International Journal of Computer Applications Technology and Research
Volume 5– Issue 5, 249 - 252, 2016, ISSN:- 2319–8656

Avoiding Man in the Middle Attack Based on ARP Spoofing in the LAN

Peta Kaleemsha
Sree Vidyanikethan Engineering College
Tirupathi, India

Pulluru Likhitha
Sree Vidyanikethan Engineering College
Tirupathi, India

Abstract: As technology is running on its wheels, networking has turned into one of our basic aspects. In this world along with networking inimical vulnerabilities are also advancing in a drastic manner, resulting in perilous security threats. This calls for the great need of network security. ARP spoofing is one of the most common MITM attacks in the LAN. This attack can show critical implications for internet users especially in stealing sensitive information's such as passwords. Beyond this it can facilitate other attacks like denial of service(DOS), session hijacking etc..,. In this paper we are proposing a new method by encrypting MAC address to shield from ARP cache poisoning.

Keywords: ARP (Address Resolution Protocol), MAC (Media access control), IP (Internet protocol), MITM, Session Hijacking, DoS, cryptography.

1. INTRODUCTION

Protecting our online data is never going to be a cake walk, especially now-a-days where attackers are regularly contriving some new techniques to sneak data. MITM attack is a serious threat to the internet users and it is far-reaching to detect as the third person, an attacker secretly places himself between two victims and he is capable of attempting any passive or active attacks. There are many techniques available today to evade MITM attack some of them are monitoring ARP traffic, making ARP cache static and highly secured data encryption. But secured data encryption cannot create a path free of ARP spoofing and it is time taking too. Instead of encrypting data we are proposing a new way of secure communication by encrypting MAC address using cryptography.

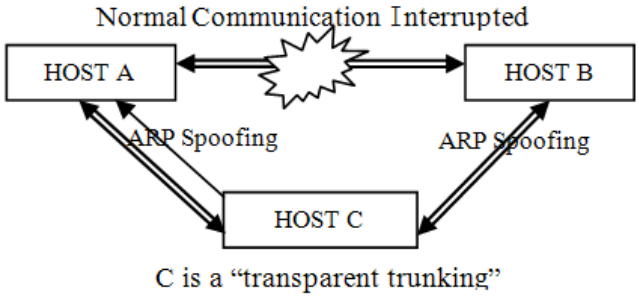
2. BASICS

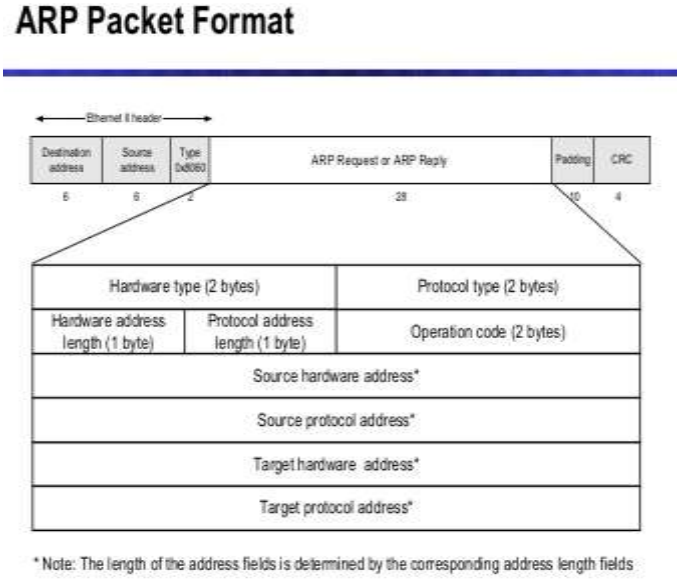
2.1 ARP communication

ARP protocol operates by broadcasting messages across a network to determine layer two MAC address of the host using predetermined IP address. Then the host with destined IP address replies back his MAC address. Thus ARP messages provide a link between IP and MAC addresses. ARP will work across a bridge. Bridges will propagate the ARP broadcasts and bridge the replies. A router will block ARP packets. This means an ARP monitor is required on each separate network segment to detect new ethernet addresses. Network switches will pass the ARP traffic because it is broadcast traffic. This means that any computer on the network can see the ARP broadcast traffic. The reply packets are usually returned directly to the requesting computer, and network switches will block this unless it is addressed to your station[1] [2].

