Detection and Prevention of ARP Spoofing using Centralized Server

D. Srinath
Associate professor
Department of Computer science and Engineering,
Panimalar Institute of Technology, India

S. Panimalar
Assistant professor
Department of Computer science and Engineering,
Panimalar Institute of Technology, India

A. Jerrin Simla
Assistant professor
Department of Computer science and Engineering,
Panimalar Institute of Technology, India

J. Deepa
Assistant professor
Department of Computer science and Engineering,
Panimalar Institute of Technology, India

ABSTRACT

The Address Resolution Protocol (ARP) due to its statelessness and lack of an authentication mechanism for verifying the identity of the sender has a long history of being prone to spoofing attacks. ARP spoofing is sometimes the starting point for more sophisticated LAN attacks like denial of service, man in the middle and session hijacking. In a current voting based method an active technique is used for finding out the legitimate one by collection of voting's from the neighboring host. The drawback of this system is most of the host in a LAN must follow the MR-ARP protocol. In this paper a centralized server will collects all the ip-mac pairs of every host in the LAN and maintains a table of legitimate host. Destination host checks the ip-mac conflict in the LAN and informs about the hacker to the centralized server which takes care of the trusted communication between the participating hosts. Hence, the proposed work detection and prevention of ARP spoofing lead to appreciable result.

Keywords

ARP protocol, MAC address, IP address, router, spoofing

1. INTRODUCTION

As we already know the importance of internet in our daily life, the measures that we need to take in order to get rid of security attacks through internet is also getting high. The Internet plays a crucial role in keeping communication going, performing as an efficient and stable network for more than 1 billion users of it. As its user was creeping more than 1 billion the need to provide security to the data passed over network was also getting increased. Data Sent over the internet is of discrete packets which follows different channels in a sequence over time and rejoins at the final destination node. One of the major threats to the Internet is low level layer attacks[1]. A computer connected to an IP/Ethernet LAN has two addresses. One is the address of the network card, called the MAC address. The MAC, in theory, is a globally unique and unchangeable address which is stored on the network card itself [3].

MAC addresses are necessary so that the Ethernet protocol can send data back and forth, independent of whatever application protocols are used on top of it. Ethernet builds "frames" of data, consisting of 1500 byte blocks. Each frame has an Ethernet header, containing the MAC address of the source and the destination computer. The second address is the IP address. IP is a protocol used by applications, independent of whatever network technology operates underneath it. Each computer on a network must have a unique IP address to communicate[5]. IP addresses are virtual and are assigned via software. IP and Ethernet must work together. IP communicates by constructing "packets" which are similar to frames, but have a different structure. These packets cannot be delivered without the data link layer. In our case they are delivered by Ethernet, which splits the packets into frames, adds an Ethernet header for delivery, and sends them down the cable to the switch. The switch then decides which port to send the frame to, by comparing the destination address of the frame to an internal table which maps port numbers to MAC addresses[6]. When an Ethernet frame is constructed, it must be built from an IP packet. However, at the time of construction, Ethernet has no idea what the MAC address of the destination machine is, which it needs to create an Ethernet header. The only information it has available is the destination IP from the packet's header. There must be a way for the Ethernet protocol to find the MAC address of the destination machine, given a destination IP. This is where ARP, the Address Resolution Protocol, comes in. ARP operates by sending out "ARP request" packets. An ARP request asks the question "Is your IP address x.x.x.x? If so, send your MAC back to me." These packets are broadcast to all computers on the LAN, even on a switched network. Each computer examines the ARP request, checks if it is currently assigned the specified IP, and sends an ARP reply containing its MAC address[7].

