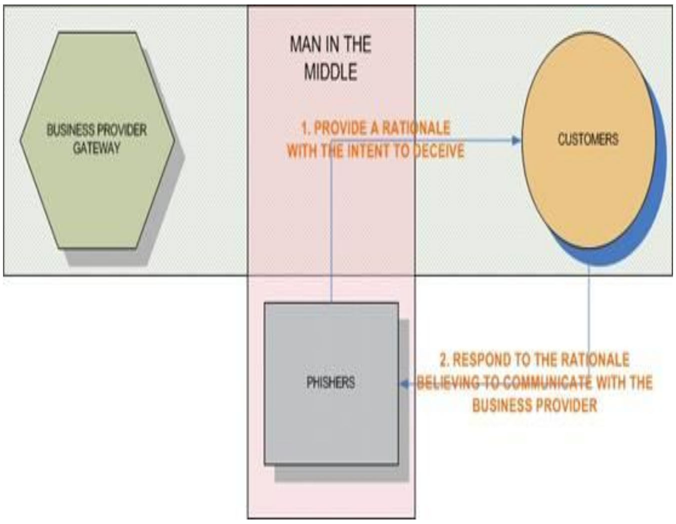
BUSINESS PROVIDER GATEWAY
MAN IN THE MIDDLE
1. PROVIDE A RATIONALE WITH THE INTENT TO DECEIVE
CUSTOMERS
PHISHERS
2. RESPOND TO THE RATIONALE BELIEVING TO COMMUNICATE WITH THE BUSINESS PROVIDER

Figure- 1 Mitm Attack

DIhFFERENCE BETWEEN NORMAL AND MAN IN THE MIDDLE FLOW

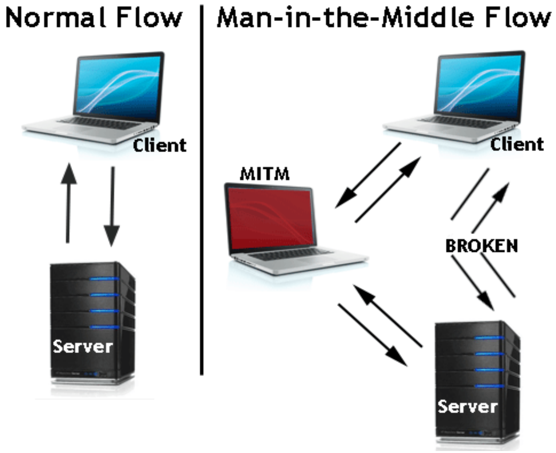

Figure -2 Normal And Mitm Flow

In the image above you will notice that the attacker inserted him/herself in-between the flow of traffic between client and server. Now that the attacker has intruded into the communication between the two endpoints he/she can inject false information and intercept the data transferred between them. [4]

Example of an attack:

Jack sends a message to Jill, which is intercepted by Peter
Peter relays this message to Jill; Jill cannot tell it is not really from Alice:
Jill responds with his encryption key:
Peter replaces Jill's key with her own, and relays this to Jack, claiming that it is Jill's key:
Jack encrypts a message with what she believes to be Jill's key, thinking that only Jill can read it:
However, because it was actually encrypted with Peter's key, Peter can decrypt it, read it, modify it (if desired), re-encrypt with Jill's key, and forward it to Jill:
Jill thinks that this message is a secure communication from Jack.

This example shows the need for Jack and Jill to have some way to ensure that they are truly using each other's public keys, rather than the public key of an attacker. Otherwise, such attacks are generally possible, in principle, against any message sent using public-key technology. Fortunately, there are a variety of techniques that help defend against MITM attacks.

Figure -3 Mitm Attack Example

The hacker is impersonating the both sides of the conversation to gain access to funds. This example holds true for a conversation with a client and server as well as person to person conversations. In the example above the attacker intercepts a public key and with that can transpose his own credentials to trick the people on either end into believing they are talking to one another securely.

INTERACTION POSSIBLE TO MITM ATTACKS

a. Financial sites – between login and authentication [5]
b. Connections meant to be secured by public or private keys []
c. Other sites that require logins – where there is something to be gained by having access.
d. Side jacking - This attack involves sniffing data packets to steal session cookies and hijack a user’s session. These cookies can contain unencrypted login information, even if the site was secure.
e. Evil Twin - This is a rogue Wi-Fi network that appears to be a legitimate network. When users unknowingly join the rogue network, the attacker can launch a man-in-the-middle attack, intercepting all data between you and the network.
f. Sniffing - This involves a malicious actor using readily available software to intercept data being sent from, or to, your device [5]

MAN IN THE MIDDLE ATTACK IN SIMPLE SECURE PAIRING

Simple Secure Pairing:

Secure simple pairing wired networks a Certificate Authority (CA) can be used for the purpose of securing the exchange of public keys. CAs are servers that can be used for verification. However, CAs cannot be used reliably in wireless networks. For example in Bluetooth technology it was proposed to nominate one of the piconet devices in the PAN to act as a CA. It was proposed that this device will generate the keys for all other devices. However, the process of securing the exchange of public keys in the communicating Bluetooth devices that uses SSP method was not fully considered. Accordingly, a new method is proposed in this paper to secure the exchange of public keys in SSP. By adopting the proposed technique, the exchange of public key becomes more secure and consequently, the process of SSP will be secure, reliable and provide protection against Man-In-The-Middle (MITM) attacks.

