IJCTA, 9(41), 2016, pp. 131-137 ISSN: 0974-5572
© International Science Press

A Detailed Survey of ARP Poisoning Detection and Mitigation Techniques

Jaideep Singh*, Sandeep Dhariwal and Rajeev Kumar*****

ABSTRACT

Among various network exploits that exist today in the ever progressing age of Information Technology and Communications, MiTM attacks have been identified as the critical assaults being used for breaching client security. These assaults are primarily encountered in wireless networks in the form of ARP Poisoning attacks. Thus it becomes important to construct systems that support protection of wireless networks from such attacks. This paper essentially discusses procedures that have been devised to protect the Wireless Networks against ARP Spoofing attacks and brings out Pros and Cons of most dominant techniques against set parameters. A comparative analysis of different techniques has been made as a measure of overall effectiveness to curb the ARP attacks.

Keywords: Address Resolution Protocol; ARP Cache; ARP Poisoning Assault; Spoofing detection; Attack prevention

1. INTRODUCTION

Each client accessing the internet in a wireless network posses two different addresses called hardware address (MAC address) and the IP address. The functionalities above the layer four use a mechanism of logical addresses to determine the receiving host by means of IP address. All nodes in a local 802.11 b/g/n network have a different IP address that are independent of respective MAC addresses. The packets are encased into frames and are delivered across the links based on hardware addresses. ARP protocol is used to develop a linkage between the IP address and consequent MAC address. Whenever any device on a subnet wishes to exchange data with other device, first of all ARP cache of the sending device is checked. If the MAC address of the receiving node is found present in the ARP cache, that address is utilised for sending the data through. However, if the address is not there in the local cache, an ARP request is broadcasted on the network enquiring which machine has the required IP address. Each receiving client machine compares the IP address in the received ARP packet to its own IP address. Those client machines whose IP address do not match with the required IP in the ARP packet dispose the packet off without any further action. The device for which the required IP address in ARP packet matches with own IP address, an ARP reply message is composed. The destination device sends a unicast ARP reply containing its IP and MAC address back to the sender. The source machine in turn processes the ARP reply and updates itself with the required MAC address and IP address it receives from the reply message. [2]

The major drawback of ARP is that there is no foolproof mechanism for validating ARP replies in the network. The reply packets are always at a risk of being spoofed by some malicious hosts on the same subnet. The method of association of MAC address of one client with the IP address of another client is known as ARP Spoofing. A number of currently operational detection systems help to detect such false bindings. An extensive survey, thus has been conducted on the different detection and mitigation strategies.

* ECE Department LPU Phagwara, *Email: jaideepsinghbawa@gmail.com*

** ECE Department LPU Phagwara, *Email: sandeep.19381@gmail.com*

*** ECE Department LPU Phagwara, *Email: rajeev.20340@lpu.co.in*

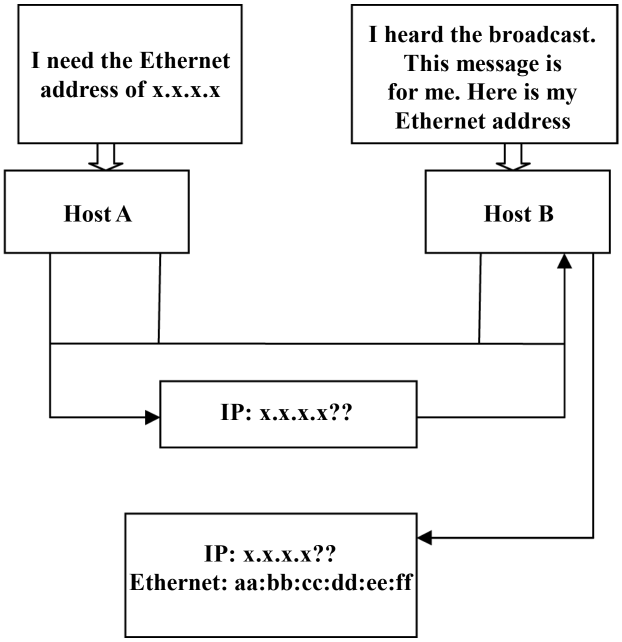
I need the Ethernet address of x.x.x.x
I heard the broadcast. This message is for me. Here is my Ethernet address
Host A
Host B
IP: x.x.x.x??
IP: x.x.x.x??
Ethernet: aa:bb:cc:dd:ee:ff