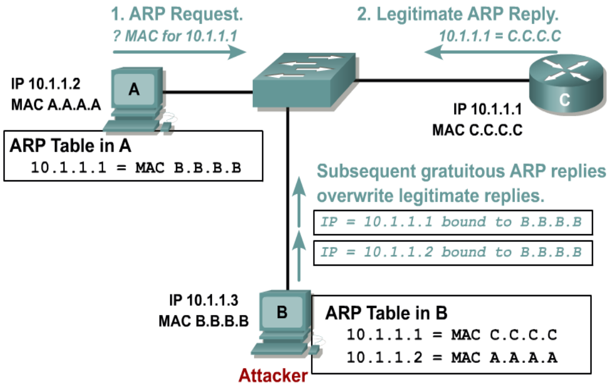

Fig 1 ARP Spoofing

To minimize the number of ARP requests being broadcast, operating systems keep a cache of ARP replies. When a computer receives an ARP reply, it will update its ARP cache with the new IP/MAC association. As ARP is a stateless protocol, most operating systems will update their cache if a reply is received, regardless of whether they have sent out an actual request. ARP spoofing involves constructing forged

ARP replies. By sending forged ARP replies, a target computer can be convinced to send frames destined for computer A to instead go to computer B. When done properly, computer A will have no idea that this redirection took place [10].

2. LITERATURE SURVEY

The “ARP spoofing” attack is based on impersonating a system in the network, making the two ends of a communication believe that the other end is the attacker’s system, intercepting the traffic interchanged [5].Already different methods have been proposed to transfer data securely over the internet. But, none of them has provided a feasible solution to counter the ARP spoofing[8].Tapping into the communication between two hosts on a LAN has become quite simple thanks to tools that can be downloaded from the Internet. Such tools use the Address Resolution Protocol (ARP) poisoning technique, which relies on hosts caching reply messages even though the corresponding requests were never sent. Since no message authentications provided, any host of the LAN can forge a message containing malicious information.[4]. S-ARP model is encryption based security model in which every host has own public/private key it will sent it to the Authoritive Key Distribution(AKD)through which the encryption and decryption of data occurs. One of the major pitfall is that each time it encrypts the message hence it takes time for every transmission [2].

Local Area Network (LAN) based attacks are caused by compromised hosts in the LAN and mainly involve spoofing with falsified IP-MAC pairs. Since Address Resolution Protocol (ARP) is a stateless protocol such attacks are possible. Several schemes have been proposed in the literature to circumvent these attacks, however, these techniques either make IP-MAC pairing static, modify the existing ARP, patch operating systems of all the hosts etc. Discrete Event System (DES) approach for detecting ARP spoofing attacks does not require any extra constraint like static IP-MAC or changing the ARP [9].

Xing et al,[11] proposed a defense mechanism against ARP attacks which is based on the inspection of ARP packets by using RAW socket programming. Secure architecture the spoofing in the address resolution protocol occurs due to lack of authentication in the lower level layer in this a new authentication procedure is followed instead of ARP procedure. It will not be compatible with existing since it is on the basis of new architecture.

Several solutions have been proposed to mitigate the ARP spoofing, but each has its limitations [12]. The solutions have been classified into five different categories [13]:

Modifying ARP using cryptographic techniques: These solutions add some cryptographic features to the ARP protocol, but will not be compatible with the standard ARP and affect the protocol performance.

Kernel-based patching: The technique adds a patch to the operating system kernel in order to prevent ARP spoofing attacks, but the problem is that not all operating systems can be patched and it may become incompatible with the standard ARP protocol.

Securing switch Ports: Use the switch port security or Dynamic ARP inspection (DAI) option to prevent ARP spoofing. However its ability of preventing ARP spoofing easily, the cost of implementing such solution may not be acceptable by most of the organizations.

ARP spoof detection & protection software: Programs or tools developed to prevent ARP spoofing attacks, but the experimental results have shown there ineffectiveness in protection.

Manually configuring static ARP entries: The most basic and effective way to prevent ARP spoofing is adding static ARP entries at each host. However this solution cannot be easily managed and cannot scale well specially in organizations that have large number of users and require a heavy workload on the network administrator.

Spoofed engine technique is another technique in which a separate spoofed engine is dedicated to find out the spoofing by diverting the traffic to that engine. The engine filtered the spoofed packets through header formats and ARP cycles. The spoofed engine architecture followed three modules to find out an spoofed ARP. If the hacker tends to be a first one then the legitimate will be considered as a spoofed one.

