A Novel Protocol Design and Collaborative Forensics Mechanism for VoIP Services

Hsien-Ming Hsu, Feng-Yu Lin, Yeali S. Sun
Dept. of Information Management, National Taiwan University, Taipei, Taiwan
Email: {d94002, d95003, sunny}@im.ntu.edu.tw

Meng Chang Chen
Institute of Information Science, Academia Sinica, Taipei, Taiwan
Email: mcc@iis.sinica.edu.tw

***Abstract*—The simplicity and low cost of Voice over Internet Protocol (VoIP) services has made these services increasingly popular as the Internet has grown. Unfortunately, these advantages of VoIP are attractive to both legitimate and nefarious users, and VoIP is often used by criminals to communicate and conduct illegal activities (such as fraud or blackmail) without being intercepted by Law Enforcement Agencies (LEAs). However, VoIP can also increase the efficiency of law enforcement and forensic collaboration. Currently, VoIP researchers have only proposed a framework for this type of partnership, and have yet to provide a common protocol for forensic Internet collaboration. As a result, Internet-based collaboration between agencies is not widespread.**

Building from the Collaborative Forensics Mechanism (CFM) and the procedures of collaborative forensics work, this paper designs a novel application-layer Collaborative Forensics Protocol (CFP) to overcome the current framework-protocol gap. Here, CFP can exchange collaborative request and response messages between collaborative forensics region centers (CFRCs) to acquire collaborative forensics information. We present a procedure for collaborative forensics and discuss the details of protocol design. In addition, we discuss the defense of PKI working with CFM against various types of attacks and analyze the features of CFP.

***Index Terms*—SIP, VoIP, Security, Collaborative Forensics, Mechanism, Protocol Design, Traceback**

I. Introduction

Over the last several decades, the Public Switched Telephone Network (PSTN) has dominated voice communications. Due to their simplicity and low cost, network telephony systems, especial VoIP services, have become popular as the Internet has grown and may one day even replace the Public Switched Telephone Network (PSTN). While VoIP services have brought many desirable communication features to the general public, they have also become a medium through which criminals communicate and conduct illegal activities (fraud and blackmail) without being intercepted by law enforcement agencies (LEAs). As a SIP-based telephony system (Session Initiation Protocol) [1] that uses packet-switched technology, VoIP shares the same major drawbacks as many services using Internet Protocol (IP) [2], particularly their vulnerability to security threats.

In an effort to offer convenient and secure networking services, researchers have proposed various defensive mechanisms over the past few years, such as intrusion detection systems (IDSs) [3], [4], [5], [6] and prevention mechanisms (PMs) [7], [8], [9], [10]. These mechanisms however, are inadequate for today's Internet. While they prevent illegal activity before or during criminal acts, both types of mechanisms require prior indications of the kind of attack taking place in order for them to provide proper security. Unfortunately, attacks are often conducted without any forewarning, so these defense mechanisms do not completely secure networks. In light of the shortcomings of these aforementioned defensive mechanisms, our previous work [11] proposed a collaborative forensics framework, named SKYEYE, that can automatically collect, associate, manage, and link information in order to reconstruct criminal acts. By correlating related events, we can determine how a network incident (i.e., crime/attack) occurred, including the origin, the method used, and the people responsible. In [12], we extend SKYEYE as a collaborative forensics mechanism (CFM) to enhance the detection and defensive ability of IPs for preventing attacks.

CFMs serve as complements to IDSs, PMs, and traceback mechanisms. While PMs prevent attacks, IDSs detect attacks, and traceback mechanisms trace the identities and geo-locations of the perpetrators, CFMs figure out how the attacks were conducted and recover the indications of the attacks. These attack indications may then be used by IDSs and PMs to enhance the detection and defensive ability of the network. In addition, CFMs produce local events (LEvs) for potential forensic investigations without forging header field values (HFVs). Required cross layers are recorded using the components

Manuscript received October 31, 2010; revised June 3, 2011; accepted August 9, 2011.
This research was partly supported by NSC Taiwan under grant NSC98-2221-E-001-005-MY3.

doi:10.4304/jcm.7.2.132-142

of SIP-based telephony. CFMs determine which header field values (HFVs) on request messages can be forged, and extract the required information to produce the characteristics for various requests. CFMs also describe the required information recorded by the SIP Registrar and NWO (including Network Address Translation/Dynamic Host Configuration Protocol, NAT/DHCP), which can be used to identify these forged HFVs by their characteristics and merge them with information from the SIP Registrar and NWO for forensic analysis.

To efficiently perform network collaborative forensics, cooperating CFMs must follow a standard procedure for communicating and exchanging information with each other over a common protocol. This allows the cooperating units to know when and what information will be sent. Based on the procedures of collaborative forensics, in this paper we design a novel protocol, named the Collaborative Forensics Protocol (CFP), for sending collaborative request and response messages to acquire information from cooperating units. This CFP protocol consists of both a header and data component. The header component defines the values that describe cooperating information. The data component holds the required information of the local event recorded by NWO and SvP. Additionally, CFM employs a public-key infrastructure (PKI) [13] to offer digital signature and cryptography services. If this relationship between CFM and CFP is widely adopted by the forensics community, collaborative forensics will be much more efficient and powerful.

The primary contributions of this paper are the follows:

- We propose a distributed *collaborative* forensics mechanism (CFM) and the procedure to execute collaborative forensics without the information support of intermediate routers. We also employ Public Key Infrastructure (PKI) with CFM to provide digital signature and cryptography services.
- We design a novel protocol, Collaborative Forensics Protocol (CFP), that defines the format and the order of messages exchanged between two network collaborative units.
- We briefly evaluate the security of collaborative mechanisms with various attacks and the features of collaborative forensics protocol.

