12th International Conference on Recent Innovations in Science, Engineering and Management
Sri Venkateswara College of Engineering & Technology,Etcherla, Srikakulam (ICRISEM'18)
17th February 2018 www.conferenceworld.in ISBN: 978-93-87793-01-9

ARP SPOOFING Attack in Real Time Environment

Ronak Sharma[1], Dr. Rashmi Popli[2]

[1]*Deptt. of Computer Engineering, YMCA University of Science and Technology, Haryana (INDIA)*

[2]*Deptt. of Computer Engineering, YMCA University of Science and Technology, Haryana (INDIA)*

ABSTRACT

Communication over network is very important in today's life. Due to increase of communication over networks the cyber attacks are also increasing. One of the most common attacks is Man In The Middle attack through ARP poisoning. ARP is a stateless or insecure protocol. MITM is very dangerous because it provides the interface to attacker to monitor the network traffic and copy the network traffic data. An attacker can break the integrity of data that is sent over the network. ARP cache updates when a new device connects or disconnects over the network. This paper presents the algorithm to prevent network from the ARP poisoning attacks.

Keywords: - ARP poisoning / spoofing, MAC, Man-in-the-Middle Attacks, Address resolution protocol, ettercap

I. INTRODUCTION

Address resolution protocol (ARP) is the basic component of the network. It is a protocol used by the data link layer to map IP address to MAC address.[1] This protocol stores the binding of the MAC address to IP address in the ARP cache.

In ARP table the IP address of a host is given to find its MAC address. Now, the source node broadcasts the ARP request packets which ask about the MAC address of the IP address given by the owner. This request is received by all devices which lies on the LAN or WLAN network. The device that owns this IP address replies with its MAC address. The ARP reply is unicast while the ARP request is broadcast. When the host receives the ARP reply, usually the IP/MAC addresses mapping are saved as entries in a table called the "ARP cache table". This table is used as a cache where the node will send an ARP request only if the ARP table does not contain the IP/MAC mapping. ARP's weakness lies in the fact that it is a stateless protocol, i.e., it accepts ARP replies without having to send an ARP request.

1. ARP Spoofing

ARP spoofing attack exploits this vulnerability by sending ARP reply messages that contain the IP address of a network resource, such as the default gateway or a DNS server, to a victim machine. The attacker replaces the MAC address of the corresponding network resource with his machine's MAC address. The victim's machine that receives the spoofed ARP replies cannot distinguish them from legitimate ones. Moreover, the ARP tables usually use the result of the last ARP reply only. The attacker then takes the role of man in the middle; any traffic directed to the legitimate resource is sent through the attacking system. The attacker reads the packet

looking for sensitive data; it may modify that data, and then passes it to the designated destination. As this attack occurs on the lower levels of the TCP/IP protocol stack, the end-user is unaware to the attack occurrence. Furthermore, ARP spoofing is also capable of performing denial of service (DoS) attacks if the attacker drops the packets instead of passing them. This causes the victim's machine to be denied from service from network resources. There exist some tools which simplify generating ARP spoofing attack, like Ettercap which is developed by Ornaghi and Valleri [2] and another tool developed by Wagner [3].

II. LITERATURE SURVEY

Gouda, M.G. and Huang, C-T A Secure Address Resolution Protocol. Computer Networks, 41, 57-71 [2003] The authors assumed that there is a central server which maintains the database of the static entries of the MAC addresses of all the devices which lies on the LAN network. This approach does not work for the dynamic networks in which many nodes join and leave the network daily, where each node should be registered in the database before it can work. Also, the attacker can still generate the attack on the database. [4]

Issac, B. Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks. International Journal of Network Security, 8, 107-118 [2009] The authors proposed a unicast ARP request instead of the broadcast 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. However, the DHCP is at the application layer. Also, the DHCP may work only for dynamic IP addresses; it does not succeed for static IP addressing.[5]

Lootah, W., Enck, W. and McDaniel, P. TARP: Ticket-Based Address Resolution Protocol. Computer Networks, 51, 4322-4337 [2007] A Ticket-based Address Resolution Protocol (TARP) was proposed by Lootah, W., Enck, W. and McDaniel. TARP implements security by distributing centrally issued secure IP/MAC ticket with the help of the DHCP. These tickets are given to clients as they join the network and are subsequently distributed through existing ARP messages. These tickets include asymmetric digital signature, which has a considerable overhead in generating the public/private key pairs, and consumes more time. It is also not suitable for the dynamic networks where many new computers join the network frequently.[6]

