Defending Man In The Middle Attacks

Radhika.P[1] , Ramya.G[2] , Sadhana.K[3] , Salini.R4

[123]*Student, Dept of Computer Science and Engineering, Panimalar Engineering College, Tamilnadu,India*
[4]*Assistant Professor, Dept of Computer Science and Engineering, Panimalar Engineering, College, Tamilnadu, India*

Abstract - *The Man-In-The-Middle (MITM) attack is one amongst the most documented attacks in pc security, representing one of the most important considerations for security professionals. MITM targets the particular information that flows between endpoints, and the confidentiality and integrity of the info itself. In this paper we overcome man in the middle attack in local file sharing systems by blocking the unauthorized user and preventing him to enter the network in future. Both the IP Address and the path of the attacker is completely blocked. As a result the attacker is reduced and the information is transmitted in a secure manner. The server keeps track of the IP Address of the attacker and notifies to the other servers in the organization to block the attacker IP Address.*

Keywords: Man-In-The-Middle (MITM) attack, MITM defense techniques, MITM classification, security, DES (Data Encryption Standard), PNFS(Parallel Network File System).

1. INTRODUCTION

The name Man-In-The-Middle is gotten from the ball situation where two players mean to pass a ball to each other, while one player between them tries to seize it. MITM assaults are some of the time alluded to as unit assaults on the other hand fire detachment assaults. MITM focuses on the real information that streams amongst endpoints, and the secrecy and uprightness of the information itself. MITM is an active eavesdropping attack where, in a communication between two devices *A* and *B*, the attacker receive *A* by pretending he is *B*. This means whenever *A* wants to send a message to B, it actually sends it to the attacker who read the message then forward it to *B* in order to make the communication still working. The attacker can read all the content of the communication including mails, images and passwords.

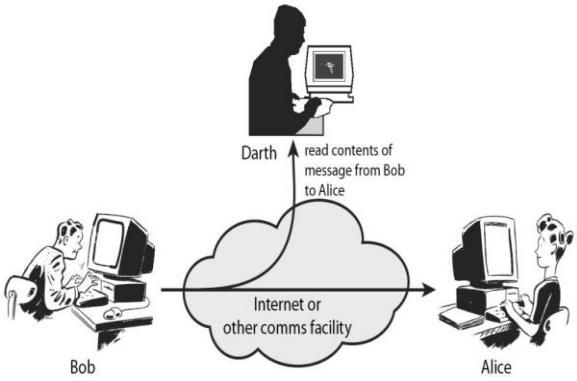

Fig.1: Man In The Middle Attack

1.1. Methodology

We used bottom-up approach so as to induce the higher understanding of the present standing of the MITM attack. Firstly, we have a tendency to reviewed most literature that mentions MITM attack, that was revealed no sooner than 2000.
Then we have a tendency to began to classify articles, papers, books, supported used protocols, and theirs contribution (such as new science bar technique, or new detection approach). Later, we have a tendency to found that some approaches square measure modifications of a lot of older one, therefore we have a tendency to extended scope by as well as a lot of older literature. At now we have a tendency to began to specialize in the foremost mentioned attacks, and bar ways, and supported them we have a tendency to created main categorization of the MITM attack.

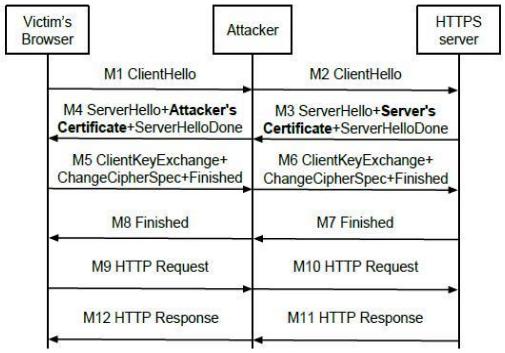

Fig.2: Attacker Accessing

1.2. Contribution of the Paper

In this paper we provide a method to block the unauthorized user from the local file sharing network. Further, in paper we classify MITM attacks based on several parameters, namely: location of an attacker in the network, nature of a communication channel, and impersonation techniques. Next, we use the impersonation techniques classification as a reference classification and we go into details for each category providing attack algorithms and categorizing prevention mechanisms.