The remainder of this paper is organized as follows. Section II contains a review of related work. In Section III, we describe the background of collaborative forensics for SIP-based VoIP services. In Section IV, we present the procedure of collaborative forensics for SIP-based VoIP services. In Section V, we describe the design of a novel protocol to support network collaborative forensics over Transmission Control Protocol (TCP) [14], and introduce the public-key infrastructure used to offer digital signature and cryptography services. Then, in Section VI, we discuss the security of CFM and the features of collaborative forensics protocol (CFP). Finally, Section VII summarizes our protocol design and indicates areas for future research.

II. Related Work

In the past, network services were protected from the constant transformation of attack techniques by stand-alone defense mechanisms. Examples include defense mechanisms such as Snort [15], a lightweight intrusion detection system with a libpcap-based [16] packet sniffer and logger original proposed by Roesch in 1999.

Currently however, security researchers have increasingly developed multiple collaborative defense mechanisms, such as TRINETR [17] and NFA [18]. In TRINETR [17], Yu et al. proposed a collaborative architecture for a multiple intrusion detection system that works together with knowledge-based detection sensors to detect real-time network intrusion. In NFA [18], Xie et al. design a network federated alliance (NFA) which allows multiple administrative domains to jointly locate the origin of epidemics spreading attacks by using random moonwalk algorithms.

The same development progression can be observed with VoIP telephony systems. Early research on VoIP defensive mechanisms started with single site systems, e.g. SCIDIVE [4], [5]. In SCIDIVE [4], Wu et al. proposed a protected system for VoIP to detect various attacks by the state of multiple packets and cross-protocol matching rules at multiple points of a single Autonomous System (AS). In [5], Sengar et al. proposed an intrusion detection system based on this protocol-state method.

Recently, collaborative forensics mechanisms have drawn considerable attention, and have been discussed within several conferences and journals, e.g. SKYEYE [11], [19], and CFM [12]. Pilli et al. survey various network forensic frameworks [20]. In SKYEYE [11], Hsu et al. propose a collaborative forensics framework to identify caller for VoIP services in multi-network environments. In [19], Khurana et al. develop a framework for effective collaborative response and investigation across multiple units when tracking an adversary. In CFM [12], our previous work, we build upon prior research [11] and propose our own collaborative forensics mechanism (CFM). This CFM not only automatically collects Local Events (LEvs) and shares this information with cooperating units, but also consults other systems for decisions and reduces long-term storage concerns via active forensics. In our mechanism, the different parts of each LEv are linked, in order to build a complete picture of an incident that can be used as evidence in a court of law. The Access Local Event Entity (ALEE) triggers active forensics procedures and thereby avoids the need to store information until law enforcement agencies have time to look at it.

However, for these collaborative forensics mechanisms (CFMs), no one has yet proposed a collaborative forensics protocol for efficiently performing collaborative forensics. Thus, collaborative forensics mechanisms have not been quickly and successfully disseminated within the law enforcement community.

In this paper, we overcome this gap by designing a novel collaborative forensics protocol (CFP) based on CFM. Our protocol uses a digital signature and cryptography merits through the PKI mechanism to

defend against network attacks and carry the necessary information for executing collaborative forensics.

III. Our Previous Work

In this section, we provide a brief explanation of SIP signaling, and discuss the required information of the header field values (HFVs) on request messages that NWO/SvP log collaboratively. Then, we briefly describe the typical SIP-based signaling attacks and the characteristics of various requests, and how to identify forged header fields values (HFVs).

A. SIP-based Signaling

SIP is an application-layer control protocol designed to establish, modify, and terminate multimedia sessions (conferences), and is used in such programs as SIP-based VoIP telephony services. The architecture of SIP-based IP telephony is shown in Fig. 1.

In order to better illustrate how SIP signaling works, let us consider a hypothetical example involving caller "Alice" and callee "Bob," who belong to the "Atlantic" and "Pacific" SIP VoIP service providers, respectively. Before calling Bob, caller Alice needs to be authenticated by a SIP authentication mechanism and register through a REGISTER request with the Pacific SIP Registrar, shown as Fig. 2 (a1-a4).

Caller Alice first sends an INVITE request to the Atlantic SIP proxy. This proxy consults the location service database to find out the current location of callee Bob, and forwards the INVITE request to the Pacific SIP proxy and the callee to complete a three-way handshake (INVITE, OK, ACK) that establishes the SIP session, shown in Fig. 2 (b1-b14).

After exchanging a set of parameters through the Session Description Protocol [21] in the SIP message body, the bi-direction of the Real-time Transport Protocol (RTP) [22] based channel is established. Either caller Alice or callee Bob can terminate this session by sending a BYE request, shown in Fig. 2 (c1-c6). The detail signaling of the SIP protocol is described in [1].

B. Weaknesses of SIP Services

For SIP-based VoIP services, authentication is executed with registration. Registration creates bindings

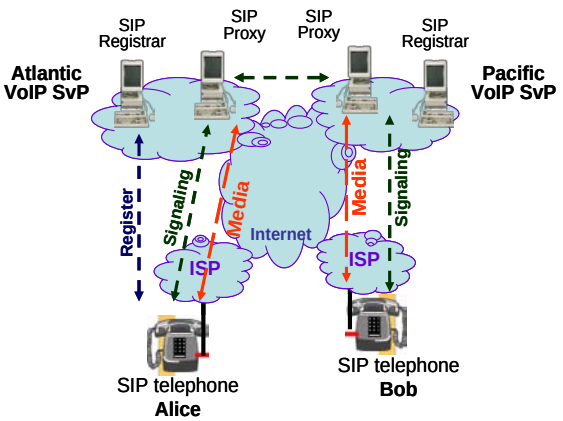

Figure 1. The SIP-based IP Telephony.