Venkatramulu, S. and Guru Rao, C.V. Various Solutions for Address Resolution Protocol Spoofing Attacks International Journal of Scientific and Research Publications, 3, 2250-3153 [2013] The authors mentioned several resolutions and solutions to solve the ARP spoof problem and grouped them into cryptographic approaches, kernel-based patch, host-based approaches, port security on switch, manually configuration of static ARP entries, ARP spoof detection & protection software, server-based approaches and ASA (anti-ARP spoofing agent) software.[7]

Hong, S., Oh, M. and Lee, S. Design and Implementation of an Efficient Defense Mechanism against ARP Spoofing Attacks Using AES and RSA. Mathematical and Computer Modelling, 58, 254-260. [2013] The authors introduced a system that consists of a MAC-Agent and a Client-Agent. The MAC-Agent makes a reliable ARP table and sends the data to the Client-Agent, which prevents the host from using ARP. Instead, the Client-Agent receives the reliable ARP table information from the MAC-Agent and updates the ARP table information as static type. However, this solution requires cryptographic authentication techniques which are not

available at the level of the data link layer. Additionally, this approach requires modifying the existing ARP protocol which is unpractical.[8]

Ramachandran, V. and Nandi, S. Detecting ARP Spoofing: An Active Technique. In: Jajodia, S. and Mazumdar, C., Eds., Information Systems Security, Springer, Berlin, Heidelberg, 239-250 [2005]

The authors introduced a technique that includes collecting and analyzing the ARP packets, and then injecting ICMP echo request packets to probe for malicious host according to its response packets. However, this approach can be detected by the attacker and can be easily fooled.[9]

III. PROPOSED PROBLEM

ARP is a stateless protocol. The source node requests for MAC address by broadcasting the ARP request to all the devices which lies on the networks. Each device gets the ARP request but only that device will reply with ARP replies which have an IP address that the source node wants. ARP buffers the response without any authentication mechanism. Source node wills dynamic update the cache directly. This situation is vulnerable to spoofing attack. By the use of open source ettercap tool the ARP spoof is possible [2].

In this paper, Arp Spoof attacks are implemented with the help of ettercap and the research work also suggests that the prevention technique which is deployed on the client machine warns them about the attack.

In Figure 1, the router is gateway to route traffic from the user. The user requests for the MAC address of the router. So the ARP request broadcasts to all the devices, the attacker replies to ARP Request and provides its own MAC address to the user.