Ai-zeng Qian[14] proposed a technique to prevent ARP spoofing by using static ARP entries but the technique still doesn’t work with dynamic networks using DHCP addressing. The administrator must assign all IP addresses along with their MAC to the server so it will be not visible for large scale network.

A method is suggested in [15] to solve ARP spoofing problem using snort IDS and static ARP entries. Yet, it still needs the administrator to add the static mappings manually. Also, it works only in static networks.

Voting based in this technique an enhancement of ARP namely MR-ARP is used if two ARP replies arrives at destination side it will make an MR_ARP request to the other host in the LAN the host will reply for that by MR_ARP reply message through the reply message the conflict got resolved. Since the updating takes place on the basis of voting from most hosts, so that many hosts needs to install this system in order to obey the MR-ARP protocol.

3. PROBLEM DEFINITION

The ARP protocol is the only protocol which gives the solution to the Mac address for the communication. Once a system knows an ip address of the communication system it will broad cast ip address to know the Mac address of the system but because of this volatile catch mechanism hacker can easily hack any system by sending its Mac address as the pair of ip address broadcast and can spoof his data.

4. PROPOSED SOLUTION

This method achieves complete detection and prevention to ARP spoofing with a minimal burden by involving three significant proposed modules a (1) Host perspective model (2) Server perspective model and (3) Server to server authentication. In our first module every communicating host has to send his ip-Mac pair to the centralized server at the time of DHCP itself and regular IP-Mac match checking is done by broadcasting a packet with its own ip and Mac in the source field and its own ip and ff:ff:ff:ff in the Mac of destination field. If any hacker is found by getting a reply for the above message. Then the destination host will send the hacker information udp/tcp message to the centralized server.

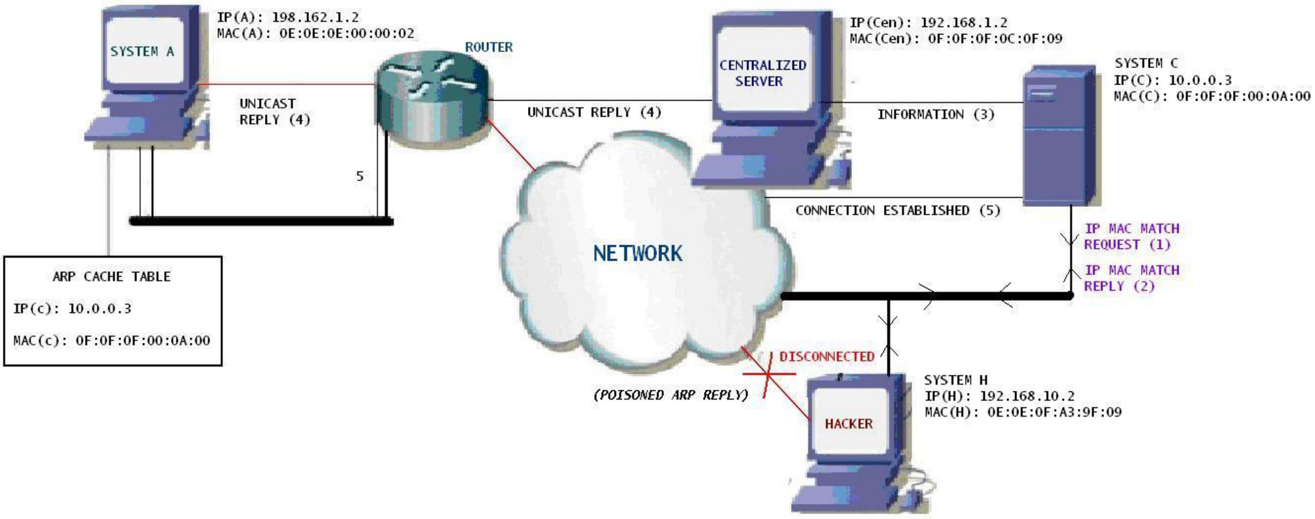

Fig.2. Diagrammatic Representation with Centralized Server

In server perspective module in which a centralized server is installed to the LAN which collects all the systems ip-mac pair at the time of DHCP itself ,generate and maintain a tabled database of an legitimate users and hackers if any information is came from the host that intimating about the hacker as a formal udp message. It will verify the information with the database and will send an udp/tcp message to the source. The final module is the server to server authentication module in which if two information messages has came to the source then the source will forward that to the centralized system of that LAN. Initially every host in a LAN has a detail of centralized server information through the authentication procedure.

