A Study on Intrusion Detection of ARP Poisoning Attack on Wireless LAN

YoungHwan Ham [*], SokJoon Lee [*], ByungHo Chung [*], KyoIl Chung [*], JinWook Chung [**]
[*] Information Security Division, Electronics and Telecommunications Research Institute,
161 Gajeong-Dong, Yuseong-Gu, Daejeon, Korea
Tel : +82-42-860-5432 Fax : +82-42-860-5611 E-mail: yhham@etri.re.kr
[**]School of Electrical and Computer Engineering, SungKyunKwan University, Chonchon-Dong,
Jangang-Gu, Suwon, Korea
Tel :·+82-31-290-7106 Fax : +82-31-290-7211 E-mail: jwchung@songgang.skku.ac.kr

Abstract: Address Resolution Protocol (ARP) cache poisoning is a MAC layer attack that can only be carried out when an attacker is connected to the same local network as the target machines. ARP is not a new problem, but wireless network introduces a new attack point and more vulnerable to the attack. The attack on wireless network cannot be detected by current detection tool installed on wired network. In order to detect the ARP poisoning attack, there must be a ARP poisoning detection tool for wireless LAN environment. This paper proposes linux-based ARP poisoning detection system equipped with wireless LAN card and Host AP device driver

1. INTRODUCTION

Wireless networks introduce a new point of entry into previously closed wired networks and must thus be treated as an untrusted source, just like the Internet. Standard technologies enable wireless client machines to connect to a local area network made up of other wireless hosts. For wireless networking to be most useful, the wireless networks must pass data on to standard wired networks connected to the Internet. Address resolution protocol (ARP) cache poisoning is a MAC layer attack that can only be carried out when an attacker is connected to the same local network as the target machines, limiting its effectiveness only to networks connected with switches, hubs, and bridges; not routers. Most 802.11b access points act as transparent MAC layer bridges, which allow ARP packets to pass back and forth between the wired and wireless networks [1]. This implementation choice for access points allows ARP cache poisoning attacks to be executed against systems that are located behind the access point. In unsafe deployments, wireless attackers can compromise traffic between machines on the wired network behind the wireless network, and also compromise traffic between other wireless machines including roaming clients in other cells. Any and all applications designed for use over wireless networks must take these risks into account.

2. ARP POISONING ATTACK ON WIRELESS LAN

2.1. ARP Cache Poisoning

ARP operates by sending out "ARP request" packets. An ARP request asks the question, "Who has the IP address 129.254.241.126?" These packets are broadcast to all computers on the LAN. Each computer examines the ARP request, checks if it is currently assigned the specified IP, and sends an ARP reply containing its MAC address. To minimize the number of ARP packets being broadcast, operating systems keep a cache of ARP replies. When a computer receives an ARP reply, it will update its ARP cache with the new IP/MAC mapping. As ARP is a stateless protocol, most operating systems will update their cache if a reply is received, regardless of whether they have sent out an actual request. ARP spoofing involves constructing forged ARP request and reply packets. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B [2][3]. When done properly, computer A will have no idea that this redirection took place. The process of updating a target computer's ARP cache with a forged entry is referred to as "poisoning". Switches determine which frames go to which ports by comparing the destination MAC on an frame against a table. This table contains a list of ports and the attached MAC address. The table is built when the switch is powered on, by examining the source MAC from the first frame transmitted on each port. Network cards can enter a state called "promiscuous mode" where they are allowed to examine frames that are destined for MAC addresses other than their own. On switched networks this is not a concern, because the switch routes frames based on the table described above. This prevents sniffing of other people's frames. However, using ARP spoofing, there are several ways that sniffing can be performed on a switched network. A "man-in-the-middle" attack is one of these. When a MiM is performed, a malicious user inserts his computer between the communications path of two target computers. Sniffing can then be performed. The malicious computer will forward frames between the two target computers so communications are not interrupted [4]. The attack is performed as follows (where C is the attacking computer, and A and B are targets):

-C poisons the ARP cache of A and B.

