IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Enhanced Security for the Prevention of Man-In-The-Middle Attacks

V. Yadagiri[1], G. Pranavi Goud[2], G.Bhargav[3], K. Komali Reddy[4]

Assistant Professor, Computer Science Department, Guru Nanak Institute of Technical Campus, Hyderabad, India [1]

Student, Computer Science Department, Guru Nanak Institute of Technical Campus, Hyderabad, India [2,3,4]

Abstract: Man-In-The-Middle (MITM) ambush is one of the majorly recorded assaults in personal computer safety. Man-In-The-Middle aims at a certain info which passes among two end terminals, and privacy and righteousness of the data. We tend to broadly study the writings on Man In The Middle to scrutinize and reach the range of Man-In-The-Middle blitz, taking into account the referral model in the similar way as OSI design and also taking into consideration of two set of widely utilized networking technologies that is the Global System for Mobile and Universal Mobile Telecommunication System.In particular the Man-In-The-Middle assaults can be occurred due to the criteria like location of the sender, receiver and the attacker according to the channel of communication, the type of transmission and the spoofing techniques and provide implementation for the all possible Man-In-The-Middle groups. We draw the resemblance by understanding the pros and cons of the existing methods which prevent attacks. Eventually, according to our analysis we provide a system which gives the secured information and reduced attacks.

Keywords: Man-In-The-Middle (MITM) attack, GSM, UMTS, OSI model.

I. INTRODUCTION

In system safety Man-In-The-Middle attack is a kind of attack in which the attacker tries to intrude in the communication between two parties, who think they are directly connected to each other through a communication channel. The attacker gets connected to the two parties independently and sends the data to them making them believe that they are actually directly connected to each other, but in reality the whole data(confidential information, password) is controlled by the attacker [1]. A broad investigation and literatures on MITM by taking into account the widely used network technologies like the Global System for Mobile and Universal Mobile Telecommunication System [8]. The MITM attacks are happening due to some of the criteria like the location of the sender, receiver, attacker and the type of data being sent and also some of the spoofing techniques. We analyse the counter measures and survey the relation among these parameters [2]. In this paper, we safeguard the MITM attacks by not providing the options for the unauthorised users and also not allowing them to invade into the network.

II. EXISTING SYSTEM

In the present existing system the Man-In-The-Middle particularly aims at the data that is flowing between the two clients who are at two different ends of the network. Man-In-The-Middle attacker mainly concentrates on the sensitivity and the rectitude of the information being passed in the network between the two end points. In the existing Man-In-The-Middle attacks as the attacker will not be able to imitate the client. The key technique that is used in this system is key management server which is used to issue a public key. In the existing system it does not brace the host which have the static IP address. Eventually it is observed that the information is secured, it is not very scalable. If the private keys cannot be protected, security is no better than password authentication.

III. PROPOSED SYSTEM

In this system according to the writings on the Man-In-The-Middle, we scrutinize the possibility of MITM attacks focusing on the OSI model and also two of the broadly utilized network technologies like the Global System for Mobile and Universal Mobile Telecommunication System [3]. The technique which is being proposed in this system is the DES(Data Encryption Standard) algorithm [6].

The DES algorithm encrypts the data and provides the secret key cryptography. It uses a unique key for both the encryption and decryption of the information. The main advantage of this system is it gives the secured information while passing through the network and reaching to the client. It totally minimises the chances of attacker to attack or steal the data. In this method, there are six different sections which perform separate operations which in total helps to provide the enhanced security to information passed between two endpoints.

A. User Interface Design

The important role for the Network user is to move login window to cloud user window. In this login page we have

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

to enter login user id and password. The server will check whether the username and password is matched or not. If we enter any invalid username or password we can't enter into login window to user window as it will shows error message. It will provide a good security for our project. It well improves the security by preventing the unauthorized users entering into the network [5]. In our project we are using JSP for creating design. Here we validate the login user and sever authentication.

B. Clients Nodes selection

Parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS) .The current Internet standard—in an efficient and scalable manner [8].This is similar to the situation that once the adversary compromises the long-term secret key [6], it can learn all the subsequence sessions. If an honest client and an honest storage device complete matching sessions, they compute the same session key. Second, two our protocols provide forward secrecy: one is partially forward secure with respect to multiple sessions within a time period.

C. Random key generation

The primary goal in this work is to design the efficient and secure authenticated key exchange protocols that meet the specific requirements of pNFS [6][7]. We describe our design goals and give some intuition of a variety of pNFS authenticated key exchange (pNFS-AKE) protocols that we consider in this work.

D. DES Encryption

The protocol should guarantee the security of past session keys when the long-term secret key of a client or a storage device is compromised. However, the protocol does not provide any forward secrecy.

To address key insurance while achieving forward secrecy simultaneously, we incorporate a Diffie- Hellman key agreement technique into Kerberos-like pNFS-AKE-I. However, we achieve only partial forward secrecy (with respect to v), by trading efficiency over security [6].

