A NEW VERIFICATION METHOD TO PREVENT SECURITY THREADS OF UNSOLICITED MESSAGE IN IP OVER ETHERNET NETWORKS

Waleed Kh. Alzubaidi[1], Dr. Longzheng Cai[2] and Shaymaa A. Alyawer[3]

[1]Information Technology Department, University of Tun Abdul Razak, Selangor, Malaysia
waleed@ieee.org

[2]University of Unitar International, Selangor, Malaysia
charles_cai@unitar.my

[3]Computer Science Department, Baghdad College, Baghdad, 645, Iraq
sha_amh@yahoo.com

ABSTRACT

Internet is widely depends on the IP over Ethernet networks architecture. IP and Ethernet protocols uses in each Local Area Network LAN, wire and wireless. Due to the rapid expansion of the technology field this architecture reveals many shortcomings. TCP/IP suite protocols are consists from layers, each layer accomplish its jobs separately. However, these layers susceptible to different attacks. Data link layer one of the most layers targeted by the attackers. Attack at lower layer may lead to more sophisticated attacks to upper layers, like Man-in-The-Middle (MiTM), DNS spoofing and Denial of Service (DoS). These attacks applicable even with encrypted protocols such as HTTPS and SSL. In this paper we discuss the security in the Data Link Layer in IP over Ethernet networks and the attacks depend on the Address resolution protocol (ARP). Moreover, explain our proposed method to prevent address resolution protocol attacks.

KEYWORDS

IP, MAC address, Ethernet, ARP, Security, Performance

1. INTRODUCTION

The continued growth and development in the technology fields have introduced new challenges in the Internet and revealed some of its insufficiency. For example, recently, there have been discussions on Internet Protocol (IP) addressing architecture and its functions [1] [2]. IP addresses were overloaded since they used to represent the node identities and networks locations. In addition, the current naming architecture in IP over Ethernet networks imposes security problems. Moreover, the basic assumption about trusting in the Internet is not valid anymore. Now a wide range of users share the Internet, while the use of the Internet in the early, mostly for academic purposes. Moreover, the arguments of the end-to-end of the Internet are violated since new mechanisms, such as firewalls, Network Address Translators (NATs), etc.,

DOI : 10.5121/ijcnc.2012.4602

are placed in the networks. As a result, there are many researches proposed a different architectures and protocols to improve the Internet in the literature.

The methodology that used to perform addressing in the link layer and the mapping between network (IP address) and data link layer (MAC address) is insufficient to provide aspects of secure in local area networks as well. IP addresses uses to identify nodes in the network layer, while Media Access Control (MAC) addresses uniquely identify network nodes in the data link layer in local networks. The binding between IP and MAC addresses in Ethernet Local Area Networks (LANs) is accomplished by the Address Resolution Protocol (ARP). See figure 1.a, 1.b. However, the binding process between the IP and MAC addresses are not secure. Moreover, despite the MAC address should be unique for each network interface card, now it can be easy to change.

In this study, we propose a compatible-backward modification on current naming architecture to secure the data link layer (Layer 2) in Internet protocol (IP) over Ethernet networks. Moreover, improve the performance by applying the reduction on the transmission process.

2. ARP Problem

ARP introduces a security risk to Data link layer, since ARP messages can easily be spoofed. Attacker can apply a serious attack like Man-In-The-Middle and MAC flooding. An attacker can send forged ARP message to host within local network to redirect the traffic that going to gateway router or another peer host to rogue that network device. This is the Man in the Middle attack. Whereas in flooding attack, the attacker sends a spoof ARP replies to the switch to overflow the buffer of CAM table where store MAC addresses and corresponding switch port number and VLAN. Depending on switch setting and capacity some switches goes to Hub mode then broadcast the frames into all ports allowing sniffing. there is another possible attacks on the Data Link Layer, Like MAC cloning, Hijacking, Denial of service (DoS) and broadcasting[9].In Denial of service, Attacker poisoning victim's ARP cache table, by sending a forged ARP message with IP of the gateway as an example and nonexistence MAC address. In this case victim cannot connect with the destination. attacker may be cheat switch CAM table to enable Denial of Service, by sending forged frame with source MAC address of the victim so any frame send to victim switch will forward it to port of attacker.

