NAIST-IS-DT0161010

Doctoral Dissertation

Studies on Retrospective Identification of Link Layer Addresses in Distributed Forensic Databases

Masataka Kanamori

Department of Information System
Graduate School of Information Science
Nara Institute of Science and Technology

March 11, 2004

Doctoral Dissertation
submitted to Graduate School of Information Science,
Nara Institute of Science and Technology
in partial fulfillment of the requirements for the degree of
Doctor of ENGINEERING

Masataka Kanamori

Thesis Committee: Suguru Yamaguchi, Professor
Hideki Sunahara, Professor
Youki Kadobayashi, Associate Professor

Abstract

This dissertation presents an approach to assist an investigator with his/her incident analysis. In unexpected security incidents, one of the most important points is to ascertain whether or not a computer crime suspect is the culprit, and to avoid false charges. For this reason, various types of digital evidence are employed by an investigator to disclose a malicious user's activity. Accordingly, assurance of evidence is needed for an investigator to reach accurate conclusions. For this purpose, this research concerns two concepts: reliability and availability of evidence in the field of Computer and Network Forensics (CNF).

An investigator performs CNF procedures on the basis that the mapping between an IP address and a link-layer address is assigned correctly. This research, therefore, first introduces the Self-Confirming Engine (SCE) for the purpose of protecting address mapping tables in both Address Resolution Protocol (ARP) in IPv4 and Neighbor Discovery Protocol (ND) in IPv6. Both address resolution protocols are indispensable in the current Internet, because hosts communicate with each other by obtaining the pair of IP address and link-layer address. Consequently, even if a malicious user tries to compromise the tables, an investigator can perform CNF based on the trails of an attack because evidential information is recorded properly by address resolution procedures with the SCE. This method makes CNF that depends on various types of evidence both possible and reliable. The proposed system, moreover, is designed to be as simple as possible, because complexity makes general-purpose uptake/installation impractical in future digital devices.

Next, this dissertation presents an approach to making individual or obsolete evidence available, i.e., evidence linking. Even if an IP address or hostname is changed a long time after the occurrence of an incident, an information source accumulated by the SCE, called the TDB, is used to resurrect the links among traces recovered by the investigator. Consequently, by applying the TDB, an investigator can retroactively identify whether or not an unauthorized access suspect is in fact the trespasser. From the difference of address mappings between a normal host and a third party, moreover,

the user can prove that he/she is not the malicious host.

Finally, the importance of the two concepts is verified by implementation. An investigator can reduce the time required to analyze a security incident, and ensure that CNF works smoothly. Consequently, an investigator can indisputably determine guilt by applying this method. In this research, reliability and availability of evidence used as an information source are improved to resolve security incidents, and also trouble with a host or network. This research indicates that adequate preparation can enable users to cope with unexpected incidents.

Acknowledgments

I would like to express my gratitude to professor Suguru Yamaguchi, my advisor and committee chairman, for his support, advice and encouragement. I also would like to appreciate what he gave me an opportunity to enter the graduate school seven years ago.

I would like to thank professor Hideki Sunahara for his long sustained support to my work. His kind support and precise comments encouraged me to make my research a more significant one.

I would like to thank associate professor Youki Kadobayashi for his accurate comments and assistance. I was affected by his attitude to work and his broad view of research.

I thanks assistant professor Katsuyoshi Iida and assistant professor Takeshi Okuda for their support. Their continuous stimulation pushed me to the goal. Their comments widened my research vision.

I also would like to offer Professor Ian R. L. Smith my hearty thanks for his constant assistance. An encounter with him is an essential part of my research life, and his smile makes me comfortable.

I would like to thank Mr. Takashi Kobayashi for his constructive comments about network security. His deep consideration and wide knowledge supported my research.

I would like to thank all members of the Internet Engineering Laboratory for their friendships, supports and comments. Specially, I would like to offer Mr. Taiji Kimura and Dr. Vasaka Visoottiviseth my soulful thanks for their help. As brothers in my doctoral life, moreover, I am thankful to Dr. Shigeru Kashihara and Mr. Ryuji Somegawa for their precious comments. I also thanks Mr. Teruaki Yokoyama, Mr. Masashi Eto and Mr. Hiroaki Hazeyama, who are doctoral candidates in the laboratory, and also Ms. Natsue Tanida and Ms. Keiko Nakano, the secretaries of the laboratory. Their kindness makes me refreshed even when I am in a hurry to submit a paper.

Furthermore, I would like to thank Dr. Nobuyuki Ishibashi, Mr. Mikio Nagahara and Mr. Motohiro Yakura for their help. Without their presence, I could not persevere

in my research up to the present.

Additionally, I also have to thank all members of my big happy family; Mr. and Mrs. Saika, Yoshida, Kakuta and Sugiura, Mr. Fumihiko Tsukuda, Masanori Nagaoka, and Wataru Kawanishi, and Ms. Izui Mayumi, Misako Kikkawa, Chieko Miyagawa, Kaori Hashimoto and Takako Matsunaga.

Finally, I would like to thank my family who always believe that I will reach my goal. I could not perform research until now without their sincere encouragement and support.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background and Problem Statement

Twenty-nine years ago, the term "internetwork", which is what we now know as the "Internet", was released by V. G. Cerf and R. E. Kahn [CK74]. Their concept enables connections among different networks, and leads to reliable packet transmission and forwarding in the Internet.

At present, the great spread of the Internet brings every one of us many wonderful experiences/opportunities, in the form of global communications connected all over the world. However, everything has a merit and demerit; the Internet also provides a threat when networks are used for computer crime. From now on, we must live with this negative factor.

Unfortunately, attack sophistication has been increasing rapidly since the early 1980s, as indicated in the report of the CERT/CC in 2000 [ACF+00]. On the other hand, intruders's technical knowledge has decreased from the later 1980s. At present, an attack can be executed easily without expertise about computer security, by Graphical User Interfaces (GUI) and operations targeted on many hosts simultaneously.

As a result of this trend, in the current Internet, the serious increase in computer crime makes incident response an everyday affair. Therefore, an investigator (e.g., a network administrator, systems operator, or security auditor) must inspect a large number of machines in his/her network to determine what happened. In this process, an investigator performs procedures for obtaining traces, restoring files and finding out an attacker's activity. However, without accurate analysis based on the trails in the victim host, an investigator may cause damaging false charges. For this reason, in the field of the Computer and Network Forensics (CNF), various types of digital evidence

are essential elements for all investigators.

Consequently, one of the most dangerous threats is an attack in which an intruder makes evidence unreliable, because evidence credibility is a necessary condition for CNF. Now, many kinds of attack exist in the Internet, such as Scan, Buffer Overflow, Cross-Site Scripting, Virus/Worm, Denial of Service (DoS) attack, Distributed Denial of Service (DDoS) attack and Spoofing attack. Similarly, there are some technologies to protect or detect their attacks, i.e., firewalls, Intrusion Detection Systems (IDS) and so on. However, intruders can make evidence unreliable in their attacks, using the technique of a Spoofing attack.

In this research, ARP Spoofing is focused on for its bad influence. ARP Spoofing is based on the Address Resolution Protocol (ARP)[Plu82]. When an attacker uses this technique, a victim host believes false advice, without doubt. As a consequence of this attack, the most important point is to believe that an advice by the attacker is leading to unreliable evidence. By this malicious achievement, the victim host records various events such as login user name, communicating host and access time, based on uncorrected advice in his/her log file. Unfortunately, during the attack, victim hosts can communicate with each other normally. That is, a victim host cannot understand that information such as an interoffice memo, a confidential file or an examination paper, is leaked to the attacker by the host itself.

The difference between this kind of attack and others is information leakage and recognition of an attack. For example, DoS and DDoS attacks perform a host and network a disservice by transmitting a large number of meaningless packets, and try to prevent hosts from communicating with each other. During these attacks, the victim cannot use services such as World Wide Web (WWW), e-mail, telnet and ftp. Therefore, the victim does not reveal his/her personal data to the attacker, and can recognize an abnormal occurrence. During an ARP Spoofing attack, however, the victim betrays his/her data to the attacker unknowingly, and may not suspect the attacker's plans. As it turns out, an APR Spoofing attack is a threat to safe communication, between it is harder to establish when the attack started, and how long it has lasted, than with other attacks. Consequently, this research focuses on such Spoofing attacks.

1.2 Design Vision

Because computer crime causes stress and disrupts the lives of its victims, it is desirable that perpetrators of security incidents should be caught as soon as possible. Adequate preparation is therefore needed so that an investigator can conclude inquiries accurately

and efficiently. For this purpose, this dissertation addresses the following issues:

Effective Evidence

To resolve a security incident, an investigator needs digital evidence to estimate whether a suspicious event is actually an attack by an intruder. This research ensures that investigative evidence is reliable enough to achieve the correct result.

Retrospective Traceability

Like any other criminal investigation, computer security incidents take time to conduct. For this reason, effective investigative evidence is needed to trace and identify an attacker, even if much time has elapsed since the occurrence of a security incident.

Distributed Forensics

With the spread of the Internet, many people become the owner of a host, i.e., a desktop or laptop personal computer, they are not merely the user, but the administrator of their own host. Therefore, every host owner must at least be able to check their own security incidents, and not simply depend on a computer specialist. For this purpose, when a general user wants to inspect an incident, an examinable infrastructure and information source are required in current networks to minimize danger.

1.3 Introductory Terms

- OSI Basic Reference Model
  Open Systems Interconnection (OSI) Basic Layer Reference Model was standardized by ISO [ISO] in 1984 as a framework of standards for the purpose of communication among different applications, as shown in Figure 1.1 [Sur02]. Various vendors, developers and researchers can only consider, create and improve a related layer. Each layer accesses only its immediate neighbors, e.g., Network layer communicates with Transport layer and Data Link layer.

- TCP/IP Protocol Suite
  Figure 1.1 also indicates the relationship between the OSI basic layer reference model and the TCP/IP protocol suite. The TCP/IP protocol suite includes many protocols, such as Address Resolution Protocol (ARP) [Plu82], Internet Protocol (IP) [Pos81b], Internet Control Message Protocol (ICMP) [Pos81a], Transmission

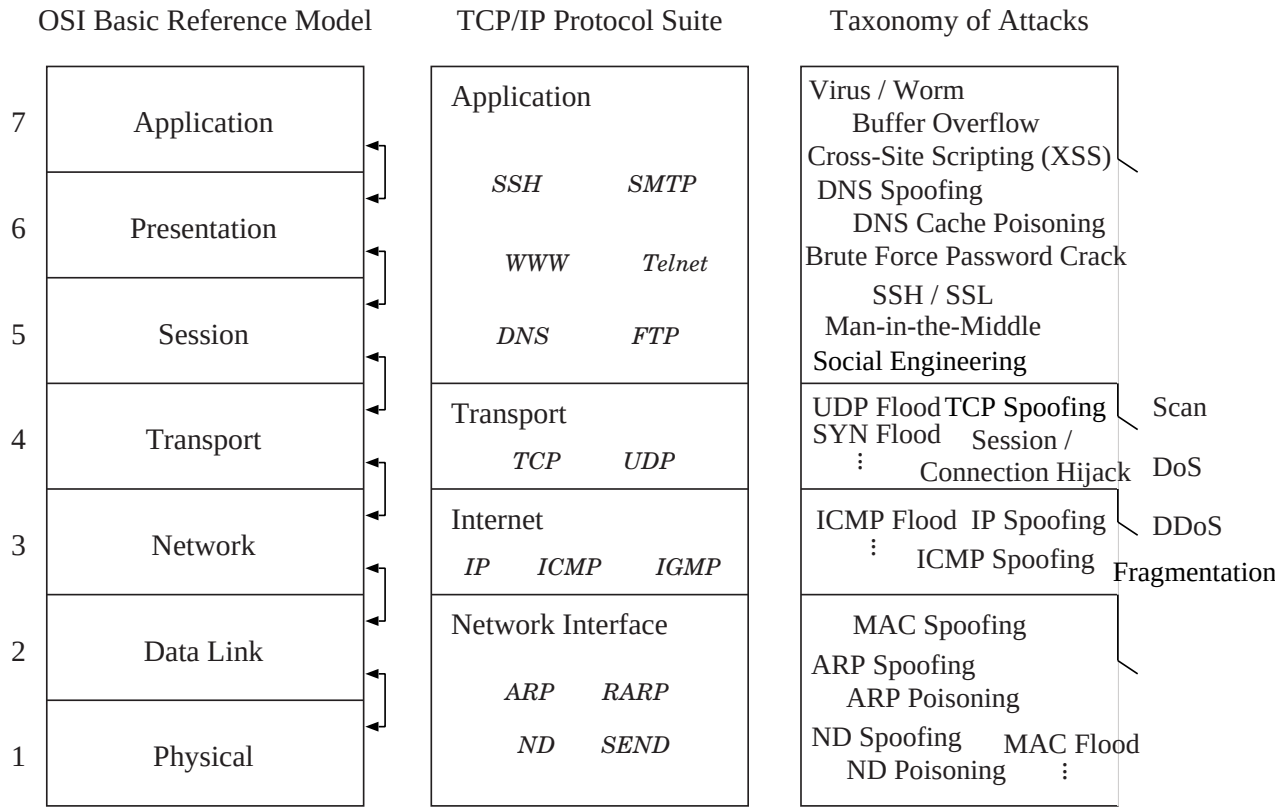


Figure 1.1: Layer Model and Taxonomy of Attacks

Control Protocol (TCP) [Pos81c], User Datagram Protocol (UDP) [Pos80] and other application protocols. For example, communicating data are addressed in each layer to specify IP address, port numbers and user name.

- Domain Name System (DNS)
  DNS is a distributed database system that maps between hostnames and IP addresses, as described in [Moc87a, Moc87b]. In the Internet, DNS is one of the most important factors for hosts to communicate each other, in systems such as the World Wide Web (WWW), Telnet, SSH, Mail, File Transfer Protocol (FTP) and many other services. Therefore, an attacker may try to compromise a DNS server for confusing the Internet, or to lead a DNS client to an incorrect server, as described in [Cen01, Sax03]. Moreover, if DNS becomes infected, all applications in the TCP/IP protocol suite will be poisoned, and record wrong information in their log files.

- Address Resolution
  Address resolution is needed to map between Network Layer address and Data Link Layer address, as shown in Figure 1.1. In the Internet, when a host begins to communicate with a destination host, address resolution procedures, i.e., Address Resolution Protocol (ARP) in IPv4 and Neighbor Discovery (ND) protocol [NNS98, TN98] in IPv6 [DH98], are performed to confirm that a target host's Data Link Layer address corresponds to its IP address.

- Computer Security Incident
  This is a computer-related event in which network administrators or general users are perplexed by abnormal activities, such as unauthorized and fraud access, disruption of data or of an entire system, and unlawful information stealing. When a computer security incident, or more simply an incident, happens, most systems and applications will record such an event to log files. There are many useful articles from the SANS Institute, established in 1989, and for example an introductory guide for information security is described in [Lin01].

- Incident Response
  This refers to the processes for investigating and analyzing a computer security incident. An investigator performs an incident response to make an incident clear, identify whether or not an incident is malicious, and avoid recurrence of the same event.

- Forensic Analysis
  Forensic analysis is the action taken to reach an exact conclusion about an incident, using every piece of gathered data such as system configuration files, application logs, captured packets and recovered data.

- Digital Evidence
  Digital evidence is the information sources that an investigator needs to analyze an incident. For example, digital evidence includes system configuration files, application logs, fragile data like running processes in memory, captured packets, and other computer-related records.

- Digital Forensic Science
  Based on results in the field of Digital Forensic Science, an investigator can perform incident response and forensic analysis about an incident or a computer-related crime, as follows:

  The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
  (A Road Map for Digital Forensic Research [Pal01])

- Computer and Network Forensics
  Computer and network forensics is the approach using both computer and network forensics to analyze an incident, and is detailed as follows.