Figure 1: ARP Mechanism

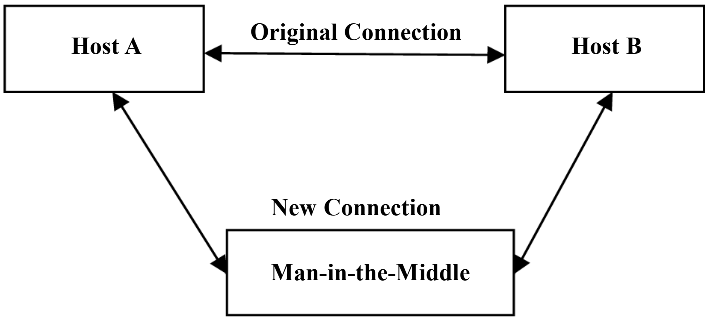

Figure 2: Scenario of ARP Poisoning

The strengths and weaknesses of investigated strategies after subsequent analysis have been discussed in Section II .

Remaining paper has been organised as follows: section II demonstrates the ARP attacks in detail, section III reports the diversity of schemes that are currently available to deal with ARP attacks, IV provides illustrations about the open issues and future scope and section V sums up the paper.

2. ARP ATTACK UTILISATIONS

The very basics of ARP Poisoning includes making up of fake ARP replies. By transmitting such replies, a receiver can definitely be persuaded to send data in return to a wrong host without any realization that the data is being sent to a fraudulent host. The practice of customizing a computer machine's ARP cache table with a spoofed entry is hereby introduced as poisoning. [3]

There are numerous other attacks which can be thought of as an extension to ARP Poisoning attacks including the following.

2.1. MITM Attacks

Whenever there is a Man in the Middle attack, a mischievous client forces his machine amid the transmission route of two communicators. Later on, sniffing is enforced by using a packet sniffer. The machine of the unethical client forwards traffic among the innocent clients to ensure that communication does not seem distroted.

2.2. DoS attacks

The rejection of frames is caused due to update of ARP entries with different supposed MAC addresses. The authentications can be sent in a bulk manner to all machines on the network in order to bring about a denial of service condition. This is an additional issue after MiM attacks, as target machines send frames to the attacker's MAC address even after the attack has virtullay stopped.[2]

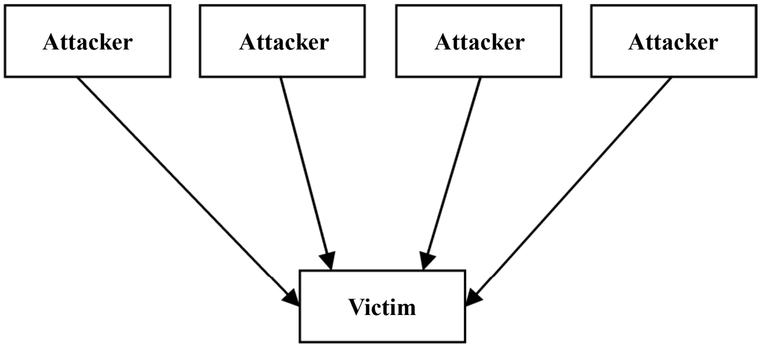

Figure 3: DoS Attack

2.3. Hijacking

Man in Middle attack can also be used to hijack sessions which can hand over the complete control of a client session to the attacker. The attacker can make necessary manipulations by hijacking the session and also send spoofed replies anywhere in the world. Impersonation can be achieved using this technique and the messages be altered as per the convenience of the attacker[3].

