International Journal of Future Generation Communication and Networking
Vol. 8, No. 2 (2015), pp. 225-232
http://dx.doi.org/10.14257/ijfgcn.2015.8.2.17

A Review of Latest Techniques to Secure Wireless Networks against ARP Poisoning Attacks

Goldendeep Kaur[1] and Dr. Jyoteesh Malhotra[2]

[1]*CSE Department, Guru Nanak Dev University, Regional Campus, Jalandhar*
[2]*ECE Department, Guru Nanak Dev University, Regional Campus, Jalandhar*
[1]*goldenchugh@gmail.com*, [2]*jyoteesh@gmail.com*

Abstract

Due to increasing network threats, it has become imperative to build a system that is meant to protect the network primarily from intrusion. A discipline that is most oblivious is the layer two of the OSI, which opens the network to dangerous assaults and compromises. Nowadays there are various sophisticated offensive tools and technologies that can exploit these vulnerabilities to create havoc in the tech-savvy generation. ARP spoofing assault is among the most hazardous procedures in local discipline networks. This paper discusses poisoning of Address resolution protocol and the most advanced schemes which mitigate such attacks. This attack has been carried out under test environment for illustrations and various preventive methods against it have been tested and compared. This paper has highlighted in the end an ideal strategy to combat ARP attacks at a superior level than the already existing techniques.

Keywords: *Address Resolution Protocol, Media Access Layer, ARP poisoning, MAC spoofing, Man in the Middle, Spoofing mitigation*

1. Introduction

Every node on an IP/Ethernet network has two types of addresses. The first is the hardware address known as Media Access Control (MAC) address and the second is its IP address. Applications, which are above the layer four, use logical address to identify the destination host, *i.e.*, IP address. IP addresses are assigned to the hosts and are logically independent of the physical address. The IP packets are enclosed into frames. The delivery of frames across the links is based on local address *i.e.*, physical address (MAC numbers). The association of IP addresses into physical addresses is done through Address Resolution Protocol (ARP) Address Resolution Protocol. So Address Resolution Protocol is a telecommunication protocol that is used for the resolution of network layer addresses into link layer addresses. It accomplishes this task by building a correspondence table of IP and MAC addresses, using specialized packets broadcast on the local network. ARP operates below the network layer as a part of the Open Systems Interconnection (OSI) link layer and is used when IP is used over the Ethernet. It is different than other protocols in the TCP/IP suite. Rather than being a peer to peer protocol, it is an interface between the IP(a Layer three protocol) and an underlying Layer two protocol, on which it depends upon for transport of datagram . [1] When a source device wants to communicate with another device, it checks its Address Resolution Protocol (ARP) cache to find if it already has a resolved MAC Address of the destination device. If there, it uses that address for communication. If ARP resolution is not there in its local cache, the source machine will generate an Address Resolution Protocol (ARP) request message with its data link layer address as the Sender Hardware Address and its own IPv4 Address as the Sender Protocol Address. It fills the target IPv4 Address as the Target Protocol Address. The destination MAC Address will be left blank, since the device is trying to find that. The source broadcasts the Address Resolution Protocol (ARP) request message to the

ISSN: 2233-7857 IJFGCN

local network. The message is received by each device on the LAN since it is a broadcast request. Each machine compares the Target Protocol Address (IPv4 Address of the machine to which the source is trying to communicate) with its own Protocol Address (IPv4 Address). Those devices whose IP address does not match will drop the packet without any action. When the targeted device checks the Target Protocol Address, it will obtain a match and will construct an Address Resolution Protocol (ARP) reply message. It takes the Sender MAC Address and the Sender Protocol Address fields from the Address Resolution Protocol (ARP) request message and uses these values for the Targeted Hardware Address and Targeted Protocol Address of the reply message. The destination device will update its Address Resolution Protocol (ARP) cache, since it needs to contact the sender machine soon. Destination device sends the Address Resolution Protocol (ARP) reply message and it is NOT a broadcast, but a unicast. The source machine will process the Address Resolution Protocol (ARP) reply from destination and stores the Sender Hardware Address as the layer 2 address of the destination. The source machine updates its Address Resolution Protocol (ARP) cache with the Sender Hardware Address and Sender Protocol Address it receives from the Address Resolution Protocol (ARP) reply message. [2] As ARP is a stateless protocol which means that it treats each request as an independent transaction, so most operating systems will automatically cache the ARP replies, inconsiderate of whether they have sent out an actual request. Since ARP does not offer any method for authenticating ARP replies in the network, ARP replies are vulnerable to be spoofed by other hosts on a network other than the one from which a response is expected. Many researchers have contributed towards counteracting the ARP poisoning attacks. Our earlier work reported in [2] was an effort to comprehend various techniques used to mitigate these attacks. This paper covers some recent techniques to secure wireless networks in continuation to our earlier reported work.

