Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis on Various Methods to Detect Arp Cache Poisoning Attack

Navneet Kaur Garcha
Student
Dept. of CSE Lovely Professional University
Phagwara, Punjab, India

Md Ataullah
Asst. Professor
Dept. of CSE, Lovely Professional University
Phagwara, Punjab, India

Abstract: Security is at the forefront of most networks. However, one area that is often left untouched is hardening layer 2 and this can open the variety of attacks and compromise. Address Resolution Protocol is the mapping of IP address to the MAC address (layer 3 to layer 2 mapping). The protocol has proved to work well under regular circumstances, but it was not designed to cope with malicious hosts. ARP provides no authentication mechanism to the incoming request packets. This is the reason that any client can forge an RP message contains malicious information to poison the ARP cache of target host. There are many possible attacks on ARP which can make the communication unsecure such as man-in-the-middle (MITM), Denial of Service (DOS), cloning attack, session hijacking and many more attacks. In this paper, we have described various detection and preventing schemes towards the ARP cache poisoning attacks and presented their advantages and disadvantages.

Keywords: ARP (Address Resolution Protocol), MITM (Man-In-The-Middle) Attack, DoS (Denial of Service)

I. INTRODUCTION

A computer connected to and IP/Ethernet LAN has two addresses: one is the MAC address, second is the IP address. The ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle attack or session hijacking attacks [10]. The Address Resolution Protocol (ARP) is used by computers to map network addresses (IP) to physical addresses (MAC). When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the Arp program to find a physical host or MAC address that matches the IP address. The ARP looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the cache for future reference and then sends the packet to the MAC address that replied.

In an Ethernet, the MAC addresses of two hosts must be available for the two hosts to communicate with each other. Each host in an Ethernet maintains an ARP table, where the latest used IP address-to-MAC address mapping entries are stored.

II. ARP PROCESS

Suppose that host A and host B are on the same subnet and that host A sends a message to host B. the resolution process is as follows:

1) Host A looks in its ARP mapping table to see whether there is an ARP entry for host B. if host A finds it, host A uses the MAC address in the entry to encapsulate the IP packet into data link layer frame and sends the frame to host B.
2) If host A finds no entry for host B, host A buffers the packet and broadcasts an ARP request, in which the source IP address and source MAC address are respectively the IP address and MAC address of host A and the destination IP address and MAC address are respectively the IP address of host B and an all-zero MAC address. Because the ARP request is sent in broadcast mode, all hosts on this subnet can receive the request, but only the requested host (namely host B) will process the request.
3) Host B compares its own IP address with the destination IP address in the Arp request. If they are the same, host B saves the source IP address and source MAC address into its Arp mapping table, encapsulates its MAC address into an ARP reply, and unicasts the reply to host A.
4) After receiving the ARP reply, host A adds the MAC address of host B into its ARP mapping table for subsequent packet forwarding. Meanwhile. Host A encapsulates the IP packet and sends it out.

Usually, ARP [8] dynamically implements and automatically seeks mappings from IP addresses to MAC addresses, without manual intervention.

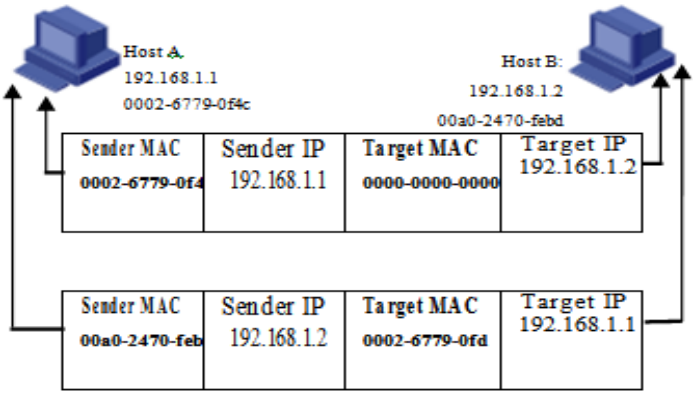

Fig 1: ARP Request and Reply

III. VULNERABILITIES OF THE ADDRESS RESOLUTION PROTOCOL

The Address Resolution Protocol (ARP) [1] is a widely used protocol for resolving network layer addresses into link layer addresses. When an Internet Protocol datagram is sent from one host to another on a Local Area Network, the destination IP address must be converted into MAC address for transmission via Data Link Layer. When another host's IP address is known, and its MAC address is needed, a broadcast packet is sent out on the local network. This packet is known as an ARP request Fig1. The destination machine with the IP in the ARP request then responds with an ARP reply fig1, which contains the MAC address for that IP.