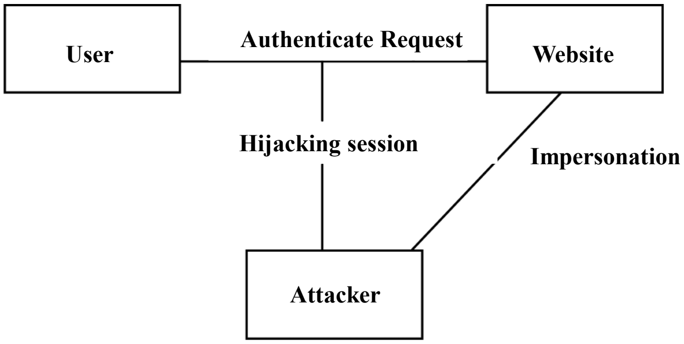

Figure 4: Connection Hijacking

2.4. Cloning

Every NIC that has been manufactured by a firm to be fitted into a smart device has a unique MAC address which serves as an identifier over the internet. These are not meant to be changed. With the ever changing new technology and open source tool formations, MAC addresses have become vulnerable to get changed. Linux, the most secure operating system allows the MAC to be altered without the use of much refined techniques, but by a single command in root terminal.

3. PREVENTION METHODS (DETECTION AND MITIGATION)

In a quest to assure unabated and protected communications, of such arduous situations must be averted. Not having proper defense may establish complete stealth while witnessing an ARP attack for the attacker.

After all the research conducted in this area, no universal defense mechanism has been reported against the attacks. A comprehensive survey has been presented next on the various techniques and advantages and disadvantages have been analyzed of each method used to detect and mitigate these attacks after a detailed analysis. As a part of initial survey, a brief study of principal techniques had been presented in a survey paper [11]. The current research provides a more in depth investigation into newly developed mechanisms and their comparative analysis with the previously existing techniques.

One of the simplest methods among the examined methods is to use static ARP entries. When DHCP is not used, the IP entries cannot be manipulated. This is a very promising defense but does not have bright prospects in larger networks . Free Detection Systems like ARPWatch [3], XArp do have good detection mechanisms but not able to provide complete defense. On the contrary, port Security puts MAC cloning problem into place but fails at preventing ARP Spoofing. Anticap [6], a Kernel patch that finds its application in UNIX systems tries to prevent attacks by refusing updates that contain MAC addresses which are not currently present in table entries against particular IP address. This solution works well but does not prove to be much fruitful in dynamic environments. An another similar kernel patch, Antidote [6] proposed by M.Barnaba acquires the ARP reply and check it with the MAC address previously stored in the ARP cache. If this MAC address is found to be different from the already cached one then it sees whether that address is still alive. If that MAC address is found to be active then this new update is refused and it is also added to the list of banned MAC addresses. Its disadvantage is that it trusts that the ARP entry already cached is the authorized one which creates a dangerous condition of a race among the attacker and the victim. If somehow, the host cache is updated with faked ARP entry before the actual host could update, the legitimate user gets banned under such circumstances.

Many more Detection Systems such as Snort [4] are there that detects the intrusion by issuing a notification to the network administrator thereby generating alarm in case of ARP attack. These systems are also available freely but the main problem with IDS is that the number of alarms generated is extreme which might not be actually originated due to an attack. So, there is a need to have somebody in the organizations dealing with these events if we want this approach to be effectual one. ARP-Guard [5] finds and locates several attacks in internal networks, of which the ARP attacks are a part by using its sensor based operation. Ebtables [8] is another Linux based utility that are used to carry out Ethernet frame filtering by creating bridging and programmable switching devices. ARP attack prevention can be implemented using Ebtables, but the efficiency of such methods have not been studied. Its limitation is that it only filters poisoned ARP messages that try to pass through the operating system, while other areas remain equally vulnerable as before. One more defense mechanism was implemented in the AP to prevent ARP cache poisoning by R. Philip . A list of right IP-to-MAC address mappings is constructed by an Access Point and referring to the DHCP leases file and DHCP acknowledgement messages. This blocks all the ARP packets with false mappings based on the built list. A drawback is that the approach is only applicable to the dynamic host configuration networks and thus fail to prevent ARP poisoning assaults in wired LAN.