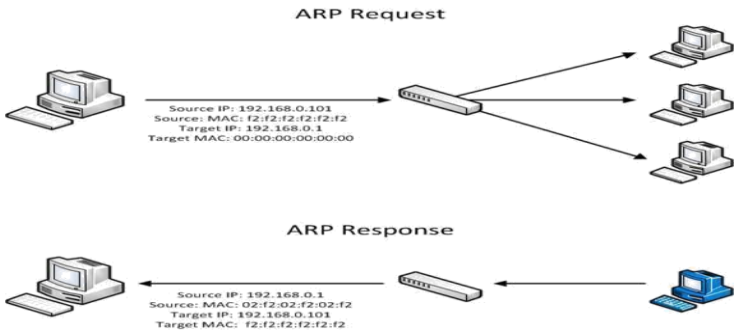

Figure 1. ARP Functionality

The remaining section of this paper is organized as follows: Section 2 describes ARP Cache poisoning, Section 3 describes the current counter measures to deal with ARP attacks, Section 4 describes the current trends and challenges, Section 5 describes the assault & apt defence mechanism, Section 6 describes the open issues and future directions and finally Section 7 concludes the paper.

2. ARP Cache Poisoning

"Address Resolution Protocol cache poisoning is the act, by a malicious host on the LAN, of introducing a spurious IP-to-Ethernet address mapping in another host's ARP cache" by which the IP traffic intended for one host is diverted to a different host. [1]

This ARP Poisoning can often be used as a part of other serious attacks:

2.1. Man-in-the-Middle Attacks

When a MiM is performed, a malicious user inserts his computer between the communications path of two target computers. Sniffing can then be performed. The vicious computer will forward frames between the two target computers so communications are not disrupted. [1]

2.2. DoS attacks

Update of ARP entries with hypothetical MAC addresses cause frames to be dropped. These requests can be sent out in a flood fashion to all clients on the network in order to cause a Denial of Service attack. This is a great setback of post-MiM attacks, since targeted computers continue to send frames to the attacker's MAC address even after they remove themselves from the communication path [2].

2.3. Hijacking

Connection hijacking allows an attacker to take control of a connection between two computers, using techniques similar to the MiM attack. This control can result in any type of session being transferred. For example, an attacker could take control of a telnet session after a target computer has logged in to a remote computer as administrator [1].

2.4. Cloning

MAC addresses are supposed to be unique identifiers for each NIC developed across the world. They were hardcoded into the ROM so that they cannot be changed. However, in the modern times MAC addresses can be easily changed. Even the Linux users can change their MAC without any sophisticated software by a single command in terminal. In this way, an attacker could DoS a target computer and then addresses themselves the IP and MAC of the target computer, receiving all frames destined for the target [3].

3. Current Counter Measures

In order to have secure communications, we should be able to detect and mitigate these attacks. Many researchers have worked in this area and a comprehensive survey has been conducted on the various techniques used to detect and mitigate these attacks.

MAC cloning can be detected by using **Reverse Address Resolution Protocol (RARP) [3].** Sending RARP request for all MAC addresses on a network determine if any machine is performing cloning, if more than one replies are received for a single MAC address.

Unix Operating Systems like **Solaris [5]** allows the new ARP reply only after the entry in the table has been expired. This makes more difficult for the attacker to poison the cache, however no longer impossible. In this mechanism, an attacker can poison the cache as long as the attacker's reply arrives before the reply from the legitimate host or by sending forged ICMP echo request that appears to come from one of the two victims.

Goyal and Tripathy proposed a variant of ARP [7] that is based on the combination of digital signatures and one time passwords to authenticate ARP <IP,MAC> bindings. An overhead is created by this method for system to produce the signature generation, key management and verification.

Ticket based ARP [9] is another method that prevents spoofing by distributing centrally issued secure <IP, MAC> addresses mapping proof called tickets through existing ARP messages. These tickets are generated at a center and verified by a Local Ticket Agent (LTA) which contains an expiry time. Tickets are attached to ARP replies so that the receiver can verify the association validity. These tickets are handed over to the

clients when they join the network.

