ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Special Issue 5, March 2017

Hijacking Prevention Attack Based On DES Algorithm

Gowtham C R[1], Ishwarya.M[2], LakshmiPriya.G[3]
Assistant Professor, Karpaga Vinayaga College of Engineering and Technology, Madurantakam [1]
UG Student , Karpaga Vinayaga College of Engineering and Technology, Madurantakam [2,3]

Abstract - The Hacker-In-The-Middle (HITM) attack is widely used attacks in all over computer network security, HITM goal to achieve the actual data that flows between two points, and the confidentiality and integrity of the data itself. we extensively review the literature on HITM to identify and separate the scope of HITM attacks, considering both a model, such as the Open Systems Interconnection (OSI) model, as well as two systems are widely in used network technologies, i.e., GSM and UMTS. In particular, we classify HITM attacks based on several parameters, like find IP address of an attacker in the network. The hacker in the middle attack target the particular information send from one point to another before sending the message encrypt the message for confidentiality. The receiver decrypt the message using the same key. If hacker to hacking the encrypted message from sender they use the fake key for decryption. But using DES(Data Encryption Standard algorithm)disconnect the hacker when use fake key.

I. Introduction

Today, Internet or cellular networks are widely used in online home banking, online entertainment and shopping, social networks, and so on. These entire online services transfer user's sensitive information, which represents a key target for hackers. In this new world of "people and things always connected" by means of the Internet. It is very common and the successful attacks to connected things and online services. One of the most successful attacks is known as Hacker-In-The-Middle (HITM), which results in gaining control over end-users transferred data. HITM attacks are sometimes referred to as bucket brigade attack. The term HITM has become a reference attack in the security community. HITM attack as one of the major threats against network security. Such publications alongside with previously specified awareness clearly show that HITM attack has become very important and widespread, in principle being able to affect every online interaction. Today there is no publication which gives an extensive overview of the HITM attack for each Internet layer. Efforts have been done to describe the problem within one specific protocol, like HITM attacks on Address Resolution Protocol (ARP) Also, there are surveys which do not go sufficiently into details of each HITM attack, but provide a partial coverage of the attack's topology. In proposed classification of the HITM attack, which do not cover all known attacks. Also, researchers did not provide execution steps of attacks, but rather gave abstract description of them. In the HITM attack, the two endpoints(client) and a third client(attacker). The attacker interrupt on communication between two end points, and can manipulate their messages. In particular, client try to initialize secure communication but Attacker intercept between M1 and M2 . After that, client1 encrypts its message by the public key, and sends it to client2 .Attacker intercepts, and decrypts it using known private key. As a result, using DES algorithm the attack is detect from the attacker key.

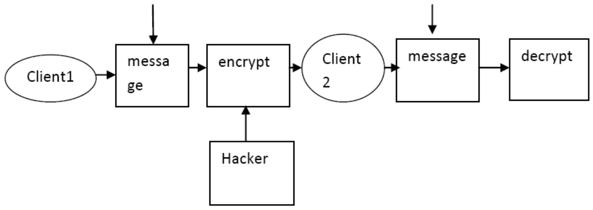

Figure 1: DES Algorithm flow

II. Related Works

A. *Spoofing based man in the middle attack*

Spoofing attack is an impersonation of a device or a user inthe network by a malicious party. Spoofing attack is used a an opening for other attacks, such as DoS, MITM, or sessionhi jacking attacks [18]. There are several types of spoofing attack that malicious parties can use: ARP spoofing, DNSspoofing, DHCP spoofing, IP spoofing. In all types of spoofing attackers use same protocols' weakness - a lack of source anddestination messages authentication.

B. *ARP spoofing defence mechanisms*

The schemes for detecting and preventing ARP spoofing attacks, and specified requirements for an ideal solution. Most of schemes may be classified from two perspectives:wayof implementation (cryptographic, voting-based, hardware),and location of solution (server-based, and host-based).

C. *Detection of ARP spoofing*

Proposed an architecture based on switched networks, which does not require special software to be installed on the network hosts.