One of the recommended actions against ARP attacks is applying static ARP entries in host cache table. Apply it will be prevents most of the attacks. But it is impractical, because each new host machine administrator should update ARP table in all other machines or when new network interface card NIC is replaced, and does not allow utilizing from Dynamic Host Configuration Protocol DHCP. In addition, most operating systems updates its ARP table when receive a gratuitous ARP even with static entries. Lastly, it does not solve the binding issue problem for IP and MAC address.

We observed a core problems related to link layer that causes vulnerabilities and creating an overhead.

First, there is no secure mapping between IP and MAC addresses. Due to that there are several possible ARP attacks on the Data Link Layer. In fact, the main cause for the problem is the naming architecture, and it is not fail from ARP. ARP is a protocol design to work with exist naming architecture used in the network stack. May be considering the naming architecture is the main reason for these issues. Ideally, a host should not have its identity tied to another address type. Instead there should be a naming architecture to identify host with one address type, without need to tie with MAC address. Another possible solution should be a mechanism to verify ARP sender and to confirm there is no conflict binding IP to MAC address.

Second, the constantly mapping IP to MAC address introduce an overhead. In IP over Ethernet networks, after the device initiated its network stack, it is identify its self with MAC as Layer 2 address, and establishes its IP address as layer 3 address. MAC address used to identify network device in local network. However, more efficient naming architecture may able to use one addressing type after initiation its network stack. So no more constantly mapping needed. Using only IP address to identify the host, and use it as a destination address in sending Ethernet frame to the target node. Like this new naming architecture may requires a change in layer 2 architecture. However, more advantages gained by satisfying optimization in the process of the layer and enhance network resources. In this case there is no need for mapping processes. Still network devices like bridges and switches need to maintain table for IP and their ports.

3. SECURITY IN DATA LINK LAYER

The data link layer in IP over Ethernet networks is susceptible to various attacks since the Layer 2 security and performance has not been take enough attention yet. The most known Layer 2 attacks are Man In The Middle (MITM), MAC spoofing, ARP poisoning, Denial of Service (DoS), MAC flooding, and port stealing.