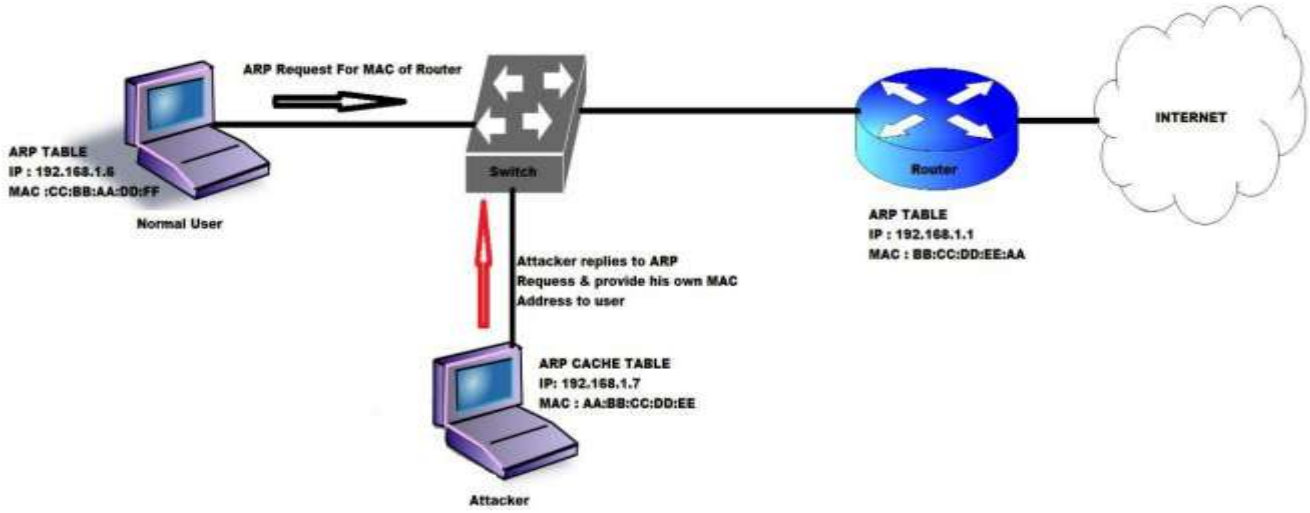

Fig. 1 ARP Request and ARP Reply

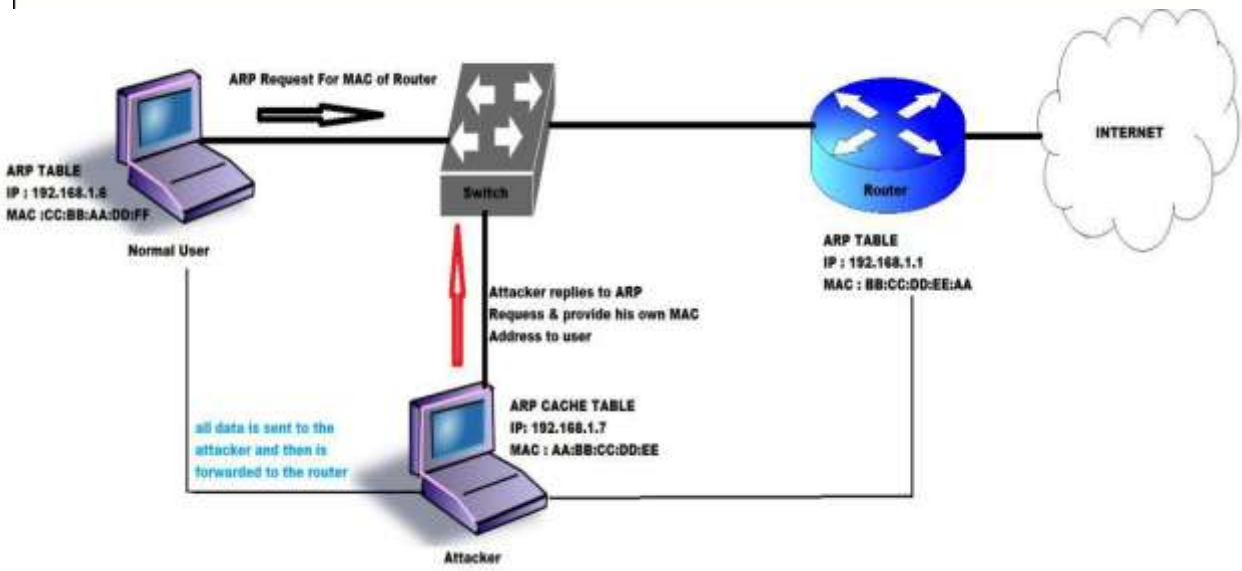

Fig. 2 ARP spoofing (MITM Attack)

In Figure 2, now the attacker mac address acts as a router mac address. The data from the user is sent via attacker device and then it passes through gateway.

IV.DETECTION AND PREVENTION

For detection purpose it continuously searches for the redundant MAC address in the ARP cache table of a node, if any redundant mac address found in the ARP cache table then the ARP spoof attack is going otherwise not.

In fig 3, all the systems stored mac address of each node in the ARP table. Now, after a certain interval of time all the systems scan redundant Mac address in own ARP tables. After continuously scanning the A system sends the acknowledgement have a redundant mac address so the system A have one actual mac address and other is spoofing mac address.