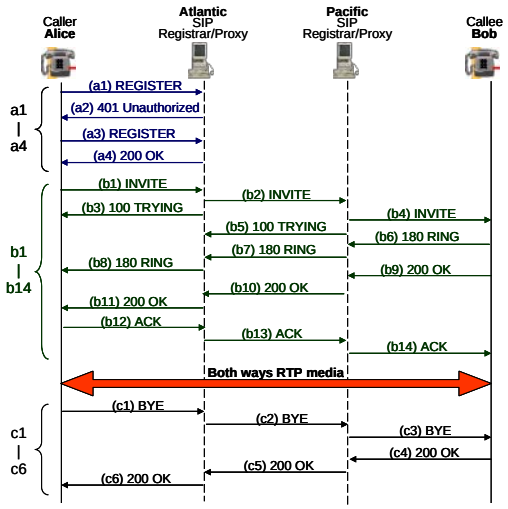

Figure 2. SIP Signaling Flow.

in a location service for a particular domain that associates an URI address with one or more contact address. When the user agent (UA) wants to make or receive a call, he or she has to add or refresh bindings whenever the most recent registration expires.

Based on this construction, SIP-based VoIP services have two major weaknesses that make them vulnerable to attack. First, they have a challenge-based authentication mechanism. Challenge-based mechanisms allow users to use a system continuously without further authentication within a set registration time period. Users only have to re-authenticate if the server suspects they are using the system without permission, and re-authentication then "challenges" the suspicious users. This type of authentication mechanism allows attackers to fairly often use the service for a long time without having to re-authenticate. If attackers had to re-authenticate more often, it would make it more difficult for them to carry out crimes. Second, SIP-based VoIP services allow users and servers to fill out or modify the information in SIP messages. Attackers readily exploit this weakness by forging messages when attacking VoIP devices and commit such crimes as fraud, blackmail and DoS attacks.

C. The Required Information that NWO/SvP Collaboratively Logs

The architecture of SIP-based IP telephony is shown in Fig. 1. The Registrars and Proxies are the SIP servers. Registrars are responsible for registration, after which the proxy servers relay the signaling to the callee's address and commence the service. Although the clients can send malicious or forged messages, they can only forge the information on messages or packets. Some important personal information, including user account information, can not be modified by users. User accounts are stored by the NWO and SvP, and are used to log-in for services and bill clients for call duration and type. Therefore, proper forensics investigations should extract the required information (information required to complete the three-way handshake), to form clues as to what attack took place. Tables I and II list the required information that the

TABLE I.
THE INFORMATION RECORDED BY SIP REGISTRAR SERVER

ATTRIBUTES	DESCRIPTION
Caller's Account	Caller's network-based phone account
Caller's Public IP/Prot	Acquired from the Caller's registration message
Timestamp and Expiration	The time when register expires
Callee's Account	Callee's network-based phone account
Callee's Public IP/Prot	Acquired from the Callee's registration message

SIP Registrar Server and NWO (NAT/DHCP) require for traceback [11].

D. Typical SIP-based Signaling Attacks and The Characteristic of Various Requests

We briefly describe typical SIP-based signaling attacks, discuss which header field values (HFVs) on request messages are forged based on the type of attack, and propose extracting the required information for producing the characteristics for the various requests (e.g., INVITE, REGISTER).

1) Typical SIP-based signaling attacks:

SIP messages are either requests (REGISTER, INVITE, BYE, CANCEL, ACK and OPTION) from a client to a server, or responses from a server to a client. Table III shows the typical SIP-based signaling attacks using REGISTER, INVITE, CANCEL and BYE requests. Attackers manipulate these requests by forging the header field values (HFVs) on different requests depending on what the attacker wishes to achieve. These attacks may be classified into three groups: forged REGISTER, INVITE, and CANCEL/BYE requests.

- *REGISTER requests:* the *attacker* sends a forged REGISTER request to the SIP Registrar.
- *INVITE requests:* the attacker sends spoofing INVITE requests to the SIP proxy, which are then forwarded to the victim.
- *CANCEL and BYE requests:* The attacker uses an SIP message to terminate an existing call.

2) Collaborative Forensics for SIP-Based VoIP Services

The required information may be extracted using the various requests and responses on the SIP proxy to form the characteristics of requests, which are required not only to run operations but also identify attackers, on the application layer. Fig. 3 lists this information. SIP Proxy Servers record certain pieces of information to form the various characteristics of calls, including the sought—after answers to various special questions—who, whom, when, where, and what. Based on the request and response (R/R) messages that attackers forge, attacks may be classified into three types: REGISTER, INVITE/OK/BYE (BIO) and CANCEL/BYE (C/B).

- *The Characteristics of REGISTER:* SIP Registrars dynamic bind the SIP User Agents IP addresses to its SIP URI contact. REGISTER requests register one or more contacts per User Agent. Seven HFVs, as shown in Fig. 3 (a), compose the characteristics of REGISTER requests on SIP-based VoIP services.
- *The characteristics of BIO:* User *agent* can make calls (send INVITE request) without further authentication before the expiration time limit set by the initial REGISTER request. Nine HFVs form the characteristics of BIO on SIP-based VoIP services based on the HFVs of BIO R/Rs, as shown in Fig. 3 (b).
- *The characteristics of BYE/CANCEL:* BYE and CANCEL attacks, which terminate victims' VoIP services prematurely, are unique in that attackers

TABLE II.
THE INFORMATION RECORDED BY NWO (NAT/DHCP)

ATTRIBUTES	DESCRIPTION
Caller's Account	User's network-based phone account
Caller's Private IP/Port	The private IP/Port with NAT
Caller's Public IP/Port	The public IP/Port assigned to NAT/DHCP
Caller's Public Media IP/Port	The public IP/Port assigned to NAT/DHCP
Time: Call	The time when call by private IP is received
Time: Hang-up	The time when call by private IP is interrupted

