A SECURITY APPROACH TO DETECT AND PREVENT ARP SPOOFING USING ACTIVE AND PASSIVE TECHNIQUES

Deepa NR[1], Ben Linus S[2], Gayathri K[3], Sanjay R[4] & Yashwanth K[5]

[1] Assistant Professor, Department of CSE,

Coimbatore Institute of Engineering and Technology, Coimbatore.

[2] Student, Department of CSE,

Coimbatore Institute of Engineering and Technology, Coimbatore.

[3] Student, Department of CSE,

Coimbatore Institute of Engineering and Technology, Coimbatore.

[4] Student, Department of CSE,

Coimbatore Institute of Engineering and Technology, Coimbatore.

deepu.me28@gmail.com[1], benlinus649@gmail.com[2],
gayathrikarunanithi448@gmail.com[3], sanjayramasamyyadav@gmail.com[4],
yashwanthyashu110@gmail.com[5].

Abstract: *Most of the computer programs/applications use logical address to send/receive messages, however the actual communication happens over the physical address. This is where ARP comes into the picture. The acronym ARP stands for Address Resolution Protocol. Its functionality is to map the dynamic Internet Protocol address to a permanent physical machine address (MAC address) in a network. When a new computer joins a network, it is assigned with a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular network arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address. The ARP spoofing is used to send fake ARP messages on a Local Area Network (LAN). Such attacks may result*

in traffic alteration, or even worse, in a temporary or permanent interruption of traffic. To avoid such attack, an active technique is used to detect ARP spoofing and prevent it from the attacker. The active and passive scanning is used for detecting the intruder and offensive and defensive modes are used for removing the intruder from the network. The MAC changer algorithm makes the hacker not to spoof into our devices anymore as the MAC changes frequently.

Keywords: Traffic Sniffing, ARP Spoofing, Dynamic ARP Inspection, MITM

1. INTRODUCTION

Cyber security is to protect the computer networks and system from the theft of the hardware, software or electronic data. There is increased reliance on computer systems, wireless network standards, the internet due to this, the field "cyber security" is more important. Due to the complexity in terms of politics and technology, cyber security is the major challenges in the contemporary world.

1.1.ADDRESS RESOLUTION PROTOCOL:

ARP or address resolution protocol is a communication protocol to discover the MAC address which is associated with the IPv4 address. ARP was defined by RFC 826 with the many combinations of network and data link layer technologies ARP has been implemented. The ARP functionalities is provided by the neighbour discovery protocol (NDP) in internet protocol version (IPv6).

1.2.PACKET STRUCTURE:

The address resolution protocol (ARP) uses only a simple message format. It contains one ARP request or response. The ARP message size depends on the network and links layer address size. The ARP message header specialties the network type which is in use at each layer and also the size of address of each. The hardware and protocol address of the sender and receiver hosts are the four addresses consists in this payload.

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

1.3.WORKING OF ARP:

When a device wants to communicate with another device over the internet. Here, ARP broadcast a packet to the source network. There, the devices in their network checks for the similarity of their IP addresses with the destination address, it responds to the source, if it is not matched, their packet reaches to the gateway of the network, then it broadcast to the devices and validates their network ID. This process continues till the destination address gets matched with network ID of the devices and in turn responds with the destination MAC address.

2. ARP ATTACKS

2.1 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.

2.2 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]

2.3 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]

2.4 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.

2.5 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.

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

2.7 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.

3. RELATED WORKS

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.

4. PROPOSED SYSTEM

This system consists of different scanning techniques that are active and passive scanning. They can do these scanning either by offensive or defensive mode. The offensive mode removes the attacker from the network and secures our connection to the network. In defensive mode the user is disconnected from the network. In this mode the audio is played if there is any activity of attacker.

It can perform active scan as well as passive scans in both defensive and offensive modes.