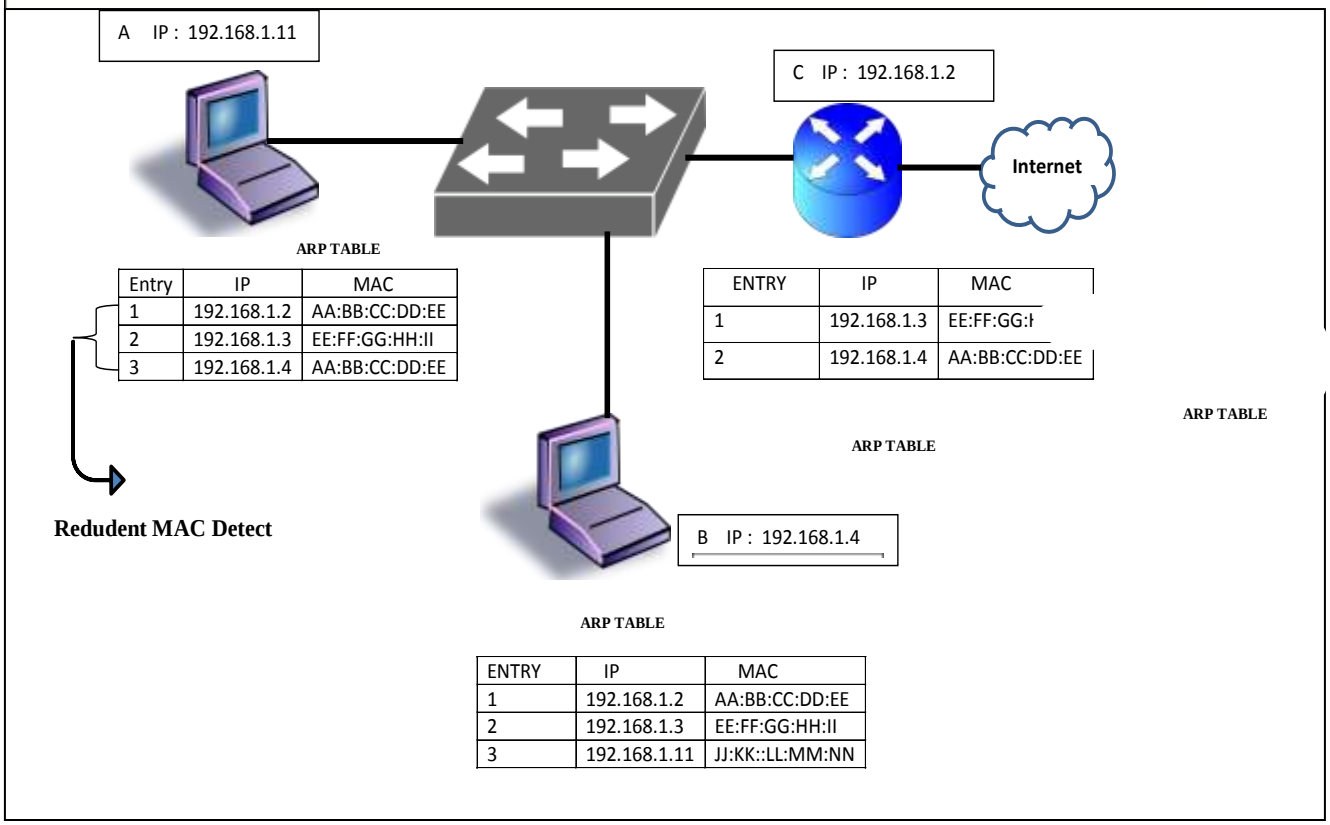

Fig. 3 Detection of ARP spoofing Attack

For prevention, after found of any redundant mac address. Block or discard the entry of that mac address which is of attacker from the ARP cache table.

So in fig 4, System a blocks or discard the attacker mac address.

