An Inventive Method for Detection and Prevention Against ARP Attacks

Sharda Dubey, Sumit Gupta

Abstract- ARP poisoning is the most perilous assault that endangers the working of MANET. This assault originates from the way the ARP convention works, since it is a stateless convention. This ARP assault might be utilized to dispatch either foreswearing of administration (DoS) assaults or Man in the middle (MITM) assaults. In order to deal with such problem there exist methods for utilizing static ARP sections to anticipate ARP parodying. However, ARP mocking relief techniques relying upon static ARP have significant disadvantages. In this paper, we propose a versatile method to counteract ARP assaults, which naturally designs static ARP sections and here each host in the neighbourhood system will have a secured non-satirize ARP store. The works is proposed by using both static and DHCP based tending to plans a system that permits securing of a substantial number of clients with no overhead. Execution investigation of the system has been led by utilizing a genuine system. The estimation comes and it is found that the customer or any node needs close to one millisecond to en-roll itself for a secured ARP reserve. The outcomes likewise demonstrated that the node participating can easily be detected and prevented by the proposed work in only few microsecond under substantial activity.

Keyword: ARP spoofing; Static ARP entries, MAC address, Spoof detection

I. INTRODUCTION

Mobile ad-hoc networks are more prone towards spoofing attacks. In personality based mocking assaults, an aggressor can fashion its character to take on the appearance of another gadget or even make various ill-conceived characters in the systems by taking on the appearance of an approved remote get to point (AP) or an approved customer [1]. An assailant can dispatch refusal of-administration (DoS) assaults, sidestep get to control systems, or dishonestly publicize administrations to remote customers. Along these lines, personality based assaults will have a genuine effect to the ordinary operation of remote and sensor systems. Parodying assaults can additionally encourage an assortment of movement infusion assaults, for example, assaults on get to control records, maverick AP assaults, and in the long run DoS[2]. Parodying can go up against many structures in the PC world, all of which include some sort fake representation of data.

1.1. IP Spoofing

Web Protocol (IP) is the convention utilized for transmitting messages over the Internet [3]; it is a system convention working at layer 3 of the Open Systems Interconnection (OSI) show. IP satirizing is the demonstration of controlled the headers in a transmitted message to cover a programmers genuine personality so that the message could seem like it is from a trusted source. IP ridiculing is utilized to increase unapproved access to a PC. The aggressor advances bundles to a PC with a source address showing that the parcel is originating from a trusted port or framework.

1.2. ARP Spoofing

Address Resolution Protocol (ARP) is utilized to guide IP locations to equipment addresses [4]. A table named as ARP store, is utilized to keep up a connection between's every Medium Access Control (MAC) address and its relating IP address. "ARP Spoofing includes building produced ARP ask for and answer bundles. By sending fashioned ARP answers, an objective PC could be persuaded to send outlines bound for PC A to rather go to PC B". This alluded to as ARP harming.

1.3. WEB Spoofing

Web or Hyperlink caricaturing furnishes casualties with false data. Web Spoofing is an assault that permits somebody to see and alter all site pages sent to a casualty's machine. They can watch any data that is gone into structures by the casualty. This can be of specific threat because of the way of data went into structures, for example, addresses, charge card numbers, financial balance numbers, and the passwords that get to these records.

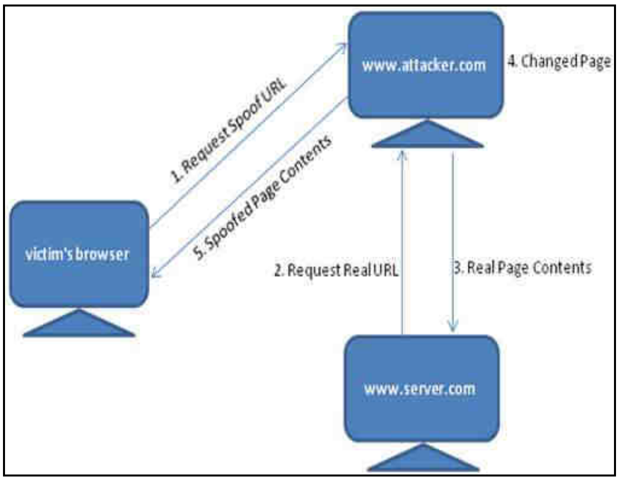


Fig.1. Working of WEB Spoofing

Revised Version Manuscript Received on July 24, 2017.