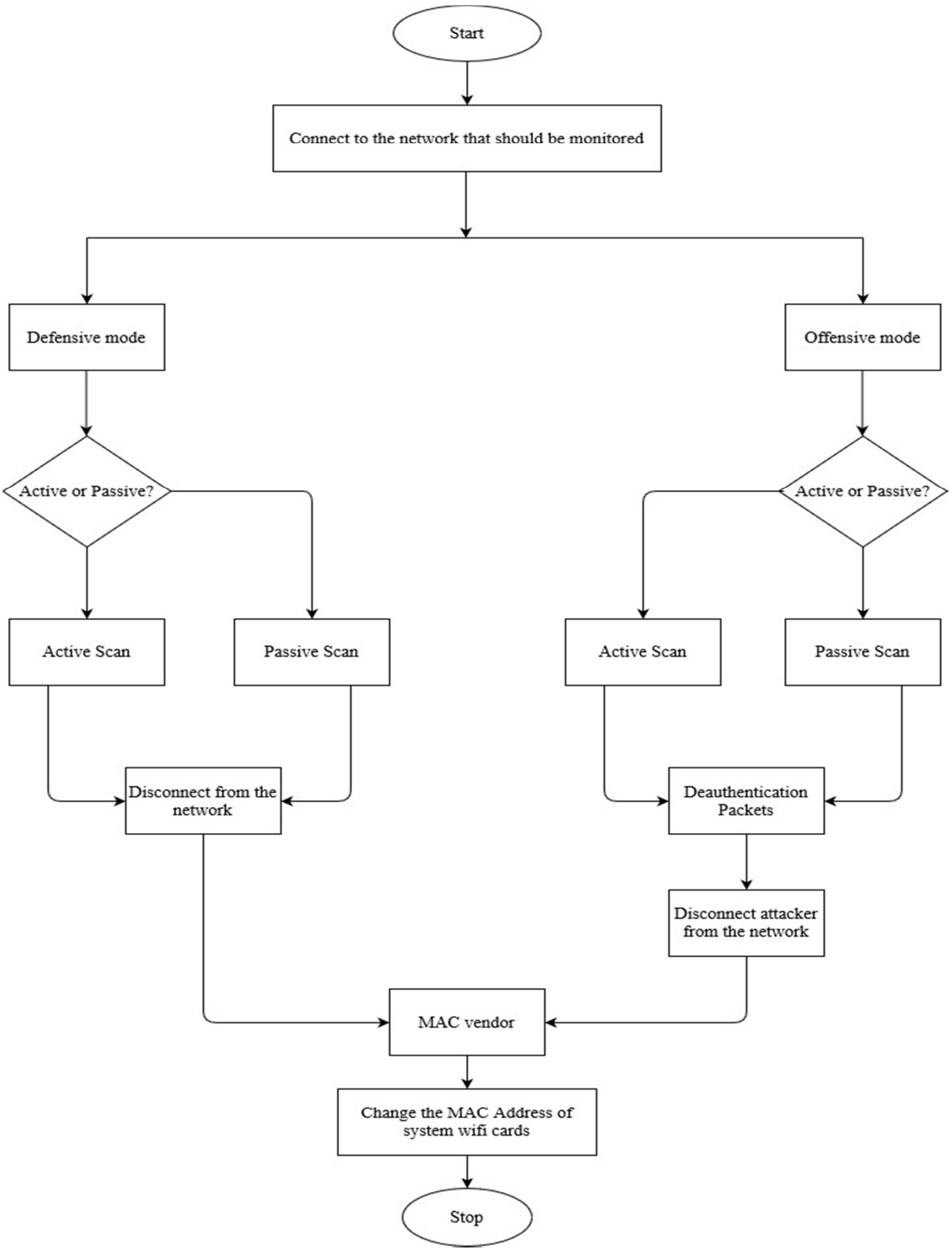
In Defensive mode it protects the end user from the spoofer by disconnecting the user's system from the network. This mode also alerts the user by an audio alert message when the spoofing by an attacker is detected.