TABLE III.
TYPICAL SIP-BASED SIGNALING ATTACKS

ATTACKS	REQUESTS	RESPONSES
De-register	REGISTER	OK
Registration Hijack	REGISTER	OK
Fraud & Blackmail	INVITE/ACK/BYE	OK
DoS- INVITE Flooding	INVITE	NR
DoS- NO ACK	INVITE	OK
Call Hijack	Re-INVITE	3xx/OK
BYE-Session Teardown	BYE	OK
CANCEL-Session Teardown	CANCEL	OK

"NR" denotes no response. "x" denotes arbitrary number

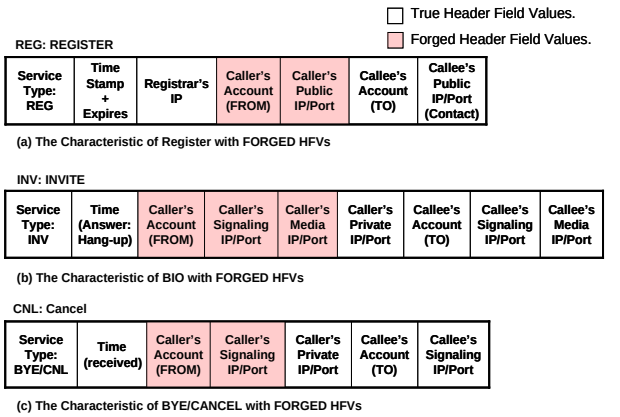

Figure 3. The Characteristics of Requests on SIP-based VoIP Services.

do not expect to receive responses from victims. With the exception of two HFVs, FROM (Caller ' s account) and Caller's Contact (signaling IP/Port) HFVs, are left forged, as shown in Fig. 3 (c).

In sum, specific HFV values on the R/Rs of the attacker are likely to be forged depending on which of the three types of characteristics of a call were manipulated i.e. REGISTER, BYE/ INVITE/OK (BIO) or CANCEL/BYE (C/B) R/Rs, but the victim's HFVs should remain genuine in spite of attack. Forensics analysis thus aims to identify the forged HFVs and merge this information with the information from the NWO and the home SIP Registrar. The details of the attacks and the characteristics of the various requests are described in [12].

E. Identifying the Forged Header Fields Values

Forensics, in the general sense, aims to figure out how crimes were committed and reveal the identities and geo-locations of the perpetrators of those crimes. In order to solve and prevent future crimes involving VoIP services, proper forensics is dependent on Network Operators, Access Providers and Service Providers (NWO/AP/SvP) collaboratively recording the identities of parties using these services and other information required for identifying geo-locations.

Forged HFVs of characteristics on SIP-based VoIP services must first be identified and then merged with information from SIP Registrars and NWOs for forensics analysis. As mentioned in the previous section, before sending attack requests, attackers have to first register with a home SIP Registrar using their true identity and public IP/Port. NWOs and SIP Registrars should record this information. These records may then be collected, extracted, and used to identify forged information on the characteristics of future requests and then merged with the characteristics of requests into a Local Event (LEv) that can be represented as an XML message and reported using the SEAL Protocol (described later in section IV) by an administrator, as shown in Table IV.

TABLE IV.
IDENTIFYING FORGED HEADER FIELD VALUES USING REQUIRED INFORMATION

The Characteristics of Requests on SIP Proxy			Forged Information Can be Identified by the Required Information Recorded on	
REGISTER	*INVITE*	*BYE/CANCEL*	*NWO*	*SvP (SIP Registrar)*
Time Stamp + Expires	Time (Answer: Hang-up)	Time (received)	Time (Answer: Hang-up)	Time Stamp + Expires
Registrar's IP				
Caller's Account (FROM)	Caller's Account (FROM)	Caller's Account (FROM)	Account	Account (FROM)
Caller's Public IP/Port	Caller's Signaling IP/Port	Caller's Signaling IP/Port	Caller's Public IP/Port	Caller's Public IP/Port (Contact)
	Caller's Media IP/Port		Caller's Media IP/Port	
	Caller's Private IP/Port	Caller's Private IP/Port	Caller's Private IP/Port	
Callee's Account (TO)	Callee's Account (TO)	Callee's Account (TO)		Account (TO)
Callee's Public IP/Port (Contact)	Callee's Signaling IP/Port	Callee's Signaling IP/Port		Callee's Public IP/Port (Contact)
	Callee's Media IP/Port			

Forged Header Field Values

IV. COLLABORATIVE FORENSICS FOR SIP-BASED VOIP SERVICES

In this section, we first present the key components of our design, outline the particulars of the Collaborative Forensics Network, and then describe the procedures that comprising units of the Collaborative Forensics Network follow for SIP-based VoIP services.

A. The Collaborative Forensics Center, SKYEYE

NWOs and SvPs may not want to share certain pieces of information e.g. security intelligence and forensic information with other NWOs or SvPs for a variety of reasons, including privacy concerns, commercial competition, company policies, culture differences, and implementation differences. NWOs and SvPs may be more inclined to share this information if the exchange of this information were supervised by an independent authority. This independent authority would have a mechanism that would aggregate, integrate, and correlate local information in the form of LEvs from operators and carry out traceback without compromising any information participating. We have designed a collaborative framework that can serve as this mechanism for an independent authority, as shown in Fig. 4, that we call the SKYEYE [11].

The Collaborative Forensics Mechanism (CFM)

1) The SKYEYE

The SKYEYE is the kernel of the collaborative forensic network in that it executes all collaborative investigations. It is comprised of the following modules: aggregation, event correlation, event information mining, integration, and expertise repository. The details of the SKYEYE and the procedure outlining how its comprising units interact are described in [11].