-A associates B's IP with C's MAC.

-B associates A's IP with C's MAC.

-All of A and B's IP traffic will then go to C first, instead of directly to each other.

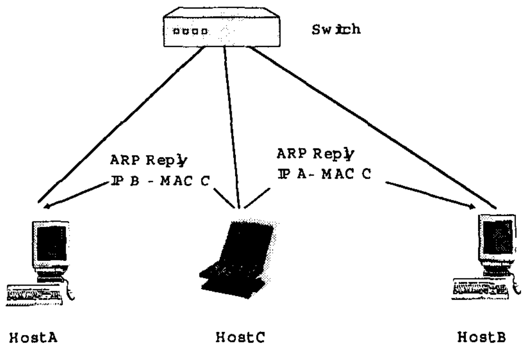

Figure 1. The ARP poisoning attack scenario

This is extremely potent when we consider that not only can computers be poisoned, but routers/gateways as well. All Internet traffic for a host could be intercepted with this method by performing a MiM on a target computer and the LAN's router. Another method of sniffing on a switched network is MAC flooding. By sending spoofed ARP replies to a switch at an extremely rapid rate, the switch's port/MAC table will overflow. Results vary by brand, but some switches will revert to broadcast mode at this point. Sniffing can then be performed. Updating ARP caches with non-existent MAC addresses will cause frames to be dropped. These could be sent out in a sweeping fashion to all clients on the network in order to cause a Denial of Service attack. This is also a side effect of post-MiM attacks, since targeted computers will continue to send frames to the attacker's MAC address even after they remove themselves from the communication path. To perform a clean MiM attack, the target computers would have to have the original ARP entries restored by the attacking computer. Connection hijacking allows an attacker to take control of a connection between two computers, using methods similar to the MiM attack. This transfer of control can result in any type of session being transferred. For example, an attacker could take control of a telnet session after a target computer has logged in to a remote computer as administrator.

ARP Cache Poisoning on Wireless LAN

Most 802.11b access points (APs) act as hubs for all the hosts on the wireless network and bridge traffic between the wireless network and the wired network (or backbone

wireless network) on the other side. The collision domains in this case are separated; all the hosts on the wireless subnet are in one collision domain and the wired network hosts are in another. The broadcast domain is not limited by the presence of the AP, and includes the wired network.

Scenario 1: Attacking both a wireless client and wired client through a wireless vulnerability.

A wireless attacker can perform a man in the middle attack against a wireless client connected to a machine on the hub or switch that the AP is connected to. Both target machines are still in the broadcast domain, and can receive the attacker's forged ARP packets.

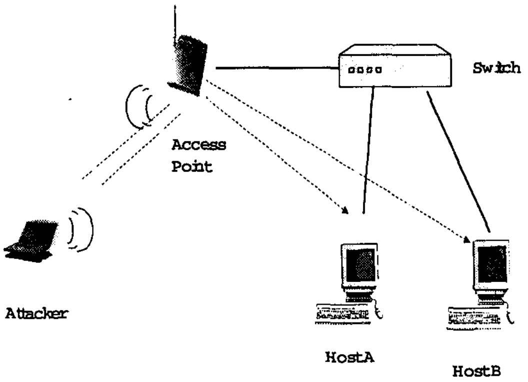

Figure 2. The attack on wired host by wireless attacker

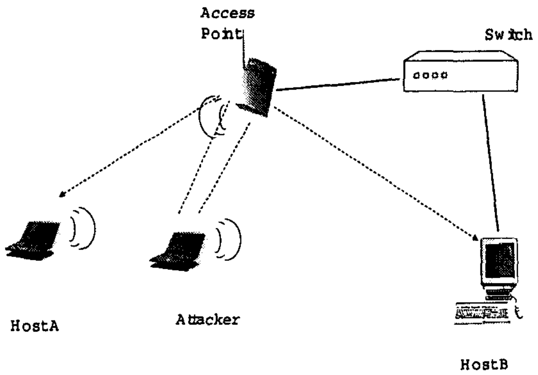

Figure 3. The attack on wired host & wireless hos:

Scenario 2: Attacking roaming wire less hosts on different APs.