The centralized servers in each LAN have some sort of secured network with other LAN servers through public key encryption and decryption algorithm. If a server conflict occurs on the source host it resolves the conflict by sending a message to the trusted centralized server in that LAN, which check the database for finding the legitimate server matching and inform that to the source host.

5. IMPLEMENTATION

The above concept is explained below with the help of diagrams. The output of simulation using NS2 is shown as graphs. The secure procedure will involve with the participating hosts and the centralized server only. This system also resolves a problem of hacker acting as a centralized server. NS2 is taken as simulation tools because of its high scalability support, where participating nodes can be increased.

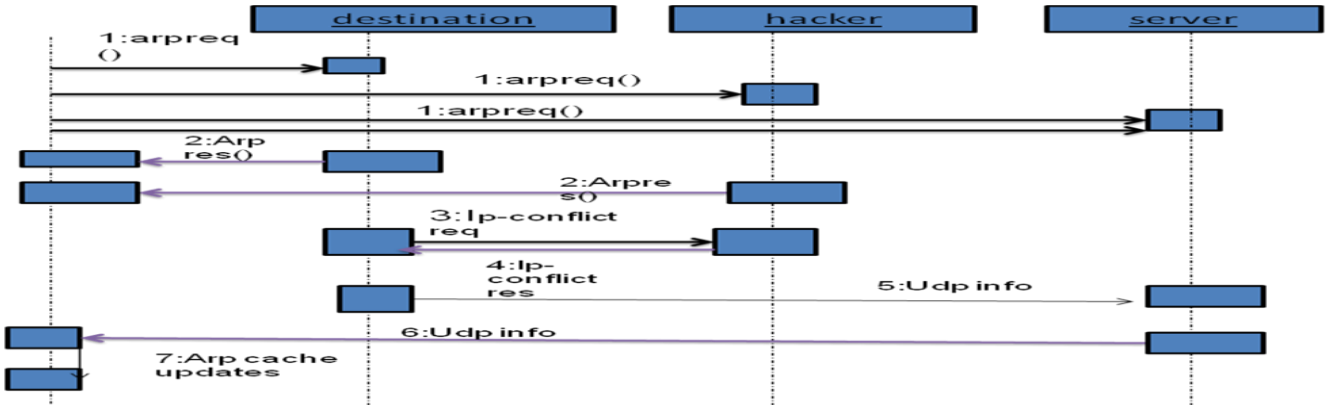

Fig.3. Sequence Diagram

5.1 Host Perspective

The source host broadcast an arp request to the destination ip host. When a destination ip receives the request sends a unicast arp reply message. At a particular period of time the destination will send ip-mac match arp request to find the suspicious hosts in a LAN. If hacker is found then it will inform to the centralized server. If information is received from centralized server to the source this will verify it and made a connection with the legitimate host.

5.2 Server Perspective

The centralized server will collect the ip-mac pair of all hosts in a LAN at the time of DHCP and maintains a table which is named as arp-prev table. When a request come from the outside host it will firstly fills up the verification table with the matched field value from DHCP table. If an UDP message is come from a host it will verify that through this table and send information to the source which made a request. If any synchronization message is come as encrypted with the public key of server with another server then the authentication procedures will be followed by the server and later authentication the acknowledgement will be received.

5.3 Server to server authentication

When a server conflict occurs at the source it sends a message to the centralized server in the LAN asking for a legitimate centralized server. The server will collects a public key of particular centralized server through the network of centralized server and an authentication is done through public and private keys of centralized servers.

6. ADVANTAGES

Few parameters have been considered to make the proposal to be defined as one of the finest solutions to ARP spoofing follows:

The propose system is compatible with the existing ARP protocol and it will not disturbs the other hosts in LAN for the secure procedure of the host. The secure procedure will involve with the participating hosts and the centralized server only. This system also resolves a problem of hacker acting as a centralized server. Since the centralized server governs the whole traffic of an LAN a secure LAN can provide with this system .