ARP is a stateless protocol. Network hosts will automatically cache any ARP replies they receive, regardless of whether or not they requested them. Even ARP entries which have not yet expired will be overwritten when a new ARP reply packet is received. There is no method in the RP protocol by which a host can authenticate the peer from which the packet originated. This behavior is the vulnerability which allows ARP spoofing to occur.

IV. AN ANATOMY OF ARP SPOOFING ATTACK

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.

After the ARP was drafted, a subtle weakness was found. In fact, 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.ARP is a simple protocol that it works on the following. ARP-request, the host wants to learn the MAC address of the another host in a particular network, broadcasts the ARP request on the network "Who has IP xxx.xx.xx.xx ? tell me your MAC address mm.mm.mm.mm.mm".

ARP-reply, all the host in the particular network receives the request. The hosts with the given IP address will reply in a unicast ARP reply and send its MAC address to the requester. 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.

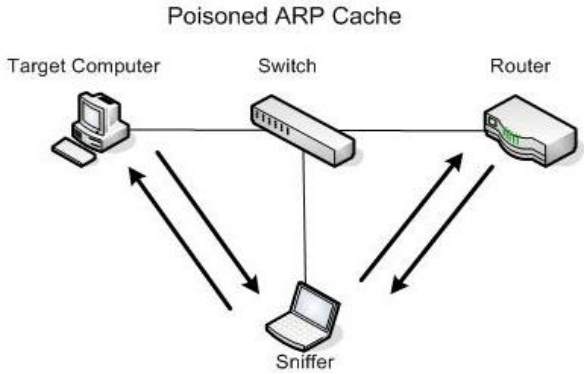

Fig 2: ARP Cache Poisoning Attack

V. THE ARP ATTACKS

A. Session Hijacking and Interception

The attacker attacks the integrity of the session by trying to hijack an authorized session from an authorized user.

B. Man-in-the-Middle 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.

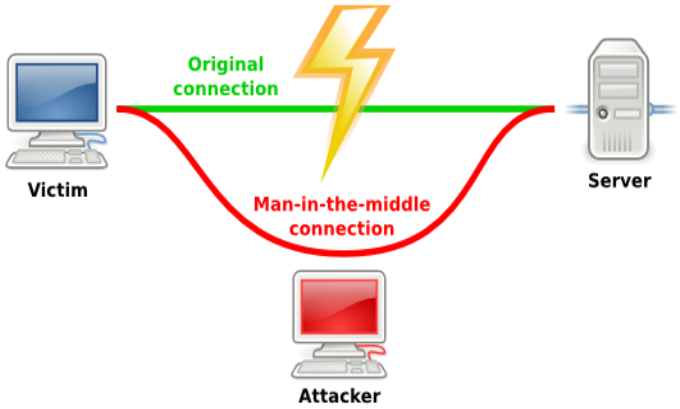

Fig 3: Man-In-The-Middle Attack

C. Denial of Service

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.

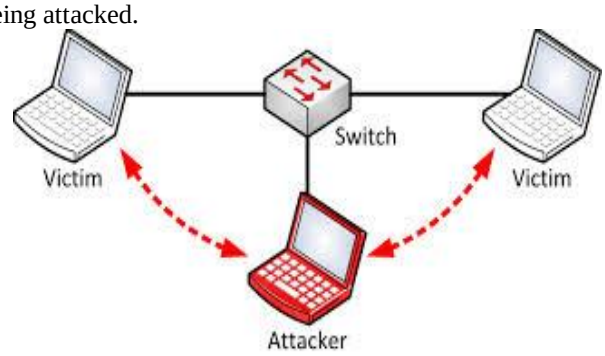

Fig 4: Denial of Service Attack

D. 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.

VI. LITERATURE REVIEW

There are several solutions proposed to solve the ARP spoof problem. However, most of them have some critical drawbacks. The previous solutions are grouped below in compact form with their strengths and limitations as follows:

A. S-ARP: a Secure Address Resolution Protocol

Bruschi et al. proposed a secure address resolution protocol (SARP), which provides the protection against ARP poisoning. Each host has a public/private key pair certified by a local trusted party on the LAN, which acts as a Certification Authority. Messages are digitally signed by the sender, thus preventing the injection of spurious and/or spoofed information. As a proof of concept, the proposed solution was implemented on a Linux box [2]. The Address Resolution Protocol cache poisoning technique relies on the hosts caching reply messages even though the corresponding requests were never sent. Since no message authentication is provided, any host of the LAN can falsify a message containing poisonous information. Performance measurements show that PKI based strong authentication is feasible to secure even low level protocols, as long as the overhead for key validity verification is kept small.