To the best of our knowledge this is the first extensive paper on defending man in the middle attacks by blocking the path of the unauthorized user and preventing him to enter the network in future. When we compare our work with the existing body of research, we see the following. Clark etal. [11] executed one of the most significant surveys of defense schemes against SSL/TLS MITM attack. Authors reviewed the spectrum of issues concerning trust model between certified authorities and browsers. Similarly, in [12]–[14], researchers carried out small studies of detecting and defeating mechanisms of SSL/TLS MITM attack. Saxena et al. [15] collected proposals, which prevent MITM attack on GSM and UMTS networks. Thus, there is no previous work in the literature that covers MITM attacks across each layer of the OSI model, classifies MITM, and categorizes MITM defense approaches. Our work fills this gap, by providing MITM attack survey over the period 1992-2015.

1.3. Architecture Diagram

System Architecture is the overall layout of the system. In the proposed architecture, the trusted systems will locally share the files by encryption and decryption using secret key. Whereas when an untrusted system generate random secret key it will be notified to the database then it blocks the system and its path completely.

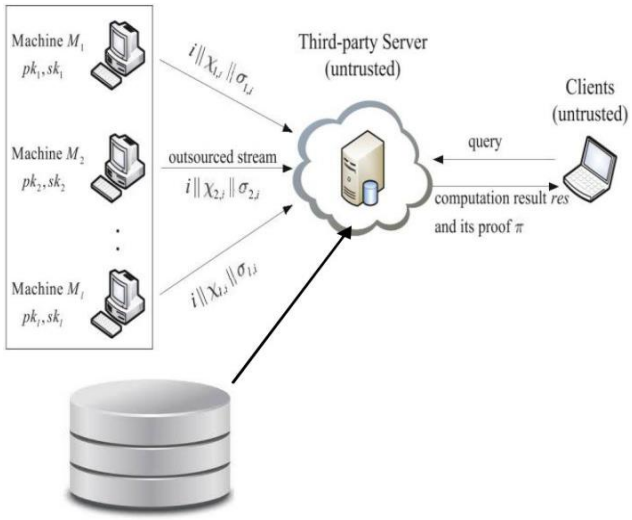

Fig.3: Architecture

1.4. DES Algorithm

The Data Encryption Standard (DES) is an obsolete symmetric-key technique for information encryption.

DES works by utilizing a similar key to scramble and decode a message, so both the sender and the recipient must know and utilize a similar private key. Once the go-to, symmetric-key calculation for the encryption of electronic information, DES has been superseded by the more secure Advanced Encryption Standard (AES) calculation.

The Data Encryption Standard is a piece figure, which means a cryptographic key and calculation are connected to a square of information at the same time as opposed to one piece at any given moment. To encode a plaintext message, DES bunches it into 64-bit pieces. Each square is enciphered utilizing the mystery enter into a 64-bit cipher text by method for stage and substitution. The procedure includes 16 adjusts and can keep running in four unique modes, scrambling pieces independently or making each figure square subject to all the past squares.

- Confidentiality, by eavesdropping on the communication.
- Integrity, by intercepting the communication and modifying messages.
- Availability, by intercepting and destroying messages or modifying messages to cause one of the parties to end communication

