Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

A Review Paper on Detection and Prevention Mechanisms for ARP Attacks

Deven Bhatt[1], Vikas Jha[1]

[1]*CS&E Dept. Parul Institute of Engineering and technology*

Abstract - Network security is very important task in today's life. Basic task of it is to providing the access rights to legitimate users and monitoring the activities of network. One 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

KEY WORDS: 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, WiMax, Bluetooth, etc. For wireless network there are many types of network standards like WEP, WPA, WPA-TKIP, WPA-AES and WPA-PSK. And for securing these types of network there are multiple approaches are there. But every approaches have challenges which needs 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 thinks that it is not possible to eavesdrop the packet in switched network or in encrypted wireless (Wi-Fi). Because they thinks 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 ArpDefender for defending and ArpWatch 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.

II. ARP POISONING ATTACKS

ARP spoofing involves constructing forged ARP replies. By sending bogus ARP reactions, a target computer could be convinced to send frames destined for computer A to instead go to computer B. When done appropriately, computer A will have no idea that this redirection took place. The process of updating a target computer's ARP cache with a bogus entry is referred to as "poisoning". [3]

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

2.1. Man-in-the-middle attacks

As the name indicates, a man-in-the-middle attack occurs when someone among you and the person by whom you are communicating is actively monitoring, capturing, and monitoring your communication transparently. For example, the attacker can re-route a data exchange. When computers are connecting at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. [1]

2.2. DoS attacks

ARP spoofing is used to change the ARP cache table of host so that every packet sent by host is directed to the attacker. In this way, the attacker blocks the communication from the host being attacked. [3]

2.3. Host Impersonation

ARP spoofing is used to change the ARP cache table of host communicating with each other so that every packet sent by host is directed to the attacker. After receiving the packet from host attacker responds to it and creates impression that host is communicating with desired destination.

2.4. MITM attacks on encrypted connections

The attacker can even sit in between a protected connection (e.g., SSL or SSH). The application (e.g., the Web browser) will warn the user that the certificate given is not valid, but many users tend to ignore this kind of warnings. Furthermore, a bug in some versions of Internet Explorer enable attackers to hijack SSL sessions without the browser displaying a warning. [2]

2.5. MAC, IP Cloning attacks

The attacker changes its IP and MAC address to become matching to those of victim host. Once the change is done there will be the two host with same addresses and victim can’t decide that who is the real host and sometimes when the real host is disconnected in network the attacker can make the benefit and can attack as real host without any problem. This situation can cause the network troubles and we can say that it will lead to DoS attacks also.

2.6. Session hijacking attacks

It is also known as cookie hijacking attacks. In this attack valid computer session is to be exploited. In this attack cookie which is used to authenticate the user to remote server is to be theft and by using that cookie attacker will hijack the session of any particular user.

III. RELATED WORK

Currently following approaches are there which are proposed for solution of ARP Poisoning Problem

3.1. Using Static ARP entries

Use of static ARP entries [1] is the best defense 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.

3.2. S-ARP

D. Bruchi et al [4] proposed a new Secure-ARP (S-ARP) 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.

3.3. 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.

3.4. 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.

3.5. Dynamic Detection Approach

Hou et al. [7] proposed a dynamic detection approach which is based on the Snort. A snort is Intrusion Detection System that monitors the traffic and analyze it against a rule set defined by the user and perform the action based on what has been identified.

3.6. Middleware Approach

Tripunitara et al. [8] discussed about the middleware approach 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

3.7. 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.

3.8. HTTPSLock

It works as SSL certificate and protocol validator 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.

3.9. Anticap and Antidote

These 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.

3.10. AntiSniff

AntiSniff application 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.

3.11. MR-ARP

To prevent ARP poisoning- based MITM attacks in the Ethernet by deploying the concept of voting. It is a non-cryptographic approach. 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 favor 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), i.e., auto rate fallback (ARF).

3.12 Detection and prevention mechanism using modified icmp and voting

For detection and prevention of ARP poisoning related attacks author has proposed this scheme which is based on ICMP and voting in the centralized scheme environment. In which initially traffic over the network is sniffed by Central Server (CS). Then, CS sends trap ICMP ping packet, analyze the response in terms of ICMP reply and successfully detects attacker. In order to prevent ARP poisoning over centralized system, voting process is used to elect legitimate CS. Validating and Correcting < IP, MAC > pair entries residing in hosts cache tables, CS successfully prevents ARP poisoning while maintaining performance of the system by using the voting mechanism.

IV. COMPARISION BETWEEN VARIOUS METHODS

Scheme	Working	Pros/cons
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 set	Free but produce high number of alarms thus increasing work of admin
ARP Guard[6]	Sniffing and generating alarms based on the rule set	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 at the	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.
Arote et al.[14]	Detection using the ICMP request-reply at central server and prevention using the voting at centralized server level	Need to protect central server against IP Exhaust attacks
Hou et al.[15]	Extension to existing Snort by using sniffing and generating alarms based on the rules	Free but increases the work of administrator by generating high number of alarms

V. CONCLUSION AND FUTURE ISSUES

From the survey done and presented there are still advantages and disadvantages of every method and there is no unique and stable method for these type of attacks. So need of that kind of method is still an open issue. For that type of ideal solution some conditions should be considered like it should be widely available, easy to implement and it should follow all the basic aspects of network layer principles and also should be backward compatible to address resolution protocol (ARP). And ideal solution should use minimum cryptographic function so that its performance is good enough.

VI. 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: Client side 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, vol. 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.