6.1 Performance Analysis

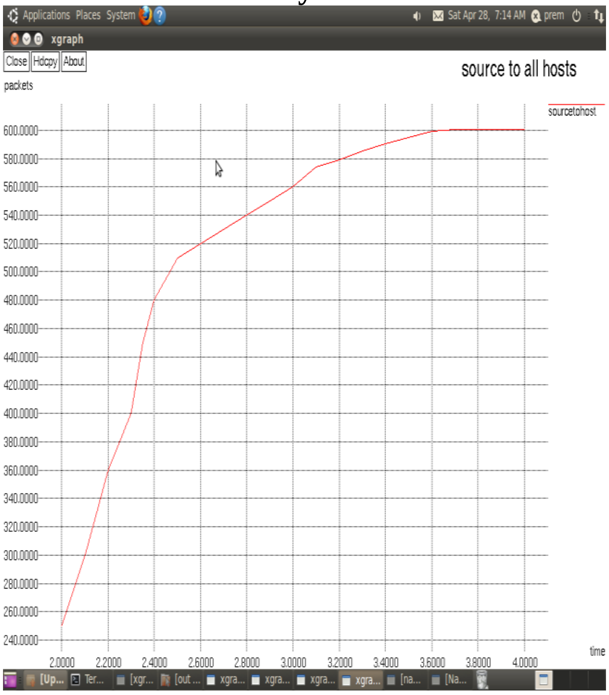

Fig.4. Packets broadcasted from source to all Host

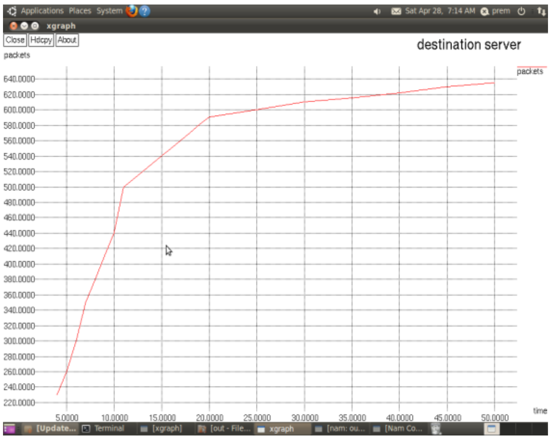

Fig.5. Packets received from all host to destination

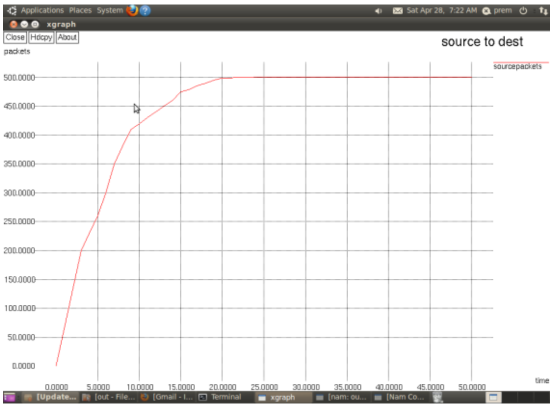

Fig.6. Packets transferred between source and destination: (Before hacking)

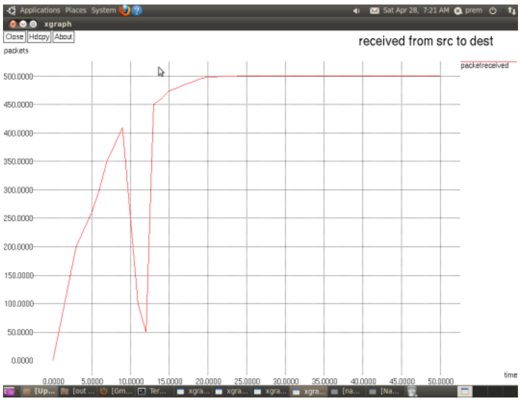

Fig.7. Packets transferred between source and destination (After hacking)