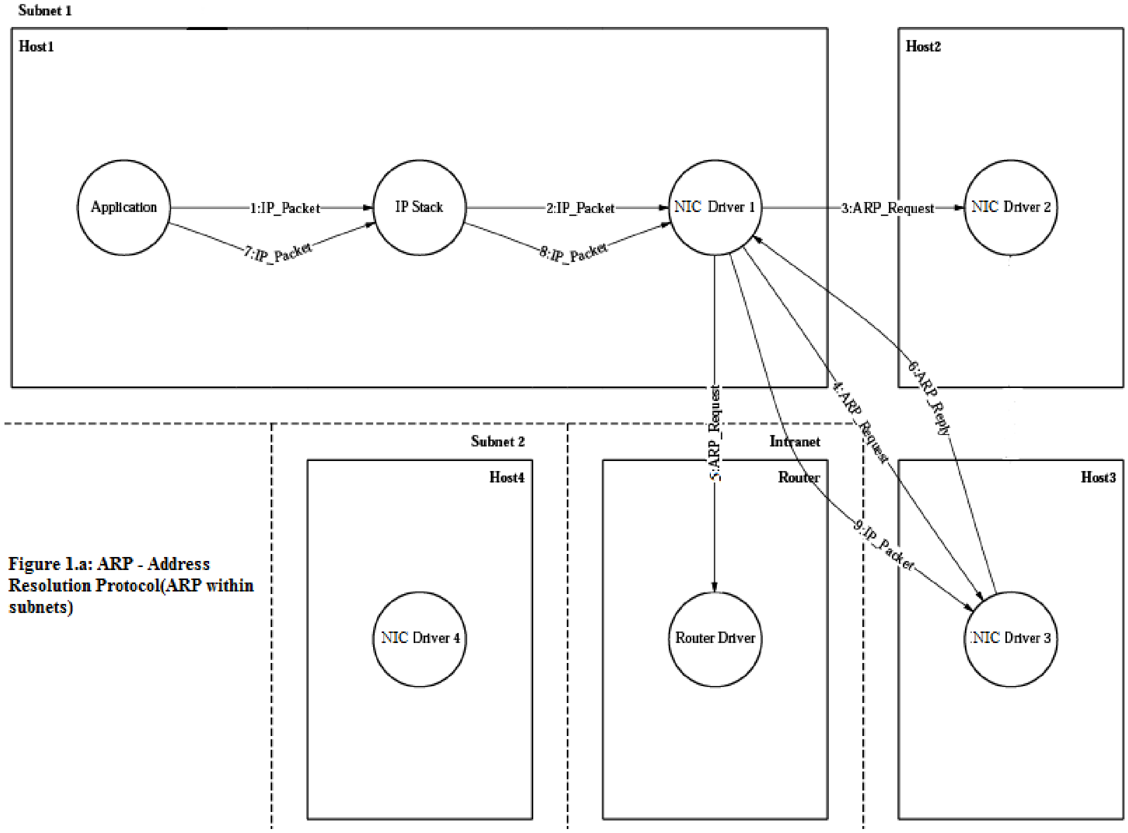


Figure 1.a: ARP - Address Resolution Protocol(ARP within subnets)

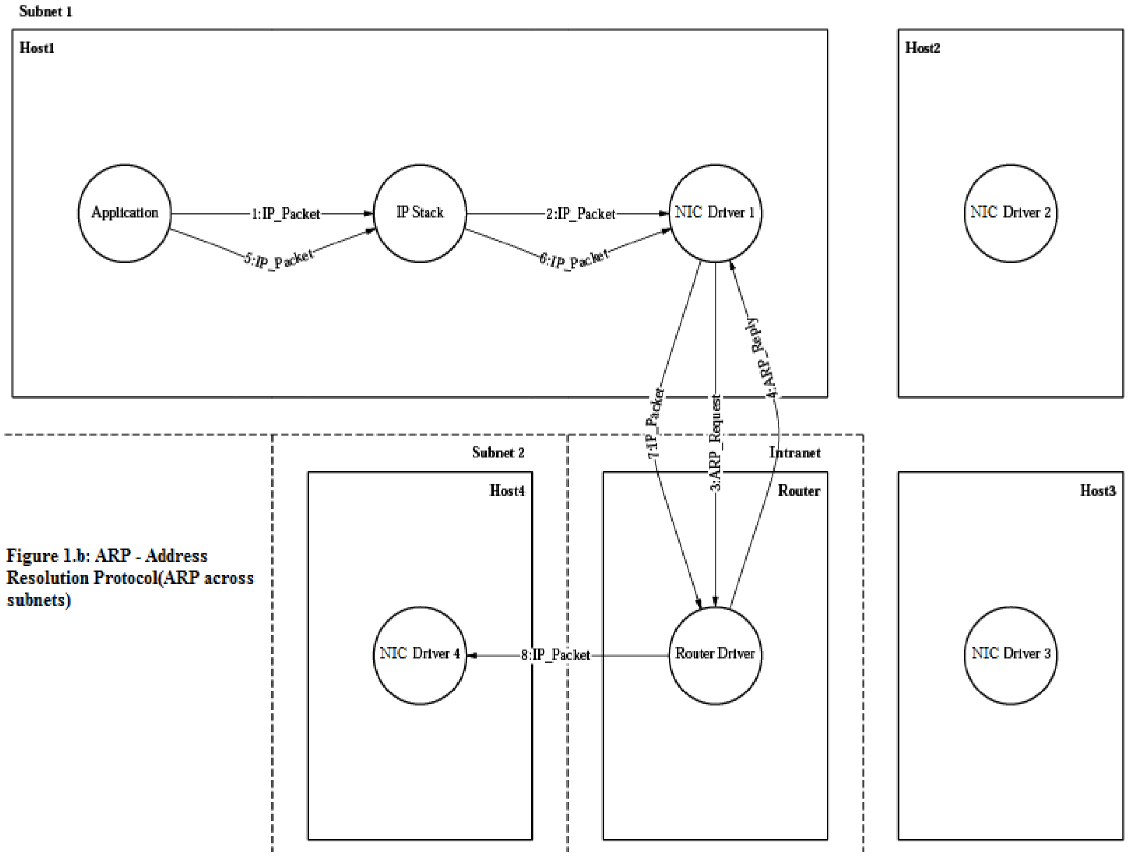


Figure 1.b: ARP - Address Resolution Protocol(ARP across subnets)

Address Resolution Protocol (ARP) is a network layer protocol that used to map the IP address to physical address (MAC Address) in the local area network. When a host wants to know the MAC address for an IP address, it broadcasts an ARP request including the IP address of the target on to the network. The node that owns the IP address return ARP reply message with its MAC address. Each node in the network build a table, called ARP cache, used to store and mapping IP addresses to MAC addresses.

