A Host Protection Framework Against Unauthorized Access for Ensuring Network Survivability

Hyuncheol Kim[1], Sunghae Kim[3], Seongjin Ahn[2], and Jinwook Chung[1]

[1] Dept. of Electrical and Computer Engineering,Sungkyunkwan University,
300 Chunchun-Dong Jangan-Gu,Suwon, Korea, 440-746
{hckim,jwchung}@songgang.skku.ac.kr
[2] Dept. of Computer Education, Sungkyunkwan University,
53 Myungryun-Dong Jongro-Gu, Seoul, Korea, 110-745
sjahn@comedu.skku.ac.kr
[3] Electronics and Telecommunications Research Institutes, Daejon, Korea,
shkim@etri.re.kr

Abstract. Currently, the major focus on the network security is securing individual components as well as preventing unauthorized access to network services. Ironically, Address Resolution Protocol (ARP) poisoning and spoofing techniques can be used to prohibit unauthorized network access and resource modifications. The protecting ARP which relies on hosts caching reply messages can be the primary method in obstructing the misuse of the network. This paper proposes a network service access control framework, which provides a comprehensive, host-by-host perspective on IP (Internet Protocol) over Ethernet networks security. We will also show how this framework can be applied to network elements including detecting, correcting, and preventing security vulnerabilities.

1 Introduction

Along with development of communication networks, the problem of network security has increasingly become a global challenge. Reflecting through these trends, the key focus on the network security is securing individual components as well as preventing unauthorized access to network services. Although IP over Ethernet networks are the most popular Local Area Networks (LANs) nowadays, an ignorance of the network security in designing TCP/IP (Transmission Control Protocol and Internet Protocol) has led important network resources to be wasted or damaged.

Among the network resources, IP address, a limited and important resource, is increasingly misused, which results from its inexperienced and malevolent purposes to cause a security problem or damage the entire networks. As an IP address is the only one to identify itself, the same IP address cannot be simultaneously used in other equipments. If IP addresses, which are respectively

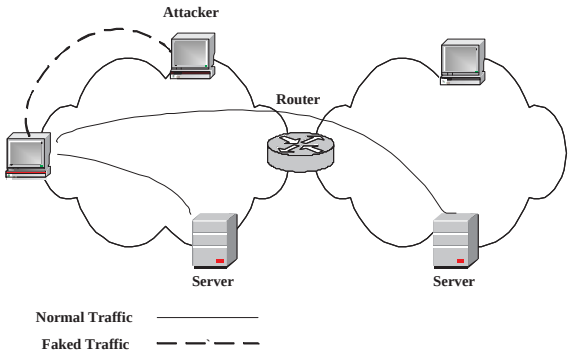

Fig. 1. ARP Spoofing and Poisoning Attack

set by hosts in the network, are misused for some inexperienced or malevolent purposes, the security problem could be triggered in the network.

IP over Ethernet networks use ARP to resolve IP addresses into hardware, or MAC (Media Access Control) addresses. All the hosts in the network maintain an ARP cache which includes the IP address and the resolved hardware or MAC addresses. ARP resolution is invoked when a new IP address has to be resolved or when an entry in the cache expires. As shown in Fig.1, the ARP poisoning and spoofing attack can easily occur when a malicious user tries to modify the association of an IP address and its corresponding hardware or MAC address by disguising himself of being an innocent host [1].

In this study, we propose an unauthorized network access control framework in IP over Ethernet networks that guarantees fast and continuous network protection. To this, we propose a network access control scheme based on ARP spoofing and demonstrate how this concept can be applied to network elements, services, and applications. In addition, we demonstrate how the security framework can be applied to all layers of the TCP/IP protocol suite.

The rest of this paper is organized as follows. The background relevant for ARP operations and details of proposed framework are described in section 2 and 3, respectively. Finally the paper concludes in Section 4.

2 Network Security and ARP Operations

2.1 Network Security

The network security technologies have been studied to prevent increasingly variable and sophisticated attacks on a network. Currently, they include an intrusion detection system that detects a sign of an attack, a firewall that mainly blocks the traffic of a detected attacker, a response system i.e., a packet filtering router to protect its domain, and many other systems to enhance network survivability.