Sharda Dubey, Department of Computer Science and Engineering, RGPV, Lakshmi Narain College of Technology Excellence, Bhopal (M.P).India, E-mail: shardasharma1407@gmail.com

Prof. Sumit Gupta, Department of Computer Science and Engineering, RGPV, Lakshmi Narain College of Technology Excellence, Bhopal (M.P). India, E-mail: sumitgupta888@gmail.com

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

1.4. DNS Spoofing

A DNS parodying assault can be characterized as the effective inclusion of off base determination data by a host that has no power to give that data. It might be led utilizing various methods running from social building through to abuse of vulnerabilities inside the DNS server programming itself. Utilizing these methods, an assailant may embed IP address data that will divert a client from an authentic site or mail server to one under the aggressor's control – along these lines catching client data through regular man-in the-centre systems.

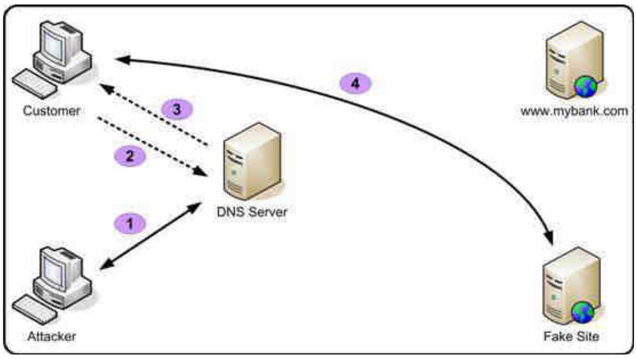


Fig.2. Working of DNS Spoofing

Be that as it may, validation requires extra infrastructural overhead and computational power connected with disseminating and keeping up cryptographic keys. An alternate approach is proposed, where in the physical property connected with every remote hub is utilized to evaluate the nearness of enemies in the remote system. This strategy is difficult to adulterate, and not dependent on cryptography as the reason for identifying parodying assaults. This approach empowers to identify and restrict different foes in the system, with high identification rate and negligible framework. In a huge scale remote system, different enemies may take on the appearance of a similar personality and work together to dispatch malignant assaults. In this way, the issue can be partitioned into 2 overlays, for example,

i. Recognize the nearness of ridiculing assaults,

ii. Decide the quantity of assailants, and limit numerous enemies.

The recognizable proof and restriction should be possible in the accompanying ways:

II. PRINCIPLE OF ARP SPOOFING

ARP convention is a free convention that interfaces two layers to be specific physical layer and system layer specifically to give the mapping amongst IP and MAC addresses. Among this different assaults e.g. ARP caricaturing assaults, man in center assault are debilitating the security of our grounds organize, which bringing on disarray inside the system. Irritated data of one system to another system illicitly. Presently different perspectives i.e. affecting system association, ARP satirizing assault [19, 20] is separated into two sorts:

i. Cheating gateway

By manufacturing a progression of IP address and the comparing mistake MAC address, and sent the produced ARP parcels to portal with certain recurrence, and afterward the right address data put away in doors be revived by the wrong address data. Therefore, the door will send the information to the wrong MAC address, so the typical host can't get the message and not get to the Internet. This ARP correspondence gives an opportunity to ARP swindle.

ii. Cheating the host of the internal network

The con artist fake door, and make the objective host invigorate its ARP store list, by along these lines the miscreant can caught the objective host' data which send to the passage. Thus ARP ridiculing permits an aggressor for DNS harming. DNS server gives back the IP address of the comparing DNS deliver to the customer program [18]. Presently this segment talk about standards of ARP ridiculing assault with two sorts, now next segment of this paper examine about results of different assault e.g. man in centre assault being performed over a system by an unauthentic client. The assignment of deciding the MAC (Media Access Control) deliver for the information to be sent on system is the obligation of ARP. ARP is utilized by the IP organize layer to guide IP locations to equipment addresses at information connect layer. ARP is working underneath the system layer as a part of the Open Systems Interconnection (OSI) connect layer, and is utilized when IP is utilized over the Ethernet.

