International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 12
ISSN: 2454-4248
126 – 130

Computer Network Routing Challenges Associated to Tackle Resolution Protocol

Manju Bala
IP College for Women,
Department of Computer Science
manjugpm@gmail.com

Charvi Vats
Dept. Of Comp. SC.,
IP College for Women,
New Delhi, India
4vivats@gmail.Com

Devanshi Mathur
Dept. Of Comp. Sc.
Ip College For Women,
New Delhi, India
mathur.devanshi2810@gmail.com

Divyanshi Agarwal
Dept. Of Comp Sc.,
Ip College For Women,
New Delhi, India
divyanshi.agrl@gmail.com

Abstract: *Computer* networks are very important in today's scenario. They have changed the way we do business and the way we live. There are several protocols that help us to establish these networks. The most widely used network protocol is ARP (Address Resolution Protocol) which is used to find the physical address of the node when its internet address is known. In this paper we have discussed the weaknesses of this protocol and have proposed various methods of active detection and prevention of ARP poisoning(spoofing) based Man-in- the-Middle(MitM) attacks on switched Ethernet LAN's, Denial-of-service (DoS), session hijacking etc. We have implemented tools and defense mechanisms such as central server on a network or subnets, encryption of data traffic etc. that help us to reduce these spoofing attacks.

Keywords: *ARP, ARP Spoofing, Man-in-the-Middle, Central Server, Mac Address, IP Address.*

*****

I. INTRODUCTION

Internet protocol addresses are assigned to hosts and logically are not dependent on their physical address. The network-layer software must depend on the data link layer to deliver data to a host on the same physical network. Therefore, the IP address must be mapped to the physical (MAC) address of the host. Address Resolution Protocol is a network layer protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address which is stored in ARP cache of each client mac address which is stored in ARP cache of each client machine.

[4]ARP is a stateless protocol (responses are given without sending ARP requests) without security features. Thus, it is prone to DoS and MitM attacks on a LAN.

ARP WORKING:-

[5][6]A node uses ARP with another node when it determines that the destination address is on a directly attached network. The node can determine if the host is local by comparing the network portion (including the subnet) of its own address with the destination address.

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

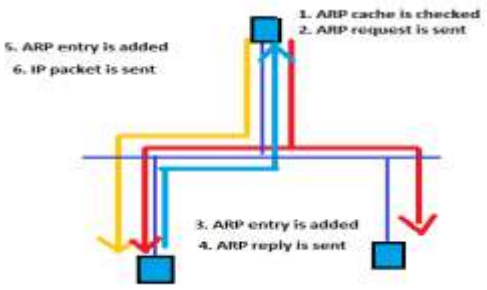

FIG 1.1 ARP WORKING

 ISSN: 2454-4248
126 – 130

II. LITERATURE REVIEW

ARP Spoofing attack is a well-known attack. Some of the existing defenses and solutions exist in literature. **[3]**In the combined works of A. Ornaghi, D. Bruschi and E. Rosti, they have assumed that each host has a public/private key pair which acts as a Certification Authority. Messages are digitally signed by the sender, thus preventing the injection of spoofed information.

[1]M.G. Gouda and C.T. Huang have assumed that there is a database deployed in the LAN which can be used to resolve the MAC address. This approach is not appropriate for dynamic networks.

[2]B. Issac proposed a unicast ARP request, with the help of a DHCP. In their approach, they assume that the DHCP will resolve the IP/MAC translation without the need for Broadcast. But this is not suitable technique for static IP addressing.

[1]S. Venkatramulu and C.V. Rao, proposed solutions to solve ARP spoof problem and grouped them into cryptographic approaches, kernel-based patch, ARP spoof detection & protection software, etc.

III. BACKGROUND

ARP Spoofing:

[2]A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this.

The basic principle behind ARP spoofing is to exploit the lack of authentication in the ARP protocol by sending spoofed ARP messages onto the LAN. ARP spoofing attacks can be run from a compromised host on the LAN, or from an attacker's machine that is connected directly to the target LAN. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Because ARP Poisoning (spoofing) attacks occur on such a low level, users targeted by ARP Poisoning rarely realize that their traffic is being inspected or modified. ARP spoofing based attacks include:

A. Session Hijacking

[5][6]Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session (sometimes also called a session key) to gain unauthorized access to information or services in a computer system.

The session refers to certain time period that communication of two computer systems or two parts of a single system takes place. When one logins to a password protected system, the session is used. The session will be valid up to the end of the communication. In the http communication, the server needs a method to recognize every user's connections. The most used method is the authentication process and then the server sends a token to the client browser. This token is composed of a set of variable width and it could be used in different ways, like in the URL, in the header of http requisition as a cookie, in other part of the header of the http request or in the body of the http requisition. The attack takes advantage of the active sessions. This compromising of session token can occur in different ways such as session sniffing and cross-site script attack.

