Analysis of various ARP Poisoning mitigation techniques : A comparison

Conference Paper · July 2014

DOI: 10.1109/ICCICCT.2014.6992942

2 authors:

Nikhil Tripathi
Indian Institute of Technology Indore
17 PUBLICATIONS **284** CITATIONS
SEE PROFILE

Babu Mehtre
IDRBT - Institute for Development & Research in Banking Technology
69 PUBLICATIONS **2,432** CITATIONS
SEE PROFILE

Analysis of various ARP Poisoning mitigation techniques : A comparison

Nikhil Tripathi[a,b], BM Mehtre[b,*]
[a]School of Computer and Information Sciences, University of Hyderabad, Hyderabad, India-500046
[b]Center for Information Assurance and Management, Institute for Development and Research in Banking Technology
Hyderabad, India-500057
Email: nikhiltripathi684@gmail.com, bmmehtre@idrbt.ac.in
(*corresponding author)

***Abstract*—Address Resolution Protocol (ARP) is the fundamental and one of the most frequently used protocol involved in computer communications. Within a LAN, ARP messages are used to resolve IP addresses into corresponding MAC addresses.Nevertheless, some of the limitations within this protocol make it rather vulnerable. The two most prominent limitations are - *unauthenticated* and *stateless* nature of ARP. The attackers can easily exploit these loopholes for their personal gain. ARP poisoning is considered as unitary of the basic attacks which is utilized to launch higher level attacks. Several solutions have been proposed in the literature to detect and prevent these attacks. However, all of the proposed solutions are limited to a certain extent. Some solutions are effective in a special set of scenarios while others are rather suited for scenarios belonging to a different band. As new techniques of ARP poisoning have evolved with time, researchers are getting motivated to propose new solutions.**

In this paper, we have presented a comparative analysis of different proposed solutions which are rather popular in the literature. We have compared different mitigation techniques based on some of the important factors that are considered as limitations to the proposed solutions. These factors are derived from the scenarios which are possible within a LAN when an ARP Poisoning attack is launched. A brief tabular format is likewise introduced in this paper which offers a fast overview of comparison between different proposed schemes. This comparative study can further be used to offer and build up a more efficient and effective scheme which, on one hand, enjoys the combined advantage of different mitigation techniques and on the other hand, does not hold the old limitations.

***Keywords* - Address Resolution Protocol, ARP Poisoning, IP Exhaustion, Network Security, Cyber Defense, Man-In-The-Middle, Hacking, Insider Threats**

I. INTRODUCTION

In computer networks, every interface of a computer is assigned a physical (MAC) address and a logical (IP) address. Address Resolution Protocol (ARP) is responsible for resolving the IP addresses into corresponding MAC addresses. Request for Comment (RFC) 826 [1] defines the specification of the ARP protocol. Within a LAN, the computers use MAC addresses for the intention of communication. For that purpose, ARP provides two different types of messages which are exchanged by the computers so as to resolve the IP addresses into corresponding MAC addresses. These messages are: *ARP Request* and *ARP Reply* messages. From this, it can be understood that ARP is an essential part of network communication. However, some of the loopholes make the ARP protocol quite vulnerable to different network attacks. These loopholes are - *unauthenticated* and *stateless* nature of the ARP protocol. Hackers easily exploit these loopholes for launching other higher level attacks. Since it is the insider who launches the attack, ARP poisoning attacks fall under the category of insider threats. Insider threats have grown because the value of data has increased, giving insiders more incentive to steal data [2]. Since insider attacks are much more targeted because they know where the data is actually placed, these attempts are likely to inflict a greater impact compared to external threats [3]. In fact, the 2010 Verizon Data Breach Investigations Report along with other studies concluded that it is pricier to fix insider attacks compared to external threats [4]. This is also confirmed by the e-crime Survey and Ponemon Institute's 2010 Cost of Cyber Crime Study [5]. One among these attacks are DoS/DDoS Attacks [6].

These loopholes and the resultant network threats always motivated researchers to offer different strategies so as to mitigate ARP Poisoning attacks and hence, the higher level attacks too. Nevertheless, attackers are still able to bypass the security furnished by those solutions. In recent scenario, it has been discovered that the attackers practice some of the latest and the obscure but most basic tricks so as to fool the proposed solutions. One of the best example is to use a flood of spoofed ARP messages with maximum link-utilization. So, there should be a robust and efficient mitigation technique which can protect the network from these attacks at a minimal possible cost, i.e. it should neither require a change in underlying infrastructure nor should it overload the network with huge traffic.