B. T-ARP: A Ticket-based Address Resolution Protocol

Lootah et al. implemented the Ticket-based Address Resolution Protocol (TARP). TARP implements security by distributing centrally issued secure MAC/IP address mapping attestations through existing ARP messages. IP networks fundamentally rely on the Address Resolution Protocol for proper operation. Unfortunately, vulnerabilities in the ARP protocol enable a raft of IP-based impersonation, man-in-the-middle, or DoS attacks. Proposed countermeasures to these

vulnerabilities have yet to simultaneously address backward compatibility and cost requirements [3]. The Researcher details the TARP protocol and its implementation within the Linux operating system. The experimental analysis depicts that TARP leads to the improvement of the costs of implementing ARP security by as much as two orders of magnitude over existing protocols. They conclude by exploring a sort of operational issues related to the deployment and administering the ARP security.

C. *Various Solutions for Address Resolution Protocol Spoofing Attack*

Security is at the backbone of most networks, and many companies implement a comprehensive security policy encompassing many of the OSI layers, from application layer all the way down to IP security [4]. However, one area that is often left untouched is hardening Layer 2 and this can open the network to a variety of attacks and compromises. Address resolution protocol is the mapping of IP address to the MAC address. ARP provides no authentication mechanism to the incoming request packets this is the reason that any client can fake an ARP message contains dangerous information to poison the ARP cache of target host. There are several possible attacks on ARP which can make the communication unsecure such as man-in-the-middle, Denial of service, cloning attack, session hijacking and many more attacks.

D. ES-ARP: An Efficient and Secure Address Resolution Protocol

Ataullah et al. proposed one of the latest and new proposal for ARP security mechanism [10]. In this paper researcher describe ARP, define many attainable ARP cache poisoning attacks and provides the careful of some attack eventualities in network having each wired and wireless hosts. It also analyzes the every planned solution, establish their strengths and limitations. Finally get that no answer offers a possible answer. Hence, this paper presents associate economical and secure version of ARP that's ready to cope up with of these varieties of attacks and is additionally a possible answer. The Address Resolution Protocol is employed by computers to map logical addresses to physical addresses. But ARP is associate all trusting protocol and is stateless that makes it liable to several ARP cache poisoning attacks like Man-in-the-Middle and Denial of service attacks. These flaws lead to security breaches therefore weakening the charm of the pc for exchange of sensitive knowledge. It's a stateful protocol; by storing the knowledge of the Request enclose the poet cache, to cut back the probabilities of assorted varieties of attacks in ARP. it's additional economical and secure by broadcasting ARP Reply enclose the network and storing connected entries within the ARP cache anytime once communication occur.

E. Active Detection and Prevention of Sophisticated ARP Poisoning Man-in-the-Middle Attacks on Switched Ethernet LANs

Kalajdzic et. al describes the two novel methods for active detection and prevention of ARP poisoning- based Man-in-the-Middle attacks on switched Ethernet LANs [11]. As a stateless and inherently insecure protocol, ARP has been used as a relatively simple means to launch Denial-of-Service and MITM attacks on local networks and multiple solutions have been proposed to detect and prevent these types of attacks. MITM attacks are particularly dangerous, because they allow an attacker to monitor network traffic and break the faithfulness of data being sent over the network. This paper introduced the backward compatible techniques to prevent ARP poisoning and deal with sophisticated stealth MITM programs.

F. Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks

This paper is designed to introduce and explain ARP spoofing and its role in Man-in-the-Middle attacks. The term Man-in-the-Middle is historical usage; it does not imply that only men can use these attacks. Perhaps Teenager-in-the-Middle or Monkey-in-the-Middle would be more accurate terms .The classic Man-in-the-Middle attack relies on convincing two hosts that the computer in the middle is the other host. This can be accomplished with a domain name spoof if the system is using DNS to identify the other host or ARP spoofing on the LAN.

G. ARP Poisoning Attack Detection and Protection in WLAN via Client Web Browser

ARP cache poisoning is operation of entering a fake IP to Ethernet address in another host's ARP table. It diverse the travelling traffic, either to a different host on the LAN or no host at all. Consequently, It can be used to cooperate the subnet, although ARP spoofing is possible only inside a LAN, it is still a security risk. ARP Spoof is a serious security problem; it can be used for Denial of Service or Man in the Middle attacks. There have been several solutions, proposed to solve this problem. Yet, all of the previous have some critical drawbacks such as infeasibility, unmanageability, high cost, performance penalty and ineffectiveness. Hence, in this paper, Behboodian et. al proposed a new solution to detect and protect clients, which is feasible, manageable, effective, low cost, platform independent and usable for both small and medium network sizes [13]. In this method they utilize user's web browser to detect the attack and protect user from ARP cache poisoning while cutting off the attacker from WLAN.

H. Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN

An improved version of address resolution protocol is proposed to prevent ARP poisoning based man-in-the-middle attacks in wired or wireless LAN environments [14]. The proposed method is based on the scheme that when a node knows the correct MAC address for a given IP address, if it does not delete the mapping while the machine is alive, then MITM attack is not possible for that IP address. For the prevention of MITM attack even for a new IP address, researcher proposed a new IP/MAC mapping conflict resolution mechanism based on computational puzzle and voting. This

proposed scheme can efficiently mitigate ARP poisoning-based MITM attacks, even in Wi-Fi hot-spots where wireless machines can easily come and leave, since the proposed mechanism does not require manual configuration if the proposed ARP is deployed through operating system upgrade. The proposed scheme is backward compatible with the existing ARP protocol and incrementally deployable with benefits to the upgraded machines.

VII. COMPARISON OF EXISTING SOLUTIONS

The table below briefly shows the comparison between the different existing solutions for ARP cache poisoning attack.

EXISTING SOLUTIONS	CATEGORY	OPERATION MODE OF ARP CACHE TABLE	COMMUNICATION PROTOCOL	MECHANISM USED
Bruschi et al.[2]	Cryptography, Server-based	Dynamic	Modified ARP	Signed ARP replies
Lootah et al.[3]	Server-based cryptography	Dynamic	ARP	Centrally issued tickets authenticate (IP,MAC) association
Ataullah et al. [10]	N/A	N/A	ARP	ARP-reply is broadcasted at every ARP request
Kalajdzic et. al [11]	Host-based	N/A	ARP	Backward compatible techniques to prevent ARP poisoning
Behboodian et. al [13]	N/A	N/A	ARP	Utilized user's web browser for detection

VIII. CONCLUSION

In conclusion, the main aim is to differentiate between the various solutions of ARP and also discuss the limitations of the existing solutions. We analyzed several available solutions, identify their strength and limitations and provide the comparison among them.

REFERENCES

[1] http://en.wikipedia.org/wiki/ARP_spoofing

[2] Bruschi, D., Ornaghi, A., Rosti, E.: "*S-ARP: a secure address resolution protocol*". Proc. 19th Annual Computer Security Applications Conf.(ACSAC2003), Las Vegas, NV, USA, December 2003

[3] Lootah, W., W. Enck, and P. McDaniel."*TARP: ticket-based address resolution protocol."* in Computer Security Applications Conference, 21stAnnual. 2005

[4] S.Venkatramulu, Dr.C.V Guru Rao, "*Various Solutions for Address Resolution Protocol Spoofing Attack*", International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.

[5] Williem Burgers, Roel Verdult, and Marko van Eekelen: "*Prevent Session Hijacking by Binding the session to the Cryptographic Network Credentials*", 2013

[6] M.A. Carnut and J.C. Gondim: "*ARP Spoofing detection on Switched Ethernet networks: A feasibility study*,"in proceedings of the 5th Symposium on Computer Security, November 2003.

[7] Andre P. Ortega, Xavier E. Marcos, Luis D. Chiang and Cristina L: *"Preventing ARP Cache Poisoning Attacks: A Proof of Concept using OpenWrt"*, 2009.

[8] http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/WLAN/Access_Point/H3C_WA2200_Series_WLAN_Access_Points/Configuration/Operation_Manual/H3C_WA_Series_WLAN_Access_CG-6W100/05/201009/691546_1285_0.htm

[9] RFC-826: "*An Ethernet address resolution protocol*", 1982.

[10] Md. Ataullah and Naveen Chauhan," ES-*ARP: an Efficient and Secure Address Resolution Protocol*",978-1-4673-1515-9/12 ©2012 IEEE.

[11] K. Kalajdzic1,2 and A. Patel, "*Active Detection and Prevention of Sophisticated ARP Poisoning Man-in-the-Middle Attacks on Switched Ethernet LANs*", Sixth International Workshop on Digital Forensics & Incident Analysis (WDFIA 2011).

[12] Robert Wagner, "*Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks*", Practical Assignment GSEC Version 1.2f (amended August 13, 2001), Updated June 2006 Jeff Bryner, CISSP,GCIH-Gold, GCFA-Gold.

[13] Navid Behboodian and Shukor Abd Razak, "*ARP Poisoning Attack Detection and Protection in WLAN via Client Web Browser*", International Conference on Emerging Trends in Computer and Image Processing (ICETCIP'2011) Bangkok Dec., 2011.

[14] Seung Yeob Nam*, Sirojiddin Jurayev, Seung-Sik Kim, Kwonhue Choi and Gyu Sang Choi,"*Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN",* EURASIP Journal on Wireless Communications and Networking, 2012.