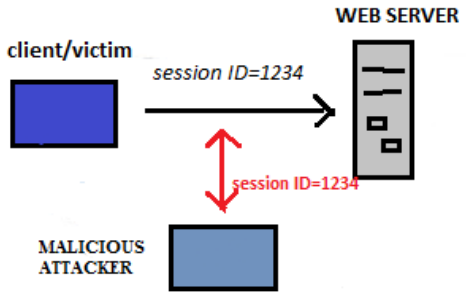

FIGURE 3.1 SESSION HIJACKING ATTACK

B. Denial of Service (DoS)

[6]A denial-of-service attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer. Denial-of-service (DoS) attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them. While an attack that crashes a server can often be dealt with successfully by simply rebooting the system, flooding attacks can be more difficult to recover from. The following may indicate such an attack:

1. Degradation in network performance, especially when attempting to open files stored on the network or accessing websites.
2. Inability to reach a particular website.
3. Difficulty in accessing any website.
4. Increased volume of spam emails than usual.

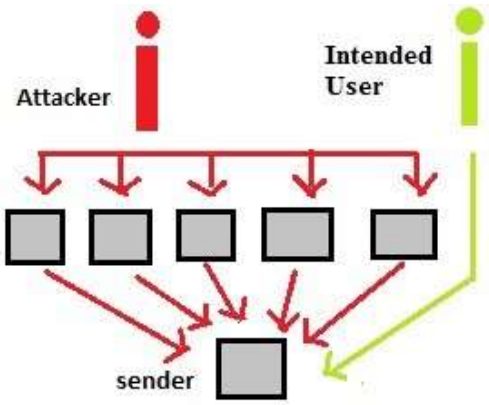

FIGURE 3.2 DENIAL OF SERVICE ATTACK

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or

 ISSN: 2454-4248
126 – 130

weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

C. Man-in-the-Middle (MitM)

[1][6]A MitM attack happens when a communication between two systems is intercepted by an outside entity. This can happen in any form of online communication, such as email, social media, web surfing, etc. **[3]**Not only are they trying to eavesdrop on your private conversations, they can also target all the information inside your devices. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Additionally, it can be used to gain a foothold inside a secured perimeter during the infiltration stage of an advanced persistent threat (APT) assault. It is a kind of session hijacking attack.

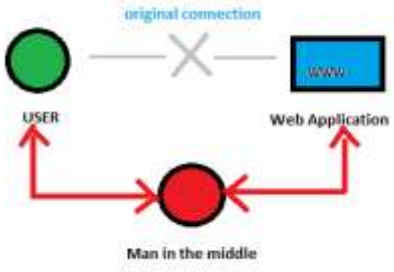

FIGURE 3.3 MAN IN THE MIDDLE ATTACK

MitM attacks are relatively uncommon in the wired Internet, since there are very few places where an attacker can insert itself between two communicating terminals and remain undetected. For wireless links, however, the situation is quite different. Unless proper security is maintained on wireless last hop links, it can be fairly easy for an attacker to insert itself, depending on the nature of the wireless link layer protocol. Man-in-the-middle attacks can be active or passive. In a passive attack, the attacker captures the data that is being transmitted, records it, and then sends it on to the original recipient without his presence being detected. In an active attack, the contents are intercepted and altered before they are sent on to the recipient.

D. MAC Flooding

[9]MAC address flooding attack is a network attack, in which the switch interface gets flooded by the Ethernet frames with different fake source MAC address sent. Flooding is done by the attacker connected to the switch port. When the switch's MAC address table is full i.e. it cannot save more addresses, then it enters into its fail-open mode and behaves like a network "hub", as a result of which, frames are flooded to all ports. **[7]**MAC table is maintained by the switches that composed of individual MAC addresses of the host computers on the network which are connected to ports of the switch. With the help of this table, switches can direct the data out of the ports where the recipient is located. Also by the use of MAC table switches can send data to the specific machines which the data is intended to be sent. The aim is to take down this MAC table and the attack is also known as MAC table flooding attack. The switch, in its "hub" mode, is too busy in enforcing port security features and just broadcasts all network traffic and all incoming packets to every computer in the network or ports, instead of just down the correct port. All the frames between the victim and another machines are delivered to the attacker's machine who could then use a packet sniffer (such as Wireshark) running in promiscuous mode to capture sensitive data from the network (such as unencrypted passwords, e-mail and instant messaging conversations).