2.1. How does ARP works:

At the point when an Ethernet casing is communicated starting with one machine then onto the next on LAN, the 48-bit MAC deliver is utilized to decide the interface for which the edge is intended to be predetermined. Deliver determination alludes to the procedure of powerfully finding a MAC address of a PC on a system. The convention gives a dynamic mapping between the two unique sorts of locations that are IP address and MAC address which is utilized by information interface layer. The procedure is changing since it happens consequently and is ordinarily not a worry of either the application client or the framework overseer. In a mutual Ethernet where has utilize the TCP/IP suite for correspondence, IP bundles should be epitomized in Ethernet outlines before they can be transmitted on to the wire.

There is a coordinated mapping between the arrangement of IP locations and the arrangement of Ethernet locations. Prior to the bundle can be exemplified in an Ethernet casing, the host sending the parcel needs the beneficiary's MAC address. Along these lines, ARP is utilized to discover the goal MAC address utilizing the IP address.

ARP does not keep up the conditions of its own and subsequently does not check whether the up and coming arp answer was really asked for or not, before upgrading the relating blending in the arp reserve of the framework. In this way, the assailant sends the sham answers to the imparting frameworks, along these lines rolling out the improvements positive to aggressor, in the matching of IP and MAC addresses. By doing this the data begins experiencing the aggressor's machine, without coming into notice of genuine hosts. Keeping in mind the end goal to minimize the quantity of ARP asks for that are being communicate, working frameworks keep up a reserve of ARP answers from various hosts. At the point when a host gets any ARP answer, it will regularly redesign its ARP reserve with the new IP/MAC affiliation passage.

Since ARP is known to be stateless convention, most working frameworks for the most part will overhaul their reserve if an answer is gotten, paying little heed to truth whether they conveyed any real demand or not.

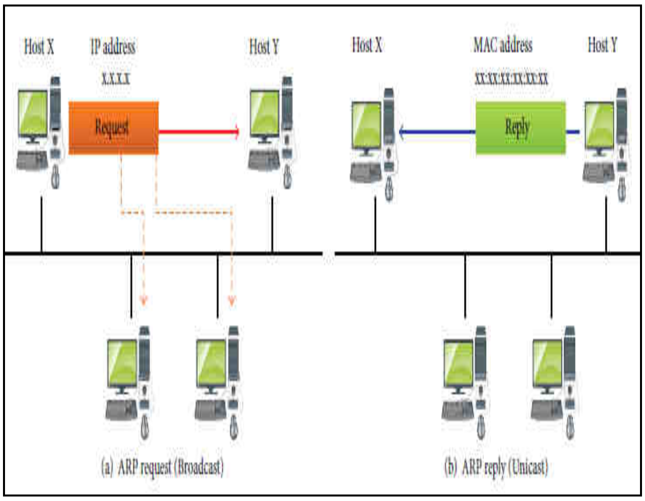


Figure 1: ARP request/reply protocol.

2.2. ARP Spoofing

ARP spoofing is mostly development of manufactured ARP answers. At the point when a produced ARP answer is sent, an objective PC could be effortlessly sought after to send outlines implied for Host A to rather go to Host B. In the event that done appropriately, Host A will have no clue that any such diverting of information has occurred. The way toward upgrading an objective PC's ARP store with a produced section is alluded to as "harming". The consequence of ARP reserve harming is that the IP activity proposed for one host is redirected to an alternate host. There are a wide range of sort of assaults that could be actualized to harm the separate arp stores of two imparting gadgets. These resemble man-in-the-center assault, sniffing, cloning, association seize, disavowal of administration, savvy IP satirizing and so forth. Scrambled associations are likewise not secure. Such assaults can likewise be performed on SSL(Secure Socket Layer) moreover. It has additionally turned out to be simple because of simple accessibility of various adventures on the web and that too are free of cost.

ARP Spoofing is a hacking procedure to send fake ARP ask for or ARP answer, ARP caricaturing issue originates from the way the ARP convention works [5]. Since the ARP convention is a stateless convention that gets and forms ARP answers without issuing ARP ask for [6], the ARP store can be contaminated with records that contain wrong mappings of IP-MAC addresses. ARP mocking can be utilized to dispatch one of two diverse assault classes [7]: Denial of Service (DoS) assaults or Man in the Middle (MITM) assaults.