2) Access Local Event Entity (ALEE)

The ALEE is the AS interface that connects and communicates with SKYEYE, which is independent of the AS realm. For each SIP-based phone call, the ALEE automatically collects the required information about the caller and callee from the NWO (NAT/DHCP), SIP Registrar, and SIP Proxy in the operating network (AS) and merges these pieces of information to produce a Local Event in XML-format.

3) The flexible SKYEYE-ALEE (SEAL) protocol

The SEAL protocol is simple in design, and merely transports Local Events in XML format between the ALEE and SKYEYE, so it can easily accommodate different access network technologies i.e. TCP, HTTP and Web servers.

4) Local Events (LEvs)

Local Event data are collected from the NWO (NAT/DHCP), SIP Registrar and SIP Proxy in an AS by

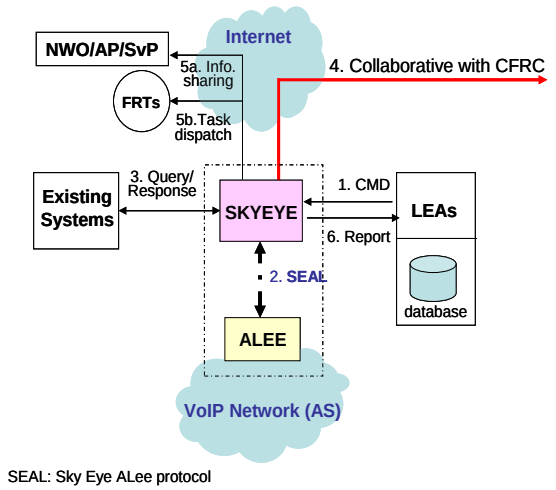

Figure 4. Procedure for Collaborative Forensics with Cooperating Units and Other Collaborative Forensics Region Centers.

the ALEE through the SkyEye-ALee (SEAL) Protocol. During a VoIP call, the ALEE makes two copies of the Local Event, and stores one of them in the local operator' s (AS') database for backup and the other is sent to SKYEYE for forensic analysis.

B. The Collaborative Forensics Work

The Collaborative Forensics Network, as it pertains to VoIP traceback, comprises multiple independent administrative region forensics centers. These region forensics centers would act as independent administrative authorities, each being composed of one or more ASs on the Internet, as shown in Fig. 5. When User Agents send SIP requests, the ALEE produces LEvs. Traceback to a particular user agent would only require the LEvs of the callee and caller, making LEvs of the intermediate ASs unnecessary. The LEvs from the caller and callee may be checked to build a complete picture of any incident, and this information could be used as evidence in a court of law. Correlating related LEvs, from the caller and callee, help to determine how a network incident e.g. attack occurred and provides such details as the origin, the method(s) used, and identities of the perpetrators.

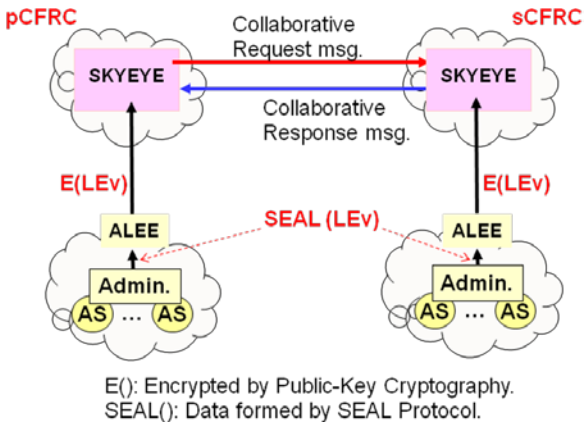

Figure 5. The Collaborative Forensics Mechanism (CFM): the primary CFRC (pCFRC), located near the caller, needs to communicate with the secondary CFRC (sCFRC) and request the LEv from the callee's AS to perform VoIP traceback.

1) Collaborative forensics work of SKYEYEs

We briefly describe the procedure that comprising units follow when conducting collaborative forensics, as shown in Fig. 4.

Step 1: The LEA sends commands to SKYEYE. Each command has two essential elements: the callee's account and the calling time-parameter. The former serves as the starting point for traceback, while the latter serves as an identifier for the call.

Step 2: SKYEYE checks its Event Data Warehouse and sends a request to the ALEE for a Local Event (LEv) search using the callee's account and calling time-parameter.

Step 3: SKYEYE may have to consult the domain experts by way of hosting a virtual panel to determine if any information is missing or confusing, and request data or evidence from other systems. The results of this process are then relayed back to SKYEYE's Control and Decision making Module to decide whether to take action.

Step 4: When the ASs of the caller and callee are located in the same Collaborative Forensics Region (CFR), the two LEvs, sent by caller and callee's ASs, are sent to the same CFR Center (CFRC) to execute VoIP trace back. Since caller and callee ASs are located in different CFR most of the time, the CFRCs receive only one LEv from either the caller or callee. In these cases, the primary CFRC (pCFRC), located near the caller, needs to communicate with the secondary CFRC (sCFRC) and request that the LEv of the callee be sent from the callee's AS in order to perform forensics.

Step 5: The LEv information is then shared with agencies such as the NWOs or SvPs to alert them about possible criminal activity, and these agencies can then report to Fast Response Teams (FRTs).

Step 6: All decisions made and the results of the incident are then relayed to the LEA.

2) The trigger for active forensics

Even now, law enforcement agencies (LEA) often take quite some time to start collaborative forensics in networks/computer systems. The stored data that they require for proper investigation often expires and has been deleted by the time they wish to have access to it. We propose using active forensics in computer systems in order to eliminate the problems of data storage and time lag in investigation. Active forensics requires that systems share security information and send alerts to cooperating units when attacks seem to have occurred. Collaborative forensics can then be executed long before the stored data has expired and been deleted.

Active forensics is triggered when the ALEE detects that one of the caller's HFVs, either their account or public IP/Port, have been forged. Active forensics and collaborate forensics, when combined, serve as the best method for handling VoIP attacks.