FIGURE 3.4.1 BEFORE MAC FLOODING

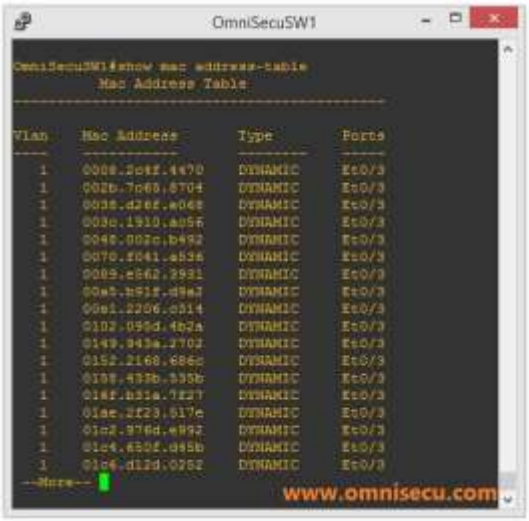

FIGURE 3.4.2 AFTER MAC FLOODING

IV. PROPOSED SOLUTIONS

We have proposed the following solutions for detection, prevention and protection:

 ISSN: 2454-4248
126 – 130

A. Packet Filtering

[3]It is one of the techniques to implement security firewall. In this filtering process we pass or block packets at a network interface that is based on source and destination addresses, ports and protocols. It is done with the help of a program called packet filter. The process is used in conjunction with packet mangling and Network Address Translation.

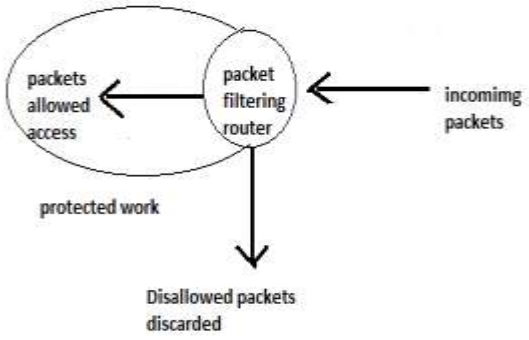

FIGURE 4.1 PACKET FILTERING

Three ways in which a packet filter can be configured are:

- The filter accepts only those packets that it is certain are safe, dropping all others. This is the most secure mode, but it can cause inconvenience if legitimate packets are inadvertently dropped.
- The filter drops only the packets that it is certain are unsafe, accepting all others. This mode is the least secure, but is causes less inconvenience, particularly in casual Web browsing.
- If the filter encounters a packet for which its rules do not provide instructions, that packet can be quarantined, or the user can be specifically queried concerning what should be done with it. This can be inconvenient if it causes numerous dialog boxes to appear, for example, during Web browsing.

B. Cryptographic Network Protocols

[1]In this technique we propose secure address resolution protocol(S-ARP). S-ARP is an extension to ARP protocol which provides authentication for ARP reply messages through public key cryptography. Secret keys are distributed to clients in the network by the server. The client should send an acknowledgement along with the address pair (IP/Mac) on receiving an invite message. The address pair is stored in a local database. Then the server resolves the Mac address by sending a reply message. Every node in the LAN using ARP is changed to use S-ARP. S-ARP's reply message is similar to that of ARP except that it is authenticated by the sender's signature (obtained from authoritative key distributer (AKD)) appended to it.

FIGURE 4.2 ENCRYPTION

The main drawback of this technique is that the prevention of MitM is not possible and dynamic assignment of IP address is not supported. There is also a problem of network congestion due to overhead. Some other secure communication protocols are transport layer security (TLS), secure shell (SSH), http secure (HTTPS).

C. Centralized Server on a Dynamic Network

[2]In this technique we prevent ARP spoofing that consists of nodes and a new entity called central server .An IP/Mac table is maintained by the central server for the subnet. The information of all nodes (have their IP addresses allocated by the nearest DHCP server) on the subnet and IP Mac binding information is present in IP Mac table. The central server is also informed (through IP-send message) by the DHCP server about the allocation of an IP address to the host on the subnet. The secret key (shared between DHCP and central server) signs this message received by the data link layer. The central server acknowledges the IP-send message by sending an IP-reply message to the DHCP server. In a network, central server receives all the ARP request and ARP reply messages. ARP request and ARP reply messages will not be communicated to the hosts or the client.

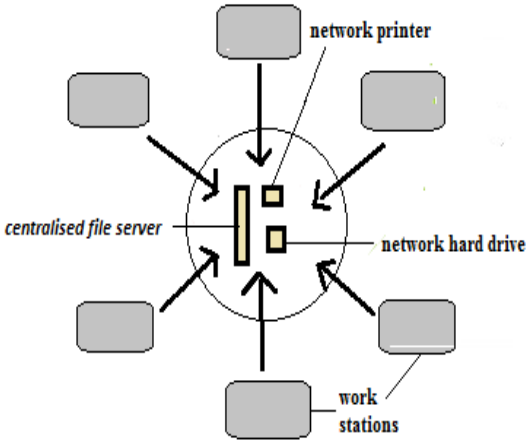

FIGURE 4.3 CENTRAL SERVER

D. Preventive measures for MAC flooding: Some of the methods to prevent MAC flooding are:

- **Port security:** In this method, limited number of MAC addresses are allowed on the port based on

 ISSN: 2454-4248
126 – 130

the organization requirements. When secure MAC address is assigned to a secure port, ingress traffic having source address is not forwarded outside the group of defined addresses. If a single secure MAC address is assigned, the device attached to that port has the full bandwidth of the port. **[7]**Also a small table of 'secure' MAC addresses is maintained with the traditional MAC address table. This table also acts as a subset of the MAC address table.