The rest of the paper is organized as follows: Section II discusses a brief background of ARP and ARP Poisoning. Section III focuses on the factors on the basis of which comparison is made. Section IV describes the performance of various proposed schemes on the basis of comparative factors. Finally, Section V concludes the paper.

II. BACKGROUND

A. ARP Protocol

Suppose host A want to communicate to host B within a LAN. For that purpose, A requires the MAC address of B. So, A will search for B's MAC address in its ARP cache. If it is found, the communication will proceed else A will send

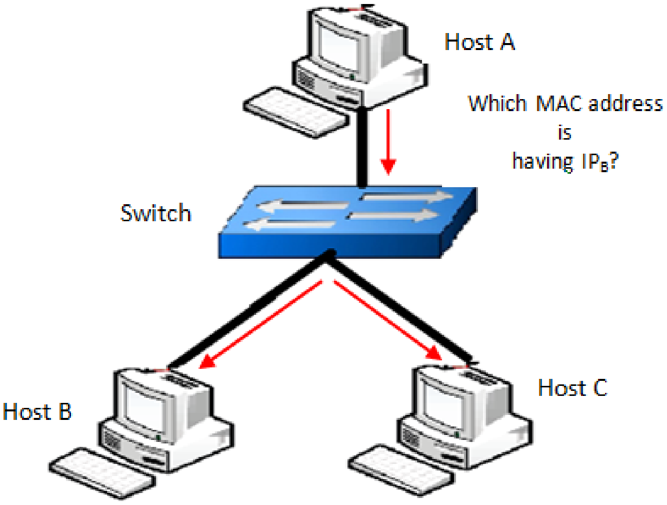

Fig. 1. Host A broadcasts ARP Request for Host B

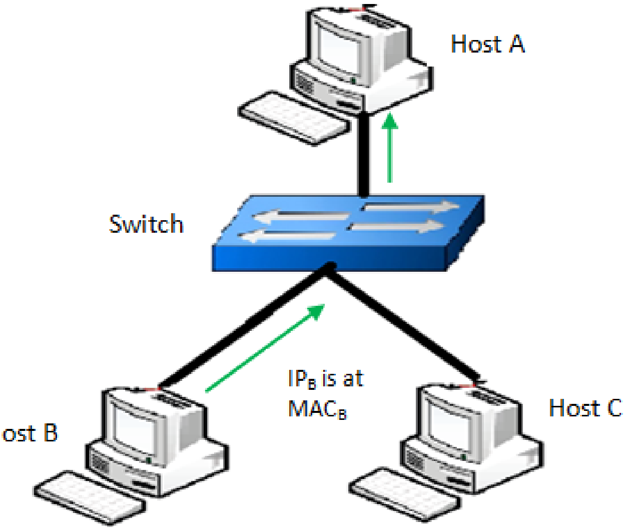

Fig. 2. Host B sends a unicast ARP Reply to Host A

a broadcast ARP request to get the B's MAC address. This ARP Request is shown in Fig. 1[7]. When B will receive this ARP Request, it will respond back with an ARP Reply having B's MAC address. The ARP Reply is shown in Fig. 2[7]. As soon as A will receive this reply, the communication will start and the MAC - IP mapping will be stored in A's primary ARP cache for a fixed amount of time.ARP Request and ARP Reply messages are utilized together to know the MAC - IP mappings of the communicating entities. ARP Request is generally a broadcast message sent to fetch the MAC address of a dedicated IP destination. In response to that, one of the hosts sends a unicast ARP reply which contains the required MAC address. After receiving the ARP Reply, the host makes an entry for this MAC - IP mapping into the primary ARP cache for a predefined amount of time. Later on the timeout, that entry is removed from ARP cache.

