ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on Various Detection and Prevention Mechanism for MITM and ARP Attacks

Akshada Hingne, Prof. Shitanshu Jain

Research Scholar, Dept. of Computer Science & Engg, Gyan Ganga Instt. of Technology & Sciences, Jabalpur, India

Professor, Dept. of Computer Science & Engg, Gyan Ganga Instt. of Technology & Sciences, Jabalpur, India

ABSTRACT: Today network security is very challenging task, as it is an integral part of network service. But due to rely on computer network for secret and important file, security has become very important part of it. ne of the network protocol is address resolution protocol (ARP). It maps the IP address to its corresponding MAC address. But the problem of this is that it is stateless protocol in ARP Poisoning attacker sends fake ARP messages on LAN, so it can gain the access and after getting access it may intercept data frames on network, modify traffic or stop the traffic. ARP Poisoning attack is the gateway for DoS attack, MITM attack and session hijacking attack. So there is the need of some unique solution which can overcome the problems of ARP poisoning attacks.

KEYWORDS*:* Virtualization, Attacks, Network Security, ARP Poisoning, IP Exhaustion, Man in the Middle attack, DoS Attack.

I. INTRODUCTION

Today internet has become the basic necessity for most of the people and in last few years its growth has significantly increased. So to use internet there are many types of network by which people have access to the internet like wired network and wireless networks. In wireless network we can include Wi
-Fi, Wi-Max, Bluetooth, etc. And for securing these types of network there are multiple approaches are there. But every approach has challenges which need to be addressed. So one of the protocol used is the Address Resolution Protocol (ARP). But there are some cons of ARP. One of them is its stateless nature. And for ARP, ARP Poisoning attack is used to disrupt the functions of it in switched network. And by doing ARP Poisoning, Man in the Middle (MITM) attack is also possible. So there should be standard mechanism from protection of ARP Poisoning attacks. In everyday environment, people think that it is not possible to eavesdrop the packet in switched network or in encrypted wireless (Wi-Fi). Because they think that switch is point to point device and computer will talk to specific endpoint of switch which it want to. But in today’s life there are many hacking and penetration tools which can hack that system, which allows anyone running these type of tools to view all traffic flowing in network and they might change the traffic flowing in the network means performing the man-in-the-middle attack. So for this type of attacks there are solutions like Arp-Defender for defending and Arp-Watch for monitoring but these solutions are costly and also have disadvantages. Means there is the need for the single solution to preventing and detecting the ARP Poisoning attack.

The Address resolution protocol is the protocol is used to map the internet protocol (IP) address into the hardware address (MAC).When the host machine wants to know a physical address for any host in the network, it broadcasts the ARP request, and the host that owns the IP address sends the unicast ARP reply message to indicating its MAC address. Each host machine maintains a table called ARP cache, used to convert IP addresses into MAC addresses There are many security threats in the ARP which leads us to unsecure communication because ARP is the stateless protocol, every time a host gets an ARP reply from another host, even though it has not sent an ARP request for that reply, it accepts that ARP entry and updates its ARP cache. The process of updating the host’s ARP cache with the forged entry is referred to as poisoning, in fact a malicious user can poison the ARP caches to impersonate hosts, perform MITM and DOS attacks.

II. PROBLEM DEFINITION

After the ARP was drafted, a subtle weakness was found. Infect Arp does not provide the authentication to the source of incoming ARP packets this is the reason that an attacker can forge an ARP message containing malicious information to poison the ARP cache of the target host.

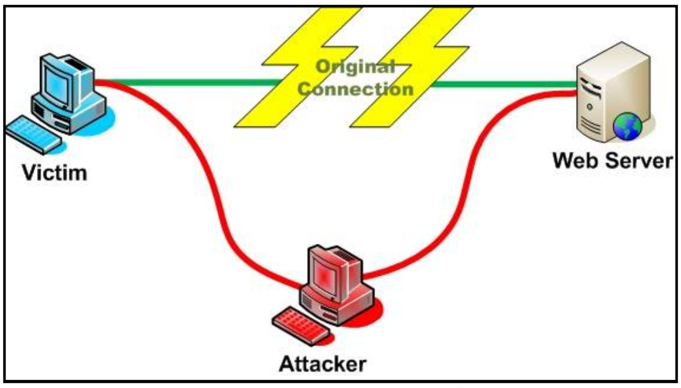


Fig 1.1 ARP Poisoning Attack

ARP suffers from the lot of threats which leads it to insecure communication and the lonely reason for these attacks is the no authentication mechanism is used in the ARP. When the victim adds an incorrect (IP, MAC) mapping to its ARP cache, this is known as the cache poisoning or Arp spoofing. The ARP poisoning is done when the attacker sends the fake <IP, MAC> address in the response of ARP request, The ARP is stateless protocol and it accepts all the incoming ARP packets and modifies the local ARP cache.ARP poisoning attacks are often used as a part other serious attacks or we can say Arp poisoning is the base for the various attacks:

A. DOS ATTACKS

An attacker can attack to victim's cache by sending the fake<IP,MAC> addresses so that every packet the sender will send will be received by the attacker instead of its real destination, In Dos attack attacker can block all the communication from the host being attacked.