D. *Cryptographic solutions*

S-ARP is a backward compatible extension to ARP that relies on public-key cryptography to authenticate ARP Replies. All hosts create public and private key pairs during the initial contact with the network, and send them with signed certificates to the Authoritative Key Distributor (AKD).

E. *Issues in existing system*

Man in middle is an attack in which the attacker intercepts a legitimate communication between two hosts by means of spoofing attack. Control of transfer data while host are not aware of a middle man existence. Man in the middle attack uses the key management server. Man in the middle attack does not support host that have static IP address.

III. PROPOSED SYSTEM

We use DES(Data Encryption Standard)is a common standard for encryption and form of secret key cryptography.It provides high level of security. DES algorithm is used to disconnect the hacker when use the fake key so only we reduce the hacker. Attackers cannot impersonate like authorized user. Based on our analysis, a categorization of HITM prevention mechanisms and we identify some possible directions. IP hijacking detection algorithm for detect using DES algorithm. Finds invalid AS path contained in BGP Update messages that do not exist in AS topology of the Internet .The client has to login page we have to enter login user id and password. It will check username and password is match or not. 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. Then send message from one place to another .client1isusing key to encrypt the message for confidentiality. Then client2 received the message using same key for decrypt the message .is 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.

A. *Functional Architecture*

Functional architecture is an architectural model that identifies the functions and describes the operations: The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys, i.e., one for encryption and one for decryption.

The proposed technique consists of following modules:
1User Interface Design
2:Client Node Selection
3:Random Key Generation
4:DES Encryption
5:HITM Attack
6:HITM Defense Technique

B. *System Design*

The admin can accept the new user request and also black 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.

C. *User Interface Design*

This is the first module of our project. The important role for the Network user is to move login window to server user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is 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.

D. *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. 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, two our protocols provide forward secrecy: one is partially forward secure with respect to multiple sessions within a time period.

E. 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 three new provably 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.

F. 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-AKE-I. However, note that we achieve only partial forward secrecy (with respect to v), by trading efficiency over security.

G. HITM 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.

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

IV. CONCLUSION AND FUTURE ENHANCEMENT

we have analyzed HITM attack and presented a comprehensive classification of such attack based on impersonation techniques. Also, we provided various HITM defense mechanisms along with their descriptions. In Table VIII, web together all HITM prevention mechanisms, according to used approaches and context (abstract layer) of applicability. To sum it up, we can collect the most effective methods in the following list. 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 Authentication using Password authenticated key exchange using distributed server is done where a cryptographic key - exchange of messages. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised.

REFERENCES

[1] G. NathNayak and S. G. Samaddar, “Different flavours of manin-the-middle attack, consequences and feasible solutions,” in 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 5. IEEE, 2010, pp. 491–495.

[2] S. M. Bellovin and M. Merritt, “Encrypted key exchange: Password based protocols secure against dictionary attacks,” in IEEE Computer Society Symposium on Research in Security and Privacy. IEEE, 1992, pp. 72–84.

[3] R. Demillo and M. Merritt, “Protocols for data security,” Computer, vol. 2, no. 16, pp. 39–51, 1983.

[4] W. Baker, A. Hutton, C. D. Hylender, J. Pamula, D. Ph, M. Spitler, M. Goudie, C. Novak, M. Rosen, P. Tippett, C. Chang, and J. Fisher, “Data breach investigations report,” Methodology, vol. Band 36, pp. 1–63, 2011. [Online]. Available: http://www.secretservice.gov/Verizon Data Breach 2011.pdf

[5] CAPEC. (2014) Capec-94: Man in the middle attack. [Online]. Available: http://capec.mitre.org/data/definitions/94.html

[6] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, “Establishing wireless robust security networks: a guide to IEEE 802.11i,” National Institute of Standards and Technology, 2007.

[7] R. Wagner, “Address resolution protocol spoofing and man-in-the middle attacks,” The SANS Institute, 2001.