Table 1: Performance comparison

No of hosts should involve in the process	Less
Authentication procedure	Less
Security	High
Time taken to resolve	Less
No of hackers can be prevented	high

7. CONCLUSION AND FUTURE ENHANCEMENTS

This paper presents a centralized server ARP model which maintains a legitimate user list with a minimal of intrusion from a host perspective where it prepares the user list at a time of DHCP. Thus the process of using packet tracking and other monitoring has been reduced. In this approach a trusted server is maintained in a LAN for updating ARP cache .Trusted server list is prepared on every host in LAN. Server authentication is filtered by forming a secured network between the centralized servers across the LAN. This was accomplished by embedding a authentication algorithm for server conflict resolution. Since the system security is depends only on the centralized servers and participating host, its enough if participating hosts only followed the proposed system.

For the past two decades in the history of ARP spoofing has been greatly increased because of the knowledge of intrusion and a great hole in a low level layer. If this type of centralized and authenticated server is going to install in a LAN, this will really prevent a type of low level layer attacks as well as other upper level layer spoofing like ip spoofing. Further in this system a secure authentication can be added for more secure communication and a well established network can be maintained for the centralized servers and a well established architecture should be maintaining for the server networks

8. REFERENCES

[1] Ahmad, I. and Ataullah, Md. “A Survey on Various Solutions of ARP Attacks” International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No.2, 2013.

[2] Bruschi,D., Ornaghi,A. and E. Rosti, “S-arp: a secure address resolution protocol,” IEEE Conference on Computer Security Applications Conference, pp. 66 – 74, 2003.

[3] Lootah, W., Enck,W. and McDaniel,P. “Tarp: Ticket-based address resolution protocol,” vol. 51, No. 15. Elsevier , pp. 4322–4337, 2007.

[4] Nam,S., Kim,D. and Kim,J. “Enhanced Arp: preventing arp poisoning based man-in-the-middle attacks,” IEEE Communications Letters, Vol. 14, No. 2, pp. 187–189, 2010.

[5] Pandey,P. “Prevention of ARP spoofing: A probe packet based technique”, IEEE Conference on Advance Computing, pp.147-153, 2013.

[6] Jinhua, G. and Kejian, X. “ARP Spoofing detection algorithm using ICMP protocol”, IEEE Conference publication on Computer Communication and Informatics, pp.1-6, 2013.

[7] Hou,X., Jiang,Z., and Tian, X. "The detection and prevention for Arp spoofing based on snort," IEEE International Conference on Computer Application and System Modeling , Vol. 5. , pp. V5-137, 2010.

[8] AmitKumar,T., SurendraKumar and PrafullKumar Singh, “ A Novel Approach to Detect and Defense against Address Resolution Protocol(ARP) Spoofing Attack”, International Conference on Advance Development in Engineering and Technology, 2014.

[9] Neminath, H., Biswas,S., Roopa,S., Ratti,R., and Nandi,S. , “ A DES approach to Intrusion Detection System for ARP Spoofing Attacks”, 18th Mediterranean Conference on Control &Automation , 2010.

[10] Xiangning, H., and Zhiping, J., “The detection and prevention for ARP Spoofing based on Snort”, International Conference on Computer Application and System Modeling , 2010.

[11] Xing,W., Zhao,Y., and Li,T., "Research on the defense against ARP Spoofing Attacks based on Winpcap", IEEE Second International Workshop on Education Technology and Computer Science, 2010.

[12] Cristina,L., and Rafael, I., "An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks,"International Conference on Distributed Computing Systems Workshops, 2007.

[13] Somnuk P and Narongrit M., “An Efficient and Feasible Solution to ARP Spoof Problem," International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, pp. 910-913, 2009.

[14] Ai-zeng Qian., "The Automatic Prevention and Control Research of ARP Deception and Implementation," WRI World Congress on Computer Science and Information Engineering, No. 2(1), pp. 555-558, 2009.

[15] Boughrara, A. and Mammar, S., "Implementation of a SNORT's output Plug-In in reaction to ARP Spoofing's attack," International Conference on Sciences of Electronics Technologies of Information and Telecommunications , pp.643,647, 2012.