In [11], switched networks are used to detect ARP spoofing attacks, it can reduce significantly of false positive, but involves a complex setup; however, these devices cannot distinguish between the legitimate modification and malicious update for ARP mapping, and they are incapable of give us high credibility in additional to the cost.

Philip *et al*. [12] proposed an approach to prevent ARP cache poisoning in wireless LAN by implementing the defense mechanism in the AP. The AP constructs the list of correct IP-to-MAC address mapping by monitoring DHCP ACK messages or referring to the DHCP leases file, and blocks all the ARP packets with an invalid mapping based on the constructed list. But this technique can be applied only to the wireless LAN in which dynamic IP addresses are allocated through DHCP, and therefore cannot prevent ARP cache poisoning occurring inside the wired LAN.

Most prevailing systems depend on cryptographic techniques to prevent spoofing attacks. However, the prolonged history of cracking the authorization and encryption mechanisms engaged in wireless networks shows the ineffectiveness of these methods in assuring a spoof-free network

Recently, an enhanced version of ARP, called **MR-ARP** is proposed in [13], to prevent ARP poisoning- based MITM attacks in the Ethernet by employing the concept of voting. It is a non-cryptographic approach. In MR-ARP if any new IP,MAC binding request comes then the authenticity of that request is checked by voting and if more than 50% reply comes into the favor of that binding then only the binding is accepted. If no reply comes then we consider this binding as genuine that's why any other node is not voting against the node and the binding will be accepted. This condition can be satisfied in the Ethernet, but may not be valid in the wireless LAN network because of the traffic rate adaptation based on the signal-to-noise ratio (SNR), *i.e.*, auto rate fallback (ARF).

Blake Ross *et.al*. proposed PwdHash [14], in which a browser plug-in tries to tackle MITM attacks by converting a using password into domain specific password. The major benefit of this PwdHash is that it provides defense against password phishing scams. Even if a phisher successfully convinces a user to visit the spoofed website, the hashed password that the phisher receives will be hashed along with the domain of the fake website. Hence this hashed password is expected to be of no value to the attackers as it will not work when used in original website because the original website expects a password to be hashed with its domain parameters.

Gouda *et. al*. [16] proposed an architecture that consists of a secure server connected to the network and two protocols used to communicate with the server. The invite-accept protocol is used by the hosts to register their <IP, MAC> mapping with the server. The request-reply protocol is used by the hosts to obtain the MAC address of a host connected to the LAN, from the database of secure server. But this technique requires changing the ARP protocol implementation of every host with this new ARP.

Nmap (Network Mapper) [20] is a network exploration tool and security scanner that is used to discover hosts and services on a computer network, thus creating a "map" of the network. To attain its goal, Nmap sends specially crafted packets to the destination host and then examine the responses. It provides a number of features for probing computer networks, including host discovery, vulnerability detection, service and operating system detection and more advanced service detection. These features are extendable by scripts that provide more advanced service detection and vulnerability detection. System administrators can use Nmap to search for illegitimate servers, or for computers that do not comply with security standards.

Colasoft-capsa 9.0 [19], a new upgraded version that can be used for monitoring, troubleshooting and analyzing wired and wireless networks, for detecting ARP storms on

the network. But detection of it needs intense traffic monitoring.

Goyal *et al*. [17] proposed a new architecture for secure address resolution. Their system is based on a Merkle hash tree, a trusted node on the network (TN) and a broadcast authentication protocol (*e.g.*, Tesla). While many broadcast networks can distribute the data to multiple receivers, they often allow a malicious user to impersonate sender and injects broadcast packets. Because malicious packet injection is easy in broadcast networks, the receivers want to ensure that broadcast packets they receive really originate from the claimed source and broadcast authentication protocol enables the receiver to verify this.

HSTS [18] acts as a secure protocol domain controller. Whenever a secure website which normally requires the secure protocol head (HTTPS) to be included, the HSTS will then validates the website with its white list domain. If the user enters the website without a secure protocol head, the HSTS will inform the user to include the HTTPS as part of its website's URL. However, the user must maintain the white list in order to keep it updated.

4. Current Trends and Challenges

In this section the available schemes to combat ARP poisoning based on the literature survey done have been tabulated below in the Table 1. The important issues and challenges of each technique have been enumerated. The comparative analysis made through this table provides for better understanding the present state of art of mitigating ARP poisoning techniques on the basis of priority.