- Computer Forensics
  Computer forensics, also called media analysis in the past, is an investigative process of an incident using evidence remaining on a victim host, as follows:

  Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence.
  (Computer Forensics: Computer Crime Scene Investigation [Vac02])

- Network Forensics
  Network forensics is an investigative process of an incident, using as evidence packets captured by Intrusion Detection System (IDS), Firewall and other traffic

recording systems. Moreover, Network forensics also includes a network inspection approach to obtain evidence remaining on a victim host, as follows:

The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities.
(A Road Map for Digital Forensic Research [Pal01])

The study of network traffic to search for truth in civil, criminal, and administrative matters to protect users and resources from exploitation, invasion of privacy, and any other crime fostered by the continual expansion of network connectivity.
(Incident Response: Investigating Computer Crime [MP01])

1.4 Dissertation Overview

This dissertation is organized as follows. Chapter 1 introduces the background to this research. Chapter 2 reviews the previous work in network security about Spoofing technique. Chapter 3 presents a design and approach to protect address mapping tables in both IPv4 and IPv6, called the Self-Confirming Engine. Chapter 4 explains an approach and its implementation to ensure evidence availability. Chapter 5 describes the conclusions of this research, its significance, and future work.

Chapter 2

Previous and Related Work

2.1 Initial Appearance

Since the first publication about the Spoofing technique by S. M. Bellovin in 1989, as described in [Bel89], this fake act continues to be used in various type of attacks to this day. One concrete effect of IP Spoofing is to deceive authentications based on an IP address, such as "r" commands, i.e., *rlogin, rsh, rcp* and so on. For example, Spoofing is found in ARP, ICMP and DNS Spoofing in each layer, as shown in Figure 1.1, because anybody can make a packet having another host's address or protocol options, and send it to a victim host on the Internet, as described in [Sch98, nem, hpi]. The IETF [IET] describes the importance of packet filtering against IP Spoofing [FS00]. One of the roles of a Firewall, the filtering technique, can be introduced to protect against Spoofing attacks, and many articles about IP Spoofing can be obtained from the Internet [di96, Cen96, Vel00]. An administrator tries to filter out malicious packets from all the traffic in a network.

2.2 Firewall

In Firewalls, as shown in Figure 1.1, access control is performed to filter packets based on IP address in Network Layer, to limit protocols (WWW, FTP and SSH) to only those permitted services defined a network administrator, and to authenticate user identification in Application Layer.

Currently, a Firewall is used by a lot of network administrators to ensure roles such as access control and event recording. For example, an administrator can define an Access Control List (ACL) to allow / deny packets along network topology and secu-

rity policy. Therefore, packet filtering is performed in Network Layer and Transport Layer, and controls packet flow using IP address and service protocol (port number) in transmitted packet headers. As an event recording function, Firewall logs various types of information, such as an accessed IP address, to unallowable ports. The network administrator can thus notice any indication of abnormal activity leading to a malicious attack.

Until a few years ago, Firewall was a technology for enabling network administrators to protect their enterprise networks against an attacker from the Internet. Nowadays, however, the explosive spread of the Internet makes Firewall more friendly for general users; this is called Personal Firewall as described in [Mar, Bor].

2.3 IDS

In ARP Spoofing, an attacker can perform complete traffic redirection, as described in [Sil03], even if a user employs a switching hub [Kin02, Son99a], and a wireless network [FD]. Man-in-the-Middle (MitM) attack, as detailed in Chapter 3., is one effect of ARP Spoofing, as described in [Wag01]. Moreover, if SSH version 1 and Secure Socket Layer (SSL) are adopted for transmitting data, a user may leak out confidential information to an attacker, as depicted in [LI01, Sys02, Bur02, OV]. In IPv4, there are several techniques to avoid and detect malicious address mapping alteration. An old technique, static assignment, in which the link-layer address corresponds to the IP address, can be used; however, the static method needs manual updating when an address mapping table changes [Bui96]. Therefore, in a wireless environment with a lot of mobile hosts, the static method is impractical for most cases.

Intrusion Detection System (IDS) tries to detect any occurrences of abnormal mappings, between the Data Link Layer and Network Layer, as shown in Figure 1.1. Several tools such as Snort [Roe99, KBR+01], Prelude [Van] and arpwatch [Grob] are available to identify malicious ARP requests or replies. These tools only report warnings when a suspicious packet is detected.

- Defined Address Pair
  Like the static method, Snort regards an address pair that is different from a correct pair already defined in the configuration file as an attack such as IP Spoofing.
- Suspicious ARP Message
  Their IDSs regard a unicast ARP request as a suspicious message from a malicious

user to attack a target's address mapping table.

- Captured Address Pair
  Arpwatch captures ARP packets for gathering address pairs and creating a database file. If an address pair is different from what is recorded in the database, arpwatch reports this. Prelude can use arpwatch as a plugin to detect ARP behavior.

However, it is possible for the attacker to use special techniques, e.g., packet insertion or evasion with fragmentation, to evade detection [PN98], because network-based IDSs monitor the packets on a network. Moreover, it is difficult for an IDS to deal with a large number of fragmented packets because it must defragment before it can analyze them. Therefore, intentional packet fragmentation causes a malicious one-way attack, and makes detection by IDS difficult for wasteful packet defragmentation [Son99b], and the IETF describes in [ZRT95, Mil01]. For this reason, there is the possibility of misdetection of a malicious ARP packet.

2.4 Access Control

In network security solutions, a network administrator must be aware of access control to protect his/her network. To reduce the management cost of IP address assignment, moreover, the administrator can use the Dynamic Host Configuration Protocol (DHCP) [Dro97] in IPv4.

For example, a university network blocks unauthorized access to the network using students's identity. For address assignment, NetReg is a registration system using the DHCP to control user access in a campus network, as described in [VW99]. NetReg needs three administrative components: DHCP, DNS and WWW servers. Until completion of an initial registration, the user is assigned a temporary IP address which allows limited access, and a fake DNS server address to guide the user into the entry procedure for NetReg. The user is then given a proper IP address and a true DNS server address to access the campus network. NetReg not only provides user registration to assign addresses such as IP and DNS server, but also lets administrators know the number of registered users on each subnet, assigned address information and user names. However, NetReg has limitations, such as wasteful address reservation, duplicate address usage and methods for bypassing temporary IP address and fake DNS server assignment.

Additionally, wireless LANs have spread rapidly and are now being used in enterprise networks and other public spaces. Because of this, IEEE 802.1X (Port Based Network Access Control), which can authenticate an accessed device's identity at a switching hub, is being focused on by network administrators. IEEE 802.1X can employ several authentication methods, such as EAP-MD5 (hashed password authentication) and EAP-TLS (mutual authentication using digital certificate)[BV98, AS99].

2.5 SEND

In IPv6, the IETF Secure Neighbor Discovery (SEND) working group [Groa] discusses how to enable autoconfiguration, in which, for example, every host begins to communicate without manual configurations with secure signaling for Neighbor Discovery with IPsec. However, there are some difficulties because [NNS98] did not explain the full architecture for using IPsec. There are also some problems with IPsec key management such as manual keying and configuration of security associations [ANKR03], e.g., on a large wireless network with roaming users using IKE [HC98]. For this reason, methods exist for trying to achieve secure communication using keys, such as Cryptographically Generated Addresses (CGA) [Aur03]. At the moment, a method called SEND [AKS+03], in contradistinction to ND, is mainly discussed to carry out secure signaling with IPsec AH and CGA generated from the host's public key and other factors.

However, there are some anxieties that incompatibility between ND and SEND, and the necessity for public-private key pairs and cryptographic mechanisms, are costly for key generation and verification and indispensable additional RFC. As mentioned above, ND remains insecure until all hosts and devices on the network use only SEND. Consequently, autoconfiguration is desired to deploy IPv6 devices for performing Plug and Play communications.

2.6 Computer and Network Forensics

In the Internet, some assistance can be found for Computer and Network Forensics (CNF). In computer forensics, tools are available for the victim host to perform data recovery, acquisition and analysis [Gar01, FV, Carb, Cara]. Of course, traditional tools, such as *dd* and *mount* commands, are used for evidence recovery and seizure. Moreover, a distributed data capture approach has been proposed, which tries to record a large number of packets for CNF, as described in [KSB03]. In after-the-fact processes,

[MY01] proposes security policies, and [YM02] describes a deception technique to promote CNF. By monitoring logs and capturing packets, [Inc] tries to track back to a malicious user in the same administrative domain.

Chapter 3

The Self-Confirming Engine

3.1 Introduction

The Internet is growing rapidly and being used for many purposes such as business, education, medical services, and entertainment. However, this growth brings us not only benefits, but also dangers such as unauthorized access. Today, people tend to connect their devices to the Internet to make their everyday life more convenient, without sufficiently considering security. This allows the malicious user to perform unauthorized access, and is why unauthorized access is currently increasing along with the growth of the Internet.

One type of unauthorized access is Man-in-the-Middle (MitM) attack, in which an attacker, located between two communicating hosts, intercepts and relays information between both hosts so that each user believes they are communicating directly with the other while, in fact, both are communicating via the attacker. In IP communications over the same local link, each host has to find out the peer's link-layer address from the IP address. If an attacker modifies the address mapping table of a legitimate host, MitM attack will be accomplished.

In the Internet, there are many ways to make successful unauthorized access. This research has focused particularly on MitM attack for the following reasons:

- Anyone can perform MitM attack easily by address mapping violation.
- During MitM attack, communication between the two victims proceeds normally. Therefore, the victims fail to recognize that an attack is taking place.
- MitM attack can be catastrophic, because data communicated between hosts can easily be intercepted and altered.

- With the widespread use of wireless and mobile access networks, MitM attack is increasing and becoming easier to perform.
- Address mapping violation can be achieved in both IPv4 and IPv6 environments.

In 3.2, this research describes address resolution and address mapping violation. Proposed technique is presented in 3.3, and verified in 3.4. Finally, summary is describes in 3.5.

3.2 Address Resolution

In a local network, a host must know both the IP address and the link-layer address of the peer host before communication. Every host has to send a request periodically to peer hosts on the local link to obtain the peer's link-layer address. If the peer host is on the local link, it sends a reply packet with its local link-layer address included.

3.2.1 Protocols

Address Resolution Protocol (ARP)

In IPv4, this mechanism is performed by the ARP [Plu82], as shown in Figure 3.1(1). Host A broadcasts an ARP request for resolving the link-layer address of host B. Host B responds to this request by sending an ARP reply with its link-layer address to host A. Host A caches both the IP address and the link-layer address of host B in its address mapping table, called an "ARP Cache". Normally, the timer to refresh the ARP cache is set to 20 minutes, and host A uses this cached information to communicate with host B. Hence host A can begin communication quickly, and has no need to perform address resolution again until the cached information expires.

Neighbor Discovery (ND)

In IPv6, ND [NNS98, TN98] is activated for address resolution, as shown in Figure 3.1(2). Host A sends a Neighbor Solicitation (NS) [NNS98] packet to the solicited-node multicast address of the peer host as the destination address. Host B then responds to the request by sending a Neighbor Advertisement (NA) [NNS98] packet with its link-layer address. As a result, the two peer hosts communicate using each other's IP address and link-layer address. Hosts A and B cache each other's IP address and link-layer address in their own address mapping tables, called a "Neighbor Cache".

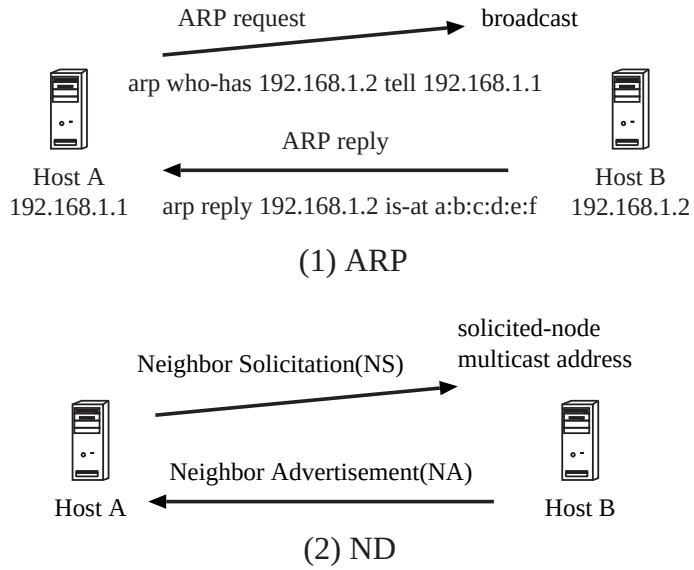


Figure 3.1: Address Resolution in ARP and ND

ND also has neighbor reachability state [NNS98] about cached hosts with an address mapping entry in its table. That is, the IP address of a peer host which has already performed address resolution does not need to be resolved again, because the host can use the information obtained from the first resolution. By this method, ND cuts down the cost of address resolution and decreases the number of address resolution packets compared to ARP.

As mentioned above, the default configuration is that the ARP Cache expires after 20 minutes. Even if the peer host is down or the network path fails, ARP still caches the information for this time limit. Therefore, ARP has the disadvantage that it cannot detect any failure before cached data expires. Like ARP, ND needs the link-layer address of a communication peer on the same link. However, because ND executes a Neighbor Unreachability Detection (NUD) procedure before beginning the communication even if the host still maintains the Neighbor Cache, the host can detect the reachability of a peer host before the cache timer expires. As a result, ND can detect the failure and invalidity of cached information faster than ARP.

3.2.2 Address Mapping Violation

In this research, the modification of the address mapping table is referred, i.e., ARP Cache and Neighbor Cache, by an attacker as "address mapping violation" because the violation includes not only ARP Poisoning but also ND Poisoning.

Here this research describes cases in which the attacker achieves address mapping violation in both ARP and ND.

The Case of ARP

In ARP, an attacker can send a malicious ARP request or reply as shown in Figure 3.2(1). The victim host has no mechanism to detect its correctness, and the attacker will use spoofed information to create or alter the victim's ARP Cache. The attacker can freely create and alter the stored ARP Cache entry of the victim host. As a result, MitM attack can be executed.

Figure 3.3 illustrates an example of MitM attack. In this figure, the attacker deceives host A to alter the ARP Cache entry for host B (*192.168.1.2*) from [*00:00:00:00:01:02*] to [*00:00:00:00:01:03*]. The attacker then deceives host B to alter its ARP Cache entry for host A (*192.168.1.1*) from [*00:00:00:00:01:01*] to [*00:00:00:00:01:03*]. From now on, when host A begins a connection to host B, the packet will be sent to the attacker through the true path. The attacker can also alter and forward data packets to host B as though the packets were originally transmitted from host A through the fake path. At this moment, host A and host B mistakenly believe that the data is being transmitted between two hosts directly.

Moreover, because of the wide use of wireless devices, the Internet can be accessed more easily and an MitM attack can be executed in a wide environment, without the support of any skillful technique and with many hacking tools obtainable from the Internet.

The Case of ND

The ARP Cache entry can easily be created or altered by a malicious ARP. Similarly, ND is vulnerable at the Neighbor Cache entry.

Accordingly, even if a host uses an ND message for address resolution in IPv6, the attacker can still alter the Neighbor Cache entry and execute an MitM attack using a malicious ND packet, as in ARP. An example of falsifying by using an NA packet to carry out address mapping violation is illustrated in Figure 3.2(2).