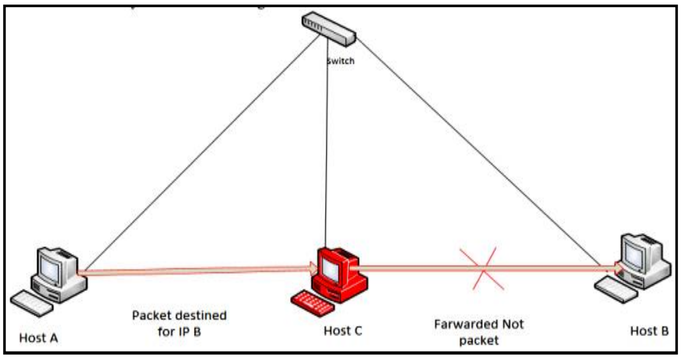


Fig 1.2 DoS Attack

B. MITM ATTACK

The man-in-the middle attack is little different than the Dos attack, in MITM the attacker attacks two hosts at the same time by cache spoofing two hosts in the network, the attacker can silently sit between the two hosts and can read/ write the communication between two victims so that they think that they are communicating with each other, this attack is passive attack and is difficult to detect.

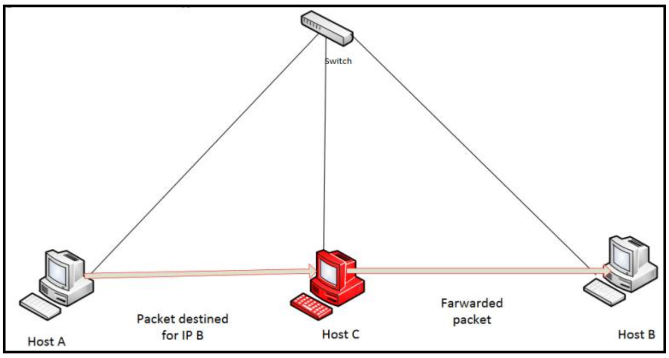


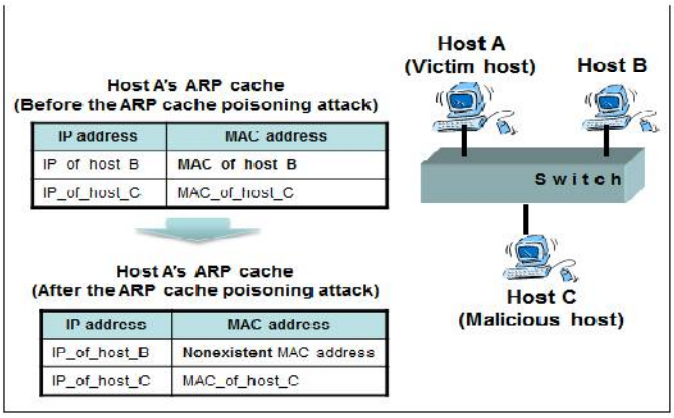
Fig. 1.3 MitM Attack

C. CLONING ATTACK

The cloning attack has the different process for attacks than above two attacks, the attacker changes its IP and MAC address to become identical to those of victim host. Once the change is done there will be the two host with same addresses and victim will get confuse who is the real host and sometimes when the real host is disconnected in network the attacker can make the advantage and can attack as real host without any hesitation. This situation can cause the network troubles and we can say that it will lead to Dos attacks also.

D. ARP CACHE POISONING ATTACK

ARP protocol specifies no rules to maintain consistency between the ARP header and the Ethernet header [3]. That means one can provide uncorrelated addresses between these two headers. For example, the source MAC address in the Ethernet header can be different from the source MAC address in the ARP header. Moreover, ARP protocol deploys no mechanism to detect and prevent invalid association of IP and MAC addresses proved in an ARP header. Hence, a malicious host may exploit this weakness in the ARP protocol to introduce a spurious IP address to MAC address mapping (fake<IP-MAC> entry) in another host's ARP cache. This malicious act of creating fake ARP entries in an ARP cache is called ARP cache poisoning attack. The attack can be performed by directly manipulating the ARP cache of a target host, independently of the ARP messages sent by the target host. ARP cache poisoning attack is used usually to perform DoS or MitM attacks in network.