Before any Bluetooth device start transmitting, pairing must be done. As a result of this two devices would form a trusted pair and a link key is constituted. The six phases of SSP are as follows [8]

Figure- 4 SSP Stages

Capabilities Exchange: During this stage devices interchange their Input/output capabilities to find out the best association model used. This phase happens when the devices had never encountered earlier or when they want to re-perform the pairing process for the some reason.

***Public Key Exchange**:* During this stage public private key is exchanged With each other .Diffie Hellman key is also calculated in this phase also.

***Authentication Stage 1**:* This stage target to render protection versus MITM attacks. It is accomplished by exchanging commitment to the nonces, set of nonces and the exchanged public key to check their integrity.

Authentication Stage 2: This phase is same in all association models. It affirms that public key exchanged took successfully.

Link Key Calculation: Once pairing is affirmed by both devices, the link key is computed using their Bluetooth address, nonce value and Diffie Hellman key.

LINK MANAGEMENT PROTOCOL

Authentication and Encryption: Encryption keys are generated in this phase.

Mitm Attack In Ssp:

MITM attacks are becoming the main problem in Bluetooth area networks. The MITM nodes are behaving like the original nodes and they can send/receive the valuable data.

These MITM nodes can modify the data between the source and destination also. The attacks are based on the falsification of information sent during the input/output capabilities exchange The motivation is to achieve the solution for avoiding the MITM attacks in secure simple pairing method.

Proposed Method Of Ssp:

A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other—it is an attack on (or lack of) mutual authentication. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. We had seen attacker intercept public key in simple secure pairing we try to protect public key with the help of newly added step before SSP. [6][9]

We encrypt the public key of each device with the help of known cryptographic function which is known to each user in advance Transfer the public key of one device to other and vice versa. This public key is decrypted with known cryptographic function.

In this way each device will have public key of each other.

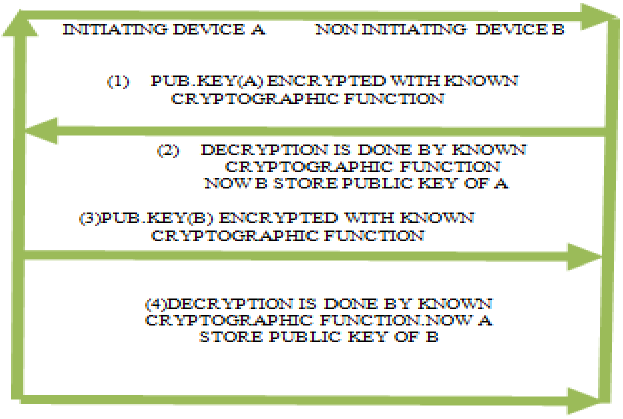
INITIATING DEVICE A
NON INITIATING DEVICE B
(1) PUB.KEY(A) ENCRYPTED WITH KNOWN CRYPTOGRAPHIC FUNCTION
(2) DECRYPTION IS DONE BY KNOWN CRYPTOGRAPHIC FUNCTION NOW B STORE PUBLIC KEY OF A
(3)PUB.KEY(B) ENCRYPTED WITH KNOWN CRYPTOGRAPHIC FUNCTION
(4)DECRYPTION IS DONE BY KNOWN CRYPTOGRAPHIC FUNCTION.NOW A STORE PUBLIC KEY OF B

Figure 5: proposed phase before ssp

Step 1:We store the public key of A in B database
Step2 : we store the public key of B in A database

Now initiate the steps of secure simple pairing as described previously. Now the steps of pairing are as follows:

Suppose there are two device A & B:

Encrypt the public key of A device with the help of known cryptographic function

Transfer the public key of A device to B. This public key is decrypted with known cryptographic function

This public key is stored in the database of B device

Encrypt the public key of B device with the help of known cryptographic function

Transfer the public key of B device to A. This public key is decrypted with known cryptographic function

This public key is stored in the database of A device.

DEFENCES TECHNIQUES OF MITM ATTACK

Trusting Keys and Certificates a client that wants to connect to an application site starts using the certificate sent by the site. An attacker can intercept the conversation and send the client a fake certificate, claiming that it comes from the application site. If the client trusts the fake certificate, the MITM attack becomes possible. [1][2][4]

a. The solution to this problem is to use a trusted Certificate Authority (CA) to verify that the certificate, digital signature, or key belongs to the person using it. By adding strong authentication on PKI systems, any certificate coming from a non-trusted CA will be revoked, including the attacker's fake certificate.
b. Public key infrastructures
c. PKI mutual authentication The main defence in a PKI scenario is mutual authentication. In this case as well as the application validating the user (not much use if the application is rogue) - the users devices validates the application - hence distinguishing rogue applications from genuine applications
d. Secret keys (which are usually high information entropy secrets, and thus more secure
e. Passwords (which are usually low information entropy secrets, and thus less secure
f. Off-channel verification

g. Carry forward verifications
h. Other criteria, such as voice recognition or other biometrics
i. Second (secure) channel verification
j. One time password are immune to MITM attacks, assuming the security and trust of the one-time pad.
k. Forensic analysis of MITM attacks
   (a). IP address of the server
   (b). Is the certificate self signed?
   (c). Do other clients, elsewhere on the Internet, also get the same certificate?
   (d). Is the certificate signed by a trusted CA?