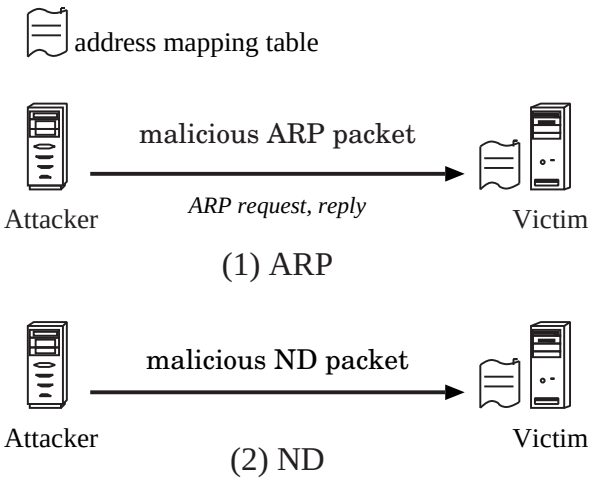


Figure 3.2: Malicious Packets in ARP and ND

Similarly, as shown in Figure 3.3, host A maintains the Neighbor Cache entry of host B. If the attacker sends an NA packet with an override flag to host A, host A will rewrite the information about host B stored in its Neighbor Cache entry. As a result, the attacker can still achieve MitM attack, even on the IPv6 network. Therefore, the prevention of MitM attack caused by address mapping violation in both ARP and ND cannot be neglected.

3.3 Proposed Method

This proposed method, called a Self-Confirming Engine (SCE), corrects address mapping violation leading to MitM attack. The SCE focuses on the following:

- Necessary Conditions
  The SCE requires no extra modification to ARP and ND. In the current version of the proposed system, however, the user must establish an IP address and a link layer address into the configuration file of the system.
- Monitoring address mapping tables
  Suppose a malicious user sends an abnormal query to the victim host. As described in the previous section, there are many mechanisms to detect malicious packets. However, there are also various techniques to evade detection by Intrusion Detection System (IDS) [Bac99]. Consequently, the best way to detect

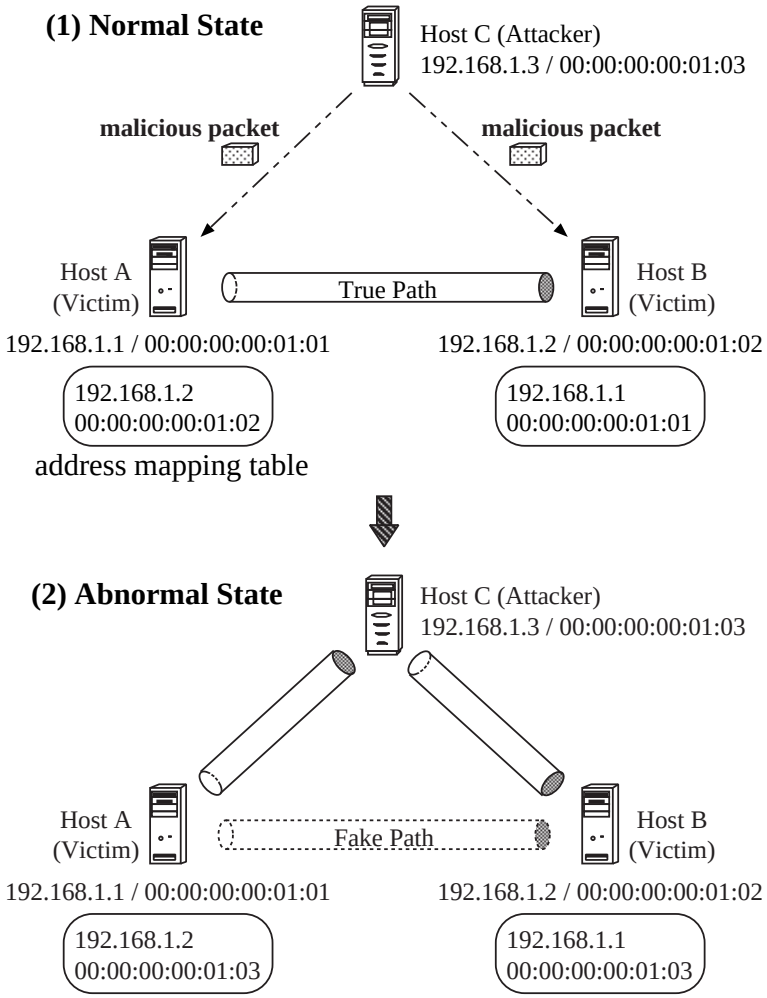


Figure 3.3: Address Mapping Violation and MitM Attack

address mapping violation and prevent MitM attack is to monitor the alteration of address mapping tables and check whether an alteration is legitimate.

- Validity of Address Resolution
  Suppose the state of two link-layer addresses assigned to the same IP address on a local link is abnormal. Generally, it is obviously abnormal for a network interface with one IP address to have two different link-layer addresses. This research can interpret this modification as an address mapping violation. For this reason, a user cannot employ the SCE if under the state, two different link-layer addresses have the same IP address, a state accepted by a network administrator as a normal environment.

- Autoconfiguration
  One of the advantages of IPv6 is autoconfiguration, as described in [TN98]. Therefore, simplicity is required as the SCE is designed to be installed in various devices in the future. Hence, this research aims to use simple architecture and have high usability for applying to future devices, such as keyboardless and monitorless equipment, on the IPv6 network. The proposal is more secure than ND and more usable than SEND [AKS+03], as shown in Figure 3.4.

In a period of transition from ND to SEND, there is no compatibility between non-SEND(ND) and SEND hosts, because an ND host cannot verify an IPsec AH [KA98b, KA98a] header in a SEND packet and discard the packet. Until SEND is deployed completely, the proposed method supports ND hosts and devices in the address resolution procedure. Otherwise, when devices require not total security with IPsec AH but usability, the proposal is effective.

3.3.1 System Overview

The SCE monitors the address mapping tables, i.e., ARP Cache and Neighbor Cache.

When an alteration of an address mapping pair occurs, the SCE checks its validity for inquiring. In this research, the SCE uses an ARP request, for ARP, or a Neighbor Solicitation (NS) packet and Router Solicitation (RS) packet, for ND.

Figure 3.5 indicates the confirmation procedure for the following roles:

- Monitor Tables
  The SCE monitors the address mapping table in IPv4. In IPv6, the SCE monitors the routing table to obtain the host's default gateway.

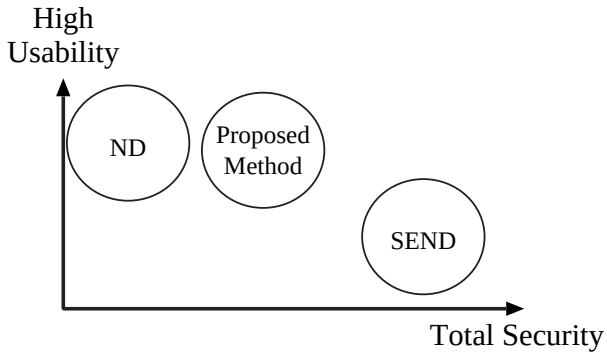


Figure 3.4: Usable Possibilities and Total Security

- Data Check
  The SCE checks whether the address mapping entry exists in recorded data of the SCE; in this research, this is called the Traveling Database (TDB).

- Record Entry
  If the entry is new, the SCE records the address mapping pair in the TDB. Moreover, the SCE applies recorded time and neighbor reachability state in the TDB to the confirmation procedure, because an attacker can perform an intentional confirmation claim arising from malicious registration (e.g., initial recording of an attacker's address, or deceitful utilization of a DHCP address pool).

- Data Comparison
  If the same IP address entry already exists in the TDB, the SCE compares the current link-layer address with the recorded link-layer address.

- ARP Confirmation (ARP)
  If the link-layer address is different from that in the TDB, the SCE sends an ARP request for confirmation.

- DAD Confirmation (ND)
  If link-layer address is different from the TDB, the SCE sends an NS packet for confirmation.

- RS Confirmation (ND)
  If the suspicious host is a router, the SCE sends a confirmation packet for RS to check router options, e.g., Prefix Information. This confirmation procedure is effective against Parameter Spoofing [NKN03].

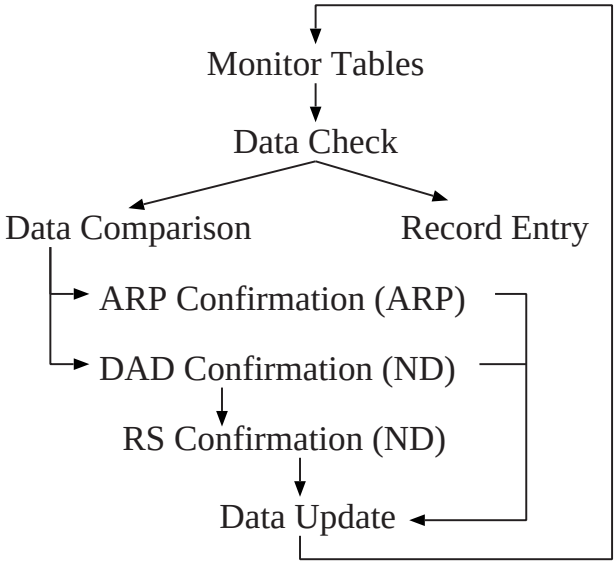


Figure 3.5: Confirmation Procedure Flow

- Data Update
  The SCE records and updates the current entry in the TDB.

3.3.2 Confirmation Model

Figure 3.6 illustrates a confirmation method in this proposal. The address mapping table of host A holds a record of host B's IP address and link-layer address. Assume an alteration to the address mapping table on host A occurs, and the table is altered from [*00:00:00:00:01:02*] to [*00:00:00:00:01:03*]. In this case, the SCE sends a confirmation packet to host B to check whether the old cached link-layer address is still active.

The Case of ARP

In ARP, when an alteration of an ARP Cache occurs, the SCE sends an ARP request as a confirmation packet to the old link-layer address corresponding to host B, as shown in Figure 3.6(1). In this case, validity can be checked by waiting for an ARP reply.

Thus this research can conclude the following, depending on whether or not a host using this proposed method receives an ARP reply:

- No ARP reply received
  No host replies to the ARP request because the host with the old link-layer

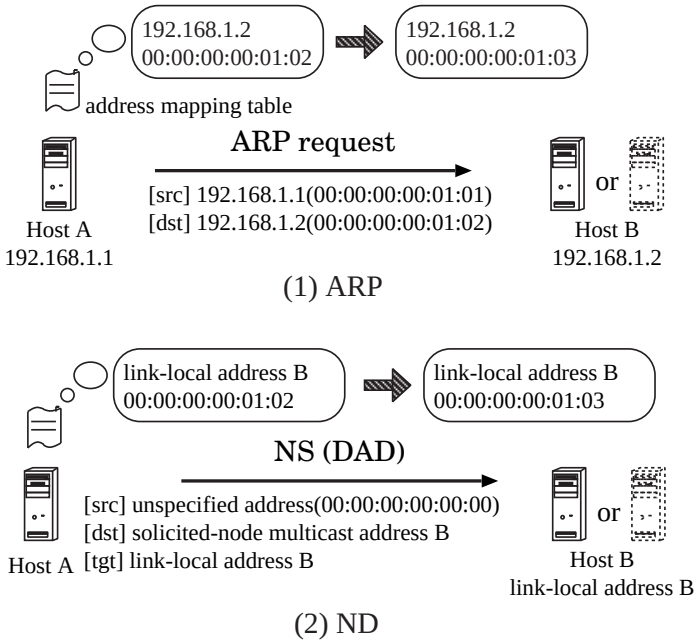


Figure 3.6: Confirmation Procedure for Address Resolution

address does not exist. This proves that the IP address is assigned to a new host. Hence the newly-altered address mapping table on host A is normal.

- ARP reply received
  Host B with the old link-layer address received the ARP request and answers. Receipt of the ARP reply indicates that host B is still using the same link-layer address and IP address. This proves that the alteration of the address mapping table on host A is abnormal. Hence the compromised address mapping table has been corrected by receipt of the ARP reply from genuine host B.

Consequently, by implementing this method, this research prevents invalid alterations. The validity of the address mapping table is confirmed by making the SCE send the confirmation packet to the uncertain host B, as shown in Figure 3.6(1).

The Case of ND(DAD)

In the case of ND, when an alteration occurs on host A, as shown in Figure 3.6(2), the SCE sends a Neighbor Solicitation (NS) packet to uncertain host B for the purpose of Duplicate Address Detection (DAD) [NNS98, TN98]. At this time, the NS packet is

sent using "solicited-node multicast address B" as the destination, "link-local address B" as the target address, and "link-layer address B" as the destination address of a link layer.

Hence the proposed system, which is monitoring the address mapping table of ND, sends an NS packet to confirm the alteration. By this process, the SCE on host A verifies the following:

- No Neighbor Advertisement (NA) packet received
  No host replies to the NS packet because the host with the old link-layer address does not exist. This proves that the IP address is assigned to a new host. Hence the newly-altered Neighbor Cache on host A is normal.
- NA packet received
  Host B with the old link-layer address received the NS packet and answers. Receipt of an NA packet indicates that host B is still using the same link-layer address and IP address. This proves that the alteration of the address mapping table on host A is abnormal. Hence the compromised address mapping table on host A has been corrected by receipt of an NA packet from genuine host B. Moreover, because the source address of the NS packet uses an unspecified address for the purpose of DAD, the NA packet is returned to "all-nodes multicast address" [NNS98] as the destination address. Therefore, all address mapping tables on compromised hosts on the same local link can be corrected at the same time.

As described above, when an address mapping violation occurs in IPv6, the validity of the altered address mapping table can be checked by using the proposed confirmation technique. In addition, if the alteration is abnormal, the compromised table is automatically corrected by the returned NA packet.

Since the proposed technique is simple, this method does not require any complicated setup and can act under existing protocols. Moreover, after booting the proposed system, the mapping data can be maintained in the TDB to take advantage of historical address mapping information in both ARP and ND.

The Case of ND(RS)

In the case of ND(RS) after DAD Confirmation, when a confirmed host is a router, as shown in Figure 3.7, SCE sends a confirmation packet to router B for Router Solicitation (RS). An RS packet from host A is then sent to the "all-routers multicast address" as the destination address with an unspecified address as the source address.

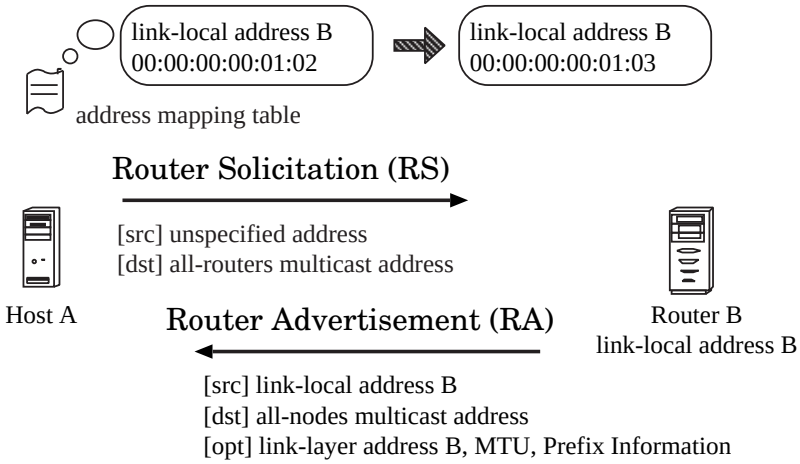


Figure 3.7: Confirmation Procedure for Router Options

Because of this confirmation procedure, host A can acquire all router options from a proper router if router B is still active. At this time, router B replies with a Router Advertisement (RA) packet to the all-nodes multicast address as the destination address. Therefore, all hosts on the same local link can reconfirm the latest router options.

As for the network environment, finally, a switching hub is not prerequisite for the SCE because the SCE employs the target host's address as the destination link layer address for confirmation packets. For this reason, each confirmation packet can be sent to the target host to correct an address mapping violation, without being noticed by an attacker. In a shared hub environment, however, an attacker may notice whether an address mapping violation is corrected by listening to a confirmation packet.

