A Survey on ARP Spoofing and Prevention of ARP Attacks

Ben Linus S, Yashwanth K, Gayathri K, Sanjay R., Deepa NR

Student, Student, Student, Student, Assistant Professor

Anna University

Abstract: ARP (Address Resolution Protocol) is a communication protocol. It is used to map IP (Internet Protocol) Address to the MAC (Media Access Control) Address. ARP performs ARP requests and ARP reply. It requests along with senders MAC address and IP address and also receivers MAC address and IP address. These ARP requests and reply are the process that are taken place between the hosts. In this communication the ARP Poisoning occurs (i.e) there is an occurrence of attack during communication between the hosts. The types of attack such as Man in the Middle (MITM) attack, Denial of Service (DOS) can be taken place in this communication. In MITM attack, is well known attack where the attacker acts as a victim to the communicating host by using victims MAC address and also acts as a communicating host (destination host) to the victim by using destination host's MAC address [2]. This spoofing attack also becomes serious in wireless networks. The previous protocol techniques used a legitimate central host using ICMP protocol which should always monitor the system to detect ARP Spoofing attack. These approaches are to detect ARP spoofing attack in the client machine with a central host to monitor always.

Keywords: ARP request, ARP reply, MAC, DOS, MITM.

I. INTRODUCTION

ARP (Address Resolution Protocol) maps a protocol address (IP) to a hardware or MAC address dynamically. Here, if any main host want to communicate with another destination host it broadcast requests to all the hosts in the network. The destination host's IP which matches to the request replies to the main host, the MAC address as the reply to the request [3]. In this type of request and reply messages the attacks occur such as MITM attack, Denial of Service, MAC flooding, MAC duplicating, MAC address spoofing, session hijacking etc.

16 bits data 16 bits data

Hardware Type		Protocol Type
MAC Address Length	Protocol Address Length	OP Code Number
Sender MAC Address		
Sender IP Address		
Receiver MAC Address		
Receiver IP Address		

Table 1: ARP Message Format

The Table 1 shows the ARP Message Format. Once the ARP cache has been poisoned, each of the victim devices send their packets to the attacker when computing to the other device [3].

II. ARP ATTACKS

A. *ARP Spoofing or Poisoning:* ARP gets poisoned during communication between the hosts. Here, the attacker can modify the data and it can terminate the data transition.

B. *DOS Attack:* In Denial of Service attack attacker sends ARP Packets to the hosts continuously that other devices cannot connect to that host or to make their system slower.[1]

C. *MITM:* In Man in the Middle attack the third party intruder involves and can easily sniff all the data of both the communicating hosts.[2]

D. *MAC Flooding:* It is a ARP cache poisoning method which can be done at the network switches. If the switch gets overloaded, it will work like a hub. Then it broadcast traffic to all the devices connected to the network. It is easy to flood a switch with forge ARP reply by the attacker.

E. *MAC Duplicating:* MAC Duplicating attack is that the attacker change the MAC address of the host similar to the MAC address of the target host whose traffic is to be captured. SO, switch gets astonished and sends reply to both original and cloned host.

F. *MAC Address Spoofing:* In MAC address spoofing, the attacker spoofs the hardware address of the authorized host and it sniffs all the sensitive data.

G. *Session Hijacking:* Session Hijacking is that takes full access over the connected host which can be victimized into getting their connection changed. Here, the attacker uses the ARP Spoofing to steal the information like session id's and the attackers gets permission to access data by using the stolen session id's. So that the attacker looks like an authorized host.

III. RELATED WORK

Zouheir Trabelsi Ph.D, Hamza Rahmani [4]. In this paper it detects the sniffing attack. Now a days attackers can steal easily sensitive data, passwords by sniffing a network. This technique ARP cache poisoning attack detect sniffing hosts in an Ethernet network. There are four anti sniffers PMD, Promi Scan, LOpht Anti sniff and SupCom anti sniffer. These anti sniffers are tested and shows the result that SupCom anti sniffer detects more sniffing host than the other anti sniffers. Anti-sniff instead of using RTT (Round Trip Time), DNS and ARP detection techniques. These techniques cannot detect sniffing. This technique detects such sniffing attack and becomes more effective. The sup com anti sniffer used here is more efficient particularly when detecting active sniffers. This is able to detect hosts running even advanced sniffers.

Raviya Rupal D, Dhaval Satasiya, Hiresh Kumar, Archit Agrawal [1].

In this technique it demonstrate a utility which provides authentication to the user and also the detection and prevention of ARP spoofing in dynamic configuration of IP. Utility provides a mechanism called ICMP (Internet control management protocol) which is used to check the pair entry of IP-MAC This includes three modules such as

a.DHCP IP configuration using DHCP server.

b.Authentication to user can be given by using radius server + MySQL database.

c.Detection and prevention of ARP spoofing. Thus it provides authentication, detection and prevention.