Due to ARP is a stateless protocol, each time a host gets an ARP reply, and even it does not send an ARP request for this reply, it will updates its ARP cache table with this ARP reply [4]. The process of updating a target host's ARP cache with a fake entry is referred to as poisoning. Attacker sends a fake ARP reply message with IP address of host B and the MAC address of attacker to host A. Additionally, the attacker sends a fake ARP reply with IP address of host A and the attacker's MAC address to host B. The traffic between host A and B pass through the attacker machine allowing sniffing. This attack called Man In The Middle (MITM), can be performed between any two nodes in the networks like host and a router as well.

Ethernet switch build a table, called Content Addressable Memory (CAM) tables. With limited size it store binding MAC addresses to physical switch port numbers, and stores Virtual Local Area Network (VLAN). In the flooding attack, the attacker floods the network switch with MAC addresses using fake ARP frames to fill the CAM table. Then, the Ethernet switch starts broadcasting the traffic without switching to right port similar to hub mode.

Another attack called port stealing attack. The port stealing attack uses mechanism of the switches in how binding MAC addresses to physical switch ports. When a switch receives Ethernet frame from a port, it binds the port number with a source MAC address. The attacker in this attack, first, floods the switch with fake ARP frames including the target host MAC address as the source address and the attacker MAC address as the destination address in ARP reply frame. Since the target host also sends normal frames traffic, with consideration a race condition. The switch receive frames from two different ports with the same source MAC address and continuously changes the binding of the MAC address to the port in CAM table. If the attacker is faster in sending frames, the frames that intend for the target host will send to the attacker's switch port instead to the target host. Attacker steals the target host’s port so the traffic going through it first, and then to the target host. The attacker then will send an ARP request. The attacker asks for the target hosts' MAC addresses in the ARP request.

During waiting for the ARP reply, the attacker stops sending fake ARP request frame. The receiving an ARP reply means that the target hosts' port in the switch has been restored to the normal binding. After receiving the ARP reply, the attacker will forward the frame to the target host. Whole process will repeats by the attacker for each new frames [5] [6].

Additionally to these attacks, there are layer-2 base attacks like broadcasting attack and Denial of Service DoS, MAC cloning, and hijacking attacks. The broadcasting attack, the attacker broadcast forged ARP replies. These ARP replies will update ARP cache table on the all network hosts setting MAC address of the network router Gateway to the broadcast address. That makes all hosts outbound traffic to be broadcasted enabling sniffing. This type of attack also exhausted network resources affects the network capacity. In Layer 2 based Denial of Service DoS attack, the attacker updates the ARP caches for the network hosts by sending nonexistent MAC addresses.

Each network interface card in the network is supposed to have a globally unique MAC address. However, now it can be easily to change enabling MAC cloning attack. The attacker uses a Layer 2 based DoS attacks to disable layer 2 network connection to the victim and then uses the pair IP and MAC addresses of the victim. In the hijacking attack that is Layer 2-based, an attacker impersonate of connection between two network hosts. For example, the attacker takes the control of Telnet session after the victim logs into the remote node.

3.1 Security problems with DHCP Protocol

In LANs, The Dynamic Host Configuration Protocol (DHCP) is used to assign IP addresses dynamically to network nodes for a period of time. It is possible to attack DHCP servers by DoS attack in the network or impersonate a DHCP server. As example, the attacker may apply a DoS attack by generating a large number of DHCPDISCOVER messages to request IP addresses, by spoofing a different MAC address for each message frame. Then the attacker (the rogue client) responds to the resulting of DHCPOFFER to quickly exhaust available IP addresses at the DHCP servers. Some of DHCP servers use a static DHCP entry list for specific MAC addresses to restrict clients. However, since clients with dynamic address response to the request query and broadcast their MAC addresses, the attacker can easily spoof these MAC addresses. An attacker may use a DoS attack to prevent a specific node accessing to the network. The attacker later can renew the IP lease of the target node, so the attacker can use the victim's IP address as a hijacking attack. Additionally, it is possible to get service on a network by listening a valid MAC address and then spoofing it [7].