A few arrangements have been proposed to moderate the ARP parodying, yet each has its restrictions [7]. The arrangements have been ordered into five unique classes [8]:

i. Changing ARP utilizing cryptographic methods

These arrangements add some cryptographic components to the ARP convention, yet won't be good with the standard ARP and influence the convention execution.

ii. Portion based fixing -

The strategy adds a fix to the working framework bit to anticipate ARP parodying assaults, however the issue is that not every working framework can be fixed and it might get to be distinctly contrary with the standard ARP convention.

iii. Securing switch Ports-

Utilize the switch port security or Dynamic ARP review (DAI) alternative to avert ARP caricaturing. However its capacity of anticipating ARP caricaturing effortlessly, the cost of executing such arrangement may not be adequate by the greater part of the associations.

iv. ARP parody recognition and insurance programming

Projects or apparatuses created to avert ARP parodying assaults, yet the exploratory outcomes have appeared there insufficiency in security.

v. Physically designing static ARP sections

The most fundamental and viable approach to avoid ARP satirizing [1] [6] [9] is including static ARP passages at every host. However this arrangement can't be effectively overseen and can't scale well uniquely in associations that have vast number of clients and require a substantial workload on the system chairman.

III. BACKGROUND AND RELATED WORK

As specified beforehand, arrangements endeavouring to anticipate ARP mocking assault utilizing the static ARP store passages are exceptionally proficient. However this class of arrangements has some real issues [7] [8]: (1) overhead required for manual design of static sections, (2) Limited versatility for expansive systems, and (3) Ability to work in static and DHCP based systems.

In the accompanying, we will overview a few strategies having a place with this classification alongside their disadvantages.

The DAPS (Dynamic ARP parody Protection System) method recommended in [8] is an answer for ARP satirizing that snoops DHCP parcels and utilize them as immunizations. However this method doesn't scale well for those systems that utilization static IP tending to plot furthermore antibodies will be invalid if DHCP starvation assault happens.

In [12], the NIDPS (Network Intrusion Detection and Prevention System) strategy is proposed have a server gathering IP-MAC mappings from clients utilizing little specialists. These mappings will be then utilized as static ARP passages to revise any wrong mapping identified. Nonetheless, specialists aren't verified to the server. Besides, it distinguishes just assaults from its LAN section. Likewise, the server looks at each bundle going in or out the LAN portion. At long last, it sits tight for the assault to happen and after that attempt to understand it.

Xiangning et al. [13] has proposed a method that grows the grunt pre-processors modules by including an ARP recognition module. The proposed procedure doesn't scale well in expansive systems because of the need of manual setup of the static mappings at the server. It likewise doesn't work in DHCP based systems.

An answer for ARP caricaturing utilizing a server is proposed as a part of [14]. The server will get mappings for the system clients from the DHCP server. It answers additionally to ARP asks. Sadly, this arrangement works just in DHCP systems. Additionally, It is not good with the standard ARP.

In addition, if DHCP starvation happens, all the server data will be invalid.

Ai-zeng Qian [15] proposed a system to avert ARP parodying by utilizing static ARP sections yet the method still doesn't work with element systems utilizing DHCP tending to. The executive must allocate all IP addresses alongside their MAC to the server so it will be not noticeable for expansive scale arrange.

A technique is recommended in [16] to tackle ARP parodying issue utilizing grunt IDS and static ARP passages. However, despite everything it needs the executive to include the static mappings physically. Additionally, it works just in static systems.

IV. PROPOSED METHOD

The proposed procedure is a customer server convention that anticipates ARP mocking via naturally designing static ARP sections. The convention works in both static, DHCP, remote systems.

Also, it can work in extensive scale systems with no overhead on the chairman. Furthermore, the strategy doesn't require unique equipment to be conveyed, as any host can act as ARP server.

The convention proposed characterizes three unique messages:

1. Enroll Message: is unicast message sent from the customer to the server. It contains its IP and MAC address. Likewise it incorporates a hashed verification key.
2. Redesign Message: is a communicate notice message sent from the server to all clients in the system showing that another client has entered the system. It additionally contains the IP and MAC address of that new client.
3. Enlist Response Message: is a unicast message sent from the server to the new client. It contains all static ARP passages of clients effectively enlisted at the server.