2.2 ARP cache poisoning

It is one of the oldest forms of MITM attacks where attacker on the same subnet can eavesdrop on network traffic between the victims. It takes the advantage of insecurity indulged in ARP protocol. The malicious attacker sends a falsified ARP message and links his MAC with attacker IP address, then the attacker takes the role of "MITM", any traffic intended for that right source is send through attacker system. As it occurs at lower level the end user is oblivious to its occurrence[1]. Let A, B are two legitimate hosts communicating with each other and C be an attacker who tries to steal the information acting in between them as shown in below figure.





2.3 Denial of Service (DoS):

DoS refers to an attack that overwhelms system with data-most commonly a flood of simultaneous requests send to a website, causing the server to crash or simply becomes inoperable as it struggles in responding to more requests than it can handle. As a result, legitimate users who try to access the websites control by server are unable to get the service. There are other types of DoS attacks that use different tactics, but they all have the same effect: preventing legitimate users from accessing the site[1][4].

2.4 Session hijacking

Session hijacking attacks consists of the exploitation of web sessions controlling mechanism, which is normally managed for a session token. As http communication uses many TCP connections the web server needs a method to recognize every user's connection. The most useful method depends on the token that the web server sends to the client browser after a successful client authentication. A session token normally consists of string of variable width and it can be in different ways like in the URL. The session hijacking attack compromises the session token by stealing or predicting a valid token to gain unauthorized access to the web server[1][4].

2.5 Cryptography

Cryptography is a method of information hiding and verification to provide security from unauthorized access. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enables verifiability of every component in a communication. It is the powerful techniques available today to go against information attackers. The two techniques of cryptography are substitution and transposition[3].

2.6 Substitution

Substitution is a method of encoding by which units of plain text will be replaced with cypher text using some fixed key, the units may be single letters, pair of letters, triplets of letters or mixture of above. As the origin letters in the text are replaced. It cannot be deciphered without knowing pre used key[3][5].

Eg: Plain text: *NETWORKING*

KEY:**2**

ENCRYPTED OUTPUT: *PGVYQTMKPI*

2.7 Transposition

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plain text are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a bijective function is used on the character's positions to encrypt and an inverse function to decrypt it[3][5].

Eg: Plain text: *NETWORKSECURITY*

KEY: *HACK*

H	A	C	K
3	1	2	4
N	E	T	W
O	R	K	S
E	C	U	R
I	T	Y	

ENCRYPTED OUTPUT: *ERCTTKUYNOEIWSR*

3. PREVIOUS WORKS

3.1 Making ARP cache static

One way to protect against ARP poisoning is to change the unsecured dynamic nature of ARP cache into a static thing. It helps only when your network configuration doesn't change often and when it is pretty simple to make a list of static ARP entries. This will ensure that device will always rely on their local ARP cache rather on ARP requests and replies[2].

3.2 Monitoring ARP traffic

This involves monitoring the network traffic of host by a third party using some intruder detection software's such as **Snort** but it is feasible when only single host is considered and it can be a bit cumbersome when entire network is concerned[2].

3.3 Virtual Private Networking

A VPN is a technology which creates an encrypted connection over a less secure network. It protects your internet and lets you browse with privacy. It extends a private network across a public network. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network The benefit of using a VPN is that it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols or traffic encryptions, such as PPTP (Point-to-point Tunneling Protocol) or Internet Protocol Security (IPSec). The most common types of VPNs are remote access VPNs and site-to-site VPNs. Using a VPN will shut down many of the places where a MITM attack might happen, but not all of them. Specifically, it will protect your traffic between your device and the VPN gateway, preventing your ISP (or most governments) from performing a MITM attack targeted toward you. However, once your traffic passes from

the VPN gateway to its eventual destination, it becomes vulnerable to a MITM attack. With a VPN, your traffic is then semi-anonymized, so it is much more difficult to target any attack toward any particular person, but an indiscriminate attack against all users of a particular website is still very possible. And it is also too expensive to setup[4][5].

3.4 Secure Shell Tunnelling

SSH tunnel transfers unencrypted traffic over an encrypted channel created using SSH protocol connection. Generally, SSH is used to securely acquire and use a remote terminal session. For setting up a tunnel the port of one machine needs to be forwarded to a port in the other machine which is at other end of the tunnel. This uses different kinds of port forwarding mechanisms namely Local port forwarding, Remote port forwarding, Dynamic port forwarding. SSH tunnel is often called as "Poor Man's VPN" as it provides some of the same features as a VPN without more complicated server setup process however an SSH tunnel doesn't offer all the benefits of a VPN. Unlike with a VPN, you must configure each application to use SSH tunnel's proxy. With a VPN we are assured that all traffic will be sent through it - but you do not have this assurance with an SSH tunnel. And it also doesn't offers high security as data is in unencrypted form[4][5].