3.3.3 Protocol Comparisons

The proposed method relies on both ARP and ND to confirm whether or not an alteration of an address mapping entry is legitimate. To show the difference between the proposed system and original protocols, protocol comparisons are made as follows:

- ND (non-SEND)
  ND does not employ public-private key pairs in address resolution. For this reason, ND has no need to create its own IP address using CGA and verify the source address in a received packet. Therefore, ND is a more lightweight protocol than SEND, and is widely used in the current Internet. However, ND

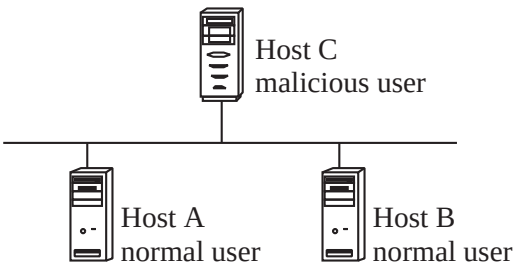
has a vulnerability in Neighbor Cache, i.e., a malicious ND packet can cause address mapping violation leading to MitM attack at any time.

- SEND
  SEND is a protocol that can replace an original ND to realize a verifiable address resolution procedure. Because SEND aims to be able to verify a sender's IP address, generated by CGA, it is very different from current ND. For this reason, SEND needs CGA and IPsec AH mechanisms for secure signaling, and must perform key generation, verification and management. However, SEND is still in draft phase to achieve its purpose. Unfortunately, SEND is not compatible with ND.

- Proposed Method
  The proposed method works under original ND. Therefore, as with ND, the proposed system does not employ a key mechanism to confirm whether an address mapping alteration is right. That is, the proposal likewise has no overheads to generate and verify an IP address. The proposal, moreover, is workable in both IPv4 and IPv6.

Therefore, address mapping tables are within a protectable area of the proposal. The proposed method detects an alteration of an address mapping entry and confirms whether the modification is right. The proposed method also confirms router options such as prefix information, if the host is a router. In this regard, the proposed method is more secure than ND (non-SEND), as shown in Figure 3.4. Moreover, the proposal has higher usability than SEND, because the proposed system uses fairly simple architecture and is widely applicable for existing protocols.

On the other hand, the proposed system cannot protect transmitting data against an attacker's sniffing and connection hijacking, because the proposed method does not encrypt data. Moreover, the proposal cannot verify using the sender's public key whether a source address is legitimate. Therefore, the proposed method is less effective than SEND with respect to total security, because the proposal does not employ CGA in address resolution. Finally, like the other methods, the current SCE is weak against a large number of false packets. For example, if an attacker tries to interfere with a confirmation packet, by which a normal host corrects its own compromised table by receiving an ARP (or ND) packet from the proper host, an attacker will send a lot of disturbing packets to the victim host in order to make proper communication between the two normal hosts impossible. In this case, both normal hosts will become aware of the existence of the attacker by receiving disturbance packets. However, The proposed



Host A [IP address] 192.168.1.1 / fe80::2b0:d0ff:fead:13c2
[link-layer address] 00:b0:d0:ad:13:c2

Host B [IP address] 192.168.1.2 / fe80::290:ccff:fea1:9c56
[link-layer address] 00:90:cc:a1:9c:56

Host C [IP address] 192.168.1.3 / fe80::290:ccff:fea6:c11e
[link-layer address] 00:90:cc:a6:c1:1e

Figure 3.8: Experimental Environment

method must make the SCE more intellectual because an attacker can obstruct a confirmation packet.

3.4 Experimental

The proposed method is implemented on FreeBSD 4.7-RELEASE. In this section, the proposal verifies the method and confirm that it is effective against address mapping violation. In the experimental environment, as is shown in Figure 3.8, hosts A and B are operated by normal users and host C is operated by a malicious user; every host belongs to the same local network, with a switching hub among them.

When a malicious ARP request is sent to host A from host C impersonating host B, the SCE on host A will detect the alteration of host B's address mapping entry in its table. Hence the system sends a confirmation packet to host B, using host B's previous link-layer address before the alteration, as shown in Figure 3.9(1). Figure 3.10 indicates the four packets exchanged at that moment. The malicious ARP request that was sent from host C to host A, using host B's IP address as the source address, is shown in Figure 3.10(1). Hence the address mapping table on host A is altered as shown in Figure 3.9(2). Figure 3.10(2) indicates host A sending an ARP reply to host

```
% arp -na
? (192.168.1.2) at 00:90:cc:a1:9c:56 on xl2 [ethernet]            --- (1)

% arp -na
? (192.168.1.2) at 00:90:cc:a6:c1:1e on xl2 [ethernet]            --- (2)
```

Figure 3.9: Address Mapping Table of Host A in ARP

```
01:31:27.181879 0:90:cc:a6:c1:1e 0:b0:d0:ad:13:c2 0806 60: arp who-has 1\
92.168.1.1 (0:b0:d0:ad:13:c2) tell 192.168.1.2                    --- (1)

01:31:27.181915 0:b0:d0:ad:13:c2 0:90:cc:a6:c1:1e 0806 60: arp reply 192\
.168.1.1 is-at 0:b0:d0:ad:13:c2                                   --- (2)

01:31:27.601744 0:b0:d0:ad:13:c2 0:90:cc:a1:9c:56 0806 42: arp who-has 1\
92.168.1.2 (0:90:cc:a1:9c:56) tell 192.168.1.1                    --- (3)

01:31:27.601936 0:90:cc:a1:9c:56 0:b0:d0:ad:13:c2 0806 60: arp reply 192\
.168.1.2 is-at 0:90:cc:a1:9c:56                                   --- (4)
```

Figure 3.10: Packets Exchanged on Host A in ARP

C and the malicious alteration succeeding.

However, when the SCE that detected the alteration sends an ARP request using the previous address mapping pair, (*192.168.1.2*) maps to [*0:90:cc:a1:9c:56*] as shown in Figure 3.10(3). Therefore, in Figure 3.10(4), the proper host B can receive the ARP request and reply to host A. The ARP Cache on host A restores the correct address in consequence, as shown in Figure 3.9(1). Accordingly, it can recover from the malicious alteration, using the ARP request as a confirmation packet generated by the proposed system on host A, and prevent the MitM attack in advance.

Next, the proposed method is verified in IPv6. Figure 3.11 shows the address mapping table of host A. When a malicious ND packet, as shown in Figure 3.2(2), is sent to host A from host C impersonating host B, the Neighbor Cache on host A is altered. Figure 3.12 indicates the packets exchanged at that moment. In Figure 3.12(1), the malicious NA packet from host C falsifies the Neighbor Cache on host A,

```
% ndp -a
fe80::290:ccff:fea1:9c56%xl2  0:90:cc:a1:9c:56   xl2 23h58m20s S  R
fe80::2b0:d0ff:fead:13c2%xl2  0:b0:d0:ad:13:c2   xl2 permanent R
fe80::1%lo0                     (incomplete)     lo0 permanent R
```

Figure 3.11: Address Mapping Table of Host A in ND

```
22:56:14.684779 0:90:cc:a6:c1:1e 0:b0:d0:ad:13:c2 86dd 86: fe80::290:ccf\
f:fea1:9c56 > fe80::2b0:d0ff:fead:13c2: icmp6: neighbor adv: tgt is fe80\
::290:ccff:fea1:9c56(RO)(tgt lladdr: 00:90:cc:a6:c1:1e) (len 32, hlim 25\
5)                                                              --- (1)

22:56:14.934139 0:b0:d0:ad:13:c2 0:90:cc:a1:9c:56 86dd 78: :: > ff02::1:\
ffa1:9c56: icmp6: neighbor sol: who has fe80::290:ccff:fea1:9c56 (len 24\
, hlim 255)                                                     --- (2)

22:56:14.934302 0:b0:d0:ad:13:c2 0:90:cc:a1:9c:56 86dd 62: :: > ff02::2:\
 icmp6:router solicitation  (len 8, hlim 255)                   --- (3)

22:56:14.934429 0:90:cc:a1:9c:56 33:33:0:0:0:1 86dd 86: fe80::290:ccff:f\
ea1:9c56 > ff02::1: icmp6: neighbor adv: tgt is fe80::290:ccff:fea1:9c56\
(RO)(tgt lladdr: 00:90:cc:a1:9c:56) (len 32, hlim 255)          --- (4)

22:56:15.187980 0:90:cc:a1:9c:56 33:33:0:0:0:1 86dd 110: fe80::290:ccff:\
fea1:9c56 > ff02::1: icmp6: router advertisement(chlim=64, pref=medium, \
router_ltime=1800, reachable_time=0, retrans_time=0)(src lladdr: 00:90:c\
c:a1:9c:56)[ndp opt] (len 56, hlim 255)                         --- (5)
```

Figure 3.12: Packets Exchanged on Host A in ND

```
16:51:54.441397 0:90:cc:a6:c1:1e 0:90:cc:a1:9c:56 0806 60: arp reply 192\
.168.1.1 is-at 0:90:cc:a6:c1:1e                                    --- (1)

16:51:54.765878 0:90:cc:a1:9c:56 0:90:cc:a6:c1:1e 0800 74: IP 192.168.1.\
2.1030 > 192.168.1.1.23: S 3451569783:3451569783(0) win 57344 <mss 1460,\
nop,wscale 0,nop,nop,timestamp 463395 0> (DF)                      --- (2)

16:51:54.798408 0:90:cc:a6:c1:1e 0:90:cc:a1:9c:56 0800 74: IP 192.168.1.\
1.23 > 192.168.1.2.1030: S 2746315679:2746315679(0) ack 3451569784 win 5\
7344 <mss 1460,nop,wscale 0,nop,nop,timestamp 178328 463395> (DF) --- (3)

16:51:54.798647 0:90:cc:a1:9c:56 0:90:cc:a6:c1:1e 0800 66: IP 192.168.1.\
2.1030 > 192.168.1.1.23: . ack 1 win 57920 <nop,nop,timestamp 463398 178\
328> (DF)                                                          --- (4)
```

Figure 3.13: Packets Exchanged on Host B without the SCE

i.e., (*fe80::290:ccff:fea1:9c56%xl2*) maps to [*0:09:cc:a6:c1:1e*]. As a result, as shown in Figure 3.12(1), the Neighbor Cache on host A is compromised.

At that time, the SCE detects the alteration and sends an NS packet for the purpose of DAD from host A, as shown in Figure 3.12(2). A confirmation packet from the SCE on host A is sent to the genuine host B, using the link-layer address before the alteration as the destination address. Moreover, in Figure 3.12(3), the SCE sends a confirmation packet for router solicitation to an all-routers multicast address because host B is a router.

Hence, genuine host B receives the packets from host A and answers, as shown in Figure 3.12(4)(5). Therefore, host A can receive the NA packet with an override flag to correct its own address mapping table and reconfirm the router options. As a consequence of this process, the proposed method confirmed that the compromised Neighbor Cache is recovered, i.e., (*fe80::290:ccff:fea1:9c56%xl2*) maps to [*0:09:cc:a1:9c:56*].

Additionally, host B replies to the packets with an "all-nodes multicast address" as the destination address as per RFCs, as shown in Figure 3.12(4)(5). Hence, the packets from a genuine host are valid to recover the incorrect alteration and reconfirm router options on the other hosts, because the packets reply to all hosts on the same local link. Therefore, if a host uses the proposed system, the compromised tables of all other hosts on the same local link are corrected when a violation occurs.

```
18:14:33.021896 0:90:cc:a6:c1:1e 0:90:cc:a1:9c:56 0806 60: arp reply 192\
.168.1.1 is-at 0:90:cc:a6:c1:1e                                    --- (1)

18:14:33.271982 0:90:cc:a1:9c:56 0:b0:d0:ad:13:c2 0806 42: arp who-has 1\
92.168.1.1 (0:b0:d0:ad:13:c2) tell 192.168.1.2                     --- (2)

18:14:33.272066 0:b0:d0:ad:13:c2 0:90:cc:a1:9c:56 0806 60: arp reply 192\
.168.1.1 is-at 0:b0:d0:ad:13:c2                                    --- (3)

18:14:46.828271 0:90:cc:a1:9c:56 0:b0:d0:ad:13:c2 0800 74: IP 192.168.1.\
2.1069 > 192.168.1.1.23: S 2299871969:2299871969(0) win 57344 <mss 1460,\
nop,wscale 0,nop,nop,timestamp 960593 0> (DF)                      --- (4)

18:14:46.828624 0:b0:d0:ad:13:c2 0:90:cc:a1:9c:56 0800 74: IP 192.168.1.\
1.23 > 192.168.1.2.1069: S 432419497:432419497(0) ack 2299871970 win 573\
44 <mss 1460,nop,wscale 0,nop,nop,timstamp 28627 960593> (DF)      --- (5)

18:14:46.833330 0:90:cc:a1:9c:56 0:b0:d0:ad:13:c2 0800 66: IP 192.168.1.\
2.1069 > 192.168.1.1.23: . ack 1 win 57920 <nop,nop,timestamp 960594 286\
27> (DF)                                                           --- (6)
```

Figure 3.14: Packets Exchanged on Host B with the SCE

Finally, the proposed method is tested whether or not this system is valid against an actual attacking tool, called an ettercap [OV], which can execute an MitM attack in IPv4. In this verification, host B twice tries to connect to host A using telnet protocol. Two types of figures show packets exchanged between hosts A and B during the attack. First, Figure 3.13 indicates that an MitM attack by malicious host C succeeded because host A does not employ the proposed system. When a malicious ARP packet, as shown in Figure 3.13(1), is sent to host B from host C impersonating host A, the address mapping table on host B is altered. For this reason, TCP's three-way handshake mechanism, as shown in Figure 3.13(2 - 4), is completed using the incorrect address mapping table on host B. Similarly, host A is compromised by host C. Consequently, normal hosts A and B cannot prevent MitM attack without the proposed method.

Second, Figure 3.14 indicates that an MitM attack failed because hosts A and

B employ the proposed method. When a malicious ARP packet, as shown in Figure 3.14(1), is sent to host B from host C impersonating host A, the address mapping table on host B is altered. At this time, as shown in Figure 3.14(2), the proposed method detects the malicious alteration on host B and sends an ARP request packet to host A using host A's link-layer address before the modification, i.e., [*0:b0:d0:ad:13:c2*]. In Figure 3.14(3), host B can receive an ARP reply packet from the proper host A to revise the incorrect ARP Cache on host B. As a result, TCP's three-way handshake mechanism, as shown in Figure 3.14(4 - 6), is completed using the correct address mapping table on host B. Similarly, host A prevents MitM attack by malicious host C by employing the system.

3.5 Discussion

3.5.1 Deployment Model

In this work, the SCE is concerned with attacks in a link local environment, because the focus of network security in the Internet is becoming closer to the user side. Until recently, a boundary existed between the Internet and an enterprise, i.e., the outside environment is exterior to the enterprise's network. For this reason, security solutions focused on perimeter defense to protect the interior network against attack from the exterior environment. However, users currently are exposed to the threat of attack from within the enterprise's network. Accordingly, the 'outside' is every part of the network except the user, even if the user exists in the enterprise network, and the 'inside' is only the individual user. In current networks, users must grasp that the boundary line exists not at the interface between the Internet and the enterprise, but at the access point where the user connects to the network.

Threats to information leakage also exist within a particular link local network, and it is hard for communicating users to perceive when transmitting data is being listened to by an attacker. For users to communicate with each other, address resolution protocols, i.e., ARP and ND, are used in a link local network, and are needed for users to know address mappings between link-layer and IP addresses before communication. Therefore, address resolution procedures must be protected to achieve proper communication against information exposure and mistaken application logging such as MitM attack.