Antisniff as proposed by V. Goyal et al. [7] is a generative application which detects the NIC in a network currently running a promiscuous mode . The software can be installed on any one machine in a network and it will indicate the particular IP address running in promiscuous mode. But for this monitoring and detection requires this software to be active all time. HProxy as put forward by N. Nikiforakis is used to detect SSL striping attacks in which secure socket layer of https protocol is stripped off by the attacker. It helps in client side detection and runs separately as an alone application proxy instead of a browser's additional plug-ins in order to support multiple browsers. It works whenever there is a request from client to server. During the request, HProxy compares the response from the server with its white list. If there is any response that fails based on its detection rule set, it blocks the response to the client's browser. Its main drawback is that it does not provide any protection to the sensitive information against the SSL striping attack. HSTS acts as a secure protocol domain controller. Normally every secured website today requires the secure protocol head HTTPS to be included instead of HTTP, this secure protocol domain controller authenticates the website with its white list. If it detects any website having HTTP as their protocol head which normally requires HTTPS, it will inform the user to include HTTPS as a part of protocol head and will allow the user to proceed further by generating an appropriate warning. HTTPS Lock works as SSL certificate and HTTPS protocol authenticator which will take the user to page nor found(error 404) whenever it detects any fake certificate. The attack can be detected by the protocol if a client receives a response from a website without any protocol header or just only HTTP header. Its main drawback is that it is a client side detection method and can only be used to detect the SSL striping attack.

M Carnut et al**.** [14] proposed a scheme in which networks are switched to detect ARP spoofing attacks. No doubt this method decreased significantly the false positive replies but it requires complex setup to ne included as a part of their implementation which is practically not possible and moreover these devices cannot differentiate between the authenticated modification and spoofed replies in a network.

On the other hand the network monitoring and troubleshooting in wired and wireless networks can be done by the newly upgraded version available known as Colasoft-capsa 9.0 [9], but detection using this needs contentious traffic monitoring. An algorithm was proposed by Gouda et al. in which secure server based method is used to resolve the protocol addresses into hardware addresses over the Ethernet. The working of this algorithm is based on the two protocols named as Invite accept protocol and Request-Reply protocol that communicates with the server on the other side. The binding of <IP, MAC> of the client is registered with the server by invite accept protocol and the MAC address of the client is obtained from the database maintained on the server side by the request reply protocol. This solution though was not found to be practical as it required changing the basic ARP protocol for every client with the new ARP thus developed. Another disadvantage of this solution discovered was that the failure of secure server brings the system to halt in the wireless network, and thereby becomes the target for denial of service attack.

One more latest and new proposal was given by Ataullah et al. called an Efficient and Secure Address Resolution Protocol for ARP security mechanism. In this method ARP reply is sent to all other machines in the network so that if there is any case of spoofing the network, the targeted device must be aware of it. The idea of sending the ARP-reply to all other machines in the network may be thought of as a better solution without third trusted party. The disadvantage of this method is that it is used to detect the attack and is not a preventive technique The broadcasting mechanism used to secure ARP can also cause cloning attack. The attacker can make use of MAC spoofing attack and ES_ARP is not capable to detect the difference between real user and the fake user. This broadcasting of ARP-reply in the network can sometimes cause congestion in the network and brings the system to halt.

3. OPEN ISSUES AND FUTURE SCOPE

A variety of methods have been analyzed in the previous section but still no fool proof method was found that could be used to detect ARP attacks. The following requirements should be taken into account while formulating an ideal solution:

- Cryptographic techniques used to convert the plain text to cipher text should be minimized as the process of ARP gets slowed down and takes more time.
- The scheme should be practically feasible for implementation at the top level as it is not possible to change the ARP protocol to a new one by making changes to every single host in the network.
- Preventive techniques should preferably be used instead of sticking to mere detection, as detection invariably increases the administrator’s work to handle the alarms generated.

