SECURITY FROM MAN-IN-THE-MIDDLE-ATTACK

Sonam Singh[1], Akshata Shinde[2], Pramita Kharat[3] , Aishwarya Vairalkar[4], Audumber Umbare[5]

[1]B.E. Computer Engineering, Dept. of Computer Engineering, Terna Engineering College, Maharashtra, India
[2]B.E. Computer Engineering, Dept. of Computer Engineering, Terna Engineering College, Maharashtra, India
[3]B.E. Computer Engineering, Dept. of Computer Engineering, Terna Engineering College, Maharashtra, India
[4] B.E. Computer Engineering, Dept. of Computer Engineering, Terna Engineering College, Maharashtra, India
[5]Professor, Dept. of Computer Engineering, Terna Engineering College, Maharashtra, India

***

Abstract – *Virtually everyone is now connected to each other via their computers with the wide use of the Internet. This has resulted in a positive impact on the social, economic and day-to-day transactions of the human environment. However, there is a major obstacle in trying to establish an effective and secure communication line: an external user, not intended to be part of the connection, may attempt to steal the information passed to a legitimate user. Therefore, information security plays a vital role in internet transactions as a security issue. A man - in - the - middle attack is a type of cyber-attack in which a malicious actor inserts him / herself into a two - party conversation, impersonates both parties and gains access to information that the two parties attempted to send to each other. A man - in - the - middle attack is a type of cyber-attack in which a malicious actor inserts him / herself into a two - party conversation, impersonates both parties and gains access to information that the two parties tried to send to each other. MITM targets the specific information flowing between endpoints and the info itself confidentiality and integrity. In this paper, by blocking the unauthorized user and preventing him from entering the network in the future, we overcome man in the middle attack in local file sharing systems. Both the attacker's IP address and path are completely blocked. The result is a reduction in the attacker and a secure transmission of the information. The server keeps track of the attacker's IP address and notifies the organization's other servers to block the IP address of the attacker.*

Key Words: **Man in the Middle Attack, Network Security, IP, Spoofing, HTTP, Advanced Diffie Hellman.**

1. INTRODUCTION

The name 'man-in - the-middle' comes from the basketball game where another player grabs the ball while two other players pass each other through the ball. A man-in - the-middle attack is a cyber-attack in which the attacker interferes in a two-party conversation, mirrors both sides and gains access to the information that both sides shared [2]. The attacker is capable of intercepting, sending and receiving information intended to be sent to someone else, or in the first place not to be sent. The attacker and his actions are not known to both the conversation parties. The term 'man-in - the-middle' is usually abbreviated as' MITM' and is therefore known as' MITM attacks' for the attacks coming under this category. The MITM attack is also better known by the following names:' Bucket-brigade attack,'' Fire brigade attack,'' Monkey-in – the middle attack,'' TCP hijacking,'' TCP session hijacking.'[3]

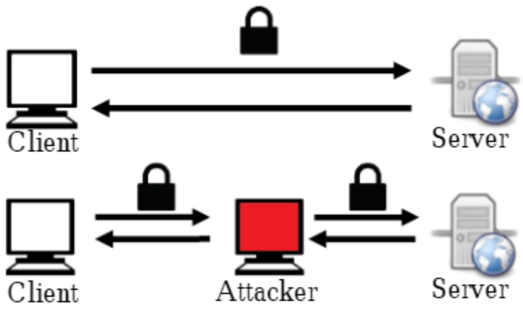

Fig 1. MITM Attack

1.1 THE ADVANCED DIFFIE HELLMAN ALGORITHM

To make the original Diffie Hellman algorithm more secure, the Advanced Diffie Hellman algorithm was proposed. Our main objective here is to use certain mathematical algorithms to calculate the secret number values chosen by the two organizations. This would ensure that the selected values of' a' and' b' are confidential; that is the secret number.

Our next objective would be to secure the data transmitted from one organization to another. In the original Diffie Hellman, Alice sends the value (gamodp) to Bob, but here we have cubed that value and then sent it to Bob. This would make it harder for man to attack in the middle. We are proposing the Advanced Diffie Hellman with this as the focus area. Fig.2 shows the algorithm of Advanced Diffie Hellman. [1]

ALICE	BOB
Calculate(p+a)	Calculate(p+b)
Multiply(p+a) with p.	Multiply (p+b) with p.
find mod of complex_1 i.e.((p+a)*p)%g	find mod of complex_2 i.e.((p+b)*p)%g
Put this value of the above in complex_1.	Put this value of the above in complex_2.
Calculate the square of (complex_1) ^2.	Calculate the square of (complex_2)^2
This value is again added to compex_1.	This value is again added to compex_2.
Calculate the square of (complex_1) ^2.	Calculate the square of (complex_2)^2
This value is again added to compex_1.	This value is again added to compex_2.
This new values is called new_complex_1	This new value is called new_complex_1
a1=g^(new_complex_1) mod p	b1=g^(new_complex_2) mod p
Take cube of a1	Take cube of b1
(a1^3) is sent to Bob.	(b1^3) is sent to Alice.