Compared with the SCE, NetReg is an approach to control user access using DHCP, DNS and WWW servers in campus networks, as described in Chapter 2. To filter out

unauthorized users, users must register with NetReg before a true IP address and the DNS server's address are assigned. Until registration, however, the user can gain access using a temporary IP address and a fake DNS server's address assigned by the DHCP server. Therefore, a malicious user may execute various types of attack to get an IP address to access every network, find the true DNS server's address, and direct normal transmitting data to the attacker using a spoofed packet. NetReg is a system, moreover, for users such as students who can enter the NetReg initial registration.

In comparison with NetReg, therefore, the SCE is a simpler architecture for future devices that lack entry methods or cannot register themselves, and a solution focused on address resolution procedures to enable correct communication even after an IP address has been assigned.

The SCE has some limitations in its solution model. The SCE is applied to address resolution procedures to confirm alterations in address mapping tables. In IPv4, therefore, address mapping tables of hosts using the SCE are protected against malicious mapping modification. That is, the SCE is a personal and individual solution, and not a borderline defense like a Firewall located in a demilitarized zone (DMZ). In IPv6, the SCE also works as a personal prevention system against address mapping violation, as it does in IPv4. Even if a host does not employ the SCE, moreover, a confirmation packet sent for DAD purposes by another host using the SCE brings about a return packet to an all-nodes multicast address as the destination address. Consequently, the SCE should be employed in each host to avoid threats from insiders.

A forwarding switch learns the address pair, i.e., an IP address and a link-layer address, connected to the port because a packet can be sent only if the port corresponds correctly to the destination address of the transmitting data. At this point, the behavior of two forwarding switches (Extreme Networks's Summit48 and Foundry Networks's FastIron Edge Switch 2402) is checked when an abnormal situation occurs in which two different hosts using same link-layer address exist. In this case, when only one of the other hosts sends a packet, communication can be executed without problems. When two both hosts send a packet simultaneously, however, the forwarding table in the switch is renewed whenever a packet is received, and packet loss occurs. Therefore, a network administrator cannot rely on address learning by the forwarding switch. On the other hand, to exclude an abnormal state, some switches have a port security method that only allows the first link-layer address to appear on the port. However, a strict port permission system limits the network administrator's capacity to establish a network environment freely.

```
# arp -s 192.168.1.1 00:00:00:00:00:01                                  --- (1)

# arp -an
? (192.168.1.1) at 00:00:00:00:00:01 on xl0 permanent [ethernet]  --- (2)

# ndp -s fe80::201:2ff:fe52:xxxx%xl0 00:00:00:00:00:01             --- (3)

# ndp -a
Neighbor                      Linklayer Address  Netif Expire    St Flags\
 Prbs
fe80::201:2ff:fe52:xxxx%xl0  0:0:0:0:0:1          xl0 permanent R --- (4)
```

Figure 3.15: Example of *arp* and *ndp* Command for Static Address Entry

3.5.2 Protocol Overhead

In each protocol, i.e., ARP and NP, a confirmation packet is sent by the SCE when an alteration of an address mapping entry occurs. Because users can know, from transmission of a confirmation packet, whether or not a change of address mapping is proper, incorrect address pairs can be recovered in address mapping tables. Therefore, the SCE sends a confirmation packet for every modification, to check and preserve the legitimacy of mapping entries in each table. That is, to confirm an alteration of address mapping tables, the SCE must send a 28-byte ARP packet, a 24-byte NS(DAD) packet and an 8-byte RS packet as extra traffic. Users can thus evade threats such as malicious listening. With recent increased network bandwidths, these additional packets sent by the SCE have a negligible effect on the network.

3.5.3 Security Considerations

In the current Internet, an attacker can execute various network disruptions. For example, to disturb network communications, an attacker can send many futile packets to waste bandwidth and sever a normal connection. Moreover, an attacker can manipulate an address mapping table into an abnormal state, using a spoofed packet to intercept user data such as in MitM attack.

An attack to the SCE is considered as one of the following:

- Service Blockade

If an attacker does not need packet capture to listen to transmitting data, a large number of spoofed packets will be sent to a network or host for service blockade, known as a DoS or DDoS attack. The SCE is also vulnerable to this type of attack, because the SCE cannot stop spoofed one-way traffic sent from a malicious user. To filter out a spoofed packet before it arrives at the SCE, the packet from an attacker must be checked at each forwarding device, such as switches and routers, to establish whether or not the packet is inappropriate. Unfortunately, it is difficult to prevent undesirable traffic entirely, because packet spoofing is possible in each layer, e.g., the Data Link, Network, or Transport layer, as shown in Figure 1.1.

- Misleading Packet
  From the beginning of the Internet, it has been possible for anyone to assume a false address to send and receive a packet. That is, a malicious user can forge a spoofed packet to confuse the sender in an attack, deceive a user into falling into a snare, and impersonate another user. This type of technique is focused on, in this work, because an attacker can achieve address mapping violation leading to MitM attack by means of a spoofed packet.

  Therefore, a privileged user maps the link-layer address corresponding to an IP address statically, as shown in Figure 3.15. Figure 3.15(1) and (2) indicate that the privileged user establishes the address mapping entry in ARP as *192.168.1.1* assigned to 00:00:00:00:00:01. Also, Figure 3.15(3) and (4) show a setting example of an address mapping entry in ND as *fe80::201:2ff:fe52:xxxx%xl0* assigned to *0:0:0:0:0:1*. Accordingly, in both ARP and ND, a user should assign address mappings about fixed hosts in a local link statically, e.g., DNS and WWW servers. Needless to say, in a forwarding switch or a router on the path to the destination host, a network administrator should also map the link-layer address corresponding to the IP address statically, because address mappings of the basic devices used in network infrastructure, such as the switch and the router, can rarely be replaced without management by the network administrator.

- Wasteful Reservation
  An attacker may wastefully reserve an address mapping entry on the target host in advance, for directing a confirmation packet from the victim host to the attacker. In this situation, the victim host will believe that a reply packet from the attacker is authentic. To avoid such wasteful reservation, the confirmation process of the SCE can be modified to take into consideration the mapping time

frame and the reachability state.

This situation can also be avoided by deploying the method proposed in the next chapter, or other security solutions such as IEEE 802.1X authentication, in which case various countermeasures must cooperate to decrease the possibility of attack. For the future, it is also important to take countermeasures to prevent malicious access by the attackers, by keeping the uniqueness of a link-layer address within and between networks. It is therefore necessary not to depend on only one layer as the security solution, but also to use other layers' protection.

- Packet Drop
  If a reply packet does not return when a confirmation packet is sent by the SCE, the following cases are assumed:

  - All hosts are in a DoS attack
    The reply packet does not return when all hosts in a link local network are attacked with a large number of useless packets. Alternatively, the confirmation packet may be dropped because of saturated bandwidth. If all hosts are undergoing DoS attack, however, a host using the SCE can know a DoS attack to capture received packets. Therefore, a retransmission mechanism is needed for the confirmation packet, and users also should employ a device such as IDS to detect meaningless DoS attacks.
  - A specific host is in a DoS attack
    The reply packet does not return when a target host for confirmation in a link local network is attacked by a large number of useless packets, because the target host cannot receive the confirmation packet from the SCE. In this case, a user employing the SCE should perform another confirmation procedure to establish the network condition of the target host, because the DoS attack cannot be detected if a switching hub is used in the network. However, the user employing the SCE will also be aware of the existence of the DoS attack, because every packet will be dropped at the switching hub.

Various security solutions, such as IEEE 802.1X or a port security solution of a network switch, should be implemented whenever possible to avoid an attack by a malicious user, because the weakest point of a network environment is targeted by the attacker to maximize disruption.

3.6 Summary

In this research, a proposed method aimed to prevent MitM attack caused by address mapping violation, which allows attackers to intercept and alter data transmitted between two hosts. This proposed method sends a confirmation packet when an alteration is detected, published as [KKY03]. If the alteration is abnormal, the compromised table is corrected by receiving an ARP reply or NA packet from the proper host, and all compromised hosts on the same local link can correct at the same time in IPv6. Moreover, if an uncertain host is a router, the SCE deploys router options to get rid of suspicion such as Parameter Spoofing. Finally, the proposal verified the confirmation approach by altering the table in the cases of ARP and ND.

Research described in this chapter aims to ensure the uniqueness of a link-layer address in a network of the specific domain, because addresses can be modified as the attacker likes. It is possible to avoid malicious overwriting if address mapping is assigned statically. In the present Internet environment, however, there are many mobile users and devices that can communicate with each other. Therefore, it is difficult for all the address mapping to be assigned statically, because this restricts usefulness and availability. Furthermore, users do not have reliable methods to determine whether their link-local address is being used for malicious purposes on another network. This problem is discussed in the next section.

Chapter 4

Distributed Forensic Databases

4.1 Introduction

Security incidents reported to CERT/CC [Cen88] have been increasing since the 1980s [ACF+00], when malicious users were computer experts and attacks were conducted manually. From the early 1990s, however, even if an assailant was not adept using at computer systems, aggression became easy to execute with Graphical User Interfaces (GUI), targeted on many hosts at once. As a result of this transition, investigators must now be able to cope with extensive and sophisticated attacks.

In the next place, as described in [Ric03], an important issue is that there are now many attacks from the inside of a network. Interior access is more serious matter than exterior access, because an insider may have the authority to know where important documents are located, and reach various types of files and logs, more easily than can be achieved by an external trespasser. A company may consequently suffer great financial losses.

In the current enterprise society, some people repeatedly change jobs to improve their skills. The resulting high staff turnover poses a threat from insider attacks. When employees resign, the network administrators of that organization must be able to detect unauthorized access from insiders. In these circumstances, measures such as firewalls between the Internet and the corporate network are ineffective to protect the company, because company employees have access from within the network. It is thus hard for network administrators to block them, and employees may carry out unauthorized actions accidentally or deliberately. Moreover, remote access from outside the company, e.g., via Virtual Private Network (VPN), makes connecting from the Internet easier and increases the risk of being attacked. Eventually, all employers

and employees will be exposed to this threat.

Moreover, security against malicious activity is not a major priority for most business employees. A company may use obsolete computers in a specific system or application. For this reason, security awareness within the company is usually inadequate.

4.2 Computer and Network Forensics

Computer and Network Forensics (CNF) describes after-the-fact actions that an investigator takes to collect, preserve, analyze, and present information about computer-related crime [Vac02]. Digital Forensic Science and Network Forensics are defined at [Pal01], and the IETF has published [BK02] as guidelines for evidence collection and archiving. Moreover, in [BK02], many kinds of evidence are identified, such as memory, temporary file systems, physical configuration and logged data.

Increasing levels of unauthorized access create a need for forensic analysis, where electronic evidence discovery, computer analysis and data recovery are important. By performing forensic analysis, network administrators can analyze security incidents such as unauthorized access and various suspicious activities. When a security incident occurs, a network administrator investigates the cause by gathering information, e.g., system and application logs, captured packets, volatile data and configuration files. Such data contain a great deal of useful information for investigators, including IP addresses, hostnames, logged times and details of events. Therefore, some existing forensic tools try to recover deleted files, to acquire non-volatile or volatile information such as active process data and libraries, and to find a variety of trails. Collected electronic evidence accordingly is the nucleus of this growing research field.

Forensic investigation requires far more time than does the intrusion itself, reported at the Forensic Challenge [Pro01]. Knowledge of the relationship among amassed proofs, moreover, is needed for accomplishing retrospective reconnaissance, because an IP address or hostname assigned to a suspicious host may be permuted in the course of time. Thus, pieces of gathered criminal data can become unlinked and obsolete on account of elapsed time.

4.2.1 Evidence-Linking

In this research, evidence-linking indicates a state in which stored pieces of individual evidence correlate with each other, even if information about the malicious host is modified with time. In forensic analysis, gathered data are important pieces of evidence,

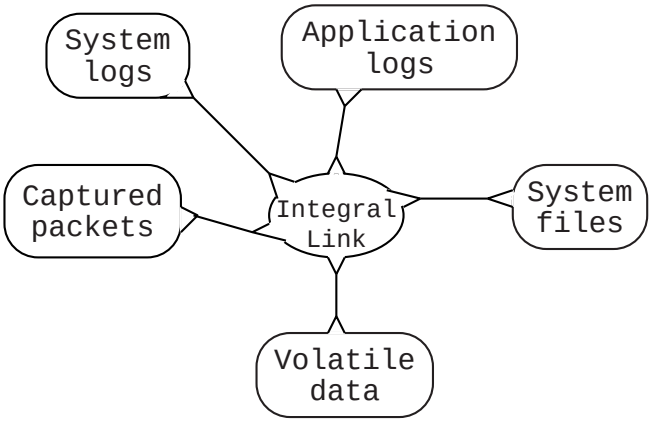


Figure 4.1: Integral Links among Individual Evidence

providing clues to solve the security incident. As shown in Figure 4.1, to prepare and retain linkage of sources is at the core of future incident response and the CNF.

In current forensics, however, if the same IP addresses are found in both evidence and network, the investigator cannot identify whether or not the two IP addresses correspond to the same host as when the incident occurred, because an IP address assigned to a host is changeable and the links among IP address, hostname and link-layer address become weaker with time. In other words, if the same IP addresses are found in both sources, the investigator cannot identify whether the two IP addresses correspond to the same host or not. Therefore, the investigator must be able to draw conclusions by employing other evidence to achieve unambiguous forensic analysis.

4.3 Forensic Time Traveler

Every user, e.g., a forensic investigator, a network administrator or a general user, has to be a forensic time traveler, if he/she wants to solve a security incident independently. Currently, a forensic time traveler needs a forensic database to trace address mappings of the past about a suspicious host. This section details an approaches to retrospective identification of security incidents with distributed forensic databases to link various types of digital evidence, as shown in Figure 4.2.

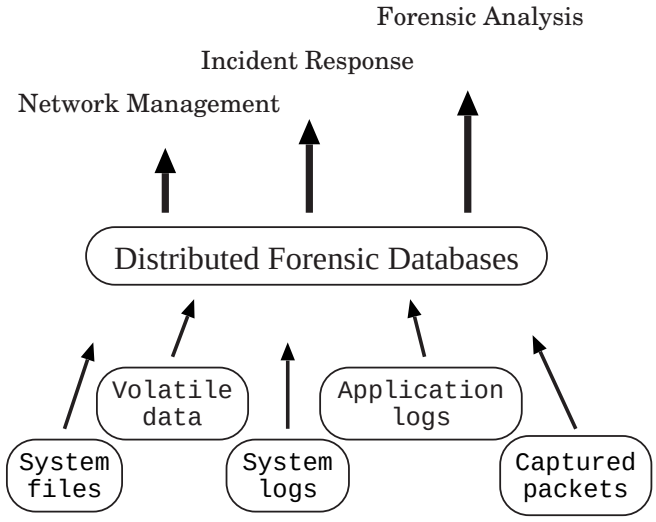


Figure 4.2: Distributed Forensic Databases as an Integral Link

4.3.1 Forensic Database

The proposed approach to execute evidence-linking for retrospective realization consists of two concepts: reliability and availability. Firstly, address resolution by Address Resolution Protocol (ARP) and Neighbor Discovery Protocol (ND) is made reliable using the Self-Confirming Engine (SCE), detailed in [KKY04]. False address mapping information in the data link layer affects logging in the upper layer, e.g., a communicated IP address. For example, a host records the fact that the user logs in or out, using address mapping data by ARP and ND. During Man-in-the-Middle attack, the victims cannot recognize that the attack is taking place because communication between the two victims proceeds normally.

During an attack, therefore, various events on the victim host are recorded in log files using compromised address mapping information. In this case, even if an investigator can reconstruct digital trails, CNF on the basis of collected evidence cannot reach true conclusions. By applying the SCE to address resolution procedures, consequently, this research makes uncertain evidence reliable and meaningful.