A wireless attacker can perform a man in the middle attack two against two wireless clients on different APs in a roaming setup involving multiple access points. Currently available roaming 802.11b networks require all APs to be connected to a common switch or hub. (Some vendors may have more advanced roaming products available, but no documentation on the implementation of these features is readily available.)

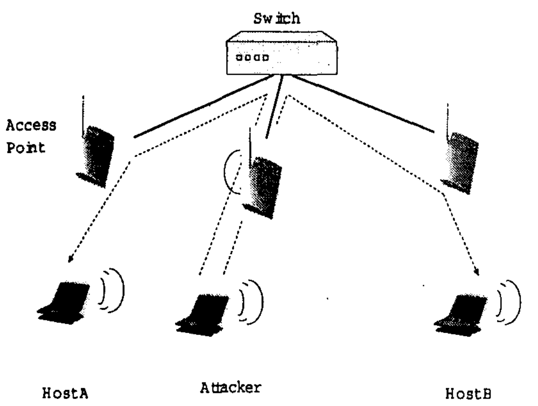

Figure 4. The attack on wireless hosts on different APs

Scenario 3: Attacking two wireless hosts on the same AP.

A wireless attacker can perform a man in the middle attack against two other wireless clients connected to the same AP. This is a trivial case that is identical to performing an ARP cache poisoning attack in a solely wired environment.

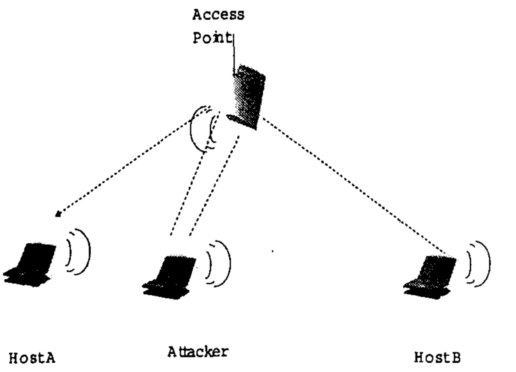

Figure 5. The attack on wireless hosts on same AP

3. ARP POISONING ATTACK DETECTION SYSTEM FOR WIRELESS LAN

In order to detect the ARP poisoning attack, there must be a ARP packet monitoring tool for wireless LAN environment. To monitor all ARP packets in wireless LAN environment, it is necessary to install monitoring tool in every host or to dedicated monitoring system. Another method is to add monitoring module to current AP, and it is very inexpensive solution. For the intrusion detection of ARP poisoning, AP must capture and analyze every ARP packet bypassing AP. This paper proposes linux-based ARP Detection AP(which can detect ARP poisoning) installed wireless LAN card with Host AP device driver. The ARP Detection AP consists of 4 threads, which is ARP Detection Module, ARP Decap, SMA Main, SMA Listener. Each thread can communicate through queue operation, and the system has two queues, as is ARP Queue, SMA Queue. The "SMA" means security management agent which plays a role of communication agent with manager system (administration console).

The IDS system(ARP Detection AP) captures every ARP reply & request packet and analyzes the IP address-MAC address mapping in the packet. The analyzed mapping data is stored in the "ARP Mapping Table" and then it is also stored in the "ARP Request Table" if the packet is ARP request. When every new ARP packet(including request & reply) arrives, the "ARP Detection Module" compares the mapping of the packet with the corresponding arp mapping in the "ARP Mapping Table". If the mapping of packet disagrees with the table mapping, the "ARP Poisoning" alarm message is sent to the SMA Main module through SMA Queue. The SMA Main module sends alarm message to the SM(Security Management) Manager which plays a role of detection server system. Also SM Manager can set the configuration & policy rule of AP.