The Data Link layer attacks presented in previous are not comprehensive. There is another attacks worth to mention like, eavesdropping, replay, message insertion, deletion, modification, failover analysis, multicast brute-force, Random Frame Stress attack, and attacks based on proprietary protocols. Attacks summarized in this section reveal that enhance the performance and securing data link layer architecture is necessary to avoid problems and prevent these vulnerabilities.

3.2 Mitigation

There are many ways to mitigate these types of attacks. One of recommended actions is using port security on the switch. The Port security option binds a physical port of the switch to a MAC address. It allows the administrator to set a list of fixed MAC addresses to a port, or it can be auto configured by the switch during the first frame transmission on the port. A change in the specified MAC address for a port or flooding of a port can be controlled in many different ways through switch configuration. The port can be configured to shut down or block the MAC addresses that exceed a specified limit. Because of the performance impact involved in keeping track of the additional MAC addresses, the recommended best practice is to shut down the port that exceeds the limit [8]. Port security prevents MAC flooding and cloning attacks. However, the port security does not prevent ARP spoofing. Port security validate source MAC address in the frame header, but ARP frames include an additional source MAC field in the data payload, and clients use this field to populate their caches [10].

Another method for the defense is to deploy Intrusion Detection Systems IDS. These systems can be configured to listen for excessive amounts of ARP traffic. However, IDS are susceptible to false positive reports. Also there are tools specifically designed to listen for ARP traffic on the networks such as Arpwatch [3]. Arpwatch monitors Ethernet frames activity and maintains a database to store pairs of Ethernet MAC/IP address detecting on the network. It generates alerts to the network administrator via email if any change happens.

Another recommended action against ARP attacks is applying static ARP entries in host cache table. Apply it will be prevents most of the attacks. But it is impractical, because each new host machine, administrator should update ARP table in all other machines or when new network interface card NIC is replaced, and does not allow utilizing from Dynamic Host Configuration Protocol DHCP. In addition, most operating systems updates its ARP table when receive a gratuitous ARP even with static entries. Lastly, it does not solve the binding issue problem for IP and MAC address.

Moreover, it possible to employ Reverse ARP protocol (RARP) to detect MAC cloning. Additionally, there are methods to detect node with promiscuous mode on the network.

4. Solving IP / MAC Address Binding Problem

We believe there are two possible approaches to solve binding problem: a new efficient protocol that use one addressing type instead of IP and MAC address. While the problem essentially in mapping process. The protocol should in Data Link Layer and do not have mapping process. The new protocol may use only IP address to identify the Host when start its network stack. Involve like this protocol have many advantages points compared to conventional one like no need for ARP cache table, that means no for attacks that depends on ARP process like spoofing ,Man in

The Middle MiTM, sniffing and all sophisticated attacks that generated from basic ARP attack , also in operating side the effect will be optimized the duties that generated to take care of ARP processes (sending, receiving and maintaining ARP cache table) and no space needed for building cache table, However, the content address memory CAM table in the switch will still need to maintain with new addressing state.

Second approach, A new verification scheme is needed to identify ARP sender identity, this approach able to confirm there is no more than one host at same time have same MAC address. In this scheme may be use More ARP process steps, like send extra ARP request to confirm ARP sender or before update ARP cache table. However in next section will discuss in more detail about this scheme.

4.1 New Model

In this section we will describe our propose solution for ARP binding process. The problem was in verifying ARP sender identity. This scheme tries to verify the ARP sender identity. When host need to know MAC address of another host it will be broadcast ARP request in the network, in this case the host that own the right target IP address will send ARP reply with its own MAC address. Also in the same time may be a malicious user that planning to attack sends forged ARP reply to coincide router gateway MAC address to apply spoof ARP attack and may be establish MITM attack. By poisoning ARP cache table, and in this point we will make a change to the procedure when host receive ARP reply or in any case to update cache table (like ICMP process when the target host receive ICMP packet it will be reply and update ARP cache table) by memorize the IP and MAC for arrived message for a temporary period of time, and that will be before update the cache table then broadcast ARP request(this step we called a verification process) in this case we will inform all host within LAN including the right host will reply and when receive it, we compare our memorized entry with deliver one if it is identical then system will update ARP cache else system will inform upper layer. For more we will describe it in steps:

To make it easy to understand the approach, scenarios in possible cases will be presented as follows:

Scenario 1: Receive solicited reply:

1. Host A broadcast ARP request to know MAC address of host B. See figure 2.

2. Host B receive the request and send a unicast reply with IP_x/MAC_y to host A

3. Host A receive the reply and memorize entry for temporary time before update ARP table

4. Host A broadcast ARP request with $IP_x/MAC_?$ (step for verification process)

5. Host A receive ARP reply if it is match with what store before then update ARP cache table

else don't update ARP cache table and inform upper layer

Host may be receive two or more reply do same in previous step

Scenario 2: Receive Unsolicited ARP reply

1. Host A receive unsolicited ARP reply with entry IPx/MACy

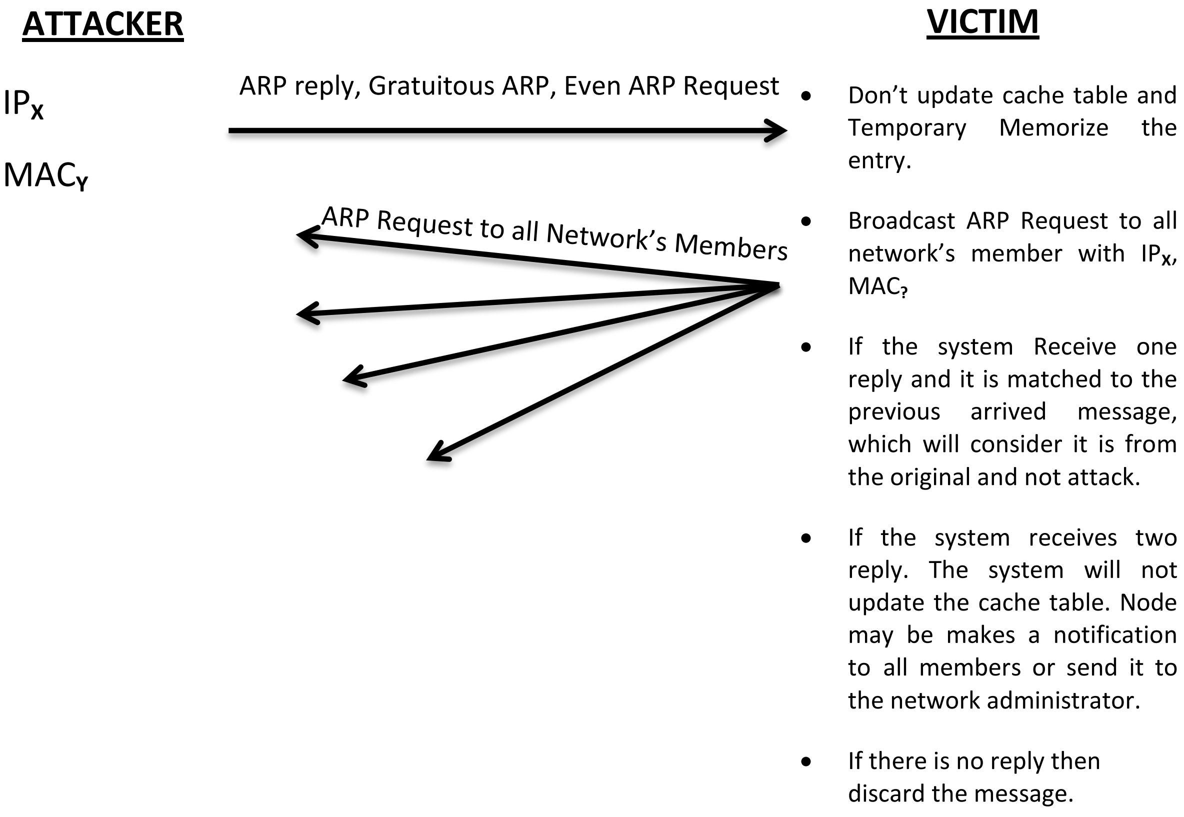
2. don't update ARP cache table and memorize the entry for temporary time until do verification process

3. Host A broadcast ARP broadcast with IPx/MAC?

4. Host A receive ARP reply, if it is match with what store then update ARP cache table

else don't update and inform upper layer

Host may be receive two or more reply then don’t update ARP cache table and inform Upper layer


ATTACKER
VICTIM
IP_X
MAC_Y
ARP reply, Gratuitous ARP, Even ARP Request
ARP Request to all Network’s Members

- Don’t update cache table and Temporary Memorize the entry.
- Broadcast ARP Request to all network’s member with IP_x, $MAC_?$
- If the system Receive one reply and it is matched to the previous arrived message, which will consider it is from the original and not attack.
- If the system receives two reply. The system will not update the cache table. Node may be makes a notification to all members or send it to the network administrator.
- If there is no reply then discard the message.