V. Design a Novel Protocol for VoIP SIP-based Network Collaborative Forensics

Based on the procedures of collaborative forensics work for SIP-based VoIP services mentioned in the previous section, this section discusses our design of a novel protocol to support collaborative forensics over Transmission Control Protocol (TCP) between two Internet Collaborative Forensics Region Centers (CFRCs). We then describe how the collaborative forensics mechanism (CFM) works with the design protocol to efficiently perform collaborative forensics and public-key cryptography and digital signature services through PKI.

A. Protocol Design for VoIP SIP-based Collaborative Forensics

Currently, existing literature contains many definitions of protocol [23], [24]. In some cases, a protocol is defined as the format and order of messages exchanged between two communicating entities, as well as the actions taken for the transmission and/or receipt of messages or other events [23]. In [24], protocol is defined as a precise format for valid messages, the procedural rules for data exchange, and the vocabulary of valid messages that can be exchanged.

Based on these definitions of a protocol and the procedures for collaborative forensics work, we design a novel application-layer binary protocol, named the Collaborative Forensics Protocol (CFP). Shown in Fig. 5, CFP is used to exchange collaborative request messages and response messages between Collaborative Forensics Region Centers (CFRCs), and to perform collaborative forensics work in SIP-based VoIP Services environments. The exchanged messages are equipped with both a CFP header and data component. They are also encrypted as a TCP payload, sent to the receiver, and then decrypted. This public-key encryption is handled by PKI, and is also clearly outlined later within this section.

1) The Collaborative Forensics Protocol (CFP) DATA

Depending on the procedures of collaborative forensics work, the prime Collaborative Forensics Region Center (pCFRC) will query collaborative information (callee's local event) from a secondary CFRC (sCFRC) through a collaborative request message. The collaborative request message carries CFP data, including information on calling time and the callee's account, encrypted by a pCFRC private key and sCFRC public key.

In response to the request by the pCFRC, the sCFRC sends data on the callee's local event (LEv) back to the pCFRC, thus initiating collaboration. The CFP data is shown in Fig. 6, SEAL Protocol.

2) The Collaborative Forensics Protocol (CFP) Header

The goal of the CFP header is to provide information necessary for cooperation. The values within the CFP header include the task (TK), forged flag (FF), forensics region (FR), Service Types (produced by the ALEE) and the time stamp given by the ALEE or SKYEYEs of the primary or secondary collaborative forensics region centers, as shown in Fig. 7. They can be used to indicate whether the local event is forged, and to identify the tasks and service types of receivers, the Collaborative Forensic Region Centers (CFRCs).

```
<? xml version="1.0" ? >
<ASN> </ASN>
<Time>
        <Time_Stamp></Time_Stamp>
        <Expire></Expire>
        <Hang-Up></Hang-Up>
        <Received_Time></Received_Time>
</Time>
<Caller>
        <Caller's _account > </Caller's_account >
        < Registrar's_IP > </Registrar's_IP >
        < Caller's_Public_IP> </Caller's_Public_IP>
        < Caller's_Public_Port> </Caller's_Public_Port>
        < Caller's_Public_IP> </Caller's_Public_IP>
        < Caller's_Media_IP></Caller's_Media_IP>
        < Caller's_Media_Port></Caller's_Media_Port>
        < Caller's_Private_IP></Caller's_Private_IP>
        < Caller's_Private_Port></Caller's_Private_Port>
</Caller>
<Callee>
        <Callee's_account ></Callee's_account >
        < Callee's_Public_IP></Callee's_Public_IP>
        < Callee's_Public_Port></Callee's_Public_Port>
        < Caller's_Media_IP></Caller's_Media_IP>
        < Caller's_Media_Port></Caller's_Media_Port>
</Callee>
```

Figure 6. The CFP Data Formed as SEAL Protocol.

- Sender's ID (32-bits) is for the receiver to identify the sender and for storage purposes. The Sender is the ALEE, who sends the local event, or SKYEYE of CFRCs who send request or response messages.
- The Total Length field (16-bits) gives the total length of the request or response message, including the CFP header and the CFP data, by the ALEE or SKYEYE.
- The Task (TK) field is 4-bits. It is used to indicate the message task. The TK are TRACEBACK, FORENSICS and STORE, represented by "0000," "0001" and "1111," respectively, while the remaining combinations are reserved for other tasks.
- The Forged Flag (FF) field, 1-bit, is used to identify whether the caller's required information is forged or not, and used to trigger an active forensics procedure. An FF of "0" means that the ALEE did not find any forged value in the local event.
- The Forensics Region (FR) is 1-bit and inserted by

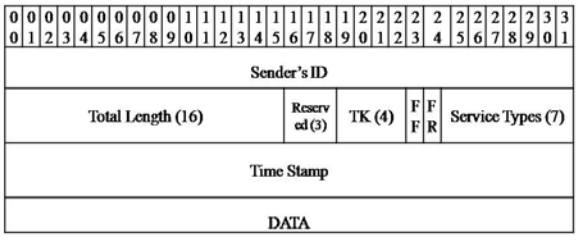

Figure 7. Collaborative Forensics Protocol (CFP): Header and Data Values.

the ALEE. A value of "1" indicates that the locations of the caller and callee belong to the same collaborative forensics region, while "0" indicates that they belong to different collaborative forensics regions.

- The Service Types field (7-bits) is used to indicate the service type of the VoIP network phone. Service types include REGISTER, INVITE, BYE, CANCEL, ACK and OPTION, represented by "0000001," "0000010," "0000011," "0000100," "0000101," and "0000110," respectively. The remaining combinations are reserved for additional service types in the future.
- Time Stamp is a 32-bits field. It indicates the time that the CFP was sent by ALEE, pCFRC or sCFRC.