4. PROPOSED IDEA

In our method we are trying to eliminate MITM attack especially ARP poisoning by using switch as a third party to encrypt the mac address of the host.so that the attacker cannot interfere. The technique used for this method is as follows:

Algorithm:

let Ceaser(C), Harrison(H) are two hosts and Shlomo(S) as a third party switch. consider a scenario where Ceaser wants to communicate with Harrison.

step 1: Ceaser sends to Shlomo his mac address attached with some key k1 and IP address of Harrison, the destination.

step 2: Shlomo broadcasts the destination IP address and waits for the reply.

step 3: Then Harrison replies with his MAC address along with his key k2.

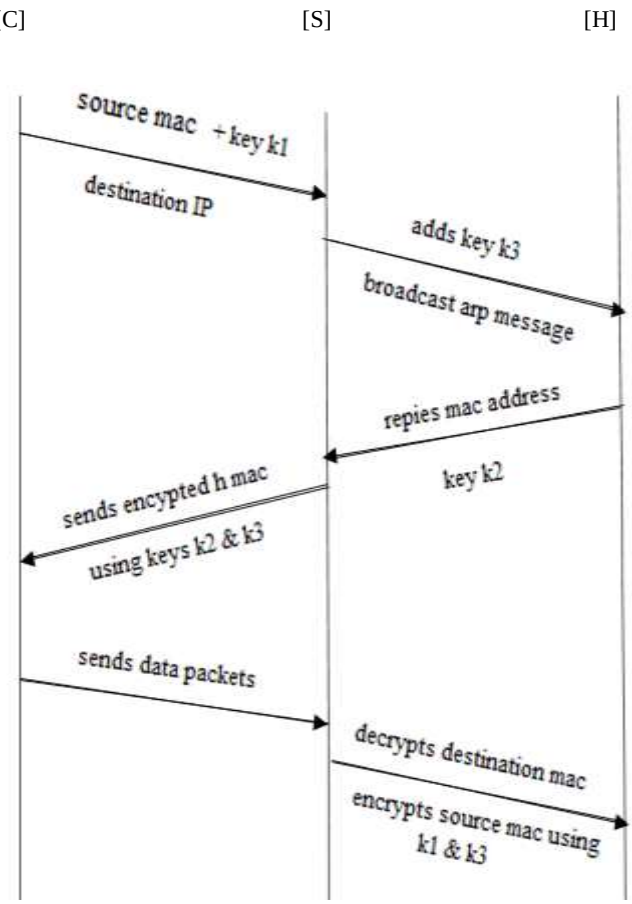
step 4: Instead of giving actual MAC address of Harrison, Shlomo encrypts it by using transposition technique with key k2 taken from him. Shlomo also adds substitution security by using his own static key k3.

step 5: Shlomo uses the same technique and encrypts the mac address of Ceaser by using transposition with key k1 and also adds substitution security with his private key k3 and gives it to Harrison.

step 6: Now the connection was established between Ceaser and Harrison without knowing their actual MAC addresses.

step 7: For replying back Shlomo decrypts the MAC addresses and goes to the right person.

step 8: For further security, amelioration we can use randomness in keys provided by hosts for different connection establishments.



5. CONCLUSION

In our technique only third party, switch knows the actual MAC addresses of the hosts in the subnet. As we are using two keys one from the host and the other from the switch, security hardens and any attacker who wants to sniff the target system's MAC address can see only the encrypted MAC. Thus there will be a great chance to get rid of ARP spoofing with our method.

6. REFERENCES

[1] Sean Whales, "*An Introduction to ARP Spoofing [EB/OL]*",http://packetstormsecurity.org/papers/protocols/, 2001.

[2] Guo Hao and Guo Tao, "*Principle of and Protection of Man-in-the-middle Attack Based on ARP Spoofing*", Journal of Information Processing Systems, Vol.5, No.3, September 2009.

[3] Whitfield Diffie and Martin Hellman, "*Multi-user cryptographic techniques*", [Diffie and Hellman, AFIPS Proceedings 45, pp109-112, June 8, 1976].

[4] Behour A. Forouzan, Sophia Chung Fegan ―" *Data Communication and Networking*", Fourth Edition 2009.

[5] William Stallings,"Cryptography *and Network Security",* Fourth Edition 2006.