Table 1. Advanced Diffie Hellman Algorithm

2. SAFEGUARDING FROM MAN IN THE MIDDLE ATTACK

2.1 MITM ATTACK

The unauthorized users i.e. users who are not allowed to access other information in this module. The server blocks the user who misuses the network when the server receives a notification message that someone accesses in unauthorized access. Once the server has blocked the unauthorized user can never be undone. [4]

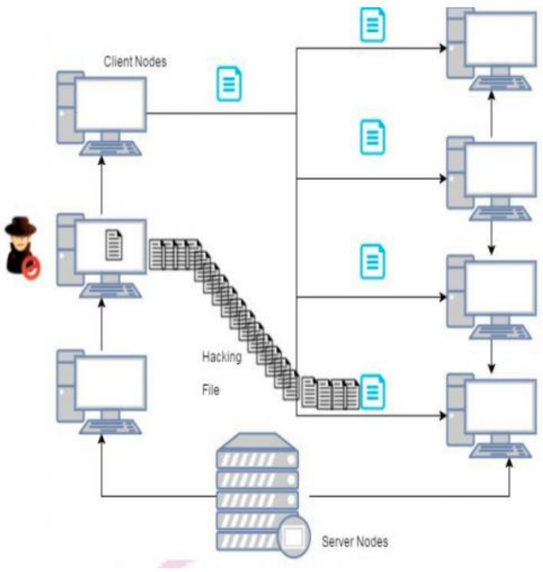

Fig 2. MITM Attack

2.2 MITM DEFENCE TECHNIQUE

The administrator can accept the new user request and block users as well. Users can upload the file to Network and the admin can allow Network to upload the files. If the file uploaded by the user from the server is not allowed, the client cannot upload the file.

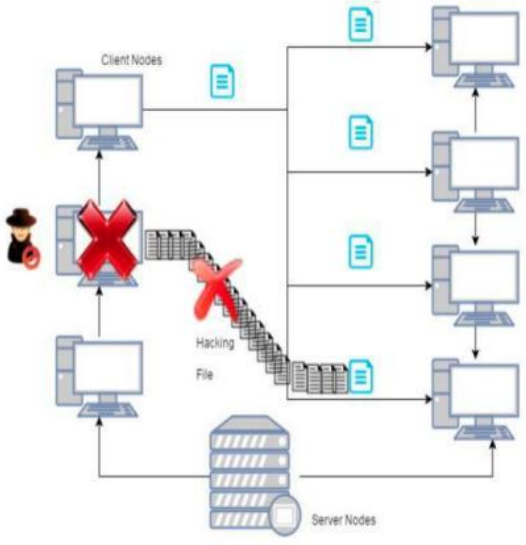

Fig 3. MITM Defence Technique

2.3 TYPES OF MITM ATTACKS

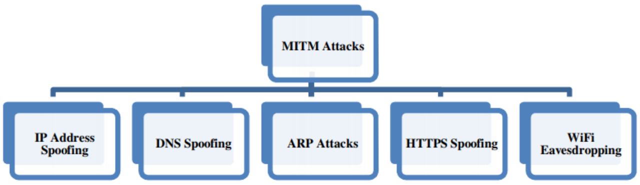

Fig 4. Systematic representation of the types of MITM Attacks

IP Address Spoofing-

a) Overview of IP address: The Internet Protocol (IP) is a method that provides a set of rules for sending or receiving data over the Internet that is present in the OSI model at layer 3. Information is transmitted as IP datagrams, also known as packets. The IP packets contain IP headers and transmitted data. The IP header contains the IP address of source and the IP address of destination.

b) Working of IP address: It's a unique 32-bit identification number. E.g.: 146.82.101.132. It has four parts, each consisting of eight binary digits. Known to be these parts are' octets.' This number is then converted by three dots into its decimal equivalent. IP addresses vary between 0.0.0.0 and 255.255.255.255.255. There are five classes of IP addresses, namely from A to E. The packets are transferred to their destination by routing process as the IP address contains the source address and the destination address. The routers will know exactly where the packets need to be transferred based on the IP address. It works with the Protocol for Transmission Control (TCP).

c) Attack mechanism of IP address spoofing: It is also called spoofing by the Internet Protocol (IP). The attacker will create an IP packet in this type of attack and send it from a forged source IP address so he / she can hide the sender's true identity. The attacker attempts to overload the legitimate user's network using two methods. The attacker sends numerous data packets from the forged or spoofed address in the first method. This makes the network of the target overload as it cannot handle so much data.

The attacker will spoof the victim's IP address in the second method and then send packets to other recipients. When these packets are received by the receivers, they respond by transmitting the packets to the IP address of the victim. The packets from many different recipients overload the network of the victim.

The hacker will change or modify the IP source address in this type of attack and will make it look like a legitimate source address and then start communicating. Hackers usually use this attack to crash the entire network of the victim by overloading massive amount of data into the network. They also use this attack to conceal the identity of the sender. [4]

3. CONCLUSION

The ' man - in - the - middle ' attack is very dangerous because it breaks the user's confidence because the user feels he / she communicates with the intended recipient over a secured network. For personal gain, the attacker may steal, modify and/or misuse private information. The proposed system therefore used the advance Diffie Hellman algorithm for key generation and encryption that improves data security. Thus, the purpose of this paper is to create a sense of awareness among the general public who are not well informed / educated about security threats / attacks like these and how they can easily fall prey unknowingly to such malicious attacks.

4. REFERENCES

[1] Advancement in Diffie-Hellman algorithm: Monalisa Jha Int. Journal of Engineering Research and Applications www.ijera.com

ISSN: 2248-9622, Vol. 5, Issue 7, (Part - 4) July 2015, pp.01-02.

[2] Defending Man In The Middle Attacks,Radhika.P1 , Ramya.G2 , Sadhana.K3 , Salini.R4, Assistant Professor,Dept of Computer Science and Engineering, Panimalar Engineering, College, Tamilnadu, IndiaVolume: 04 Issue: 3 | Mar -2017.

[3] Tulika Shubh Shweta Sharma M.Tech(CE) Assistant Professor IJCSMC, Vol. 5, Issue. 6, June 2016.

[4] An Overview of the Man-In-The-Middle Attack Sonia Rachel1 , Subhashkar S2 1(Department of Computer Science, St. Joseph's College (Autonomous), Bangalore) National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS)- Dec 2017.