E. MITM Attack

In this module the unauthorized user i.e., the users who are not having permission to access other information. The user who uses the network in a wrong manner may block by the server when the server gets a notification message that someone is accessing in unauthorized access. Once the Unauthorized user blocked by the server cannot be undone ever.

F. MITM Defense Technique

Accept &Allow user file:

The admin can accept the new user request and also block the users. The users can upload the file to Network. And the admin can allow the files to Network then only the file can store the cloud. If the file uploaded by the user is not permitted from the Server means the file cannot be uploaded by the Client [3].

IV. SYSTEM ARCHITECTURE

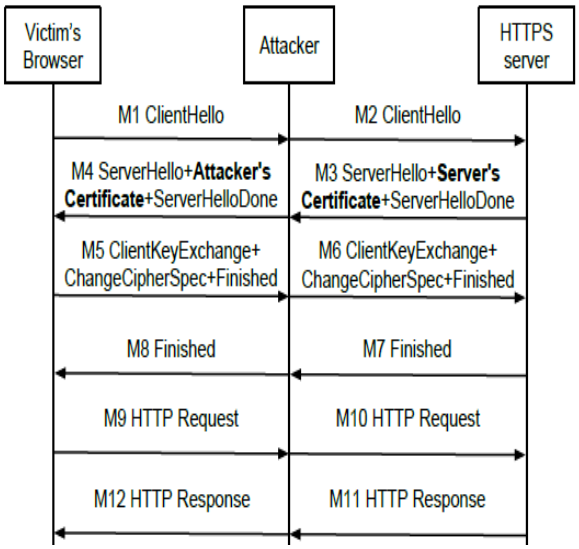

Fig 1. System Architecture of Man-in-the middle attacks

System Architecture of Man-In-The-Middle Attack shows how the number of clients accessing server parallel and server producing Authenticated Key to client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file which will be in the encrypted form. Once the key is given it will decrypt into original form [7]. A Server can add a new client and he can able to block the existing client in case of any malicious activities take place.

V. RESULTS

In this project, we can completely eliminate the problems of MITM attacks. The admin has the complete authority on the users using the application. The IP address of an attacker can be traced if he finds anything suspicious. Through this project, we describe the activities from user side, attacker side and the admin side as well. We use java framework to execute the above method to show the working of the system.