Table 1. Comparison Summary

Scheme	Mechanism Employed	Pros/Cons
Reverse Address Resolution Protocol [3]	Detects MAC cloning by sending RARP request for all MAC addresses on a network.	Only detects the ARP attacks but does not provide any corrective measure.
Solaris [5]	Accept ARP reply only after the entry in the table has been expired.	Makes harder for the attacker to poison the cache but not impossible.
Colasoft-capsa 9.0 [19]	Used for detecting ARP storms on the network.	Detection Needs contentious traffic monitoring.
OTP [7]	Based on the combination of digital signatures and one time passwords to authenticate ARP reply.	Clever use of cryptography allows it to be significantly faster.
Ticket based ARP [9]	Implements security by distributing centrally generated tickets.	Backward compatible with ARP but is susceptible to replay attacks.
Access Point List [12]	Blocks all the ARP packets with a false mapping based on the constructed list.	Cannot prevent cache poisoning attacks occurring inside wired LAN.
NMap[20]	Network exploration tool and security scanner that allows system administrator to scan large networks for unauthorized servers.	Capable of even adapting to network conditions including latency and congestion during scan.
Switched networks [11]	Uses Switched networks for detecting spoofing Attacks	Complex set up, incapable of giving high credibility.
HSTS [18]	Secure protocol domain controller.	User must maintain the whitelist to keep it updated.
Merkle Hash Tree [17]	Uses broadcast authentication protocol Tesla to authenticate replies.	No cryptography operations required but not backward compatible with ARP.
MR-ARP [13]	Enhanced version of ARP to prevent attacks based on the concept of voting.	May not be valid in 802.11 networks due to auto rate fallback.

PwdHash [14]	Tackle MITM attacks by hashing user password with domain parameters.	Effective solution as it provides defense against phishing scams.
Modified ARP[16]	Architecture consisting of server and two protocols to communicate with the server.	Requires changing the ARP protocol implementation on every host with new ARP.

5. Assault and Apt Defense Mechanism

From the analysis presented and survey conducted, it can be inferred that out of all the schemes, HSTS is the best for the prevention of ARP spoofing. Many more advanced attacks such as cookie hijacking and session stealing can also be prevented using this technique. Its working mechanism is far better and apt among all the available solutions. The ARP attack has been performed under test environment and its prevention has been successfully tested using HSTS mechanism. Tools such as Ettercap and sslstrip have been used to create an environment for ARP poisoning mitigation.

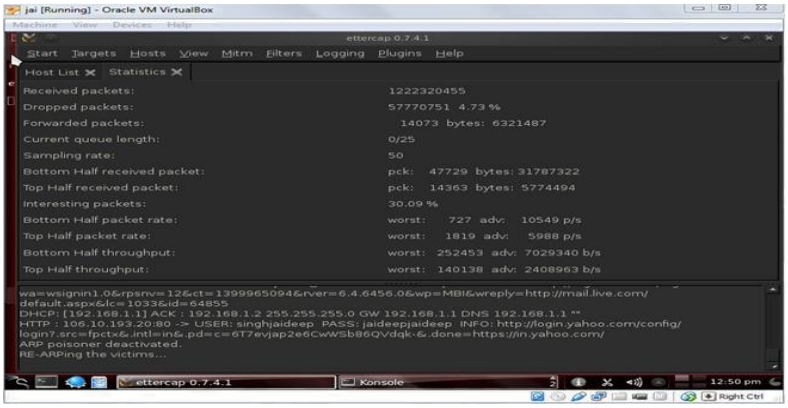

Figure 2. Attack under Test Environment

The ARP attack shows that the entire network has been poisoned and even the user credentials for a URL have been hijacked successfully. In defence to this attack, the HSTS mechanism was implemented as an add-on to the browser. The ARP poisoning is done in conjunction with an SSL strip here.

Figure 3. Defense Mechanism

The next attempt for the same attack led to the above error message, thus disabling the user to continue browsing in an insecure way. Thus the ARP attack now bears no fruit.

6. Open Issues and Future Directions

The need of an ideal solution is still an open issue at the network level. The HSTS mechanism prevents the ARP spoofing on the client side only and is not applicable at the network level. Moreover, the user must maintain the whitelist of websites that requires https protocol head instead of http. So the formulation of ideal strategy to be implemented at the whole network is still the future work.