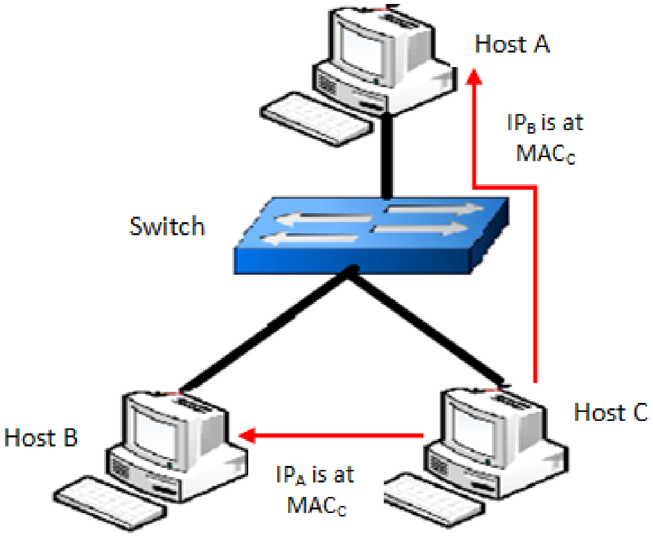

Fig. 3. Host C performing ARP Poisoning on A and B

B. ARP Cache Poisoning

Due to unauthenticated nature of ARP, attackers can easily send fake ARP messages to poison the ARP caches of the hosts within the LAN. Fig. 3[7] shows the ARP Poisoning attack launched by C. C sends a spoofed ARP message to A saying B's IP address belongs to C's MAC address. Likewise, C sends a spoofed ARP message to B saying A's IP address belong to C's MAC address. As a result, C will get the Man-In-The-Middle position for the whole communication that is going on between A and B.

III. Factors considered for the comparison

We have considered five different factors to compare the previously proposed schemes. They are:

1. Flood of spoofed ARP messages.
2. IP Exhaustion problem.
3. Backward compatibility with the existing network infrastructure.
4. Single point of failure problem.
5. Compatibility with the IP aliasing configurations.

We have discussed each of these factors in this section.

A. Flood of spoofed ARP messages

Various proposed solutions in the literature use probing process to mitigate ARP poisoning attacks. The probing process involves the usage of ARP/ICMP messages to validate the ARP messages received by them. These probe packets (ARP/ICMP messages) are sent when an ARP message is received by a host.

Suppose A is a host which uses probing process. Now, C sends an ARP message to A saying B's IP address, IP (B) belongs to C's MAC address, MAC (C). When A will receive this ARP message, it will transmit back a broadcasted ARP probe request, stating, "Who is having IP (B)?". This ARP request will be received by both, B and C. Since B really possesses IP (B), it will respond to the ARP Request. On the other hand, if C wants to conceal his/her individuality, s/he has to reply to all queries for IP (B). Now A will get to know that C may have sent a spoofed ARP message because two different MAC addresses can not possess same IP address at a time. Therefore, A can raise an alert saying ”ARP Poisoning is detected for IP (B)”.

However, if C sends a flood of spoofed ARP replies saying ”IP (B) belongs to MAC (C)” with a speed of maximum link-utilization, A will not be able to get B's response. This is due to the fact that the C's spoofed flood will overwhelm the B's real response. As a result, B's response will be dropped. Ultimately, in this case, A will think that B has gone offline and IP (B) has been allotted to MAC (C). This spoofed mapping, IP (B) - MAC (C), will be stored in A's primary cache which finally leads to ARP poisoning attack.

There are many tools and customized packet generators which are used to craft packets with custom headers. These tools even allow the attackers to specify the speed with which the packets are to be sent. One among these tools are packEth [8].

B. IP Exhaustion problem

Some of the proposed solutions within the literature consider that if a MAC address, MAC (X), is the first one to claim that an IP address, IP (P), belongs to it, IP (P) - MAC (X) mapping is a genuine one. Thereafter, the subsequent ARP messages claiming IP (P) belong to any other MAC address will be considered as the fake one.

The IP Exhaustion problem is essentially a type of ARP poisoning attack. The attacker broadcasts multiple ARP messages on the behalf of all unused (i.e. Not alive) IP addresses in the subnet. The attacker claims that all the unused IP addresses inside the subnet belong to my MAC address. When the other hosts receive this message, they update their primary ARP cache accordingly.

Suppose that hosts inside the subnet are executing the above mentioned scheme. If an attacker launches the IP Exhaustion attack, the hosts will update their cache accordingly. Now, hosts will assume that all the possible IP addresses inside the subnet are currently in use. So whenever, a genuine host will come into the network and it will send an ARP message, all other hosts will consider the new host as illegitimate one. Finally, a genuine host may get banned while on the other hand, the attacker can enjoy total exemption within the network.