The network survivability refers to continuing the operation of a system to provide services even though it has been damaged by network attacks, system

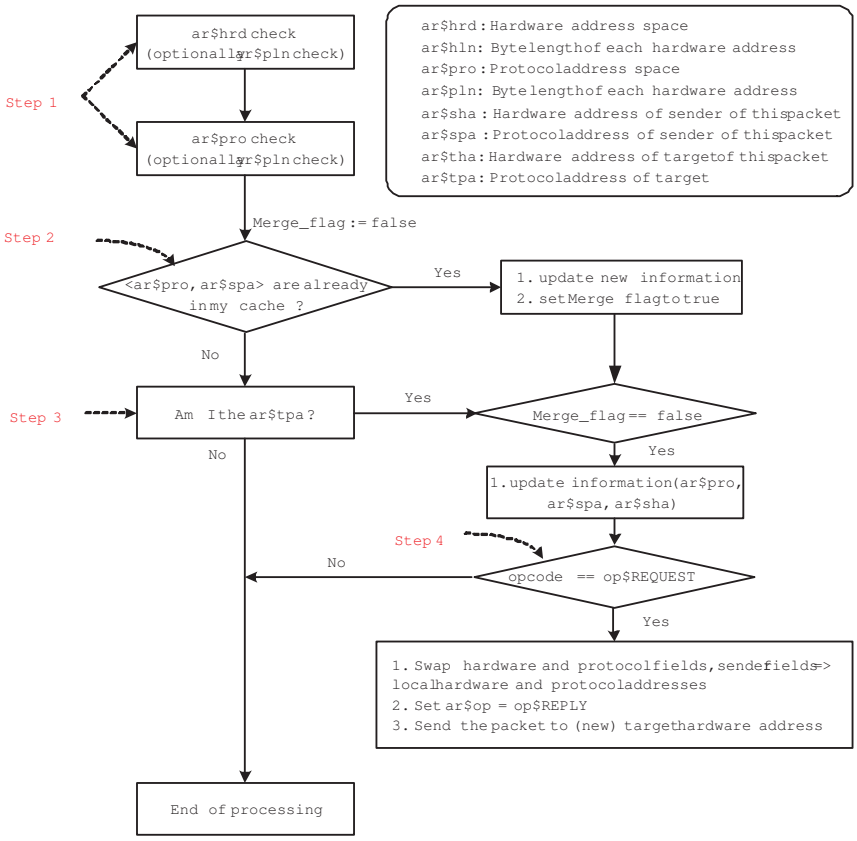

Fig. 2. ARP Mechanism

failures, and other overloads. While early security technologies mainly covered screening for a single computer attack, the contemporary security technologies have been developed to resolve and resist those network attacks. That is, the network survivability has focused on systematically managing the configuration of the network and its components.

The IP address management refers to securing the network survivability by monitoring and disabling the function of the host when a system detects the worms or other abnormal behaviors, as well as an intentional or malicious changes of the IP address. Thus, the IP management and blocking the misuse of IP address come to serve as a new concept in the security solution for controlling the network.

2.2 ARP Operations

The rest of this section briefly states how ARP operates. The ARP provides mapping between the IPv4 address and the Ethernet address. When an Ethernet

Table 1. Windows (A) to Windows (B) Gratuitous ARP

Type	Sender	Receiver	Source IP	Source MAC	Target IP	Target MAC
Request	B's MAC	All	B	B's MAC	B	Ignored
Response	A's MAC	B's MAC	A	A's MAC	B	B's MAC
Request	A's MAC	All	A	A's MAC	A	Ignored

frame is sent from one host to another, the 48 bit Ethernet address determines the interface to which the frame is destined. When a host needs to send an IP datagram as an Ethernet frame to another host whose MAC address it ignores, it broadcasts a request for the MAC address associated with the IP address of the destination. Every host on the subnet receives the request and checks if the IP address in the request is bound to one of its network interfaces. If this is the case, the host with the matching IP address sends a unicast reply to the sender of the request with the <IP address, MAC address> pair. Every host maintains a table of <IP, MAC> pairs, called ARP cache, based on the replies it received, in order to minimize the number of requests sent on the network.