In Offensive mode it disconnects the user's system from the network and further kicks out the attacker. The attacker is disconnected by sending De-authentication packets to his system, this does not let him reconnect to the network until the program is manually reset.

The Active Scan is used when the system is left idle most of the time. Active scan is most efficient method to protect the system and the network from ARP-spoofing incidents.

The Passive Scan is used when the system is busy transferring data through the network. Passive scan is efficient certain constant data transferring devices as the device and therefore the network would be secured from ARP-spoofing incidents without compromising the speed or the network bandwidth.

Flow Diagram:



5. METHODOLOGY

The proposed methodology for detecting and preventing ARP SPOOFING contains techniques like Defensive mode, Offensive mode, Active scan and Passive scan.

A. Defensive mode:

Defensive mode protects the top user from the spoofer by disconnecting the user's system from the network. This will also alerts the user by a sound message as soon as attacker is detected. If an attacker sends bogus ARP packets to a host device or user network, the device or network the local ARP entries, leading to packet forwarding failures. The function of defence against ARP spoofing attacks can prevent such attacks. Before configuring defence against ARP spoofing attacks, connect interfaces and set physical parameters for the interfaces to ensure that the physical status of the interfaces is Up.

Aircrack-ng:

Aircrack-ng is a 802.11 WEP , WPA/WPA2-PSK key cracked module.

Aircrack-ng can be get the WEP key will have enough encrypted packets been captured with the airodump-ng. The part of aircrack-ng determines the WEP key using the fundamental methods. The first method will be via the PTW approach. This will be done in two phases. In the first phase it uses ARP packets. If the key is not found it uses all packets in capture. Not all packets can be used for PTW method.

Cracking session:

Cracking can sometimes take a very long time and it is sometimes necessary to turn off the computer or put it to sleep for a while. In order to handle this kind of situation, a new set of option has been created.

It will create or update a session of the cracking (every 10 minutes) as well as all the options used, wordlists and capture files used. Multiple wordlists can be used and it works with WEP and WPA.

B. Offensive mode:

Offensive mode will disconnect the user from the host network and further kicks out the spoofer by sending the De-authentication packets to the attacker system, this will not let him to reconnect with host until the program is reset.

This mode will able to kick out the attacker from the network and will not able to connect again to the network because the offensive mode keeps sending the de-authentication packets to the mac-address of the attacker. The mac-address of the attacker will be obtained by running the active scan or the passive scan in the offensive mode. The gateway of each scan will be changing in the certain interval of time to avoid the attacker to connect back to the network and the aircrack-ng will be killed once the active scan or passive scan is selected in the program.

Before configuring offensive against ARP spoofing attacks, connect interfaces and set physical parameters for the interfaces to ensure that the physical status of the interfaces is Up. Configuring the physical parameters will give the value of each time to be declared as the time interval so that the packets will send accordingly. The ARP will be given in the solution of each packets and the attacker will be forcefully removed from the organization network to provide the solution in the form of each value by the number of scans in offensive mode. This can be used as same as the previous parameters like both in the wired network and the wireless network to form a solution of the entire value.

C. Active scan:

It will be used when the system is left idle. Active scan is most efficient method to protect the system and the network from ARP-spoofing incidents. This method is used after the defensive mode by getting the entire process that means the defensive mode will be the top segment of the process when each it get scanned for the attacker to look for the effective details to disconnect the attacker form the respective network connection to establish the value of each give procedure to get the scan and make it as a possible way to identify the attackers way to control the process and maintain the network secure.

Airodump-ng:

Airodump-ng is employed for packet capturing of raw frames and is particularly for collecting WEP for the intent of using them with aircrack-ng. If a GPS receiver connected to the computer, airodump-ng can be logging the coordinates of the found access points.

Additionally, airodump-ng will write out many files containing the small print of all access points. It's a network software consisting of a detector and a packet sniffer.