Next, recovered or gathered proofs are made available, even if an IP address or a hostname assigned to the malicious host is altered. That is, this research tries to produce essential links among evidence gathered by an investigator. In the current Internet, an IP address assigned to a suspicious host is variable, because a host can take advantage of the DHCP in IPv4 and Stateless Address Autoconfiguration [TN98]

Table 4.1: TDB Records (IPv4 and IPv6)

Item	*Explanation*
Time	logged time
link-layer address	host's link-layer address
IP address	host's IP address
hostname	host's hostname
Network Interface	communicating interface name
ND State	ND reachability state
Router	host is a router or not
Default Gateway	host is a default gateway or not

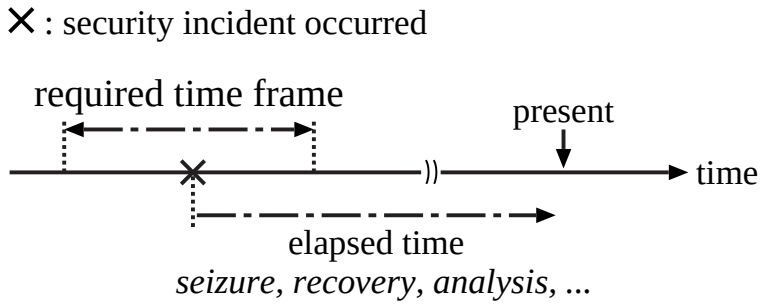


Figure 4.3: Required Time Frame for Retrospective Inquiry

in IPv6. Unfortunately, as reported in [Pro01], forensic analysis requires much more time to comprehend an intruder's traces than the time needed to compromise a victim. Therefore, requisite evidence for detailed analysis may become obsolete and unavailable. In this method, then, the SCE accumulates various information about the host in a database of the SCE, this research calls the Traveling Database (TDB). The TDB has a great deal of records, as shown in Table 4.1. To use transient address pairing in the TDB, an investigator can find address mapping data about a suspicious host retroactively. As a consequence of this inquiring, an attacker's tracks become clear and can be scrutinized if an examiner expends much time on incident analysis.

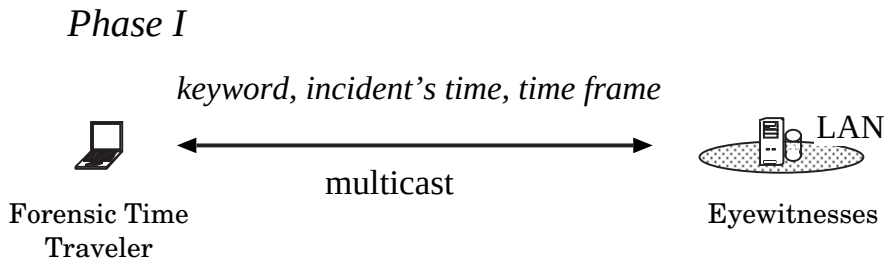


Figure 4.4: Search for Eyewitnesses

```
% ftt -s -k <keyword> -b <occurrence time(hours)> -m <time frame(minutes\
)>                                                                  -- (1)

% ftt -c -k <keyword> -b <occurrence time(hours)> -m <time frame(minutes\
)> -d <destination address>                                         -- (2)
```

Figure 4.5: Example of Commands for Phase I and II

4.3.2 Phased Approaches

This research describes two procedures to execute retrospective tracing with the TDB. The TDB allows the use of address mapping data such as IP address, link-layer address and hostname during the required time frame, as shown in Figure 4.3. CNF does not depend on elapsed time for seizure, recovery, analysis and so on. An investigator can request and obtain the TDB in the following way:

Search for Eyewitnesses (Phase I)

First of all, as phase I, the investigator searches a host having the TDB during the time frame around the security incident, such as in Figure 4.3. One of the most important constituent elements for retrospective identification is that the investigator can obtain the address mapping data in the TDB, because CNF depends on a time factor.

In phase I, as shown in Figure 4.4, a multicast address is adopted as the destination address for the purpose of retrieving the TDB easily in both IPv4 and IPv6. As shown in Figure 4.5(1), an investigator performs the search procedure in phase I by indicating parameters, keyword, incident time and time frame. The current version of this system, moreover, searches for information about users logged in as "*/var/log/wtmp*", which

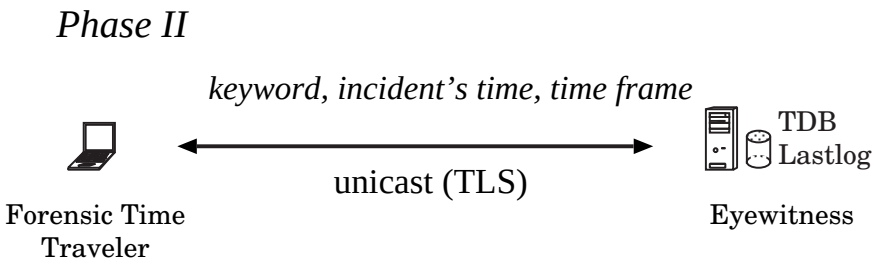


Figure 4.6: Collection of a Mapping Snapshot

this research calls lastlog, at the same time.

Collection of a Mapping Snapshot (Phase II)

In the second phase, as shown in Figure 4.6, the examiner actually obtains the TDB about the incident if the address mappings are found in phase I. As a consequence of phase II, logged mappings, such as IP address, link-layer address or hostname, make individual evidence pull together based on recorded time in the TDB. The system similarly obtains information about when a user logged in, during the required time frame, as shown in Figure 4.3. Similarly, as shown in Figure 4.5(2), an investigator performs the collection procedure in phase II by indicating parameters, keyword, regress time, time frame and destination addresses of witnesses.

To encode forensic evidence, moreover, the connection between a forensic time traveler and an eyewitness uses Transport Layer Security (TLS)[DA99] encryption. Phase II adopts the Public Key Infrastructure (PKI) framework, based on a digital certificate X.509 version 3 format, and employs the client/server certificate signed by a private Certification Authority (CA), as shown in Figure 4.6 and 4.7. In the IETF PKIX working group, to use the merits of a digital certificate, PKI achieves encryption of transmitting data, detects manipulations using a digital signature, and authenticates users. Digital certificates are standardized by the International Telecommunication Union (ITU)[ITU] and used for TLS, S/MIME[DHR+98, DHRW98, RE99a, RE99b, HE99], IPsec and EAP-TLS[AS99].

In the PKI framework, the following are enabled by use of a digital certificate:

- Unilateral Authentication
  When a user performs online shopping with TLS in the Internet, his or her credit number will be required. In this case, a server certificate is only needed for the

```
# ssldump -i xl2 port 8000
New TCP connection #1: 192.168.1.1(1607) <-> 192.168.5.9.(8000)
1 1  1.3047 (1.3047)  C>S SSLv2 compatible client hello
1 2  1.3062 (0.0015)  S>CV3.1(74)  Handshake
      ServerHello
        cipherSuite         TLS_RSA_WITH_3DES_EDE_CBC_SHA
1 3  1.3062 (0.0000)  S>CV3.1(1630)  Handshake
      Certificate
1 4  1.3062 (0.0000)  S>CV3.1(13)  Handshake
      CertificateRequest
      ServerHelloDone
1 5  1.3194 (0.0131)  C>SV3.1(1601)  Handshake
      Certificate
1 6  1.3194 (0.0000)  C>SV3.1(134)  Handshake
      ClientKeyExchange
1 7  1.3194 (0.0000)  C>SV3.1(134)  Handshake
      CertificateVerify
1 8  1.3194 (0.0000)  C>SV3.1(1)  ChangeCipherSpec
1 9  1.3194 (0.0000)  C>SV3.1(40)  Handshake
1 10 1.3330 (0.0135)  S>CV3.1(1)  ChangeCipherSpec
1 11 1.3330 (0.0000)  S>CV3.1(40)  Handshake
1 12 1.3336 (0.0006)  C>SV3.1(24)  application_data
1 13 1.3336 (0.0000)  C>SV3.1(56)  application_data
1 14 1.6750 (0.3413)  S>CV3.1(1504)  application_data
1    1.6750 (0.0000)  S>C  TCP FIN
1    1.6755 (0.0004)  C>S  TCP FIN
```

Figure 4.7: Example of a TLS Handshake

```
--- Server Side ---
% fttd -s
Enter PEM pass phrase:
listen to :: 8000
listen to 0.0.0.0 8000
SSL(TLSv1...
Certificate: Verified
...

--- Client Side ---
% ftt -v -4 -c -p -k keyword -t 2003/11/15+13:33:00 -m 3 -d 192.168.1.1
trying 192.168.1.1:8000 ...
Enter PEM pass phrase
Server Certificate
Certificate: Verified
...
```

Figure 4.8: Example of Phase II with TLS

consumer to verify whether or not the supplier's WWW server is legitimate.

- Mutual Authentication
  When both the client and the server need to verify each other, transmitting data is strictly secured from eavesdropping by a malicious user. However, each party requires a digital certificate, which must be signed by a private CA, for this authentication.

In phase II, the proposed method performs mutual authentication using client/server certificates signed by a private CA, as shown in Figure 4.8, and encrypts communication packets. Digital certificates, moreover, can be adopted not only in phase II but also in other security solutions such as 802.1X and S/MIME. Therefore, the use of digital certificates on the basis of the PKI is valuable to both network administrators and investigators.

Table 4.2: Machine Specifications

Item	*Type*
Computer Type	PC/AT Compatible Machine
CPU	Pentium III 800MHz
Memory	128MB
Network Interface	Ethernet 100baseT
Operating System	FreeBSD 4.2/4.6-RELEASE

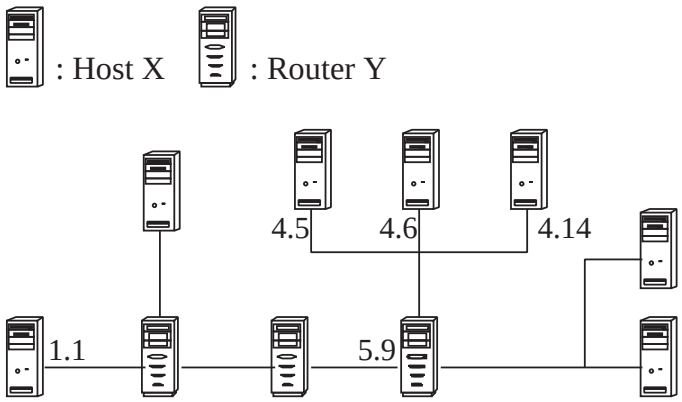


Figure 4.9: Experimental Network

4.4 System Verification

The proposed method is implemented using the machine specifications listed in Table 4.2. In this section, the method is verified in IPv4, and discussed its effectiveness for retrospective identification. Hosts A, C, E, F, H and I and routers B, D and G in the experimental network, as shown in Figure 4.9, communicate with each other by the Ethernet, and *1.1* on host A indicates *192.168.1.1/24*. Therefore, host A communicates with host F through routers B, D and G.

4.4.1 The Case of the Same Host

In an incident analysis it becomes possible to distinguish whether or not the IP address corresponds to the same host, because a forensic time traveler such as an investigator can refer to the link-layer address and logged time in the TDB. When the

```
% ftt -v -s -4 -k 192.168.4.14 -t 2003/12/01+07:37:00 -m 1
from[keyword, tdb4, tdb6, lastlog]
192.168.4.6[192.168.4.14, 1, 0, 0]
192.168.5.9[192.168.4.14, 1, 0, 0]
192.168.4.5[192.168.4.14, 1, 0, 0]
... completed.
```

Figure 4.10: Retrieval of Host *H*

```
% traceroute 192.168.4.14
traceroute to 192.168.4.14 (192.168.4.14), 64 hops max, 40 byte packets
 1  dos (192.168.1.2)  0.185 ms  0.125 ms  0.095 ms
 2  ocho (192.168.3.8)  1.184 ms  1.050 ms  1.134 ms
 3  nueve (192.168.5.9)  1.233 ms  0.268 ms  0.254 ms
 4  catorce (192.168.4.14)  0.505 ms  0.353 ms  0.334 ms
```

Figure 4.11: Result of *traceroute* command

incident has occurred on host A, an investigator analyzes various evidence, such as *"/var/log/messages"*, *"/var/log/wtmp"* or other system/application logs on the victim. As a result, if a trail such as suspicious hostname or IP address is found, an examiner initially tries to search the TDB.

This experiment supposes the occurrence time of the incident is 07:37:00 on Monday 1st December, 2003. By retrieving the TDB, which has address mappings of objective time, an investigator can recover evidence-linking among gathered individual trails, even if much time has elapsed. That is, as shown in Figure 4.10, the investigator can know that hosts E, F and G have the TDB in objective time about host H. Figure 4.11 describes the result of *traceroute* command from host A to host H; host G is the nearest router to host H. Next, as shown in Figure 4.12, the investigator collects the TDB from hosts E and F, and router G. Consequently, as shown in Figure 4.13, the investigator can analyze a security incident using the TDB in objective time. Three eyewitnesses give evidence that host H uses IP address *192.168.1.14*, mapped link-layer address *00:01:02:52:cf:5e*, and hostname *catorce.example.com*. Therefore, at the current time 08:33:48, as shown in Figure 4.13, the investigator decides correctly that host H is malicious, if the link-layer address assigned to the IP address *192.168.1.14*

```
% ftt -v -c -4 -k 192.168.4.14 -t 2003/12/01+07:37:00 -m 1 -d 192.168.4.\
5,192.168.4.6,192.168.5.9
trying 192.168.4.5:8000 192.168.4.14 20031201073700+-1 ...
... done! <192.168.4.5_20031201073700+-1_192.168.4.14.tdb>

trying 192.168.4.6:8000 192.168.4.14 20031201073700+-1 ...
5... done! <192.168.4.6_20031201073700+-1_192.168.4.14.tdb>

trying 192.168.5.9:8000 192.168.4.14 20031201073700+-1 ...
... done! <192.168.5.9_20031201073700+-1_192.168.4.14.tdb>
```

Figure 4.12: Collection of Host H

```
% date
Mon Dec  1 08:33:48 JST 2003
% ftt -a -f 192.168.4.5_20031201073700+-1_192.168.4.14.tdb
[TDB4](mac ip hostname - time)
00:01:02:52:cf:5e 192.168.4.14 catorce.example.com - Mon Dec  1 07:36:01\
 2003
...(snip)
00:01:02:52:cf:5e 192.168.4.14 catorce.example.com - Mon Dec  1 07:37:42\
 2003
% ftt -a -f 192.168.4.6_20031201073700+-1_192.168.4.14.tdb
00:01:02:52:cf:5e 192.168.4.14 catorce.example.com - Mon Dec  1 07:36:10\
 2003
...(snip)
00:01:02:52:cf:5e 192.168.4.14 catorce.example.com - Mon Dec  1 07:37:51\
 2003
% ftt -a -f 192.168.5.9_20031201073700+-1_192.168.4.14.tdb
00:01:02:52:cf:5e 192.168.4.14 catorce.example.com - Mon Dec  1 07:36:16\
 2003
...(snip)
00:01:02:52:cf:5e 192.168.4.14 catorce.example.com - Mon Dec  1 07:37:56\
 2003
```

Figure 4.13: Confirmation of Host H

```
% date
Mon Dec  1 08:53:21 JST 2003

% ftt -a -f 192.168.4.5_20031201085300+-1_192.168.4.14.tdb
[TDB4](mac ip hostname - time)
00:01:02:52:d1:be 192.168.4.14 catorce.example.com - Mon Dec  1 08:52:04\
 2003
...(snip)
00:01:02:52:d1:be 192.168.4.14 catorce.example.com - Mon Dec  1 08:53:44\
 2003
% ftt -a -f 192.168.4.6_20031201085300+-1_192.168.4.14.tdb
00:01:02:52:d1:be 192.168.4.14 catorce.example.com - Mon Dec  1 08:52:08\
 2003
...(snip)
00:01:02:52:d1:be 192.168.4.14 catorce.example.com - Mon Dec  1 08:53:48\
 2003
% ftt -a -f 192.168.5.9_20031201085300+-1_192.168.4.14.tdb
00:01:02:52:d1:be 192.168.4.14 catorce.example.com - Mon Dec  1 08:52:01\
 2003
...(snip)
00:01:02:52:d1:be 192.168.4.14 catorce.example.com - Mon Dec  1 08:53:41\
 2003
```

Figure 4.14: Current Mappings of Host *H*

is *00:01:02:52:cf:5e*. As a result of these proofs, the investigator reaches the true conclusion about the security incident by obtaining the TDB at the occurrence time of the incident.