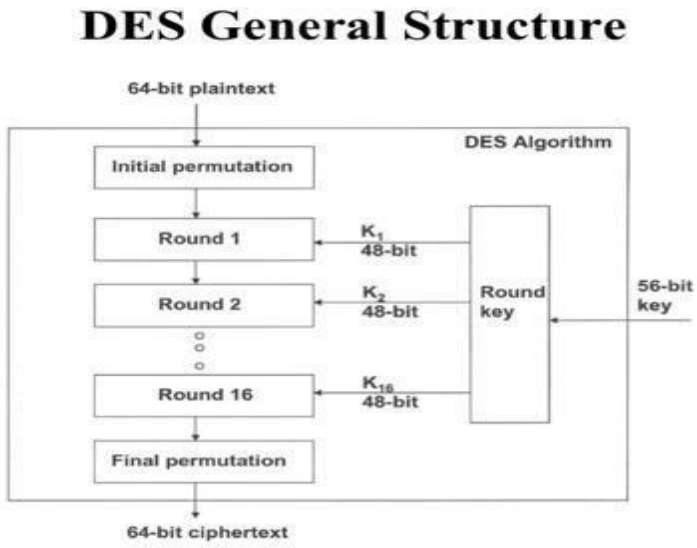

Fig.4: DES Structure

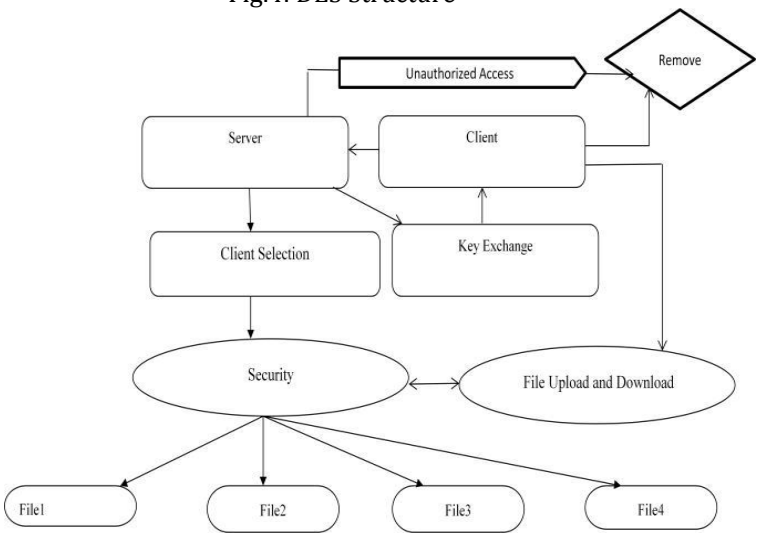

Fig.5: E-R Diagram

2. SAFE GUARDING FROM MAN IN THE MIDDLE ATTACK

MITM attack aims to compromise

2.1. User Interface Design

The important role for the Network user is to move login window to user window. This module has been created for the security purpose. In this login page we have to enter login user id and password. It will check username and password match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and sever authentication.

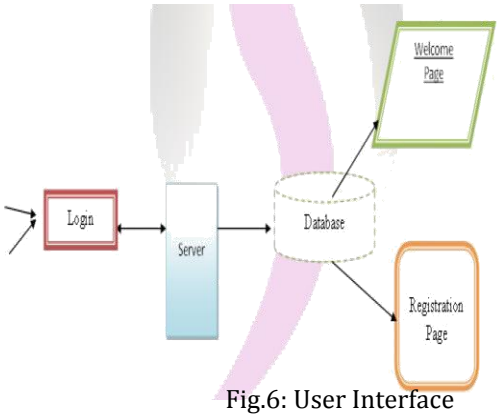

Fig.6: User Interface

2.2. Client Node 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. This is similar to the situation that once the
adversary compromises the long-term secret key, 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, our protocols provide forward secrecy: partially forward secure with respect to multiple sessions within a time period.

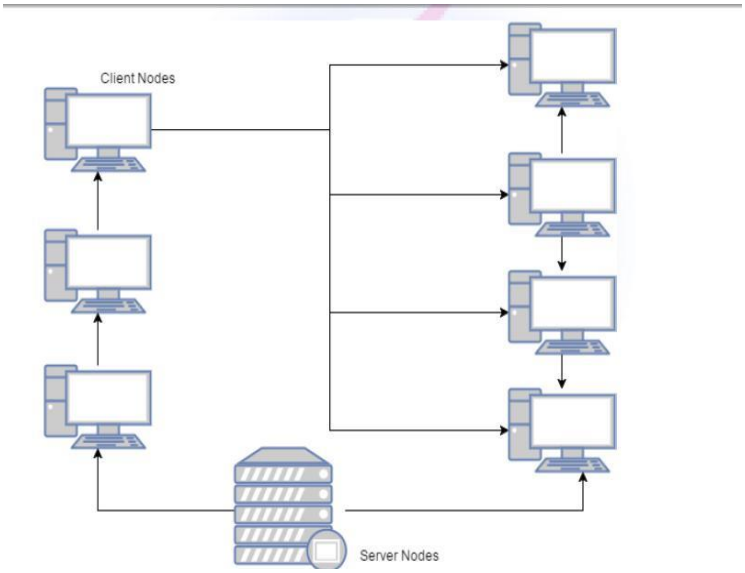

Fig.7: Client Node Selection

2.3. Random Key Generation

Our primary goal in this work is to design efficient and secure authenticated key exchange protocols that meet specific requirements of PNFS. The main results of this paper are the new secure authenticated key exchange protocols. We describe our design goals and give some intuition of a variety of PNFS authenticated key exchange6 (PNFS-AKE) protocols that we consider in this work.

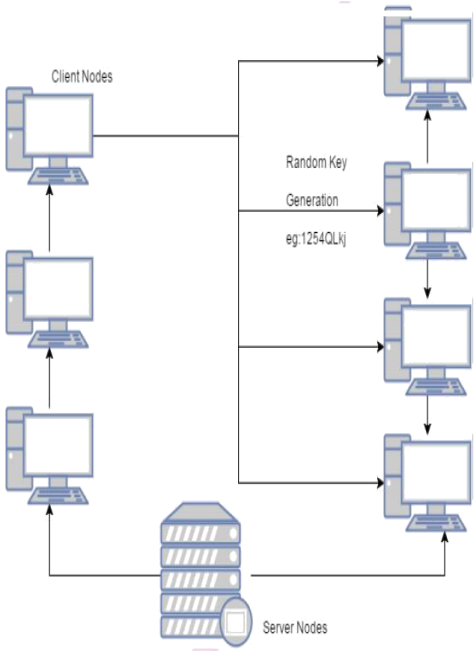

Fig.8: Random Key Generation

2.4. 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 escrow while achieving forward secrecy simultaneously, we incorporate a Diffie- Hellman key agreement technique into Kerberos-like PNFS-AKEI. However, note that we achieve only partial forward secrecy (with respect to v), by trading efficiency over security.