D. Passive Scan:

When the system is busy transferring data through the network. Passive scan is efficient in for constant data transferring devices as your device and the network will be safe from attackers incidents without compromising the speed or the network bandwidth. The Defensive mode has two scanning techniques one is active scan which was explained in the previous sub heading and the other one is passive scanning under defensive mode will get the same scanning technique like active scan but it can used to scan a constant data transferring devices and the total speed of the network with bandwidth speed in the network.

Hardware address:

It is a 6-byte hexadecimal number which is represented by 12 digits. So it will act as a signature or fingerprint of your computer.

Each value of the hardware will give its mean address to the specific attacker and the hardware address will make the certain value of the attacker to target which address the ARP spoofing should be done. When the spoofing is estimated the value will give its turn to

maintain the WLAN or LAN hardware address to the attacker and from that address the taken value will be easily featured to the spoofing time and given the protection.

E. De-Authentication Packets

This will show you how to disable a devices connection to Wi-Fi using a de-authentication attack.

A de-authentication attack is a type of attack which targets the communication between router and the device. Effectively disabling the Wi-Fi on the device.

The de-authentication attack isn't some special exploit of a bug. It's a created protocol and is being used in real world applications.

De-authentication attack's use a de-authentication frame. This frame sent from a host to the device to disconnect.

6. EXPERIMENTAL RESULT

This project proposed an active and passive scanning method to provide security against ARP spoofing. This system will detect an attacker who tries to spoof data and it will automatically disconnect the third person involved called the attacker. Here in this project, the two sub modules called offensive and defensive modules. The offensive module disconnects the user and audio message if spoofing has been detected. The defensive module disconnects user from the attacker and disconnects attacker by sending the de-authentication packets. The performance is more in implementing the active and passive scanning to detect and remove the attacker. In present days, people demand for user security. The goal of our project is to detect the major attack happening in security called ARP spoofing attack and to remove it by using its MAC and IP Address.

S.NO	LAN	WLAN	PTW APPROACH	DISCOVERABLE METHOD	de-authentication
Paper 1	YES	YES	NO	NO	NO
Paper 2	YES	NO	YES	NO	NO
Paper 3	YES	NO	NO	YES	NO
Our project	YES	NO	YES	YES	YES

7. CONCLUSION

This project proposed an active and passive scanning method to provide security against ARP spoofing. This system will detect an attacker who tries to spoof data and it will automatically disconnect the third person involved called the attacker. Here in this project, the two sub-modules called offensive and defensive modules are used. The offensive module disconnects the user and audio message if spoofing has been detected. The defensive module disconnects user from the attacker and disconnects attacker by sending the de-authentication packets. The performance is more in implementing the active and passive scanning to detect and remove the attacker. In present days, people demands for user security. The goal of our project is to detect the major attack happening in security called ARP spoofing attack and to remove it by using it's MAC and IP address.

This system will help that our future work would facilitate security against all attacks instead of solving single attack.

REFERENCES:

1. Arote Prerna and Karam Veer Arya (2015) “Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting.” Computational Intelligence and Networks (CINE), International Conference on IEEE.
2. Bruschi, A. Ornaghi and E. Rosti (2003) “S-ARP: A secure address resolution protocol”, Annual Computer Security Applications Conference (ACSAC).
3. Ferdous Ahmed Barbhuiya, Neminath Hubballi,Sukumar Nandi and Santosh Biswas (2011) “A Host Based DES approach for detecting ARP Spoofing”, Computational Intelligence in Cyber Security (CICS).
4. Gao Jinhua and Xia Kejian, (2013) “ARP Spoofing Detection Algorithm using ICMP Protocol”, International Conference on Computer Communication and Informatics.
5. Haider Salim, Zhitang Li and Zhengbian Guo (2012) “Preventing ARP spoofing attacks through gratuitous decision packet”, Distributed Computing and Application to Business, Engineering and Science(DCABES).
6. Jae Dong Lee,Young-Sik Jeong and Min su Song (2014) “A new detection scheme for ARP spoofing attacks based on Routing trace for ubiquitous environment”, The Scientific world Journal.