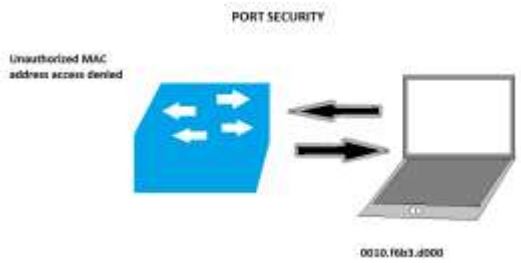

FIGURE 4.4.1 PORT SECURITY

- **Authentication with AAA server: [7][8]**Authentication, authorization, and accounting is a framework that controls access to computer resources, enforce policies, audits usage, and provides the information necessary to bill for services. In this method, the discovered MAC addresses are authenticated against an authentication, authorization and accounting server (AAA server) and are subsequently filtered. These combined processes are considered important for effective network management and security. Remote Authentication Dial-In User Service (RADIUS) is the current standard by which network access server interface with the AAA server.

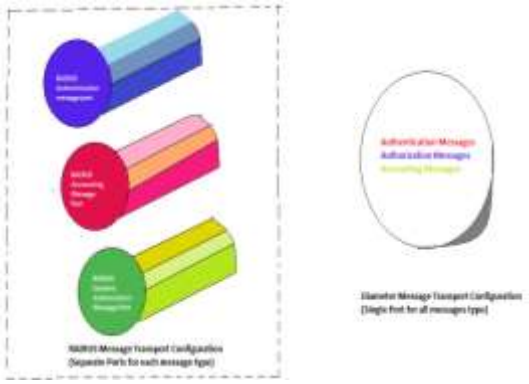

FIGURE 4.4.2 IMS AAA SERVER

- **Security measures to prevent IP Spoofing: [7]**In some cases, security features that are meant to prevent IP Address Spoofing may also perform additional MAC address filtering on unicast packets. However this is an implementation-dependent side effect.
- **Implement IEEE 802.1X suites: [7]**Implementing IEEE 802.1X suites will allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address.

V. CONCLUSION AND FUTURE SCOPE

Throughout the presentation, we talked about Address Resolution Protocol and the improvements that can be made in future to improve the routing capabilities. Every technique discussed in the presentation has its own designs, advantages and limitations. We need to consider every aspect of a particular technique to make it successful. Different techniques could be further developed and discovered. By using packet filtering, we can inspect packets as they are transmitted across a network, thereby blocking packets with conflicting source address information. Encryption of data traffic helps in secure transmission from sender's side and authentication at receiver's side. Centralized server in LAN helps to prevent server conflict at the source by asking for authentication of public and private keys provided by that particular server. After discussing all the aspects of Address Resolution Protocol we conclude that there can be many ways for improving routing issues.

In future further improvement of routing performance will be suggested by considering several methods that can prevent ARP Spoofing to a greater extent in future.

REFERENCES

[1] S. Venkatramulu, Dr. C.V Guru Rao, "Various Solutions for Address Resolution Protocol Spoofing Attacks", International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.

[2] Abhishek Samvedi, Sparsh Owlak, Dr. Vijay Kumar Chaurasia, "Improved Secure Address Resolution Protocol", 2014, arXiv.org

[3] Ghazi Al Sukkar, Ramzi Saifan, Sufian Khwaldeh, Mahmoud Maqableh, Iyad Jafar, "Address Resolution Protocol(ARP): Spoofing Attack and Proposed Defense", Communication and Network, 2016, 8, 118-130, Published Online August 2016 in SciRes, http://www.scirp.org/journal/cn, http://dx.doi.org/10.4236/cn.2016.83012

[4] K. Kalajdzic and A. Patel, "Active Detection and Prevention of Sophisticated ARP-Poisioning Man-in-the-Middle Attacks on Switched Ethernet LANs", Proceedings of Sixth International Workshop on Digital Forensics & Incident Analysis (WDFIA 2011).

[5] www.wikipedia.org

[6] www.weopedia.com

[7] www.interserver.net

[8] www.searchsecurity.techtarget.com

[9] www.omnisecu.com