Algorithm-1: Client Algorithm

The convention additionally characterizes two unique elements:

a) ARP Client: is programming introduced on client's machines. It satisfies the accompanying:

i. Naturally get the IP and MAC address of the client and utilize them to send enroll message to the server.

ii. Get overhaul and enroll reaction messages from the server.

iii. Check that upgrade or enroll reaction messages got are originating from a trusted server.

iv. Utilize the IP and MAC sets got in the overhaul or enroll reaction message to add static ARP passages to the client ARP store.

b) ARP Server: is a server programming that can be introduced on any gadget in the system. It can likewise be introduced on a committed server, and has the accompanying capacities:

i. Get enroll messages from the ARP customers.

ii. Check that the message is originating from a trusted client.

iii. Make utilization of the IP and MAC sets epitomized inside the enlist message to make a rundown of trusted clients in the system.

iv. Send communicate upgrade message to advise them that another client has gone to the system.

v. Send enroll reaction message to the new clients.

vi. Make the correct move with respect to clients who attempt to abuse the convention security rules.

Algorithm-2: Server Algorithm

The proposed convention characterizes two distinct calculations for the customer and server keeping in mind the end goal to keep the ARP mocking assault.

4.1. Client Algorithm

The client algorithm described in **Algorithm 1** adds static entry for the server in the client ARP cache to avoid the rogue server threat. Furthermore, it obtains the user IP and MAC address automatically to make the user has no opportunity to send fake information to the server.

The algorithm checks the source IP address of the received message to be sure that it is coming from the trusted server. It only accepts the IP and MAC addresses encapsulated in the message if the key is correct.

In order to work in networks where IP and MAC mappings are frequently changing, the algorithm searches for the MAC encapsulated in the message. If matched map is found, it will be changed to the new mapping. Otherwise a new mapping will be added.

Finally if any of the conditions are not met, the algorithm will discard the message and return to listen for another message from the server.

4.2. Server Algorithm

The server algorithm, described in **Algorithm 2**, listens to incoming register messages from the clients, checks the hash code to be sure that the message is coming from a trusted host. Users are given only three trials to send the correct hash code. If it fails to send the correct hash code within the three trials, the server will block this user. The blocking action depends on the addressing scheme being used, for networks, the MAC address of the user will be added to deny list. Hence, it will not be able to obtain IP configuration from the server again, for static networks, the server will prevent traffic from this user to reach the server by obstructing its IP address.

If the key is correct and the number of wrong trials doesn’t reach the threshold, the server will search its ARP cache for matching between MAC address encapsulated in the register message received and MAC address in ARP cache.

This gives the algorithm the ability to work with networks. In turn, it prevents an intruder having the hash code to spoof all ARP cache entries. As a matter of fact, it can only spoof one at a time.

If it tries to spoof another one the old spoofed entry will be deleted. User who has successfully registered at the server will receive a register response message contains the IP and MAC addresses of all successfully registered users to add them as static ARP entries. Moreover, all other users will receive an update message contains IP and MAC address of the new user to add it as a static entry in their ARP cache. Using the client and server algorithms, every user in the network will have its ARP cache filled with static ARP entries for all other users in the network. Hence, it will not suffer from the ARP spoofing problem again. And everything is done automatically without any overload on the administrator; this gives the algorithm a greater scalability.

4.3. Principle of Winpcap

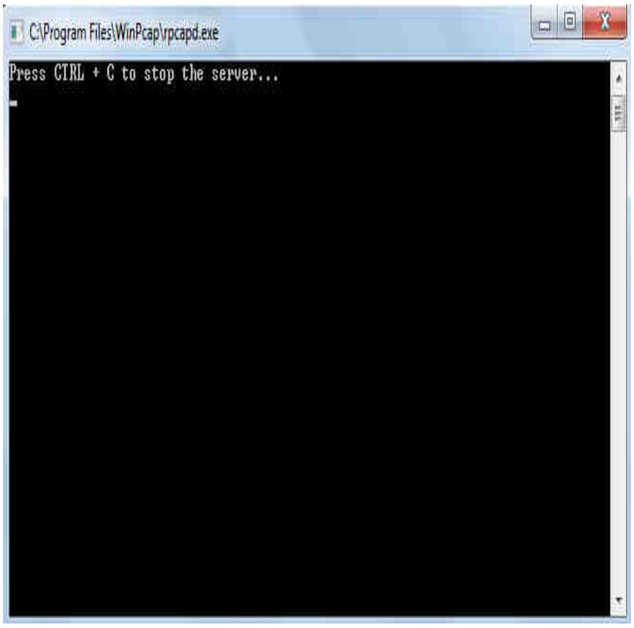
Generally winpcap (windows Packet capture) is a network layer access tool to access system under the windows platform, which provides the following functions:

a) To capture the raw datagram, including datagram sent/received by or to the hosts in the sharing network and as well as the exchange of between;

b) To filter some special datagram in accordance with the user defined rules before sent to the application process.