7. Jaideep Singh, Goldendeep Kaur and Jyoteesh Malhotra (2015) “A Comprehensive Survey of Current Trends and Challenges to mitigate ARP attacks”, International Conference on Electrical, Electronics, Signals and Optimization.
8. Jaideep Singh, Sandeep Dhariwal and Rajeev Kumar (2017) “A detailed survey of ARP poisoning detection and mitigation techniques”, International Journal of Control Theory and Application.
9. M. Conti, N.Dragoni and V.Lesyk, (2016) “A survey of man in the middle attacks”, IEEE Communications Surveys & Tutorials.
10. Mei Guo, Min Xiao and Hui Xie (2018) "Research on preventing ARP attack based on computer network security", IoP conference series.
11. Neminath H, S Biswas, S Roopa, R Ratti, R Nandi, F A Barbhuiya, A Sur and V Ramachandran, (2010) “A DES Approach to Intrusion Detection System foe ARP Spoofing Attacks”, Mediterranean Conference on Control & Automation (MED), IEEE.
12. Nikhil Tripathi and BM Mehtre (2013) “An ICMP based secondary cache approach for the detection and prevention of ARP poisoning”, International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1 – 6.
13. Prerna Arote and Karam Veer Arya, (2015) “Detection and Prevention against ARP Poisoning Attack using Modified ICMP and Voting”, International Conference on Computational Intelligence & Networks.
14. Ravi Raj Saini and Himanshu Gupta, (2015) “A Security Framework Against ARP Spoofing”, IEEE International Conference.
15. Raviya Rupal D, Dhaval Satasiya, Hiresh Kumar and Archit Agrawal, (2016) “Detection and Prevention of ARP Poisoning in Dynamic IP configuration”, IEEE International Conference On Recent Trends In Electronics Information Communication Technology.
16. S. Kumar and S. Tapaswi (2012) “A centralized detection and prevention technique against ARP poisoning in Cyber Security”, Cyber Warfare and Digital Forensic (CyberSec),Page(s): 259 - 264.
17. Seungpo Hong and Sangjun Lee (2013) “ Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA", Mathematical and Computer Modelling(vol-58).

18. Somnuk Puangpronpitag and Narongrit Masusai, (2009) “An Efficient and Feasible Solution to ARP Spoof Problem”, IEEE.

19. Sumit Kumar and Shashikala Tapaswi, (2012) “A Centralized Detection and Prevention Technique against ARP Poisoning”, IEEE International Conference.

20. SY Nam, D Kim and J Kim (2010) “Enhanced ARP: preventing ARP poisoning based Man in the middle attacks”, IEEE.

21. T. Demuth and A. Leitner (2005) “ARP spoofing and poisoning:” Traffic tricks. Linux Magazine, 56:26– 31.

22. V. Goyal and V. Abraham (2013) “An efficient Solution to the ARP cache poisoning problem”, Australasian Conference on Information Security and Privacy, pp 40-51.

23. W.Lootah, W.Enck, and P. McDaniel (2005) “TARP: Ticket-based address resolution protocol”, Annual Computer Security Applications Conference (ACSAC).

24. Weifeng Sun and Minchun Zheng (2015) "Research on ARP Spoofing detection strategies in unreliable LAN" International conference on Human centered computing.

25. Wenjian Xing, Yunlan Zhao and Tonglei Li, (2010) “Research on the defence against ARP Spoofing Attacks based on Winpcap”, International Workshop on Education Technology and Computer Science, IEEE.

26. Yang Liu, Lan Dong, Bin Li and Kaikun Dong (2008) " Research of the ARP spoofing principle and a defensive algorithm" International Journal of Communication.

27. Zouheir Trabelsi and Hamza Rahmani, (2006) “An Anti-Sniffer Based on ARP Cache Poisoning Attack”, Information Systems Security.