C. Backward compatibility with the existing network infrastructure

Several proposed schemes require a modification in the existing ARP specification. The required changes include the integration of cryptographic schemes with the ARP specifications.

However, the modification of ARP specifications will make the protocol incompatible with the existing network infrastructure. Though these types of strategies are rather efficient, they are not that much popular in the real world implementation because of the cost to be incurred.

D. Single point of failure problem

Some of the proposed solutions in the literature suffer from the problem of single point of failure. This is due to their centralized nature. Most of such solutions are based on a detection server. The detection server is responsible for validating the ARP entries present in the primary ARP cache of all the hosts within the subnet.

However, if the server goes down, the network becomes insecure. In such instances, the attackers can easily establish the attack without the concern of becoming arrested.

E. Compatibility with the IP aliasing configurations

Sometimes, the network administrators configure IP aliasing for some of the MAC addresses. Using IP Aliasing configurations, the network administrator can allot more than one IP addresses to a single MAC address. However, when such configurations are present within the LAN, the proposed schemes may give false alarms.

Suppose that IP aliasing is configured for MAC (A) and it possesses IP (X) and IP (Y) at the same time. Now, when two ARP messages with different source IP addresses (i.e. IP (X) and IP (Y)) but same MAC address (MAC (A)) will be received by other hosts, they will raise the alarm saying IP Exhaustion attack is launched by MAC (A). But, in reality, the host with an interface (MAC (A)) is a genuine one. So, this limitation results in execution of false alarms.

IV. Related Work

In this section, we have discussed some of the proposed schemes. Along with that, we have also presented their behavior against the comparative factors which are talked about in the previous section. The proposed schemes are as follows:

A. Cryptography based schemes

Different modifications in ARP specifications are proposed in some of the schemes like Secure ARP [9] and Ticket based ARP [10].

Secure ARP is based on the concept of public/private key certificates. These digital certificates are used for the authentication of every ARP replies within the network. The Authoritative Key Distributor (AKD) acts as a central server to distribute the public keys to different hosts. This scheme makes use of Secure-DHCP (Dynamic Host Configuration Protocol) instead of usual DHCP.

Ticket based ARP involves the use of a ticket with each ARP message. Local Ticket Agent (LTA) is responsible for the distribution of this ticket.

The behavior of the scheme based on the five factors is as follows:

1) Resistant to flood of spoofed ARP messages: Since this scheme is not based on the probing process, it is not vulnerable to flooding of spoofed ARP messages.

2) Resistant to IP Exhaustion problem: Since the digital certificates and tickets are used to validate every ARP reply within the LAN, the attacker cannot send spoofed ARP messages. Therefore, the scheme is effective against IP Exhaustion attack also.

3) Backward compatibility with the existing network infrastructure: Due to such high level implementations, this scheme requires changes in the ARP standard specification. As a consequence, this scheme is not compatible with the existing networks.

4) Single point of failure problem: Since the scheme involves the use of centralized entities like AKD server and LTA agent, the scheme suffers from a single point of failure problem.

5) Compatibility with IP Aliasing configurations: Since the digital certificates and tickets are used to validate ARP replies, the hosts can easily detect the genuine and fake bindings. Thereafter, the hosts can update their primary ARP cache accordingly. Thus, the scheme is compatible with IP Aliasing configuration.

B. Kernel based Patches

Several kernel based patches are also proposed in the literature as mitigation scheme to prevent ARP poisoning attacks. The Antidote [11] approach is the most popular among them at an individual host level. According to Antidote scheme, when a host receives an ARP reply whose MAC address differs from the previously cached one, it tries to check if the previously learnt MAC address is still alive. If the previously learnt MAC address is still alive, the updated binding is rejected and the offending MAC address is appended to a list of banned addresses.

The behavior of the scheme based on the five factors is as follows:

1) Resistant to flood of spoofed ARP messages: Since this scheme involves probing process to check if the previously learnt MAC address is still alive, it is vulnerable to flooding of spoofed ARP messages.

2) Resistant to IP Exhaustion problem: There may arise a situation when attacker sends spoofed ARP replies with some random source MAC address. S/he may do so for all the unused IP addresses within the network. After this, whenever the attacker will receive ARP requests for these fake bindings, s/he may send a fake reply so that the detecting host would consider that the older MAC is still alive. The detecting host will now consider that all the IP addresses of the pool are currently in use. Thus, the scheme does not prevent IP Exhaustion problem.