ARP is a stateless protocol, i.e., a reply may be processed even though the corresponding request was never appeared. When a host receives a reply, it updates the corresponding entry in the cache. While a cache entry should be updated only if the mapping is already present, some operating systems, e.g., Linux and Windows, cache a reply in any case to optimize performance. Another stateless feature of ARP is the so called gratuitous ARP. A gratuitous ARP is a message sent by a host requesting the MAC address for its own IP address. It is sent either by a host that wishes to determine if there is another host on the LAN with the same IP address or by a host announcing that it has changed its MAC address, thus allowing the other hosts to update their caches [1].

The Gratuitous ARP checks if there is any other host using its IP address when the host initially boots itself to start the network. A system that uses an unauthorized IP address may cause some problems to other hosts using Gratuitous ARP. For example, a server system of which IP address has already been preoccupied by another system during its rebooting can-not use the network. That is, the IP address may cause internal security problems in the network, not from externally [2][3][4].

3 Proposed Network Access Control Framework

3.1 Gratuitous ARP

Using the gratuitous ARP, a host can check if the IP address is used by other hosts in order to avoid using duplicated IP address. Table 1, Table 2, Table 3, and Table 4 shows different types of collisions in using gratuitous ARP for each OS respectively. The ON (Offending Node) denotes a host which tries to use the IP, and the DN (Defending Node) denotes a host using the IP.

Table 2. Windows (A) to Linux (B) Gratuitous ARP

Type	Sender	Receiver	Source IP	Source MAC	Target IP	Target MAC
Request	B's MAC	All	B	B's MAC	B	Ignored

Table 3. Linux (A) to Windows (B) Gratuitous ARP

Type	Sender	Receiver	Source IP	Source MAC	Target IP	Target MAC
Request	B's MAC	All	0.0.0.0	B's MAC	B	Ignored
Response	A's MAC	B's MAC	A	A's MAC	0.0.0.0	B's MAC

Table 4. Linux (A) to Linux (B) Gratuitous ARP

Type	Sender	Receiver	Source IP	Source MAC	Target IP	Target MAC
Request	B's MAC	All	0.0.0.0	B's MAC	B	Ignored
Response	A's MAC	B's MAC	A	A's MAC	A	A's MAC

Table 5. Vulnerable Points of ARP

Number	Problems	Cause
1	Duplicated IP address	UNIX/Linux Server
2	ARP Cache Forgery	MAC address Forgery
3	Authorized IP Blocking	Malicious gratuitous ARP Response to authorized host
4	Unauthorized IP Misappropriation	IP address alteration of unauthorized host

3.2 An Unauthorized Access Control Framework

Fig.2 illustrates an algorithm by the hosts in processing an ARP message. In processing the ARP algorithm, there can be many different types of attacks such as ARP Spoofing, MAC Flooding, ARP Redirect, MAC Duplicating, etc. Different types of attack that can occur for each step is as follows.

- <Step 1> : <Step 1> is a stage that defines the types of hardware interface and upper layer protocol. The host needs to provide verification function to check if the protocol and the packet format have a valid MAC layer access protocol.
- <Step 2> : <Step 2> is a process that updates its current ARP cache based on ARP request message. If the hardware address and the protocol address is already exists in the cache table, the host only needs to update the table. At this point, network security problem may occur if the third party broadcasts a packet with invalid MAC address. For example, if a host send an ARP request message with the invalid MAC address of A, the hosts that were communicating with the host A will change its cache with the invalid MAC

address of host A. Thus, the host A would not be able to use the network. The attacker will continually generate the packet with the invalid MAC address. Thus, it can perform different forms of packet sniffing such as ARP table flooding, APR Spoofing, ARP Redirect, MAC Duplicating, etc [5].

- <Step 3> : <Step 3> is a process in which the host sends an ARP reply message for ARP request with its destination address. The problem of this step is that if the host is in hardware reboot status or if the host tries to change its non-used IP address, the host would be unable to use the network if a third-party deliberately sends a fake reply message.

Table 5 shows the security problems that can occur during the ARP operation. The two types of solution to the security problem 1 to 4 are modifying ARP process and managing IP and MAC addresses by monitoring ARP packets. The modifying method recognizes the fact that the IP and MAC address can always be changed by anyone thus it has no way of finding out who is privileged user. But, this method is not a perfect solution, due to the fact that the verification of gratuitous ARP is impossible and the ARP packet cannot be altered. But the security problem can be solved by managing IP and MAC addresses by monitoring ARP packets.