Figure 2: Algorithm to Manipulate Unsolicited

Scenario 3: Receive ICMP packet (Ping) or gratuitous ARP (GARP)

Some operating systems its ARP cache table when receive ICMP packet or gratuitous ARP. Interestingly, even in static ARP case, the system when receive Gratuitous ARP it will be update its ARP cache table. Our propose approach is very effective in this case and the scenario will be as follow. Also see figure 3:

1. Host A receive ICMP packet or gratuitous ARP with IP_X/MAC_Y

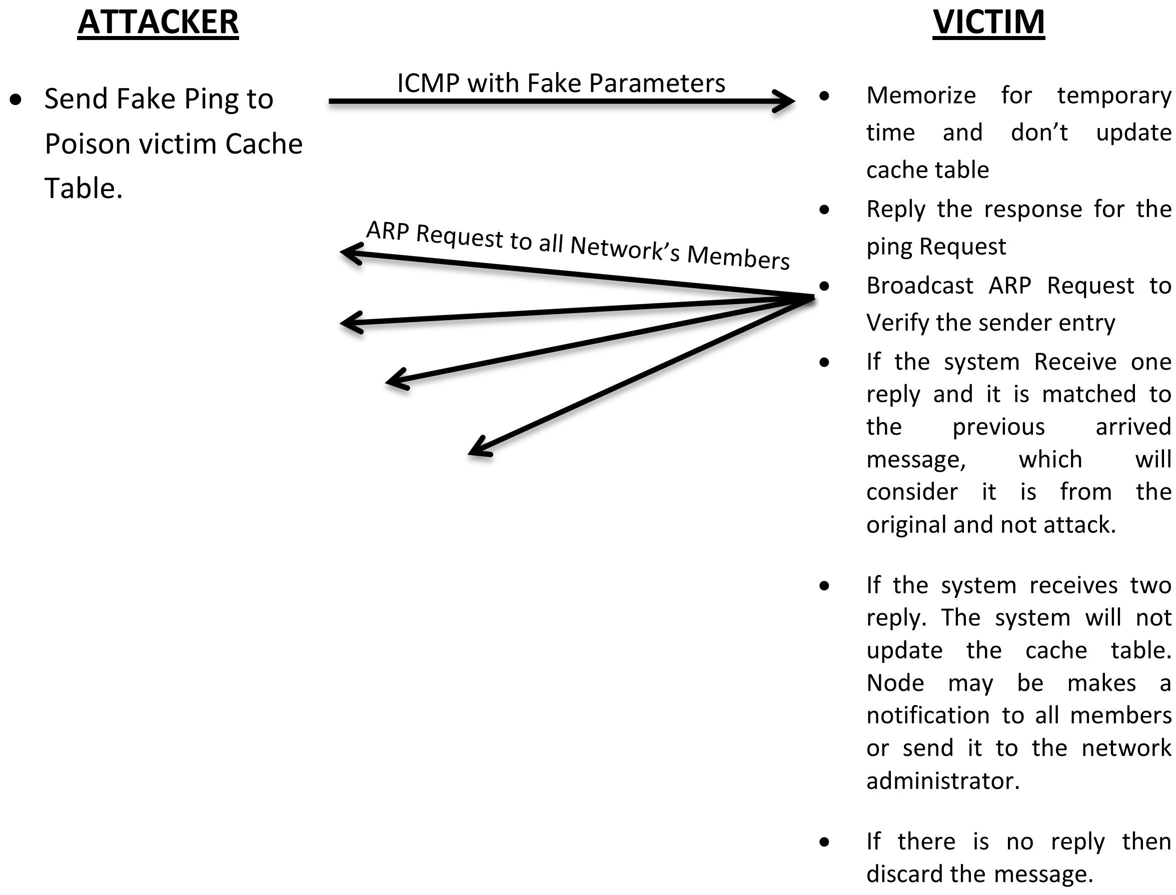
2. Memorize entry for temporary time and don’t update ARP cache table

3. Host A broadcast ARP request with $IP_X/MAC_?$

4. Host A receive ARP reply, if it is match then update ARP cache table

Else don't update and inform upper layer

Host may be receiving two or more reply with small period of time, and inform the upper layers.