Although PKI on its own is not a sufficient mitigating control against MITM attacks, when it is coupled with mutual authentication, the solution is more appeal-ing. Mutual authentication is the concept of requiring not just a client to authenticate to a server but also the server to authenticate to the client. With many client and server implementations, the initial trust is only confirmed by a one-way verification between the client and the server. With mutual authentication, the server verifies the client and the client verifies the server to ensure legitimate communications are being exchanged. Verification can be conducted by using public and private keys.Some implementations of port security will determine access based on what hardware addresses are connected to each port. For example, in a situation where port security is enabled and a desktop computer is plugged into the switch port, the switch will learn the physical address of the desktop computer and only allow that hardware device to connect on that port. Should someone disconnect the desktop. Computer and attempt to plug in a laptop or other device, the port would identify the change and shut down the port. Once again, a notification may be sent to administrators to warn of potential issues. Although this sounds like a logical method of restricting access, if an attacker has the physical address of the initial device connected to the port he or she may be able to spoof the physical address to gain access via the port.[6] But Diffie-Hellman suffers from a well-known problem: An attacker inserts himself between the two parties and, for each one, pretends to be the other, sending each one his own Diffie-Hellman message. Both parties end up sharing their secret key with the attacker, who then has full access to the communications between them.[14]

CONCLUTION

The middleman has traditionally been seen as evil by security protocol designers, and attempts are made to exclude him. In real life. We think the time has come for a rethink.

To summarize, the man-in-the-middle defense is a good way to do two things. First, it is a sensible place to introduce a dynamic and upgradeable element which allows a slower but more careful evolution of an underlying protocol, or the retrofitting of protection to a protocol which is too expensive to change. Second, it gives us an opportunity to bring the human back into the protocol where there was no window for manual intervention before. Man-in-the-Middle attacks are generally network-related attacks used to sniff network connections or to act as a proxy and hijack a network connection without either of the victims being aware of this. The main advantage of our proposed algorithm is that we can detect man-in-the middle attack during the second stage of simple secure pairing i.e. simple secure pairing. Proposed algorithm is very effective since public key is stored with each device database.

REFERENCES

[1]. Man in the middle attackhttp://hackerthedude.blogspot.in/2009/10/man-in-middle-attack-mitm.html

[2]. Man-in-the-middle attack http://en.wikipedia.org/wiki/Man-in-the-middle_attack

[3]. K. Haataja and P. Toivanen. Practical Man-in-the-Middle Attacks Against Bluetooth Secure Simple Pairing. In 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08, pages 1–5, Oct. 2008.

[4]. Learn about mitm attack, veracode.com/security/man-in-the-middle-attack

[5]. Key Concepts of a Man in the Middle Attack , veracode.com/security/man-in-the-middle-attack

[6]. Safari books online .com , chapter name-defences against man in the middle attack page-114, chapter-6

[7]. B. B. Gupta, R. C. Joshi, M. Misra, ―Defending against Distributed Denial of Service Attacks: Issues and Challenges,‖ Information Security Journal: A Global Perspective, vol. 18, issue 5, Taylor & Francis, UK, pp. 224-247, 2009.

[8]. K. Haataja and K. Hypponen. Man-In-The-Middle attacks on Bluetooth: A Comparative Analysis, A Novel Attack, and Countermeasures. In 3rd International Symposium on Communications, Control and Signal Processing, ISCCSP'08, pages 1096–1102, March 2008.

[9]. J. Dunning. Taming the Blue Beast: A Survey of Bluetooth Based Threats. IEEE Security & Privacy, 8(2):20–27, Mar-Apr. 2010

[10]. Bluetooth SIG. Bluetooth Technology in Hands of One Billion. Press release, http://www.bluetooth.com/ Bluetooth/SIG/Billion.htm, November 14, 2006.

[11]. Mohamed Ghallali, Driss El Ouadghiri, Mohammad Essaaidi, and Mohamed Boulmalfm, ―Mobile phones security: the spread of malware via MMS and Bluetooth, prevention methods,‖ In Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia (MoMM '11). ACM, New York, NY, USA, pp. 256-259, 2011

[12]. Kugler and Dennis. \man in the middle attacks" on bluetooth. In FinancialCryptography, volume 2742 of Lecture Notes in Computer Science, pages 149-161. Springer Berlin / Heidelberg, 2003.

[13]. http://en.wikipedia.org/wiki/D-H_Algorithm

[14]. Going Around with Bluetooth in Full Safety‖ , FSecure. http://www.securenetwork.it/ricerca/whitepaper/download/bluebag_brochure.pdf