Somnuk Puangpronpitag,Narongrit Masusai[5].

ARP spoof is a serious security problem which can be used to Denial of Service (DOS) or Man-In-The-Middle (MITM) attack. Here, they designed a prototype system called Dynamic ARP spoof protection and surveillance (DAPS) system. AVASS which is an ARP spoof detection software which has been designed and implemented to detect ARP spoofing.

Sumit Kumar, Shashikala Tapaswi[6].

This paper adds a feasible solution to the ARP cache poisoning, removing inconsistencies from all ARP tables of all hosts in the network. It uses a centralized system and ARP central server and uses ACS to manage table.

Gao Jinhua, Xia Kejian[3].

The paper proposed a efficient algorithm based on ICMP protocol to detect malicious hosts that performing ARP spoofing attack. It won't disturb the activities of the hosts on the network.

Prerna Arote, Karam Veer Arya[7].

In proposed mechanism of detection, initially traffic over the network is sniffed by central server (CS). Then CS sends trap ICMP ping packet. In order to prevent ARP poisoning over centralized system, voting process is used to elect legitimate centralized system.

S. NO	Name of the paper	Journal Name	Year	Benefits	Drawbacks
1.	An Anti-Sniffer Based on ARP Cache Poisoning Attack	Information Systems Security	2006	It used anti sniffers such as Promi scan,PMD and LOpht anti sniff instead of using RTT(Round trip time),DNS and ARP detection techniques.	These techniques cannot detect sniffing attack when the sniffer do not generate reply, ARP & DNS messages or it put heavy traffic on the network. So these techniques become useless.
2.	Detection and Prevention of ARP Poisoning in Dynamic IP configuration	IEEE International Conference	2016	It overcome the loop holes such as infeasibility, cost, backward compatability, efficiency,effectiveness and unmanageability. There is less network traffic	This technique is applied only in LAN not in wireless network.
3.	An Efficient and Feasible Solution to ARP Spoof Problem	IEEE International Conference	2009	Performance and effectiveness has achieved. DAPS has lower overhead and easier to manage. DAPS and AVASS can tolerate heavy attacks.	Design is not very efficient also it is not easy to manage
4.	A Centralized Detection and Prevention Technique against ARP Poisoning	IEEE International Conference	2012	This uses Access Control system as a centralized system to remove inconsistencies in ARP table.	It affect the activities which is happening in the host network.
5.	ARP Spoofing Detection Algorithm using ICMP Protocol	International Conference on Computer Communication and Informatics	2013	It uses the internet control message protocol to detect the attacker without affecting the activities in host network as a centralized system(CS).	The centralized system used in this method will have to be monitored and when the reasonable attack takes place the system will ask for further step to proceed.
6.	Detection and Prevention against ARP	International Conference on Computational	2015	This is the enhanced version of ICMP protocol method where if	The packets voting process will take more time than the

	Poisoning Attack using Modified ICMP and Voting	Intelligence & Networks		uses some protocol but makes the process of packets to count on devices connected and take processed packet votes to determine the attacks.	other methods to detect and prevent the attacker.

Table 2: Summary of different works

IV. CONCLUSION

In this survey paper, we retrieved all the techniques proposed. But there are some loop holes that have been identified. This survey makes it necessary to propose a new scheme which would satisfy all the aspects of complete solution of ARP poisoning. It would be implemented in near future.

V. REFERENCES

[1] Raviya Rupal D, Dhaval Satasiya, Hiresh Kumar, Archit Agrawal, "Detection and Prevention of ARP Poisoning in Dynamic IP configuration", IEEE International Conference On Recent Trends In Electronics Information Communication Technology.

[2] M. Conti, N. Dragoni and V. Lesyk, "A survey of man in the middle attacks", IEEE Communications Surveys & Tutorials, 2016.

[3] Gao Jinhua, Xia Kejian, "ARP Spoofing Detection Algorithm using ICMP Protocol",International Conference on Computer Communication and Informatics.

[4] Zouheir Trabelsi Ph.D, Hamza Rahmani, "An Anti-Sniffer Based on ARP Cache Poisoning Attack", Information Systems Security,2006

[5] Somnuk Puangpronpitag, Narongrit Masusai,"An Efficient and Feasible Solution to ARP Spoof Problem", IEEE, 2009

[6] Sumit Kumar, Shashikala Tapaswi, "A Centralized Detection and Prevention Technique against ARP Poisoning",

[7] Prerna Arote, Karam Veer Arya, "Detection and Prevention against ARP Poisoning Attack using Modified ICMP and Voting",International Conference on Computational Intelligence & Networks, 2015.