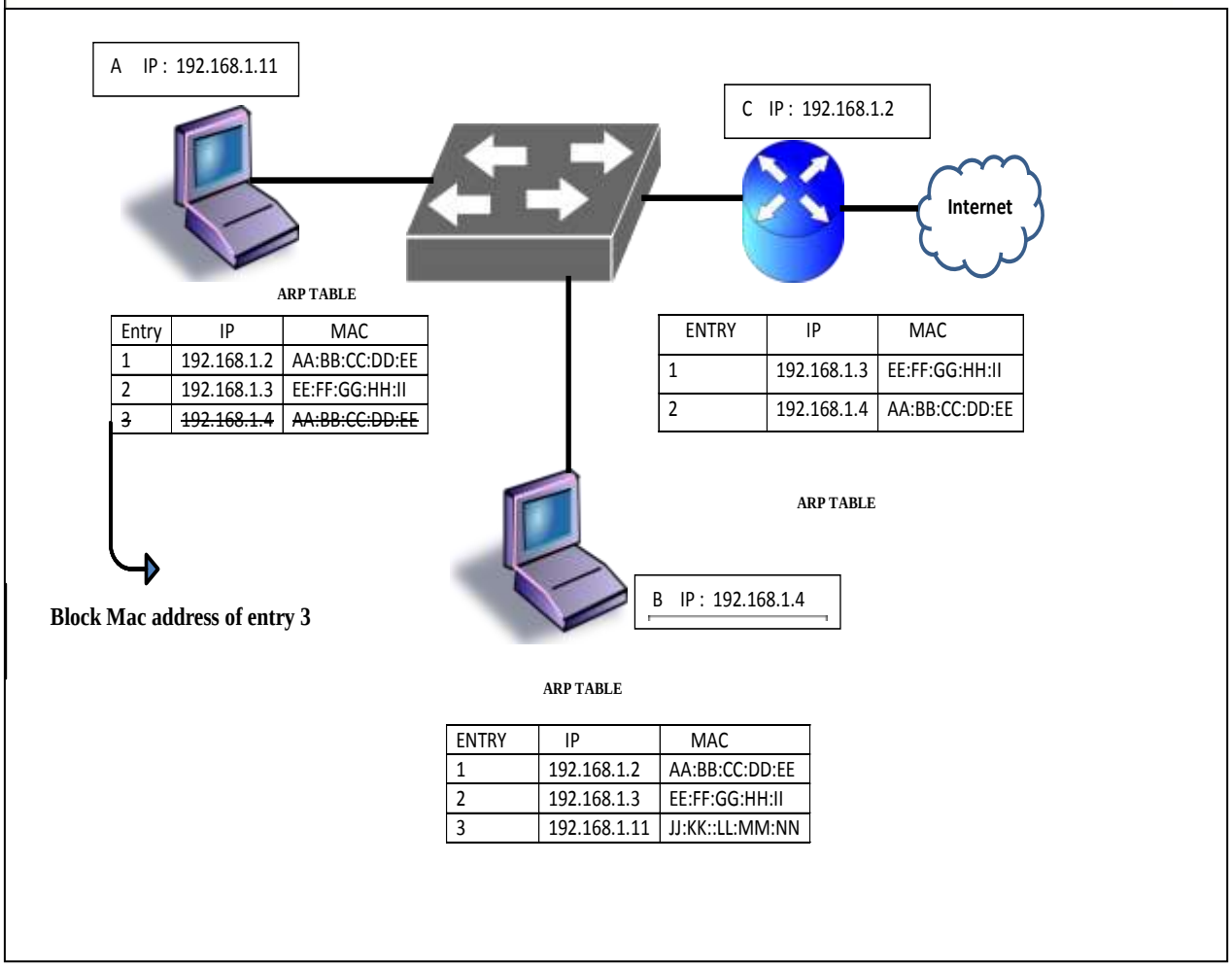

Fig. 4Prevention from ARP Spoofing Attack

This method is easy to implement and efficient to detect and prevent the ARP Spoofing attack.

IV. CONCLUSION

ARP protocol is a stateless protocol has very dangerous consequences. An attacker could modify the connection of the users, steal their information, and even redirect their traffic to different websites than the ones they requested. Network administrators should become more aware of these attacks and take countermeasures against them. Users should also become more aware of them and use security solutions to prevent getting their data stolen.

In this paper, after explaining the vulnerabilities of the ARP protocol we discuss about the detection and prevention from the ARP spoofing.

REFERENCES

[1]. Plummer, D.C. (1982) An Ethernet Address Resolution Protocol. RFC 826

[2]. Ornaghi, A. and Valleri, M. (2004) A Multipurpose Sniffer for Switched LANs. http://ettercap.sf.net

[3]. Wagner, R. (2001) Address Resolution Protocol Spoofing and Man in the Middle Attacks. SANS Institute. https://www.sans.org/reading-room/whitepapers/threats/address-resolution-protocol-spoofing-man-in-the-middle-attac ks-474

[4]. Gouda, M.G. and Huang, C-T. (2003) A Secure Address Resolution Protocol. Computer Networks, 41, 57-71.http://dx.doi.org/10.1016/S1389-1286(02)00326-2

[5] Issac, B. (2009) Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks. International Journal of Network Security, 8, 107-118.

[6] Lootah, W., Enck, W. and McDaniel, P. (2007) TARP: Ticket-Based Address Resolution Protocol. Computer Networks, 51, 4322-4337. http://dx.doi.org/10.1016/j.comnet.2007.05.007

[7] Venkatramulu, S. and Guru Rao, C.V. (2013) Various Solutions for Address Resolution Protocol Spoofing Attacks. International Journal of Scientific and Research Publications, 3, 2250-3153.

[8] Hong, S., Oh, M. and Lee, S. (2013) Design and Implementation of an Efficient Defense Mechanism against ARP Spoofing Attacks Using AES and RSA. Mathematical and Computer Modelling, 58, 254-260. http://dx.doi.org/10.1016/j.mcm.2012.08.008

[9] Ramachandran, V. and Nandi, S. (2005) Detecting ARP Spoofing: An Active Technique. In: Jajodia, S. and Mazumdar, C., Eds., Information Systems Security, Springer, Berlin, Heidelberg, 239-250. http://dx.doi.org/10.1007/11593980_18

[10] Pansa, D. and Chomsiri, T. (2008) Architecture and Protocols for Secure Land by Using a Software-Level Certificate and Cancellation of ARP Protocol. ICCIT'08 3rd International Conference on Convergence and Hybrid Information Technology, 2, 21-26.

[11] Jinhua, G. and Kejian, X. (2013) ARP Spoofing Detection Algorithm Using ICMP Protocol. International Conference on Computer Communication and Informatics, Coimbatore, 4-6 January 2013, 1-6. http://dx.doi.org/10.1109/iccci.2013.6466290