User Activities

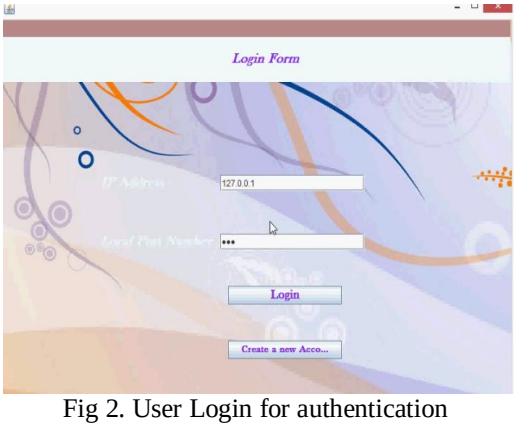

Fig 2. User Login for authentication

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

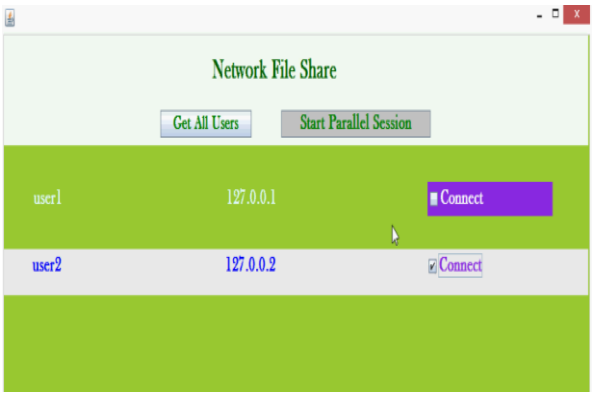

Fig 3. User1 connecting with User2 to exchange files

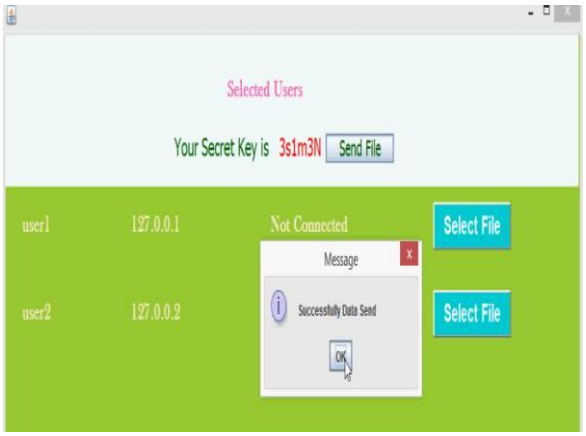

Fig 4. Generation of secret key when data is sent to user2

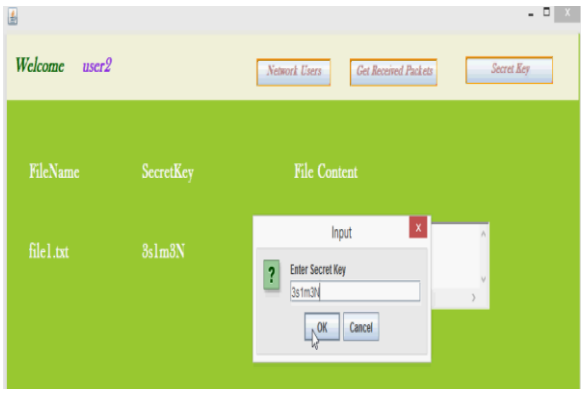

Fig 5. User2 decrypts the file using the secret key

Fig 6. Information displayed after decryption

Attacker Activity

Fig 7.Attacker (user3) trying to hack user1 data

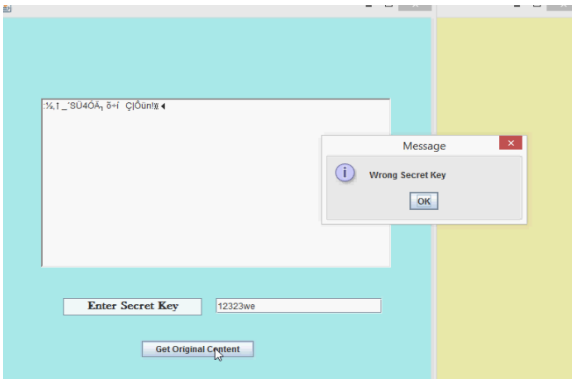

Fig 8. Attacker trying to open the encrypted file

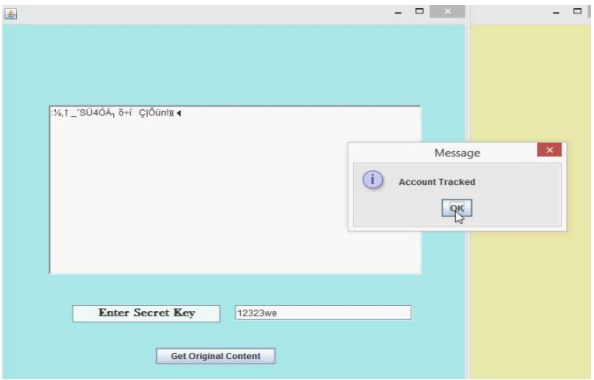

Fig 9. Attacker's account tracked

Admin Activity

Fig 10. Admin getting the notification of the hacker

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Fig 11. Admin blocks the hacker(user3)

VI. CONCLUSION

We have analysed MITM attack and presented a comprehensive classification of such attack based on impersonation techniques. Also, we provided MITM defense mechanism along with its description. In this paper, we provide all MITM prevention mechanisms, according to used approaches and context (abstract layer) of applicability [1]. To sum it up, we can collect the most effective methods to eradicate these MITM attacks. These methods have been discussed throughout the whole paper, so here we refer only to the section in which the method has been presented more in detail.

ACKNOWLEDGMENT

We feel it as a great pleasure in submitting this paper on "Enhanced Security for the prevention of Man-In-The-Middle Attacks". Firstly we express our deep sense of gratitude and sincere thanks to Assistant Prof. Y. Yadagiri for the best support, opinions, views and comments which had helped us greatly.

REFERENCES

[1] M. Abd-El-Malek, W.V. Courtright II, C. Cranor, G.R. Ganger, J. Hendricks, A.J. Klosterman, M.P. Mesnier, M. Prasad, B. Salmon, R.R. Sambasivan, S. Sinnamohideen, J.D. Strunk, E. Thereska, M. Wachs, and J.J. Wylie. Ursa Minor: Versatile cluster-based storage. In Proceedingsof the 4th USENIX Conference on File and Storage Technologies (FAST), pages 59–72. USENIX Association, Dec 2005.

[2] C. Adams. The simple public-key GSS-API mechanism (SPKM).The Internet Engineering Task Force (IETF), RFC 2025, Oct 1996.

[3] M.K. Aguilera, M. Ji, M. Lillibridge, J. MacCormick, E. Oertli, D.G. Andersen, M. Burrows, T. Mann, and C.A. Thekkath. Blocklevelsecurity for network-attached disks. In Proceedings of the 2nd International Conference on File and Storage Technologies (FAST).USENIX Association, Mar 2003.

[4] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Communications of the ACM, 53(4):50–58. ACM Press, Apr 2010.

[5] Amazon simple storage service (Amazon S3). http://aws.amazon.com/ s3/.

[6] M. Bellare, D. Pointcheval, and P. Rogaway.Authenticated key exchange secure against dictionary attacks. In Advances in Cryptology– Proceedings of EUROCRYPT, pages 139–155. Springer LNCS 1807, May 2000.

[7] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Advances inCryptology – Proceedings of CRYPTO, pages 258–275. Springer LNCS 3621, Aug 2005.

[8] B. Callaghan, B. Pawlowski, and P. Staubach.NFS version 3 protocol specification.The Internet Engineering Task Force (IETF), RFC 1813, Jun 1995.