ATTACKER
VICTIM
ICMP with Fake Parameters
ARP Request to all Network’s Members

- Send Fake Ping to Poison victim Cache Table.

- Memorize for temporary time and don’t update cache table
- Reply the response for the ping Request
- Broadcast ARP Request to Verify the sender entry
- If the system Receive one reply and it is matched to the previous arrived message, which will consider it is from the original and not attack.
- If the system receives two reply. The system will not update the cache table. Node may be makes a notification to all members or send it to the network administrator.
- If there is no reply then discard the message.

Figure 3: Algorithm to Manipulate ICMP Case

5. DISCUSSION

This mechanism will prevent updating the cache table with unverified entries. By sending ARP request for each arrived unsolicited message or even by ICMP packet, will eliminate the possibilities for the attackers to poison the cache table with fake information. Moreover, it will provide the ability to give alarm that there are an attack possibility or attempt. Another advantages it possible to eliminate the overflow of the cache table, duo to each unsolicited message will require to verifying. Our new method avoids breaking the standard by bringing a novel mechanism and elements to attach to the current network architecture. In result, the complexity degree will not increase and keep the current scheme simple and clear. We made a modification on current scheme by adding an extra request trigger on each unsolicited message with requirement to update ARP cache table. That will provide an easy step to adopt like such scheme in current network architecture. Like such scheme need only an update for operating system to add the proposed steps to meet with needs. The most stubborn attacks in IP over Ethernet networks are Man-In-The-Middle, and this attack are prevented by the new proposed scheme. This attack depends on poisoning to redirect layer 2 traffic toward third party. Another layer 2 attack is DoS attack, by poison the cache table of the victim with nonexistence IP/MAC pair for another machine in the network, which means it can’t reach for this destination. With our proposed scheme now can verify each process of cache table update before proceeding with it.

6. CONCLUSIONS

Data link layer have a serious position in OSI model. It considers a good position to provide a security to whole network layers. We analyze the solution that proposed in the literature and found most of studies focus on the securing mapping process, while the problem still there. Few are proposed new architecture, which may create unforeseen additional security vulnerabilities. Focusing on implementation while the problem is in the design. Focus on increase security features, which make protocol heavy and more complex. Nothing seen yet on one addressing form use as a flat address to represent Layer 2 and Layer 3 in OSI model.

REFERENCES

[1] Craig Shue. 2009. A Better Internet Without IP Addresses. Ph.D. Dissertation. Indiana University, Indianapolis, IN, USA.

[2] Hayriye C. Altunbasak, "Layer 2 Security Inter-Layering In Networks," Thesis dissertation, Georgia Institute of Technology, Dec. 2006.

[3] “Arpwatch," November 2012. [Online]. Available: http://www.ee.lbl.gov/ .

[4] Ishii, J.; Razali, A.; Uda, R.; , "Confidential Information Poisoning Methods by Considering the Information Length in Electronic Portable Devices," *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on* , vol., no., pp.78-84, 26-29 March 2012

[5] Fayyaz, F.; Rasheed, H.; , "Using JPCAP to Prevent Man-in-the-Middle Attacks in a Local Area Network Environment," *Potentials, IEEE* , vol.31, no.4, pp.35-37, Aug. 2012.

[6] Meddeb, A.; Elgueder, E.; Harrathi, I.; Youssef, H.; , "Benefits of a pure layer 2 security approach in Metro Ethernet," *Computers and Communications, 2009. ISCC 2009. IEEE Symposium on* , vol., no., pp.48-49, 5-8 July 2009

[7] Rouiller, S. A., “Virtual LAN Security: Weaknesses and counter measures," November 2006. [Online]. Available: http://www.sans.org/rr/papers/38/1090.pdf.

[8] Howard, C., “Layer 2 The weakest link: Security considerations at the Data Link Layer," *PACKET*, vol. 15, First Quarter 2003.

[9] Dessouky, M.M.; Elkilany, W.; Alfishawy, N.; , "A hardware approach for detecting the ARP attack," *Informatics and Systems (INFOS), 2010 The 7th International Conference on* , vol., no., pp.1-8, 28-30 March 2010

[10] Plummer, D. C., “Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware." IETF RFC 826, November 1982.