Host A's ARP cache
(Before the ARP cache poisoning attack)

IP address	MAC address
IP of host B	MAC of host B
IP_of_host_C	MAC_of_host_C

Host A's ARP cache
(After the ARP cache poisoning attack)

IP address	MAC address
IP_of_host_B	Nonexistent MAC address
IP_of_host_C	MAC_of_host_C

Fig. 1.4 Host A's ARP cache before and after the ARP cache poisoning attack

III. A BRIEF REVIEW

Till present time there are many solutions for ARP-attacks to prevent the ARP-cache poisoning attacks and also provides the solution for security of ARP. Many researchers have done a good job and effort to prevent the attacks in

ARP but these solutions have some drawbacks which cannot be tolerated by the network communication mechanism these solutions and their drawbacks. The drawback is that some of the solutions have no backward compatibility option and some of them use cryptography to exchange encrypted data which is not feasible because it takes too much time in encrypting the packets and few of them uses the server middleware based solution which has the big drawback that a single crash of server can lead to failure in communication.

A. USING STATIC ARP ENTRIES

Use of static ARP entries [1] is the best defence method for ARP cache poisoning attacks. We can make the MAC address static, hence it will make the entries constant and the hacker will not be capable to apply ARP spoofing in the network. This entry is done using windows command prompt like ARP-sip_addressmac_address. However this method is not suitable for big networks as it would be very complicated for the network administrator to manage and update these tables throughout the network.

B. S-ARP

A new Secure-ARP (S-ARP) [4] in which key distribution, public and private keys for signing every ARP message have been used. These keys are distributed by the trusted third party known as certification authority.
But this method has no backward compatibility means takes large cost and tough hard work to implement in the existing ARP.

C. DYNAMIC ARP INSPECTION

Some High-end Cisco switches presented a feature known as Dynamic ARP Inspection [6] that allows the switch to block invalid <IP, MAC> combinations. It uses local pairing table that is built using a feature recognized as DHCP snooping to detect which pairings are invalid. But the high costing of switches makes this feature ineffective.

D. ARP WATCH AND ARP GUARD

ARP watch [5] and ARP Guard [6] are the manual solutions that form an active protection against internal ARP attacks by constantly analyzing all the ARP messages, sending appropriate alerts in real time and identifying the source of attack.

E. DYNAMIC DETECTION APPROACH

A dynamic detection approach [7] was presented which is based on the Snort. A Snort is intrusion detection system that monitors the traffic and analyzes it against a rule set defined by the user and performs the action based on what has been identified.

F. MIDDLEWARE APPROACH

The middleware approach [8] that blocks unsolicited replies and raise alarms when the reply is inconsistent with the currently cached entry. But this scheme is not effective as it requires installation of middleware on every host in the network.

G. HPROXY

HProxy [9] works when there is a request from client to server. If so, then it will check the response from the server with its whitelist. If there is any response that fails based on its rule set, then it will block the response to the client's browser.

H. HTTPS LOCK

It works as SSL certificate and protocol validator [10] that will redirect a user to an error page when it detects fake certificate
or website which requires HTTPS protocol. The protocol can detect this whenever a client collects a response from a website without any protocol header or just only HTTP header.

I. ANTICAP AND ANTIDOTE

These [11] are the kernel based patches that does not allow updating of host ARP cache that comprises a MAC address different from the one already in the cache. However, their patch can only be used with some specific kernel.

J. ANTISNIFF

AntiSniff application [12] that is network card promiscuous mode detector. It works by sending a series of carefully made packets in a certain order to a target system, sniffing the results and performing the timing tests against the target. By measuring the timing results and monitoring the target's responses on the network, it can be determined if the target is in promiscuous mode, i.e. sniffing the network.

K. MR-ARP

It is a non-cryptographic approach [13]. In MR-ARP if any new IP, MAC binding request comes then the genuineness of that request is checked by voting and if more than 50% reply comes into the favour of that binding then only the binding is accepted. If no reply will come 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).

IV. COMPARISION BETWEEN VARIOUS METHODS

Scheme	Method	Advantages / Disadvantages
Static Cache entries[1]	Use of static ARP cache entries.	Simple method but not appropriate for large networks.
S-ARP[4]	Signed ARP messages using public private keys.	Failure of third party leads to failure of whole network.
ARP Watch [5]	Monitors the traffic and generate alarms based on the rule.	Free but produce high number of alarms thus increasing work of admin.
ARP Guard [6]	Sniffing and generating alarms based on the rule.	Seems to be good but costly.
Dynamic Detection Approach based on Snort [7]	Sniffing and generating alarms based on the rules.	Free but increases the work of admin by generating high number of alarms.
Middleware Approach [8]	Block unsolicited replies and generating alarms based on the rule set.	Not a practical approach as it requires changes on all the hosts.
HProxy [9]	Client side recognition method for SSL striping attack.	Does not give any protection only detects.
HTTPSLock [10]	Protocol validator that will redirect the user to an error page in case of bogus certificate.	Depend on client side detection.
Anticap and Antidote[11]	Mechanism used to block ARP replies.	Blocks ARP reply having MAC Receiver different from the one in the cache but suitable only for specific Kernel.
AntiSniff [12]	Detecting the node currently running in loose mode.	Detects the node but requires constant monitoring and scanning.
MR - ARP [13]	Extended version of ARP to prevent attacks based on the concept of voting.	Might not be valid in 802.11 networks due to auto rate fallback.