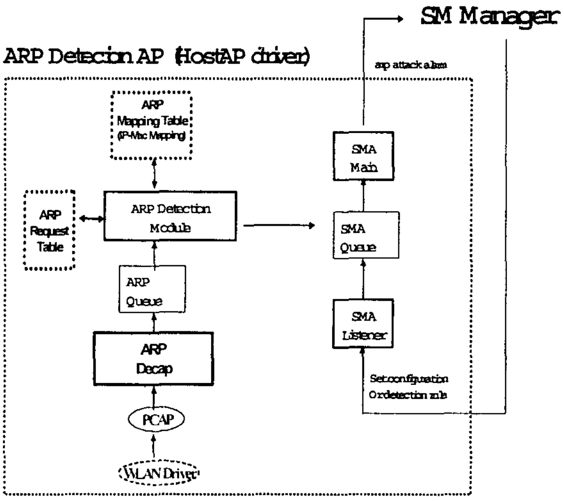

Figure 6. The Structure of ARP Poisoning Detection System

The pseudo code of "ARP Detection Module" is as follows.

```
ARP_Detection()
{
Pop event from ARP queue;
Switch(event)
{
    case ARP request packet;
        store the request IP-Mac mapping to
            ARP- Request-Table;
    case ARPreply packet;
        store the reply IP-Mac mapping to ARP-
            Mapping-Table;
        compare IP-Mac with data in ARP-
            Mapping- Table;
        if( not equal) {
            send alarm message to SM_Manager;
        }
        compare IP-Mac with data in ARP-
            Request- Table;
        If( no matching request) {
            send alarm message to SM_Manager;
        }
} //switch
} //ARP_Detection()
```

If the new ARP reply packet arrives without previous ARP request packet, the alarm message is also sent. When the DHCP system is operating in the wireless LAN system, above IDS system can make false alarm (false positive) message. To prevent this problem, the presence of DHCP system is notified to the IDS system [5][6]. The IDS system can set the timeout information with IP-MAC mapping data. When the inconsistent ARP reply packet is occurred within the timeout time of mapping data, the IDS system can make alarm message with more probability.

4. CONCLUSION

Wireless networks involve installation of a wireless Access Point on a normal internal network. This Access Point is usually connected to the wired network through a switch or a hub. The attacks are based on an adaptation of a well-understood network attack from the non-wireless world known as ARP cache poisoning. In order to detect the ARP poisoning attack, there must be a ARP poisoning detection tool for wireless LAN environment. This paper proposes linux-based ARP IDS system installed wireless LAN card with Host AP device driver. The proposed ARP Detection AP system captures every ARP packet and analyzes the IP address-MAC address mapping in the packet. If the new ARP reply packet arrives without previous ARP request packet or new ARP packet(including request & reply) is inconsistent with previous IP-MAC mapping , the alarm message is delivered to the network administrator. With proposed ARP poisoning detection AP, the administrator can easily detect the "man-in-the-middle" attack by ARP poisoning attack and avoid the network security hole caused by wireless network.

References

[1] Plummer. D, "An Ethernet Address Resolution Protocol - or - Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware", RFC826, November 1982.

[2] T. Bradley, C. Brown, A. Malis, "Inverse Address Resolution Protocol", RFC2390, September 1998.

[3] Finlayson. R, Mann. R, Mogul. J, "A Reverse Address Resolution Protocol", RFC 903, June 1984.

[4] Bob. Fleck, Jordan. Dimov, "Wireless Access Points and ARP Poisoning", Cigital Inc white paper, 2001.

[5] Droms. R, "Dynamic Host Configuration Protocol", RFC2131, .March 1997

[6] Smith. C, "The Name Service Search Option for DHCP", RFC2937, September 2000