3) Backward compatibility with the existing network infrastructure: Since the scheme does not require any modification in ARP specification, it is backward compatible with existing network infrastructure.

4) Single point of failure problem: Being distributed in nature, the scheme does not create single point of failure problem.

5) Compatibility with IP Aliasing configurations: When this scheme receives an ARP message, it checks if the source IP address of the ARP message is already present in the cache. If it is present, the scheme will check if the previously learnt MAC address is alive. Otherwise, the scheme will simply store the mapping into the cache independent of the source MAC address of ARP message. In the case of IP Aliasing also, until and unless the source IP address of the ARP message is not present in ARP cache, the scheme will continue to learn the IP - MAC mappings. So, it is compatible with IP Aliasing configuration.

C. Passive Detection

ARPWATCH [12] is one of the most popular tools which works as a passive detection tool. It sniffs the ARP Requests/Replies from the network and constructs a MAC - IP address mapping database. If it notices a change in any of these mappings in future ARP traffic, the alarm is raised concluding that an ARP spoofing attack is going on.

The behavior of the scheme based on the five factors is as follows:

1) Resistant to flood of spoofed ARP messages: This scheme is totally dependent on at what time the attack is launched. If attacker launched the flood of ARP spoofing attack before the detection tool was started for the first time, the tool will learn the spoofed IP - MAC bindings and thus, fake bindings will be stored in address mapping database. However, if the detection tool started its execution before the flood was launched, the flood will be detected easily. Since there is a scenario in which attack cannot be detected, we consider that the scheme is vulnerable to flood of spoofed ARP messages.

2) Resistant to IP Exhaustion problem: In a network, an attacker can always find the list of IP addresses which is not being used by any host at a particular instant. After this, the attacker can send various spoofed ARP replies (with different randomly generated MAC addresses) on the behalf of unused IP address. As a consequence, the detection tool will store these mappings in the primary ARP cache. Thus, the host, on which detection tool is running, will consider that all the IP addresses are currently in use. Due to this reason, the new incoming hosts in the network will be considered as illegitimate hosts which will finally result into false alarm execution. Thus the scheme is not effective against IP Exhaustion problem.

3) Backward compatibility with the existing network infrastructure: Since the scheme does not require any modification in ARP specification, it is backward compatible with existing network infrastructure.

4) Single point of failure problem: Being distributed in nature, the scheme does not create single point of failure problem.

5) Compatibility with IP Aliasing configurations: Since the detection tool raises the alarm if it notices a change in IP - MAC mappings, this scheme will create false alarms if the IP Aliasing is configured for some of the MAC addresses. So, this scheme is not compatible with IP Aliasing configuration.

D. Centralized Detection and Validation Server

Sumit Kumar and Shashikala Tapaswi [13] proposed a centralized technique for detection and prevention of ARP poisoning. In this scheme, an ARP Central Server (ACS) validates the ARP tables' entries of all the hosts within the network. Clients also maintain a secondary long term cache in this scheme.

The behavior of the scheme based on the five factors is as follows:

1) Resistant to flood of spoofed ARP messages: Since the ACS server is based on the probing process to check if the previous IP - MAC mapping is still valid, this scheme is also vulnerable to flood of spoofed ARP messages.

2) Resistant to IP Exhaustion problem: If an IP - MAC mapping is not present in ACS cache, the attacker can send spoofed ARP messsage with some random MAC address. As a result, the ACS will store this mapping into the cache as well as secondary ARP table. Since, ACS itself contains this mapping, all other hosts within the LAN will honour this mapping. Attacker can send multiple such ARP messages spoofed with different IP address. This will lead to IP Exhaustion problem.

3) Backward compatibility with the existing network infrastructure: Since the scheme does not require any modification in ARP specification, it is backward compatible with existing network infrastructure.

4) Single point of failure problem: ACS server, being centralized in nature, creates single point of failure problem.

5) Compatibility with IP Aliasing configurations: Since the scheme allows mapping of a MAC address with more than one IP address, the scheme is compatible with IP Aliasing configurations

E. Usage of ICMP packets as probe packets

Poonam Pandey [14] proposed an approach which involves the usage of ICMP packets as probe packets to validate the ARP messages.