B. The PKI for Digital Signature and Cryptography Services

To perform collaborative forensics, the local events (LEvs) need to be exchanged between two cooperating units (e.g. between pCFRC and sCFRC), by collaborative forensics protocol (CFP). For security reasons, this collaborative information (LEvs) must be encrypted before being exchanged. In this paper, we introduce Public-Key Infrastructure (PKI) [13] for our collaborative forensics mechanism (CFM) to provide digital signature and cryptography services, and to enable the secure, convenient and efficient acquisition of public keys.

Regardless of the number of cooperating units, collaborative information can be exchanged between any two (Administrator, ALEE or CFRCs), with the CFP message (including data and header) encrypted by the sender's private key and the receiver's public key. The ciphertext is then treated as the TCP payload and sent to the receiver. When the receiver receives the ciphertext message, it decrypts the message using its private key and the sender's public key.

For collaborative request messages, the CFP data is the calling time and callee's account. According to the calling time and callee's account in the request message, the sCFRC needs to offer a collaborative response message to the pCFRC. Both collaborative request and response messages are encrypted, and serve as the TCP payload between collaborative units for collaborative forensics.

VI. THE PROCEDURE OF GENERATING COLLABORATIVE FORENSICS MESSAGES AND DISCUSSION

In this section, we describe the procedure for generating collaborative forensics information. Then we present a BYE session Teardown Attack scenario to describe how the collaborative forensics mechanism (CFM) works with collaborative forensics protocol (CFP). Finally, we discuss the security of PKI working with collaborative forensics mechanism to against various types of attacks, and the features of the collaborative forensics protocol.

A. Collaborative Forensics Procedure

Based on the procedures for collaborative forensics, the collaborative forensics mechanisms perform collaborative forensics work by exchanging collaborative request and response messages. The procedure of generating collaborative forensics information has three phases. In the first phase, required pieces of information are collected from the NWO, SIP Registrar and SIP Proxy in an autonomous system (AS), represented as an XML message, and reported using the SEAL Protocol by an administrator. Then the required information is encrypted by the administrator's private key and the ALEE's public key, as the TCP payload is sent to the ALEE.

In the second phase, when the ALEE receives the required information, it first decrypts the TCP payload, identifies whether the local event values are forged, and checks the caller's and callee's IP to determine if they belong to the same forensics region. Based on the results, the ALEE inserts the suitable TK, FR, FF and SOT values into the CFP header. Then the ALEE encrypts the CFP header and CFP data by its private key and the public key of the sCFRC, and sends the ciphertext message to the SKYEYE of the sCFRC.

In the third phase, When SKYEYE of sCFRC receives the ciphertext message (i.e., CFP data and CPF header), the SKYEYE of sCFRC decrypts the message using its private key and the public key of the SKYEYE of pCFRC, and identifies the RF value. If it is carrying an FR bit of "1," it can do the forensics tasks in its own regional forensics center without generating collaborative request message to acquire collaborative information from cooperating units. If SKYEYE reads the FR bit as "0," it needs to generate a collaborative request message to the sCFRC.

The collaborative request message is composed of the CFP header and CFP data. The CFP data of the collaborative request message is the calling time and callee's account encrypted by the pCFRC private key and then by the sCFRC public key as an authenticator. The collaborative request message then is sent to cooperating units (sCFRC) for query collaborative information. The collaborative information, the callee's LEv encrypted by the sCFRC private key and pCFRC public key, is the CFP data of the collaborative response message sent back to the pCFRC. Both CFP messages, provided by the ALEE of pCFRC and the CFP response message offered by sCFRC, serves as evidence of collaborative forensics for VoIP services.

B. A Scenario with Collaborative Forensics Protocol

Here, we present a scenario, BYE Session Teardown Attack, to describe how the collaborative forensics protocol (CFP) works with collaborative forensics mechanism (CFM). Under a multi-AS environment, Alice and Bobs' IP are located at different service providers (SvP) and they are communicating in a VoIP session. After Attacker completes registration and impersonates Alice to send a spoofing BYE request to terminate her session. When session is teardown, the pieces information

of LEvs collected from NWO, SIP registrar and proxy are sent to ALEE by the administrators of SvP.

Active forensics is triggered when ALEE of Attacker's CFRC detects that the values of local event (LEv), the Attacker's account (From) and signal public IP/Port HFVs, have been forged. ALEE then sets CFP header values, forged flag (FF="1"), task (TK="0001"), forensic region (FR="0") and service type (SOT="0000011"). The CFP data contains Bob's account and calling time. The CFP header and CFP data are sent to SKYEYE of the pCFRC. When this SKYEYE identifies the CFP header, it knows the forensics task is assigned and then it checks the Bob's public IP address to recognize which Forensics Region Center need to collaborate.

Then the SKYEYE of the pCFRC communicates with the SKYEYE of the sCFRC. The SKYEYE read the CFP header with task value "0001" and then relays back the Bob's LEv for subsequent forensics investigation. Therefore the SKYEYE of pRCFC can correctly perform the forensics of BYE Session Teardown Attack.

C. Discussion

In this section we introduce the types of attacks on network and the ways our system to handles those attacks. The types of attacks on networks can be classified into two types: passive attacks and active attacks.

Passive attacks include the "release of message contents" and "traffic analysis" [25]. A "release of message content" attack determines the message content of the transmission. A "traffic analysis" attack attempts to circumvent message encryption by guessing the nature of the communication. These passive attacks are very difficultly to detect, because they only "observe" rather than modify data on packets transmitted on the network.

The latter category, active attacks, are further divided into four types: "masquerade," "replay," "modification of messages," and "denial of service." Except "denial of service" attacks, these active attacks function by modifying portions of data or creating false values within the message.