4.4.2 The Case of a Different Host

As described above, an investigator can decide whether or not host H is malicious, if the present time is 08:33:48 as shown in Figure 4.13. However, if much time has elapsed since an incident occurred, the investigator cannot identify an attacker. Namely, if the present time is 08:53:21 as shown in Figure 4.14, the investigator knows that suspicious IP address *192.168.1.14* is assigned to the link-layer address *00:01:02:52:d1:be*. Therefore, without the TDB from the three eyewitnesses, the investigator may give false

charges to a normal user. Even if an IP address or hostname *catorce.example.com* are the same, the investigator understands that current host H is not malicious because the link-layer address of host H is different. Accordingly, to analyze security incidents and execute CNF certainly, the TDB with eyewitnesses is needed by an investigator.

4.5 Discussion

4.5.1 Storage Overhead

Whenever an unexpected incident occurs, an investigator needs to travel retrospectively using TDBs gathered by eyewitnesses in the network. For this reason, a large number of TDBs are required for the investigator to make a thorough examination. To achieve comprehensive forensic time traveling, however, the cost of saving the TDB cannot be avoided for the investigator. The worst-case logged interval is assumed to be when a single eyewitness in a link local network logs address mappings to the TDB every second, which is sufficient to avoid address mapping violation. Under these conditions, the eyewitness records data in the form shown in Table 4.1 and Figure 4.15. Table 4.3 shows storages rates required by the TDB; the TDB requires 64 bytes of memory per second in IPv4, as shown in Figure 4.15(1), and 83 bytes of memory in IPv6, as shown in Figure 4.15(2). Results of the *Forensic Challenge* [Pro01] show that up to 104 hours is required for forensic analysis. Therefore, if there is only one eyewitness in the network, an investigator needs to analyze the TDB for as much as a month to be able to identify address mappings which occurred at the time of the incident. To reduce the volume of the TDB eyewitness records, an investigator should increase the number of eyewitnesses. However, the number of eyewitnesses and the logging time will depend on a network's environment and machine performance. An exclusive host should therefore be adopted to collect the TDB from eyewitnesses in the network if they cannot store records for many days.

This consumption of the storage is smaller than that of a traffic recorder which captures and logs of all the transmitting packets. Moreover, it is impractical for the investigator to deploy such a recorder not at the border between the Internet and the enterprise network, but at a relay point for each link local network.

4.5.2 Eyewitnesses in the Internet

An eyewitness on the Internet is different from an eyewitness in the real world, whose memory deteriorates over time. In the Internet, however, forensic evidence about

```
1075623328 00:01:02:52:cf:5e 192.168.4.14 catorce.example.com 0   --- (1)

1070696672 00:01:02:52:cf:5e fe80::201:2ff:fe52:cf5e catorce.example.com\
 xl0 1 0 0                                                        --- (2)
```

Figure 4.15: Example of Logged Entries in the TDB

Table 4.3: Required Storages for the TDB

	1 sec	1 min	1 hour	1 day	1 month
IPv4	64.0 B	3.8 KB	230.0 KB	5.5 MB	165.9 MB
IPv6	83.0 B	5.0 KB	298.8 KB	7.2 MB	215.1 MB

computer-related crime remains intact unless somebody removes or rewrites it. Therefore, it is important to prepare the bases for retrieving and gathering forensic evidence on the Internet; if there is no gathered information, an investigator cannot assemble criminal evidence in the rapidly growing Internet environment.

A critical question in incident response and/or forensic analysis is how the collected computer-related evidence is used in an investigation. For this reason, a forensic investigator must clarify current computer-related legal issues, identifying what is inadequate in relation to forensic evidence and proposing what is needed to develop new laws for legitimate investigation on the Internet. To use digital evidence in court, forensic information may also need to be interpreted so that it can easily be understood by jurors, attorneys and judges who are neither CNF nor computer experts. Therefore, in various types of computer-related technical cases, an investigator must be able to clarify the importance of seized forensic evidence to ensure that the law is enforced.

4.5.3 Security Considerations

Address Spoofing

A link-layer address is believed to be a globally unique address in the Internet, but this is not always true in the case of a security incident. For example, a privileged user can change his/her host IP and link-layer addresses by using the *ifconfig* command, as shown in Figure 4.16. Figure 4.16(1) indicates that the IP address is con-

```
# ifconfig xl0 inet 192.168.1.1 netmask 255.255.255.0          --- (1)

# ifconfig xl0 ether 00:00:00:00:00:01                         --- (2)

# ifconfig xl0 inet6 fe80::201:2ff:fe52:xxxx                   --- (3)
```

Figure 4.16: Example of *ifconfig* Commands

figured as *192.168.1.1*, and the link-layer address is changed to *00:00:00:00:00:01* as shown in Figure 4.16(2). Similar to IPv4, the IP address in IPv6 is also established as *fe80::201:2ff:fe52:xxxx*, as shown in Figure 4.16(3). Moreover, even if the IP or link-layer addresses do not change expressly, an attacker can send a spoofed packet by using packet injection tools [nem, hpi].

In terms of this address inconsistency, a forensic time traveler, e.g., a general user or a network administrator, should know to search and collect TDBs of each eyewitnesses whether or not a link-layer address is unique in a particular administrative domain. Namely, the investigator inquires whether or not the same link-layer address exists in different networks at the same time. If the link-layer address is found in both networks of a particular domain, the investigator can recognize an abnormal occurrence. Accordingly, the investigator will be able to eliminate abnormal conditions leading to information leakage from the whole administrative domain such as an Enterprise network.

Precarious Eyewitness

In this work, an investigator uses TDBs, saved by eyewitnesses, which existed when an incident occurred. For this reason, it is important for the investigator to establish whether an eyewitness is credible. Therefore, the investigator needs to know the following:

- Combination Attack
  If eyewitnesses conspire to distort records, the investigator may not be able to reach true conclusions. In such cases, the investigator must find the truth from distorted evidence by gathering and examining information from other sources. If an honest user exists among the eyewitnesses, however, there will be differences in the forensic evidence among the gathered TDBs and other system/application logs. Consequently, the investigator can notice an abnormality.

- Single Liar
  False evidence may confuse the investigator if one of the eyewitnesses is an attacker. By comparing and verifying collected evidence from many eyewitnesses, however, the investigator will notice the existence of a liar because of inconsistencies in the gathered forensic evidence.

- Observing Position
  If only a forwarding switch is used as an eyewitness, as an observing position, the network administrator will be able to decrease the storage costs of TDB. However, to ensure getting true evidence, and identifying lies, the more eyewitnesses there are, the better.

Safety in each Phase

In each phase, there is a point to consider in searching for and collecting forensic evidence. For example, in phase I, an attacker may listen to transmitting data to find the keyword retrieved by an investigator. As a result, the attacker can know the keyword, and existence of an eyewitness who has evidence, if the attacker can capture all traffic between the investigator and eyewitnesses. To impersonate an eyewitness and deceive the investigator, moreover, the attacker may send a reply message to the investigator immediately after gaining the keyword. Therefore, the investigator must always be careful whenever he/she searches for forensic evidence in phase I. By collecting TDBs from many eyewitnesses in phase II, however, the investigator should be able to conclude whether or not a reply message is authentic: a faked reply message from the attacker causes a factual inconsistency, for example, or the attacker cannot impersonate the appropriate eyewitness because the attacker does not have a server certificate signed by a private CA.

It is hard to protect a host from the variety of possible network attacks if an administrator takes measures for only one layer in a layered network such as a TCP/IP. Malicious users can find any vulnerable point in the system and break into it. The network administrator should thus apply not only the measures proposed in this research but also other network security solutions to protect each layer. Coordination with other security solutions yields a highly reliable network, which means one that is hard to intrude; in which it is easy to detect an attack; and in which incidents can be analyzed quickly and deeply. Such complex network security can provide a safe network for users, including network administrators and forensic investigators.

4.6 Summary

Two concepts, reliability and availability, are needed for an investigator to attain CNF accuracy. In chapter 3, uncertain evidence was made reliable by applying the SCE, published as [KKY04]. In the next stage, individual evidence was made available by employing the TDB, i.e., realization of evidence linking, even if an investigator has to expend much time for acquisition, restoration and analysis. As a result of this effort, obsolete evidence becomes a significant information source. As a consequence of the proposed approach, the investigator can inspect a security incident retrospectively.

In this chapter, the proposed system provides the user with an infrastructure for ascertaining whether or not link-layer addresses in different networks are the same. Such a system is needed so that normal users can determine whether or not their link-layer address is used by a malicious user in an attack. Currently, the proposed method is only an interactive retrieval system, but it is a first step to manage and control the uniqueness of link-layer addresses within a particular network and among different networks.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

This section summarizes the contributions of this dissertation and outlines suggestions for future work. To accomplish incident response and the CNF by an investigator such as a network administrator, this dissertation is based on two concepts: reliability and availability. In Chapter 3, to prevent address mapping violation and MitM attack, the SCE improved a weakness of address resolution procedures in both ARP and ND by confirming whether or not an alteration of a mapping entry is true. For this reason, the SCE made system and application logs reliable enough to be used for incident response and the CNF by the investigator, because system and application logs are dependent on the result of the address resolution, and proper forensic evidence needs accurate address mappings.

In Chapter 4, the distributed TDB made obsolete evidence available to permit the true conclusion to be reached, however much time has elapsed from the occurrence of an incident, because system and application logs make the investigation grow meaninglessly unless the TDB is recorded by the SCE in each host. Therefore, whenever an unexpected event has occurred and much time has passed, the investigator can gain the appropriate forensic evidence from the SCE and the distributed TDB.

5.2 Research Contributions

This research makes the following contributions:

- **Evidence Reliability**
  The SCE is developed as a software prototype for sustaining reliability of address mapping tables affected in all systems and application logs in both IPv4 and IPv6. By using the SCE to protect address resolution procedures in both ARP and ND, an investigator or network administrator can reach true conclusions for performing network management, and for handling security incidents and CNF in the future.

- **Information Leakage**
  Preserving an address mapping table correctly leads to prevention of unwanted information leakage, because a user can avoid Man-in-the-Middle attack. As a result, a users can communicate with one another directly and correctly.

- **Simplicity**
  The SCE is designed to be as simple as possible, because complicated mechanisms or prerequisite conditions would prevent its wide applicability in future digital devices. Moreover, various types of developers can recognize the threat of information leakage, and incorporate this research result into their own systems or applications. For this reason, existing protocols such as ARP and ND are introduced in this research.

- **Evidence Availability**
  The TDB, stored by the SCE, as detailed in Chapter 3, is used to link individual pieces of evidence with each other, even if a long time has elapsed since the occurrence of an incident. By applying this approach, evidence linking is sustained for future incident analysis. As a result, an investigator or network administrator can distinguish, when analyzing security incidents, whether or not a host using the same IP address in the past and the present is actually the same host. Therefore, the investigator can draw an exact conclusion, without the risk of false charges.

- **Alternative Approaches**
  This research approach provides an occasion to acquire information about a communicating host, such as hostname, IP address and link-layer address. The method can be used in an alternative approach, where the user can confirm him/herself whether or not the mapping between hostname and IP address is correct. If the mapping obtained by DNS and by this method is different, the user should suspect an attack about/on the DNS server.

5.3 Future Work

The reference model in this work is limited to a particular administrative domain, and does not verify mapping information between hostname and IP address resolved by a DNS server. To investigate a security incident smoothly, moreover, an eyewitness could be sought, to collect many system and application logs as forensic evidence. Furthermore, it will be indispensable in future for an investigator to be able to search among different administrative domains. Accordingly, this research can be extended as follows:

- **Self-Confirming Engine:**
  - Protocols
    When an alteration of address mappings occurs, the SCE will use addresses, such as IPv4, IPv6 and link layer, to perform collaborative confirmation against a dual stack host. Moreover, if SEND is adopted as the address resolution protocol in IPv6, the SCE would need to be compatible with the current protocol. For this purpose, the SCE must be improved to handle each protocol in the future.
  - DNS Extension
    The current system does not confirm whether hostname information from the DNS server is true or not. Therefore, to make the forensic database more valuable, the SCE must have a function for ascertaining mapping correctness between hostname and IP address from now on.
- **Distributed Forensic Databases:**
  - Applicability
    This system needs to handle various types of evidence, because an investigator requires considerable time for CNF to resolve an unexpected incident. For this reason, the system will use a variety of logs to reduce the requisite time for analysis.
  - Globalization
    The current system focuses on a same administrative domain to realize retrospective identification of link-layer addresses. Therefore, to lead an investigator to the resolution of any security incident globally, this system requires information retrieval and exchange among different administrative domains in the future.

In the Internet, when a user joins a new network environment and an unexpected event occurs, everyone needs to be a forensic time traveler to protect him/herself. At this time, various types of forensic evidence are needed for the user, such as IP address, link-layer address, hostname and other traces of a target host. Therefore, it is desirable that anyone can easily search and investigate forensic evidence retrospectively by him/herself, to confirm past records of the target host in a similar manner to *ping* and *traceroute(tracert)* commands.

Knowledge of and preparation for unexpected events are ways to protect yourself and your identity against a malicious attack or false charges. Moreover, you must remain vigilant in order to make sure of your network's safety.

5.4 Open Issues

Unexpected security incidents will still occur, because the Internet is still growing widely and new applications are continuously appearing. For this reason, a major concern is how to prepare a secure infrastructure for protecting our data before we are attacked by a malicious user. Determining the cost of preparing a highly reliable network is one aspect of risk management. Several issues - within a specific domain, among different domains, and others - are described in the following subsections.

5.4.1 Issues within a Specific Domain

In the Internet, any part of a link-layer address, except its hard coding, can be changed by anyone. For this reason, to perform incident response and forensic analysis efficiently, a unique link-layer address in all networks of a specific domain must be maintained by an investigator. The current version of this research can search for and collect distributed TDBs of all eyewitnesses, but it cannot remove a malicious user using the link-layer address of another legitimate user. Therefore, the establishment of a removal method is needed in the future to protect legitimate users. Investigators can search for and collect various types of forensic evidence, and so an adaptable forensic infrastructure is also required for tracing.

To achieve prompt incident response and forensic analysis, distributed TDBs should be used in all networks of a specific domain to protect communication infrastructure. For example, to control the use of spoofed addresses by a malicious host, methods for checking the uniqueness of a link-layer address should be improved from manual operation by an investigator to automatic management by the policy of a network

administrator and a forensic expert. Moreover, the specification of a network, forensic policy, and careful consideration of user privacy must all be examined and discussed in detail.

When automatic management is achieved, an address spoofing attack in the specific domain can immediately be detected and prevented. When an attack occurs, the link-layer address will be grasped by the network management policy as soon as a host accesses the network, and adopted to security devices for forensics in the network for protection against address spoofing. Link-layer addresses learned by the security devices for forensics can be verified in each layer, such as IEEE 802.1X, whether or not a user's digital certificate is legitimate.