Table 1.1 Comparisons of Various ARP Prevention Methods

DOI: 10.15680/IJIRCCE.2016. 0411225

V. RESILIENCE AGAINST ARP CACHE POISONING

During an ARP cache poisoning attack, the malicious host can either create a new fake ARP entry in the target host's ARP cache or update an already-existing ARP entry using fake IP and/or MAC addresses proved in the ARP header of the ARP message. In principal, to corrupt an ARP entry, the malicious host may use a method based on generating either fake ARP reply messages or fake ARP request messages. These two methods are explained as follow:

ARP cache poisoning based on ARP reply messages: The malicious host may attempt to send fake ARP reply messages to a target host even though the malicious host did not receive any ARP request message from the target host. If the operating system deployed in the target host accepts any ARP reply message without checking whether or not an ARP request message was generated before, then the received ARP reply message can corrupt the target ARP entry or create a new fake ARP entry.

ARP cache poisoning based on ARP request messages: Alternatively, instead of sending fake ARP reply messages, the malicious host may attempt to send fake ARP request messages to corrupt the target ARP entries or create new fake ARP entries. In this case, when a target host receives a fake ARP request message, it believes that a connection is going to be performed, and then, updates the target ARP entry or creates a new ARP entry utilizing the fake IP and MAC addresses provided in the message's ARP header. However, in practice, the success of this malicious activity depends both on the operating system deployed in the target host, and the existence of the IP and MAC addresses of the fake ARP entry in the target ARP cache before the attack attempt [3]. In fact, whether the malicious host uses fake ARP request or reply messages, there will be three possible cases that may occur. In the first case, the fake ARP message attempts to corrupt only the MAC address of an already existing ARP entry. In the second case, the fake ARP message attempts to corrupt only the IP address of an already-existing ARP entry. However, in the third case, the fake ARP message attempts to create a new fake ARP entry in the target ARP cache. That is, neither the IP address nor the MAC address of the fake ARP entry exists already in the target ARP cache.

VII. CONCLUSIONS

In conclusion the main aim of this paper is to study and differentiate between the various solutions of address resolution protocol and also discuss the limitations of these existing solutions. We analyzed several currently available solutions; identify their strengths and limitations and provide comparison among them. So we can say that this paper may be used as a reference by researchers when deciding how to secure the ARP protocol ARP needs an simple, efficient and feasible solution to tackle the possible attacks, the existing solutions has their individual drawbacks which will lead them to security threat in communication, here is a need of such mechanism which will be provide enough security and also should be feasible as per cost and effort.

REFERENCES

[1] S. Whalen, "An introduction to ARP spoofing," 2600: The Hacker Quarterly, vol. 18, no. 3, Fall 2001,.Available:http://servv89pn0aj.sn.sourcedns.com/_g bpprorg/ 2600/arp spoofing intro.pdf

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

[3] 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, Nov.2010.

[4] D. Bruschi, A. Ornaghi, and E. Rosti. S-ARP: A secure address
resolution protocol. In Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC '03), Dec. 2011.

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

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

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

[8] M. Tripunitara and P.Dutta. A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning. In Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC'99), Dec. 2013

[9] N. Nikiforakis, Joosen, "HProxy: Clientside detection of SSL striping attack", Proceedings of the 7th Conference on Detections of Intrusions and Malware & Vulnerability Assessment, 2010.

[10] A. Fung, K. Chueng, "SSLock: Sustaining the Trust on Entities brought by SSL, Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, 2010.

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

[12] 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.
[13] S. Y. Nam, D Kim and J Kim, "Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks" IEEE Common Lett, ol. 14, no. 2, (2010), pp. 187–189.
[14]Arote Prerna, and Karam Veer Arya. "Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting."Computational Intelligence and Networks (CINE), 2015 International Conference on. IEEE, 2015.
[15] Hou, Xiangning, Zhiping Jiang, and Xinli Tian. "The detection and prevention for ARP spoofing based on Snort."Computer application and System Modeling (ICCASM), 2010 International Conference on. Vol. 5. IEEE, 2010.