c) To send original datagram on the network.

d) To collect statistics in the network communication process.



C:\Program Files\WinPcap\rpcapd.exe

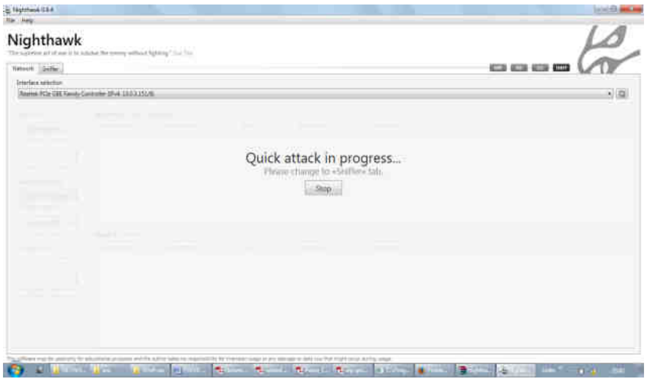
```
Press CTRL + C to stop the server...
```

Fig 4.1Initialization of Winpcap Services

Hence this section discusses various defence mechanisms against ARP spoofing attack using winpcap. Now next section discuss about network monitoring using sniffer tread (winpcap).

4.4. Nighthawk Attacker

Nighthawk is an experimental implementation of ARP/ND spoofing, password sniffing and simple SSL stripping for Windows. It requires WinPcap and .NET Framework 4 (Client profile) and works best on windows platform.



Nighthawk

Network | Sniffer

Interface selection

Quick attack in progress...

Please change to «Sniffer» tab.

Stop

Fig 4.2 Nighthawk Attacker for ARP Spoofing Attack

4.5. ARP Attack Detection and Prevention

We have implemented a ARP detection and prevention mechanism based on .NET framework.

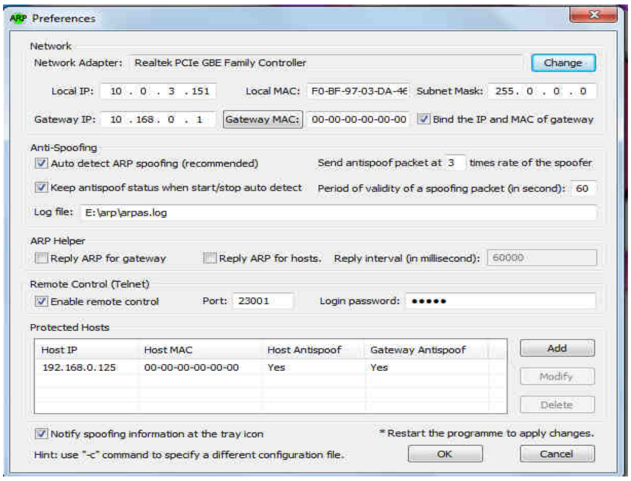
Detection-

Active checking of host-level: Another preventive measure of ARP deception detection is to arrange host to send ARP request packet about its own IP address while starting system or periodically [2,17]. If could receive another ARP response, report ARP deception to the host user or administrator.

b) Passive detection of host-level: Checking whether the target address matches with IP address of the local web application, we can know whether the message sent to own. If yes, we need to send an ARPresponse. Once the operating systems was interrupted, checking whether the sender's IP address correspondent with its own IP address, and if same, indicates that it is ARP deception [4,7].

c) Network-level detection: To detect network level through periodic polling. Through regular review of the ARP high-speed cache, it will be able to detect these correspondence changes between IP Address in high-speed cache of these machines and hardware address [1, 9].

d) Server-class detection: In order to establish its authenticity, when the server has received the ARP response, it will regenerate a RARP request from the MAC address given by the response message according to Reverse ARP (RARP), and, which asked the question: "If you are the owner of the MAC address, please reply to your IP address".