Table 1
Comparison Summary

Scheme	*Method of Action*	*Arguments in Favor/ Against*
Static ARP Method[5]	Manual binding made between IP and MAC Address	Straightforward method but does not have bright prospects for large networks.
ARPWatch [3]	Filters network packets and alarms when rule set is offended.	Free but requires somebody dealing with these events to handle large number of alarms.
XArp [3]	Compare <IP,MAC> bindings with the one stored in cache and detects attack if there is any mismatch.	Traffic Filtering and Monitoring requires to be enabled all the time.
Port Security	Reduces the total MAC address numbers that are to be serviced on any port.	Straightforward to use but does not block all types of attacks.
Anticap [6]	Implements specific regulations to stop ARP replies on the receiver side.	Add ARP reply in the block list if it is having different Mac than the already stored in the ARP cache, with a disadvantage being that it is applicable only for Linux Kernel.
Antidote [6]	Rules to block ARP replies at the receiver.	Add reply of ARP request to the block list if it is having different Mac ,also only suitable for Linux kernel.
Snort [4]	Detects false <IP, MAC> bindings.	Free but generates large number of alarms thereby increasing the need of round the clock administrator.
ARPGuard [5]	Performs Sniffing in the network and generate alarms based on the rule set constructed.	Good technique but not free available.
Ebtables [8]	Linux based utility that detects ARP spoofing attacks.	Used for linux based kernel only.
Colasoft Capsa [9]	Software that detects ARP Storm Attacks on the network.	Monitoring should be enabled all the time.
Antisniff [7]	Generative application that detects the NIC currently running in promiscuous mode.	Requires continuous monitoring to detect the machine running in promiscuous mode.
HProxy [11]	SSL striping attack is detected on the client side.	Does not provide any protection but only detects.
HSTS [12]	Acts as a protocol domain controller that redirects the user to error page if there is any fake certificate detected.	A whitelist needs to be updated to keep it updated.
HTTPS Lock	Protocol authenticator that will take the user to an error page in case a forged certificate is detected and will not allow the user to proceed further.	client side method used to detect the attack.
Sniffed Networks	Makes use of extensive switching in the networks to detect ARP attacks.	Not much credible due to complex setups involved.

As a future work, a new scheme presented at a recent international conference is being worked upon for implementation that complies with our requirements for an ideal solution to deal with these attacks.

4. CONCLUSION

Address Resolution Protocol has always been and is still very much prone to ARP poisoning attacks. As address resolution mechanism is an unavoidable network necessity, defense mechanisms need essentially to be implemented for utmost protection. A high percentage of methods have already been implemented to salvage against the spoofing attacks, yet a few soft spots need to be addressed. This research paper exhibits ARP poisoning problem and available solutions in a structured way. On the whole it would be prudent to conclude the fact that almost all the mitigation software available at hand are confined to work with specific kernel and some require relentless traffic filtering. For developing better standards and software to address this problem of ARP poisoning, the paper may be used as a ready reference to bring out a mechanism that can block ARP exploits keeping in view the limitations of the already reported methods.

REFERENCES

[1] Cox. B, How does ARP work, 2005.

[2] D. Plummer. An ethernet address resolution protocol, Nov.2010.RFC 826

[3] L. N. R. Group. arpwatch, the Ethernet monitor program; for keeping track of ethernet/ip address pairings. (Last accessed April 17, 2012).

[4] Snort Project, The. Snort: The open source network intrusion detection system. <http://www.snort.org>.

[5] "ARP-Guard," (accessed 28-July-2013). [Online]. Available: http://www.arp-guard.com.

[6] M. Barnaba, "anticap", (accessed 17 April 2013) Online. Available: http://www.antifork.org/anticap.

[7] V. Goyal and V. Abraham " An efficient Solution to the ARP cache poisoning problem", in Proceedings of 10th Australasian Conference on Information Security and Privacy, Jul 2013, pp 40-51.

[8] B. D. Schuymer, "ebtables: Ethernet bridge/switch tables," Mar. 2006, (accessed 28-July-2013). Available:http://ebtables.sourceforge.net.

[9] Donato, N. (2005). Poisoning Attack and Mitigation Techniques. Retrieved from Windows ARP attack tools.

[10] Ahsaan Arefeen, Srabanti Dey, Mingyue Yu, "Network Security Scanner (Nmap)", http://linuxcommand.org/man_pages/nmap1.html

[11] Jaideep Singh, Goldendeep Kaur, Dr. Jyoteesh Malhotra, "A Comprehensive Survey of Current Trends and Challenges to mitigate ARP attacks", In proceedings of 1st International Conference on Electrical, Electronics, Signals and Optimization, ISBN: 978-1-4799-7678-2, 2015 IEEE.

[12] Moxie Marlinspike, "SSLStrip, Black Hat DC 2009", Retrievedhttp://www.thoughtcrime.org/software/sslstrip.