The behavior of the scheme based on the five factors is as follows:

1) Resistant to flood of spoofed ARP messages: Since this scheme involves probing process to validate the ARP messages, it is vulnerable to flooding of spoofed ARP messages.

2) Resistant to IP Exhaustion problem: By modifying his/her network stack, the attacker can generate corresponding spoofed ICMP replies in response to the probe ICMP echo requests. Using this technique, an attacker can create IP Exhaustion problem.

There are various tools available which can be used to modify the whole network stack of a computer system. The most popular technique is to use NFQUEUE [15] along with iptables [16]. Though this technique is highly advanced, these tools make it much easier to implement.

3) Backward compatibility with the existing network infrastructure: Since the scheme does not require any modification in ARP specification, it is backward compatible with existing network infrastructure.

4) Single point of failure problem: Being distributed in nature, the scheme does not create single point of failure problem.

5) Compatibility with IP Aliasing configurations: This scheme is compatible with IP Aliasing configurations since the interfaces on which IP aliasing is configured, will reply to all the probe ICMP echo requests destined to them. These IP - MAC bindings will simply be stored in the primary ARP cache.

F. Using Host based Discrete Event System

Ferdous A. Barbhuiya et al. [17] proposed one scheme using host based Discrete Event System (DES). The scheme is based on a DES model for the system under normal condition and also under each of the failure conditions. Along with that, a state estimator called diagnoser (or detector, if only detection of failure is required) is designed which observes events generated by the system to decide whether the states through which the system traverses correspond to the normal or faulty DES model. This scheme uses ARP packets as probe packets to validate the ARP replies.

The behavior of the scheme based on the five factors is as follows:

1) Resistant to flood of spoofed ARP messages: Since this scheme involves probing process to validate the ARP messages, it is vulnerable to flooding of spoofed ARP messages.

2) Resistant to IP Exhaustion problem: An attacker can easily send spoofed ARP Replies saying that different IP addresses (which are not yet verified by the victim host) belong to his/her MAC address. When victim will send probe ARP Requests for these replies to verify them, attacker can send spoofed replies again. As a result, the victim host will store these bindings into the verification table. So, the new upcoming hosts ARP Requests/Replies will be added to the victim host's spoofed table directly though these new hosts are genuine ones. This leads to IP Exhaustion problem.

3) Backward compatibility with the existing network infrastructure: Since the scheme does not require any modification in ARP specification, it is backward compatible with existing network infrastructure.

4) Single point of failure problem: Being distributed in nature, the scheme does not create single point of failure problem.

5) Compatibility with IP Aliasing configurations: Since all the interfaces on which IP Aliasing is configured, will respond to the probe ARP requests, these mappings will simply be stored in primary ARP cache. Thus, the scheme is compatible with IP Aliasing configurations.

G. ICMP based secondary cache approach

Nikhil Tripathi and B .M. Mehtre [7] proposed an ICMP based secondary cache approach to detect and prevent ARP Poisoning. It was shown how the entering and existing algorithms could detect and prevent these attacks by validating the ARP messages using entries present in secondary ARP table. This scheme uses ICMP echo requests for probing process to check if the previous IP - MAC mapping is still valid.

The behavior of the scheme based on the five factors is as follows:

1) Resistant to flood of spoofed ARP messages: Since this scheme involves probing process to validate the ARP messages, it is vulnerable to flooding of spoofed ARP messages.

2) Resistant to IP Exhaustion problem: Since this scheme allows only one mapping for a MAC address in secondary ARP table, it is resistant to IP Exhaustion attack.

TABLE I. COMPARISON OF VARIOUS PROPOSED SCHEMES BASED ON THE FIVE COMPARATIVE FACTORS

	Cryptography based schemes	Kernel based Patches	Passive Detection	Centralized Detection and Validation Server	Usage of ICMP packets as probe packets	Using Host based Discrete Event System	ICMP based secondary cache approach
Resistant to flood of spoofed ARP messages	✓	*X*	*X*	*X*	*X*	*X*	*X*
Resistant to IP Exhaustion problem	✓	*X*	*X*	*X*	*X*	*X*	✓
Backward compatibility with the existing network infrastructure	*X*	✓	✓	✓	✓	✓	✓
Resistant to single point of failure problem	*X*	✓	✓	*X*	✓	✓	✓
Compatibility with IP Aliasing configurations	✓	✓	*X*	✓	✓	✓	*X*

3) Backward compatibility with the existing network infrastructure: Since the scheme does not require any modification in ARP specification, it is backward compatible with existing network infrastructure.