Just as IP spoofing, ARP spoofing also prevents a host in the network from functioning normal network processing by preventing it to perform ARP reply for ARP requests. If the host tries to perform ARP reply, the attacker uses the IP address of the incompetent host and configures it as a target host. When a victim host tries to communicate with the incompetent host, the attackers system will perform ARP reply to all the ARP broadcast request instead of the incompetent host. Thus, the MAC address of the victim system is stored in the attackers ARP cache, and the victim system will mistake the attacker as the incompetent system and perform normal communication with the attacker [1] [6] [7]. Ironically, techniques of preventing ARP poisoning and spoofing can be used to prohibit unauthorized network access and resource modifications.

The distributed network environment covered in this study includes manager and agent system. The agent is installed in each broadcast domain (including Virtual LAN) to collect packets generated within the domain. The manager enforces policies to block the unauthorized accesses detected by the agent in the network. The Agent uses the ARP spoofing technology to manage the network. It also creates the ARP packet under the order from the manager to confirm the up/down status of the network nodes and to obtain the MAC address, additionally shutting down the network against an unauthorized IP. Particularly, the ARP Request means an important message to define the ARP cache table of all hosts in the network through the ARP spoofing. Fig.3 shows the module structure of the manager and agent system and Fig.3 shows the process architecture of the agent system, respectively.

3.3 Unauthorized Access Control Schemes

Table 6 shows how to block the IP address. "Blocked" refers to the blocked host and "Common" refers to another common host (C) on the same network.

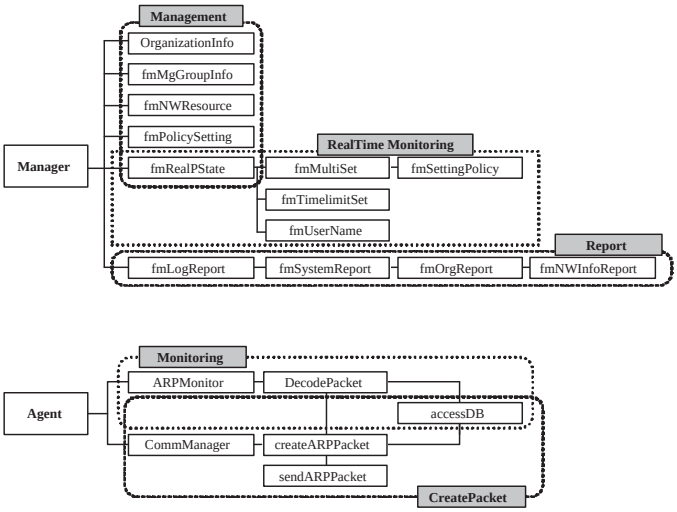

Fig. 3. The Module Architecture of Manager and Agent System

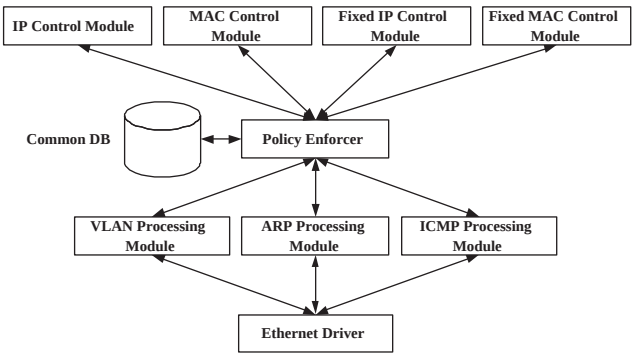

Fig. 4. The Process Module of Agent System

Table 6. ARP message process to block IP address

Type	Sender	Receiver	Source IP	Source MAC	Target IP	Target MAC
Request	Agent	All	B	Incorrect	B	Not used
Response	Blocked	Incorrect	B	B's MAC	B	Incorrect