Preferences

Network

Network Adapter: Realtek PCIe GBE Family Controller [Change]

Local IP: 10 . 0 . 3 . 151 Local MAC: F0-BF-97-03-DA-4€ Subnet Mask: 255 . 0 . 0 . 0

Gateway IP: 10 . 168 . 0 . 1 [Gateway MAC:] 00-00-00-00-00-00 ☑ Bind the IP and MAC of gateway

Anti-Spoofing

☑ Auto detect ARP spoofing (recommended) Send antispoof packet at 3 times rate of the spoofer

☑ Keep antispoof status when start/stop auto detect Period of validity of a spoofing packet (in second): 60

Log file: E:\arp\arpas.log

ARP Helper

□ Reply ARP for gateway □ Reply ARP for hosts. Reply interval (in millisecond): 60000

Remote Control (Telnet)

☑ Enable remote control Port: 23001 Login password: •••••

Protected Hosts

Host IP	Host MAC	Host Antispoof	Gateway Antispoof
192.168.0.125	00-00-00-00-00-00	Yes	Yes

[Add] [Modify] [Delete]

☑ Notify spoofing information at the tray icon *Restart the programme to apply changes.

Hint: use "-c" command to specify a different configuration file. [OK] [Cancel]

Fig 4.3 ARP Spoofing Identification and Prevention System

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Prevention-

According to ARP response packet theory, relevant source address corresponding to its target MAC address in these two protocols should be the same As per the principle of actualization of TCP/IP protocol stack, upper layer protocol sends data packet to its corresponding lower layer protocol and the lower layer seals that data packet as the data of his own; when receiving data packets, every layer only handles protocol of its own. After handling this, it hands the data parts to upper layer protocol. But now during this process, cross-layer verification cannot be done. Now check relevant items in data packet when system sends or receives ARP response data packet over a network.

So whether relevant source MAC address and target MAC address match or not to verified in the ARP data packet; link layer head information. Now if it does not match the information of host computer, directly block data packet and prompt the user. This check can effectively prevent users from other users' ARP virus attack and avoid users ARP virus attacking other users. This ARP communication provides a chance for ARP cheat [12].Check rules are as follows:

a) ARP response packet sent: Check whether source MAC address in ARP packet totally matches displayed destination MAC address in link layer head information. Discard it, if not; check whether destination IP address in ARP packet totally matches destination MAC address in link layer head information [12,15]. If not, Directly discard it; check whether source MAC address in ARP data packet is the MAC address of this host, if not, discard it directly; check whether source IP address is the IP address of host, if not, directly discard it. On the basis of Host blocking attack, Host sends ARP response data packet to gateway and informs the gateway the address avoiding gateway being cheated [2].

b) The ARP response packet received*:* check whether source MAC address in ARP packet totally matches source MAC address in link layer head information [8]. Discard it, if not; check whether destination MAC address in ARP packet totally matches destination MAC address in link layer head information. If not, Directly discard it; check whether destination IP address is the IP address of host, if not, directly discard it.

Result Comparison:

The comparison between the proposed method and the existing systems is shown in the table below:-

Table 4.1: Comparisons of Existing and Proposed System

S. No.	Comparison Criteria	Proposed System	Previous Systems
1	Cryptographic Security	Yes	No
2	Secure Layer Implementation	Yes	No
3	Multi-Platform Architecture	Yes (Windows, Android)	Single Platform Architecture
4	Dynamic Scanning of Attacks	Yes	No
5	Higher Bits Security Mechanism	SSL-128 Bits	Not Implemented

V. CONCLUSION

In this paper, a solution to the problem of ARP spoofing has been proposed; the arrangement is a programmed and adaptable strategy for designing static ARP sections rather than physically arranging. The arrangement tackles the principle issues identified with this class of arrangements Usage of static passages, computerization, versatility, sensibility, counteractive action, and cost are the fundamental components of the proposed strategy. The proposed strategy has characterized two separate calculations, one for the customer, and the other for the server. Trial assessment was led on the LAN arrange. The reaction time metric is utilized to assess the framework. Likewise unique sorts of movement workloads were utilized amid the measuring the reaction to demonstrate the impact volume of activity on the reaction time values. The outcomes demonstrate how quick and precise the proposed calculation is since any new client needs short of what one millisecond to be sheltered from ARP issue for substantial workloads.