4) Single point of failure problem: Being distributed in nature, the scheme does not create single point of failure problem.

5) Compatibility with IP Aliasing configurations: Since this scheme does not allow more than one mapping for a MAC address in secondary ARP table, it is not compatible with IP Aliasing configurations.

This section described the behaviour of the proposed schemes based on the five comparative factors. Table I shows a summarized comparison among these schemes based on the five factors. The checkmark (✓) shows that the scheme's behaviour possesses that property while the crossmark (*X*) shows that the scheme does not possess that property.

V. CONCLUSION

In this paper, we have presented a comparative study of various ARP poisoning mitigation schemes based on the five factors of comparison. We have shown that some solutions are effective in a special set of scenarios while others are rather suited for scenarios belonging to a different band. No proposed solution can be considered as a versatile solution. However, one solution among these can be preferred over another if the five comparative factors are given some weight. Higher is the weight, higher will be the priority. A solution which satisfies the factors having higher priority, can be considered better.

This comparative analysis provides a pre-designing plan which should be considered while proposing new ARP poisoning mitigation techniques. This comparative study can further be used to develop a more efficient and effective scheme which, on one hand, enjoys the combined strength of different mitigation techniques and on the other hand, does not hold the old limitations. We are sure that this comparative study will motivate researchers to develop more advanced mitigation techniques against ARP Poisoning.

REFERENCES

[1] David C. Plummer, *An Ethernet Address Resolution Protocol*, RFC 826, Internet Engineering Task Force, November 1982.

[2] Fyffe, George. *Addressing the Insider Threat*. Network Security. Mar. 2008: Science Direct. Web. 25 June. 2011.

[3] Jennings, Frank. *Beware the Enemy Within*. SC Magazine. Jul. 2008: Business Source Complete. Web. 25 June. 2011.

[4] Kaplan, D.. *Internal Review*. SC Magazine. 1 Feb. 2011: ABI/INFORM Trade & Industry, ProQuest. Web. 25 June. 2011.

[5] Blades, M.. *The Insider Threat*. Security Technology Executive. 1 Nov. 2010: ABI/INFORM Trade & Industry, ProQuest. Web. 25 June. 2011.

[6] Nikhil Tripathi, BM Mhetre, *DoS and DDoS Attacks: Impact, Analysis and Countermeasures* in National Conference on Advances in Computing, Networking and Security (NCACNS), Publication year: 2013, pp: 93-98.

[7] Nikhil Tripathi, BM Mehtre, *An ICMP based secondary cache approach for the detection and prevention of ARP poisoning* in 4th IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Publication year: 2013, pp. 1 - 6.

[8] PackEth [Online].
Available at: http://packeth.sourceforge.net/packeth/Home.html

[9] D. Bruschi, A. Ornaghi, and E. Rosti, *S-arp: a secure address resolution protocol* in Computer Security Applications Conference, 2003. Proceedings. 19th Annual. IEEE, 2003, pp. 66 - 74.

[10] W. Lootah, W. Enck, and P. McDaniel, *Tarp: Ticket based address resolution protocol* vol. 51, no. 15. Elsevier, 2007, pp. 4322 - 4337.

[11] Teterin, I. (2003) *Antidote*. [Online] Available at: http://antidote.sourceforge.net

[12] Leres, C. (2006) *ARPWATCH tool: ARP Spoofing Detector*. [Online] Available at: ftp://ftp.ee.lbl.gov/arpwatch.tar.gz

[13] S. Kumar, S. Tapaswi, *A centralized detection and prevention technique against ARP poisoning* in Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, Publication Year: 2012 , Page(s): 259 - 264.

[14] Poonam Pandey, *Prevention of ARP spoofing: A probe packet based technique* In: IEEE International Advance Computing Conference (IACC), 2013. pp. 147 - 153.

[15] NFQUEUE [Online]. Available at: http://www.ohloh.net/p/nfqueue-bindings

[16] iptables [Online].
Available at: http://www.netfilter.org/projects/iptables/index.html

[17] Barbhuiya, F. A., Biswas, S., Hubballi, N., Nandi, S., *A host based DES approach for detecting ARP spoofing* In: IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2011. pp. 114 - 121.