7. Conclusion

This paper provides the comparative analysis of all techniques used to prevent ARP spoofing. In doing so the best method among all of these has been highlighted. From the survey conducted it can be concluded that if HSTS is enforced as a defense mechanism in the modern browsing arena, the ARP poisoning can be defied to a large extent. The most dangerous attacks such as user credential hijacking and cookie stealing can be prevented. The only limitation in this regard is that preloaded list "STS", a list that contains known sites supporting HSTS needs to be maintained. On the whole, there is a dire need of a method that can prevent ARP assaults at the network administrator level, so that the novice users can be protected from this menace.

References

[1] S. Whalen, "An introduction to ARP spoofing," 2600: The Hacker Quarterly, Fall Available:http://servv89pn0aj.sn.sourcedns.com/_g bpprorg/ 2600/arp spoofing intro.pdf, vol. 18, no. 3, **(2001)**.
[2] J. Singh, G. Kaur, and Dr. J. 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.
[3] D. Plummer, "An Ethernet address resolution protocol, RFC 826, **(2010)** November.
[4] T. Bradley, C. Brown, and A. Malis. "Inverse address resolution protocol", RFC 2390, **(2010)** September.
[5] T. Demuth and A. Leitner, "ARP spoofing and poisoning, Traffic tricks", Linux Magazine, vol. 56, **(2011)** July, pp. 26–3.
[6] D. Bruschi, A. Ornaghi, and E. Rosti, "S-ARP: A secure address resolution protocol" In Proceedings of the19th Annual Computer Security Applications Conference (ACSAC '03), **(2011)** December.
[7] H. Neminath, S. Biswas, S Roopa, R. Ratti, R. Nandi, F.A. Barbhuiya, A. Sur, and V. Ramachandran, "A DES Approach to Intrusion Detection System foe ARP Spoofing Attacks", 18th Mediterranean Conference on Control & Automation (MED), ISBN: 978-1-4244-8091-3, IEEE **(2010)**.
[8] V. Goyal and R. Tripathy, "An efficient solution to the ARP cache poisoning problem", in Proc of Australasian Conference on Information Security and Privacy (ACISP), vol. 1. **(2011)** July, pp. 40-5, Brisbane, Australia.
[9] W. Xing, Y. Zhao and T. Li, "Research on the defense against ARP Spoofing Attacks based on Win cap", 2010 Second International Workshop on Education Technology and Computer Science, Digital Object Identifier: 1O.l109IETCS.201O.75, 2010 IEEE.
[10] W. Lootah, W. Enck and P. McDaniel, "TARP: Ticket-based address resolution protocol", In Proceedings of the 21st Annual Annual Computer Security Applications Conference (ACSAC'05), **(2012)** December.
[11] M. Carnut and J. Gondim, "ARP spoofing detection on switched Ethernet networks: A feasibility study", In Proceedings of the 5th Simp´osio Seguranc¸a em Inform´atica, **(2011)** November.
[12] R. Philip, "Securing Wireless Networks from ARP Cache Poisoning", Master's Thesis, San Jose State University, **(2012)**.
[13] S. Y. Nam, D Kim and J Kim, "Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks" IEEE Common Lett, vol. 14, no. 2, **(2010)**, pp. 187–189.
[14] B. Ross, C. Jackson, N. Miyake, D. Boneh and J. C. Mitchell, "Stronger Password Authentication Using Browser Extension", Proceedings of the 14th Use nix Security Symposium, **(2013)**.
[15] 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, **(2013)** July, pp 40-51.

[16] M. Gouda and C. T. Huang, "A secure address resolution protocol", Computer Networks, vol. 41, no. 1, **(2012)** January, pp. 57–71.
[17] V. Goyal, V. Kumar, and M. Singh. A new architecture for address resolution, **(2012)**, available at <http://www.itbhu.ac.in/departments/comp/crypto/mayank.htm>.
[18] H. C. Jackson and A. Barth, "HTTP Strict Transport Security (HSTS)", IETF, Internet draft, **(2012)**.
[19] N. Donato, "Poisoning Attack and Mitigation Techniques", Retrieved from Windows ARP attack tools. **(2005)**.
[20] A. Arefeen, S. Dey, M. Yu, "Network Security Scanner (Nmap)", http://linuxcommand.org/man_pages/nmap1.html.