REFERENCES

1. Yafeng Xu and Shuwen Sun , “The study on the college campus network ARP deception defense," 2010 2nd International Conference on Future Computer and Communication (ICFCC), 3(1), pp. 465-467, May 2010.
2. R. W. Stevens. TCP/IP Illustrated, Volume 1: The Protocols. Addison–Wesley Professional Computing Series, January 1994.
3. D. Plummer. An Ethernet address resolution protocol, Nov. 1982. RFC 826.
4. Mohamed Al-Hemairy, Saad Amin, and Zouheir Trabelsi, “Towards More Sophisticated ARP Spoofing Detection/ Prevention Systems in LAN Networks," 2009 International Conference on the Current Trends in Information Technology (CTIT), pp.1-6, December 2009.
5. Hu Xiangdong, Gao Zhan, and Li Wei "Research on the Switched LAN Monitor Mechanism and its Implementation Method based on ARP spoofing," International Conference on Management and Service Science.(MASS '09), pp. 1-4, Sept. 2009.
6. Marco Antônio Carnut and João J. C. Gondim, "ARP spoofing detection on switched ethernet networks: a feasibility study," 5th Symposium on Security in Informatics held at Brazilian Air Force Technology Institute, November 2003.
7. Cristina L. Abad and Rafael I. Bonilla, "An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks," 27th International Conference on Distributed Computing Systems Workshops, 2007. (ICDCSW '07), page(s): 60, June 2007.
8. Somnuk Puangpronpitag and Narongrit Masusai, “An Efficient and Feasible Solution to ARP Spoof Problem," 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2009. (ECTI-CON 2009), 3(1), pp. 910—913, May 2009.
9. S. Whalen, "An introduction to ARP spoofing," 2600: The Hacker Quarterly, 18(3), 2001, (accessed 13-9-2012). [Online].:http://servv89pn0aj.sn.sourcedns.com/gbpprorg/2600/arp spoofing intro.pdf
10. http://technet.microsoft.com/en-us/library/cc958841.aspx. ARP Cache, (accessed May 8, 2013).
11. Zouheir Trabelsi and Wassim El-Hajj, "Preventing ARP Attacks using a Fuzzy-Based Stateful ARP Cache," IEEE International Conference on Communications.(ICC '07), pp. 1355 -1360, June 2007.
12. Dr. S. G. Bhirud and Vijay Katkar, "Light Weight Approach for IP-ARP Spoofing Detection and Prevention," 2011 Second Asian Himalayas International Conference on Internet (AH-ICI), page(s):1-5, November 2011.
13. Xiangning HOU, Zhiping JIANG, and Xinli TIAN, "The detection and prevention for ARP Spoofing based on Snort," 2010 I
14. Andre P. Ortega, Xavier E. Marcos, Luis D. Chiang and Cristina L. Abad, " Preventing ARP cache poisoning attacks:

A proof of concept using OpenWrt," Latin American Network Operations and Management Symposium. (LANOMS), pp. 1-9, Oct. 2009.

15. Ai-zeng Qian, "The Automatic Prevention and Control Research of ARP Deception and Implementation," 2009 WRI World Congress on Computer Science and Information Engineering, , 2(1), pp. 555-558, April 2009.
16. Boughrara, A.; Mammar, S., "Implementation of a SNORT's output Plug-In in reaction to ARP Spoofing's attack," 2012 6th International Conference on Sciences of Electronics Technologies of Information and Telecommunications (SETIT), pp.643,647, 21-24 March 2012
17. R. K. Jain, “The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling,” Prince Hall, April 1991.
18. Ferdous A. Barbhuiya, Santosh Biswas, NeminathHubballi,”A Host Based DES Approach for Detecting ARPSpoofing”, IEEE, 2011.
19. TAO Jun, LIN Hui, “IDSV: Intrusion Detection Algorithm based on Statistics Variance Method in User Transmission Behavior”, International Conference on Computational and Information Sciences, 2010.
20. JanghunBae, SeongjinAhn, “Network Access Control and Management using ARP Spoofing in Various Windows Environment”, IEEE, 2011.