5.4.2 Issues among Different Domains

Because it can be altered by anyone, the uniqueness of a link-layer address in the Internet cannot be verified. For this reason, as described above, uniqueness is indicated in all networks of the specific domain. Uniqueness of a link-layer address among different administrative domains is also needed. However, there are some differences to deal with regarding digital certificates, such as Certificate Policy (CP) and Certification Practice Statement (CPS), if an investigator tries to exchange forensic evidence among different domains. Therefore, at the beginning of a communication between different domains, an investigator must establish a trust relationship to be able to search for and collect various types of forensic evidence. Using digital certificates signed by a trusted CA, and irrespective of whether the attacker is an insider or an outsider, an incident response and a forensic analysis should be performed to reach a true conclusion whenever an unexpected incident occurs. For this purpose, the digital certificate must be adopted consistently at each layer, as shown in Figure 1.1, for user authentication and authorization. In this process, it is important to provide a way of checking whether or not the digital certificate is revoked.

Next, if negotiations about difference policies for trust relationship described above are cleared, the investigator will aim to search for and collect forensic evidence to trace an attacker, however much time has elapsed since the occurrence of an incident. When CNF can be accomplished among different administrative domains, the Internet will have gained a new security solution against spoofing attacks. In the Internet, early detection and prevention of spoofed attacks, such as DoS and DDoS attacks, can be achieved by security and CNF devices based on a global unique link-layer address. In the future, a user who commits a computer-related crime will not be able to escape from tracking by the investigator, despite the passage of time, because - in contrast to

real-world forensics - the investigator will be able to obtain forensic evidence linked by the TDB whenever he/she wants.

5.4.3 Other Issues in the Internet

Alternative DNS DNS is a very important component of the Internet, and maps an IP address corresponding to a hostname and the opposite. DNS also provides other Internet services, such as mail transportation and the Telephone Number Mapping (ENUM) service [Fal00, FMY03]. Most users, however, do not have a way to evaluate whether or not an answer from the DNS is correct. If a malicious user fakes a DNS answer, a victim user will access an unintended host. To avoid a fake DNS response, normal users need an alternative way of checking whether or not the DNS response is correct. An alternative confirmation method should consider using the research proposed in this dissertation, which is based on verifying that address mappings and hostnames, continuously referenced by many users, can be trusted.

Grid Forensics In the current Internet, the Grid tries to make distributed resources (such as computers and databases) virtually single to increase their ability. For this purpose, in a Global Grid Forum (GGF)[GGF] like the IETF, many working groups discuss and try to standardize Grid architecture, application and security. From the point of view of Grid Forensics, however, problems such as incident response and CNF need more consideration so that users, virtual computers and organizations can be fully protected from attackers.

Bibliography

[ACF+00] J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner. "State of the practice of intrusion detection technologies". Technical Report CMU/SEI-99TR-028, January 2000.

[AKS+03] J. Arkko, J. Kempf, B. Sommerfeld, B. Zill, and P. Nikander. "SEcure Neighbor Discovery (SEND)". draft-ietf-send-ipsec-01.txt, June 2003.

[ANKR03] J. Arkko, P. Nikander, T. Kivinen, and M. Rossi. "Manual Configuration of Security Associations for IPv6 Neighbor Discovery". draft-arkko-manual-icmpv6-sas-02.txt, March 2003.

[AS99] B. Aboba and D. Simon. *PPP EAP TLS Authentication Protocol*, October 1999. RFC 2716.

[Aur03] T. Aura. "Cryptographically Generated Addresses (CGA)". http://www.research.microsoft.com/users/tuomaura/CGA/, January 2003.

[Bac99] R. G. Bace. *"Intrusion Detection"*. MacMillan Technology Series. Macmillan Technical Publishing, December 1999.

[Bel89] S. M. Bellovin. "Security problems in the TCP/IP protocol suite". *Computer Communications Review*, 19(2):32–48, April 1989. http://www.research.att.com/s̃mb/papers/ipext.pdf.

[BK02] D. Brezinski and T. Killalea. *Guidelines for Evidence Collection and Archiving*, February 2002. RFC 3227.

[Bor] S. Boran. "Personal & SOHO Firewall tests". http://boran.linuxsecurity.com/security/.

[Bui96] P. Buis. *"Names and Addresses"*, September 1996. http://www.cs.bsu.edu/homepages/peb/cs637/nameadd/.

[Bur02] P. Burkholder. *"SSL Man-in-the-Middle Attacks"*. SANS Institute, February 2002. http://www.sans.org/rr/papers/60/480.pdf.

[BV98] L. Blunk and J. Vollbrecht. *PPP Extensible Authentication Protocol (EAP)*, March 1998. RFC 2284.

[Cara] B. Carrier. "Performing an Autopsy Examination on FFS and EXT2FS Partition Images: An Introduction to TCTUTILs and the Autopsy Forensic Browser". http://www.cerias.purdue.edu/homes/carrier/forensics/.

[Carb] B. Carrier. "The Sleuth Kit, The @stake Sleuth Kit and TCTUTILs". http://sourceforge.net/projects/sleuthkit/.

[Cen88] CERT Coordination Center, 1988. http://www.cert.org/.

[Cen96] CERT Coordination Center. *"CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks"*, September 1996. http://www.cert.org/advisories/CA-1996-21.html.

[Cen01] CERT Coordination Center. *"CERT Advisory CA-2001-02 Multiple Vulnerabilities in BIND"*, January 2001. http://www.cert.org/advisories/CA-2001-02.html.

[CK74] V. G. Cerf and R. E. Kahn. "A Protocol for Packet Network Intercommunication". *IEEE Trans on Comms*, Com-22(5), May 1974.

[DA99] T. Dierks and C. Allen. *The TLS Protocol Version 1.0*, January 1999. RFC 2246.

[DH98] S. Deering and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*, December 1998. RFC 2460.

[DHR+98] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, and L. Repka. *S/MIME Version 2 Message Specification*, March 1998. RFC 2311.

[DHRW98] S. Dusse, P. Hoffman, B. Ramsdell, and J. Weinstein. *S/MIME Version 2 Certificate Handling*, March 1998. RFC 2312.

[di96] route deamon9 and infinity. "IP-spoofing Demystified: Trust-Relationship Exploitation". *Phrack Magazine*, 7(48), June 1996. http://www.phrack.org/show.php?p=48&a1̄4.

[Dro97] R. Droms. *Dynamic Host Configuration Protocol*, March 1997. RFC 2131.

[Fal00] P. Faltstrom. *E.164 number and DNS*, September 2000. RFC 2916.

[FD] B. Fleck and J. Dimov. *"Wireless Access Points and ARP Poisoning"*. Cigital, Inc. http://www.cigitallabs.com/resources/papers/download/arppoison.pdf.

[FMY03] M. Foster, T. McGarry, and J. Yu. *Number Portability in the Global Switched Telephone Network (GSTN): An Overview*, February 2003. RFC 3482.

[FS00] P. Ferguson and D. Senie. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, May 2000. RFC 2827.

[FV] D. Farmer and W. Venema. "The Coroner's Toolkit (TCT)". http://www.porcupine.org/forensics/tct.html.

[Gar01] L. Garber. "Computer Forensics: High-Tech Law Enforcement". *IEEE Computer Society's Computer Magazine*, 34(1), January 2001.

[GGF] Global Grid Forum. http://www.globalgridforum.org/.

[Groa] IETF Securing Neighbor Discovery(SEND) Working Group. http://www.ietf.org/.

[Grob] Lawrence Berkeley National Laboratory Network Research Group. "arpwatch". http://www-nrg.ee.lbl.gov.

[HC98] D. Harkins and D. Carrel. *The Internet Key Exchange (IKE)*, November 1998. RFC 2409.

[HE99] P. Hoffman and Ed. *Enhanced Security Services for S/MIME*, June 1999. RFC 2634.

[hpi] hping: command-line oriented TCP/IP packet assembler/analyzer. http://www.hping.org/.

[IET] The Internet Engineering Task Force (IETF). http://www.ietf.org/.

[Inc] Cyber Solutions Inc. "CyberKoban". http://www.cysol.co.jp/.

[ISO] International Organization for Standardization. http://www.iso.ch/.

[ITU] International Telecommunication Union. http://www.itu.int/home/.

[KA98a] S. Kent and R. Atkinson. *IP Authentication Header*, November 1998. RFC 2402.

[KA98b] S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol*, November 1998. RFC 2401.

[KBR+01] C. Ko, P. Brutch, J. Rowe, G. Tsafnat, and K. Levitt. "System Health and Intrusion Monitoring Using a Hierarchy of Constraints". In *RAID2001*, pages pp. 190–204, October 2001.

[Kin02] T. King. *"Packet Sniffing In a Switched Environment"*. SANS Institute, August 2002. http://www.sans.org/rr/papers/38/244.pdf.

[KKY03] M. Kanamori, T. Kobayashi, and S. Yamaguchi. "A Proposed Method of Avoiding Address Mapping Violation". In *1st International Forum on Information and Computer Technology(IFICT) 2003*, pages 88–93, January 2003.

[KKY04] M. Kanamori, T. Kobayashi, and S. Yamaguchi. "A Self-Confirming Engine for Preventing Man-in-the-Middle Attack". *IEICE Transactions on Communications*, E87-B(3), March 2004.

[KSB03] A. Savant K. Shanmugasundaram, N. Memon and H. Bronnimann. "ForNet: A Distributed Forensics Network". In *MMM-ACNS-2003: The Second International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security*, September 2003.

[LI01] J. P. Lanza and S. V. Ittersum. "SSH-1 allows client authentication to be forwarded by a malicious server to another server". Vulnerability Note VU#684820, CERT Coodination Center, January 2001. http://www.kb.cert.org/vuls/id/684820.

[Lin01] C. E. Lindner. *"Information Security Primer"*. SANS Institute, August 2001. http://www.sans.org/rr/papers/48/443.pdf.

[Mar] H. S. Markus. "Personal Firewall Reviews". http://www.firewallguide.com/software.htm.

[Mil01] I. Miller. *Protection Against a Variant of the Tiny Fragment Attack (RFC 1858)*, June 2001. RFC 3128.

[Moc87a] P.V. Mockapetris. *Domain names - concepts and facilities*, November 1987. RFC 1034.

[Moc87b] P.V. Mockapetris. *Domain names - implementation and specification*, November 1987. RFC 1035.

[MP01] K. Mandia and C. Prosise. *"Incident Response: Investigating Computer Crime"*. McGraw-Hill Osborne Media, June 2001.

[MY01] Y. Manzano and A. Yasinsac. "Policies to Enhance Computer and Network Forensics". In *2nd Annual IEEE Systems, Man, Cybernetic Information Assurance Workshop*, June 2001.

[nem] Nemesis Packet Injection Utility. http://www.packetfactory.net/projects/nemesis/.

[NKN03] P. Nikander, J. Kempf, and E. Nordmark. "IPv6 Neighbor Discovery trust models and threats". draft-ietf-send-psreq-03.txt, April 2003.

[NNS98] T. Narten, E. Nordmark, and W. Simpson. *Neighbor Discovery for IP Version 6 (IPv6)*, December 1998. RFC 2461.

[OV] A. Ornaghi and M. Valleri. "ettercap - A multipurpose sniffer over switched LANs". http://ettercap.sourceforge.net/.

[Pal01] G. Palmer. "A Road Map for Digital Forensic Research". Technical Report DTR-T001-01, the First Digital Forensic Research Workshop (DFRWS), November 2001.

[Plu82] D.C. Plummer. *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware*, November 1982. RFC 826.

[PN98] T. H. Ptacek and T. N. Newsham. *"Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection"*. Secure Networks, Inc., January 1998.

[Pos80] J. Postel. *User Datagram Protocol*, August 1980. RFC 768.

[Pos81a] J. Postel. *Internet Control Message Protocol*, September 1981. RFC 792.

[Pos81b] J. Postel. *Internet Protocol*, September 1981. RFC 791.

[Pos81c] J. Postel. *Transmission Control Protocol*, September 1981. RFC 793.

[Pro01] The Honeynet Project. "Forensic Challenge", January 2001. http://project.honeynet.org/challenge/.

[RE99a] B. Ramsdell and Ed. *S/MIME Version 3 Certificate Handling*, June 1999. RFC 2632.

[RE99b] B. Ramsdell and Ed. *S/MIME Version 3 Message Specification*, June 1999. RFC 2633.

[Ric03] R. Richardson. "2003 CSI/FBI Computer Crime and Security Survey". *Computer Security Institute*, 2003.

[Roe99] M. Roesch. "Snort - Lightweight Intrusion Detection for Networks". In *13th System Administration Conference - USENIX LISA*, November 1999. http://www.snort.org/.

[Sax03] D. Sax. *"DNS Spoofing (Malicious Cache Poisoning)"*, August 2003. http://www.giac.org/practical/gsec/Doug_Sax_GSEC.pdf.

[Sch98] M. D. Schiffman. Libnet Packet Assembly, January 1998. http://www.packetfactory.net/projects/libnet/.

[Sil03] R. Siles. *"Real World ARP Spoofing"*, August 2003. http://www.giac.org/practical/GCIH/Raul_Siles_GCIH.pdf.

[Son99a] D. Song. dsniff: a collection of tools for network auditing and penetration testing, December 1999. http://www.monkey.org/ dugsong/dsniff/.

[Son99b] D. Song. Fragrouter: network intrusion detection evasion toolkit, May 1999. http://www.securityfocus.com/tools/176.

[Sur02] G. Surman. *"Understanding security using the OSI model"*. SANS Institute, March 2002. http://www.sans.org/rr/papers/44/377.pdf.

[Sys02] Internet Security Systems. "SSH1 and SSH2 protocol hostkey change "man-in-the-middle" attack", July 2002. http://xforce.iss.net/xforce/xfdb/9652.

[TN98] S. Thomson and T. Narten. *IPv6 Stateless Address Autoconfiguration*, December 1998. RFC 2462.

[Vac02] J. R. Vacca. *"Computer Forensics: Computer Crime Scene Investigation"*. Charles River Media, Inc., June 2002.

[Van] Y. Vandoorselaere. "Prelude - A general-purpose hybrid intrusion detection system". http://www.prelude-ids.org.

[Vel00] V. Velasco. *"Introduction to IP Spoofing"*. SANS Institute, November 2000. http://www.sans.org/rr/papers/60/959.pdf.

[VW99] P. Valian and T. K. Watson. "NetReg: An Automated DHCP Registration System". In *13th System Administration Conference - USENIX LISA*, November 1999. http://www.netreg.org/.

[Wag01] R. Wagner. *"Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks"*. SANS Institute, August 2001. http://www.sans.org/rr/papers/60/474.pdf.

[YM02] A. Yasinsac and Y. Manzano. "Honeytraps, A Network Forensic Tool". In *The 6th World MultiConference on Systemics, Cybernetics and Informatics (SCI2002)*, July 2002.

[ZRT95] G. Ziemba, D. Reed, and P. Traina. *Security Considerations for IP Fragment Filtering*, October 1995. RFC 1858.

Appendix A

List of Publications

A.1 Journal

1. Masataka Kanamori, Takashi Kobayashi and Suguru Yamaguchi, “A Self-Confirming Engine for Preventing Man-in-the-Middle Attack”, IEICE Transactions on Communications, Vol.E87-B, No.3, March, 2004.

2. Masataka Kanamori, Takashi Kobayashi and Suguru Yamaguchi, “An Evidence-Linking Approach for Retrospective Identification”, IPSJ Journal (submitted).

A.2 International Conference

1. Masataka Kanamori, Takashi Kobayashi and Suguru Yamaguchi, “A Proposed Method of Avoiding Address Mapping Violation”, In Proc. of 1st International Forum on Information and Computer Technology (IFICT2003), pp.88-93, January 2003.

2. Masataka Kanamori, Takashi Kobayashi and Suguru Yamaguchi, ”A Forensic Analysis with Records of Address Mapping”, In Proc. of The 3rd International Symposium on Communications and Information Technologies (ISCIT2003), September 2003.