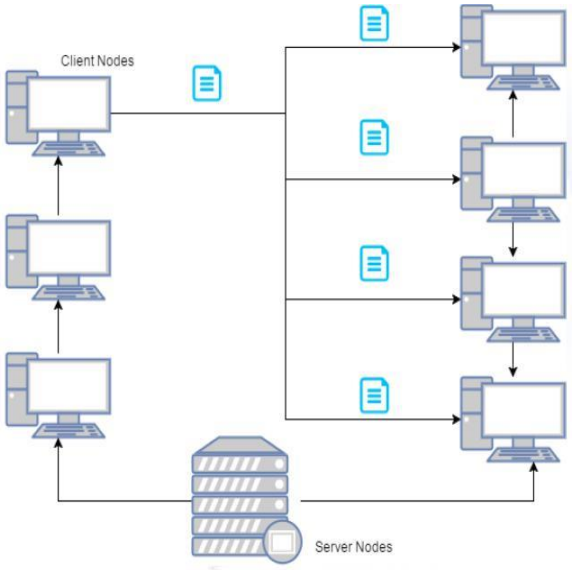

Fig.9: DES Encryption

2.5. 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 are blocked 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.

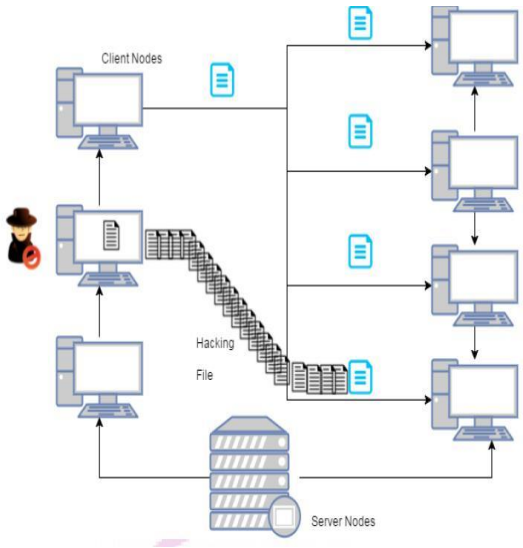

Fig.10: MITM Attack

2.6. MITM Defense Technique:

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. If the file uploaded by the user is not permitted from the Server means the file cannot be uploaded by the Client.

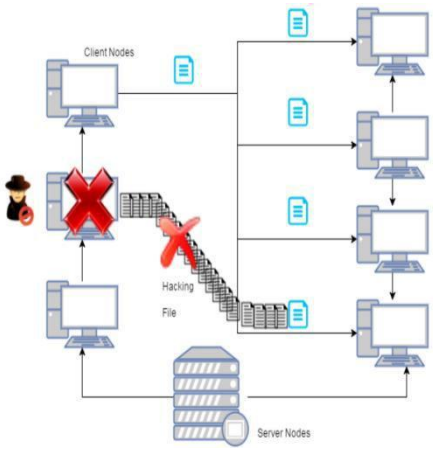

Fig.11: MITM Defense Technique

3. TECHNOLOGY USED

- MVC
- Jsp
- Servlet
- Java Script
- Interfaces
- Bean Classes
- JDBC

4. CONCLUSION

In this paper we have defended Man- In –The-Middle-Attacks by blocking the unauthorized user from the local file sharing network and not allowing the unauthorized user to enter into the network in future. We have analyzed MITM attack and presented a comprehensive classification of such attack based on DES techniques. Also, we provided MITM defense mechanism along with their descriptions.

5. FUTURE ENHANCEMENT

The security can still be improved by preventing other kinds of attacks such as spoofing attack, DOS attacks, Sniffer attacks, Data Modification Attacks, and so on.

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 *Proceedings of 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] A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer. FARSITE: Federated, available, and reliable storage for an incompletely trusted environment. In *Proceedings of the 5th Symposium on Operating System Design and Implementation (OSDI)*. USENIX Association, Dec 2002.

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

[5] 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.

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

[7] 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.

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

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