Table 7. ARP message process to interfere with the access of the blocked host

Type	Sender	Receiver	Source IP	Source MAC	Target IP	Target MAC
Request	Blocked	All	B	B's MAC	C	Not used
Response	Common	Blocked	C	C's MAC	B	Incorrect
Request	Agent	All	B	Incorrect	B	Not used
Response	Blocked	Incorrect	B	B's MAC	B	Incorrect

Table 8. ARP message process to interfere with the access to the common host

Type	Sender	Receiver	Source IP	Source MAC	Target IP	Target MAC
Request	Common	All	C	C's MAC	B	Not used
Response	Blocked	Common	B	B's MAC	C	C's MAC
Request	Agent	All	B	Incorrect	B	Not used
Response	Blocked	Incorrect	B	B's MAC	B	Incorrect

Host blocking and releasing includes processes that send/receive the ARP Request messages to select a host to be blocked/released, and to confirm the MAC address. In line 1, the Agent broadcasts the incorrect MAC address of (B) to update the ARP cache table, which contains the address of the blocked host, with incorrect MAC address of other hosts.

Table 7 shows the process in which the blocked host attempts to have an access to other hosts. If (B) sends the ARP Request message to request the MAC address of (C), (C) will normally response to allow the blocked host to communicate. If this is the case, the Agent broadcasts the ARP Request message containing the incorrect MAC address to set the incorrect (B) MAC address in the ARP cache table of (C).

Table 8 shows the process where the Agent interferes with the access of other hosts to (B). If (C) sends the ARP Request message to request the MAC address of (B) in order to access (B), the (A) sends the ARP Response message containing the incorrect MAC address of the blocked host. Then, (C) will have the incorrect MAC address of (B) by updating the ARP cache table with the request message lately received from the Agent.

Table 9 shows how to release the blocked IP. The blocked IP will be released when (A) sends the gratuitous ARP packet for (B). Other hosts can obtain the correct MAC address of the blocked host, freely sending/receiving the ARP request/response message without future interferences from (A).

Table 9. ARP message process to block IP address

Type	Sender	Receiver	Source IP	Source MAC	Target IP	Target MAC
Request	Agent	All	B	B's MAC	B	Not used
Response	Blocked	Agent	B	B's MAC	B	B's MAC

4 Conclusions

IP address which is a limited and important resource is increasingly misused, which results from its inexperienced and malevolent purposes to cause a security problem or damage the entire networks. Because a system that uses an unauthorized IP address may cause some problems to other hosts, the IP ad-dress may cause internal security problems in the network, not from externally.

In this paper, we propose an unauthorized network service access control framework focusing on the management and security of the IP, a network resource. This system consisting of agent and manager uses the network monitoring and the IP blocking algorithm to integrate the networks so as to effectively manage the IP resources. The agent can be expanded by installing Simple Network Management Protocol (SNMP) agent to the IP integration management.

This system also presents the possibility of developing the integration management system to protect the network from the external virus attacks. This study worked upon a system operating under the IPv4 environment, which will come to be needed under the IPv6 that is expected to get its popularity. The same network blocking mechanism as in the IPv4 network can optionally be operated on Internet Control Message Protocol version 6 (ICMPv6).

References

1. D. Bruschi, A. Ornaghi, et al.: S-ARP: a Secure Address Resolution Protocol, ACSAC '03 (2003) 66–74
2. WAndrew R. McGee, S. Rao Vasireddy, et al.: A Framework for Ensuring Network Security, Bell Labs Technical Journal, Vol. 8, (2004) 7–27
3. Anirban Chakrabarti, G. Manimaran: Internet Infrastructure Security: A Taxonomy, IEEE Network, Nov./Dec. (2002) 13–21
4. Soonchoul kim, Youngsu Choi, et al.: Study of Security Management System Based on Client Server Model, ICC, Vol 2. (1999) 1403–1408
5. Steven J. Templeton, Karl E. Levitt: Detecting Spoofed Packets, DISCEX03, Vol 1, (2003) 164–175
6. Bruce McDonald, Taieb Znati, et al.: Comparative Analysis of Neighbor Greeting Protocols: ARP versus ES-IS, SIMULATION '96, Apr. 1996 (71–80)
7. Ping Lin, Lin Lin: Security in Enterprise Networking: A Quick Tour, IEEE Communications Magazine, Jan. (1996) 56–61