1) Discussion on the Security of PKI Working with Collaborative Forensics Mechanisms (CFMs)

For collaborative forensics mechanism (CFM), we employ PKI to encrypt the header and data of CFP to avoid unauthorized observations of TCP payload content, and to partly interfere with the execution of "modification of message" and "masquerade" attacks. Furthermore, PKI offers authentication and key pair update management, which can prevent "replay" attacks before key pairs and certificate life time expires. However, the one downside to PKI services is that they require more resources to function, and thus are more susceptible to "denial of service" attacks.

2) Discussion the Features on Collaborative Forensics Protocol (CFP)

In this section we discuss four features of our collaborative forensics protocol (CFP): completeness, flexibility, jitter and overhead.

- *Completeness:* the CFP data carries collaborative information that tells the forensics investigator where, when, by whom, and how an attack takes place. The CFP header keeps information on the collaborative request and response messages of cooperating units.
- *Flexibility:* in the CFP header, the fields indicate only some of the services and tasks. If additional services and tasks are necessary, they can be defined and added without modification. Some bits are reserved fields for addition services and tasks. The CFP data (local event) is offered and follows the SEAL protocol, and thus this amount of data is fixed. If some extra amount of data needs to be appended at the end of a local event, we can change the length of the CFP data accordingly.
- *Jitter:* because our collaborative forensics mechanism performs digital forensics investigation, it involves actions that are executed after an event takes place. Therefore, we are not particularly concerned with delay issues when required information and collaborative request and response messages are sent.
- *Overhead:* for our collaborative forensics mechanism, the protocol header keeps some of the required information for cooperation, such as the sender's ID, which provides information about the sender's key. There are some header values that are not directly required for collaborative forensics (the length of CFP data), but can be used to improve processing efficiency.

In sum, for our collaborative forensics mechanism, the CFP header has enough data to exchange collaborative information, while additional data can be added if necessary. The header also maintains required information for collaborative forensics. In light of these and other functions, we judge that the CFP has the necessary attributes of completeness, flexibility and low overhead.

VII. CONCLUSION AND FUTURE WORK

For preventing and fighting cyber crime, collaborative forensics may provide an efficient solution. Existing research had only proposed a collaborative forensics mechanism, but did not develop a common protocol to perform Internet-based collaborative forensics work. This is the principal reason why collaborative forensics is not successfully widespread. In order to fill this gap within the current literature, this paper designs a novel collaborative forensics protocol (CFP). The CFP is used to exchange collaborative request and response messages with cooperating units. This collaborative forensics protocol design and mechanism represent the preliminary steps towards performing collaborative forensics for SIP-based VoIP services on the Internet.

In this paper, we only consider SIP-based IP telephony. However, developing compatible methods for other types of telephony, such as H.323 or MGCP telephony, is also an important area for research. Further research on other

types of network attacks as well as anonymous VoIP services is also necessary before our collaborative forensics mechanism (CFM) and proposed protocol (CFP) can be broadly applied. Despite our success in handling typical SIP-based signaling attacks, other SIP-based signaling attacks have not been considered, including malicious acts without SIP proxy services. Furthermore, some VoIP services (e.g. Skype) offer anonymous services to clients, where clients may sign on without a user name, and these must also be considered in future network forensics research.

Lastly, when fighting cybercrime we generally target networks of individuals, rather than one isolated lawbreaker. Our defense strategy must successfully identify all participating parties, discover their motives (through communication intercepts or surveillance), and track their IPs to determine their geo-location. Therefore, further work is needed to determine how our protocol and framework can serve other uses, such as IP location, and real-time interception and surveillance. Altogether, these areas represent numerous possibilities for future research, and highlight the need to expand the use of framework for combating cybercrime.

REFERENCES

[1] J. Rosenberg et al. "SIP: Session Initiation Protocol (SIP)," RFC 3261, IETF Network Working Group, 2002. Available: http://www.ietf.org/rfc/rfc3261.txt.

[2] J. Postel, "IP: Internet Protocol," RFC 0791, IETF Network Work Group, 1981. Available: http://www.ietf.org/rfc/rfc0791.txt .

[3] B. Reynolds and D. Ghosal, "Secure IP Telephony using Multi-layered Protection,' In Proc. of the Network and Distributed System Security Symposium (NDSS), February 2003.

[4] Y.-S. Wu, S. Bagchi, S. Garg, N. Singh and T. Tsai, "SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments," In IEEE Dependable Systems and Networks Conference, 2004, pp. 433-442.

[5] H. Sengar, D. Wijesekera, H. Wang, and S. Jajodia, "VoIP Intrusion Detection Through Inter-acting Protocol State Machines," In IEEE Dependable Systems and Networks Conference 2006, pp. 393-402.

[6] H. Sengar, D. Wijesekera, H. Wang and S. Jajodia, "Fast Detection of Denial-of-Service Attacks on IP Telephony," 14th IEEE Internation Workshop on Quality of Service 2006, pp. 199-208.

[7] P. Ferguson, and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," RFC 2827, IETF Network Working Group, May 2000. Available: http://www.ietf.org/rfc/rfc2827.txt.

[8] B.-B. Anat, and H. Levy, "Spoofing Prevent Method," In Proc. of IEEE INFORCOM 2005.

[9] G. Zhang, S. Ehlert and T. Magedanz, "Denial of Service Attack and Prevention on SIP VoIP Infrastructures Using DNS Flooding," In Proc. of the 1st international conference on Principles, systems and applications of IP telecommunications, 2007.

[10] G. Ormazabal, S. Nagpal, E. Yardeni and H. Schulzrinne, "Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems," In Proc. of the 2nd international conference on Principles, systems and applications of IP telecommunications 2008.

[11] H.-M. Hsu, Y. S. Sun and M.-C. Chen, "A Collaborative Forensics Framework for VoIP Services in Multi-network Environments," In Proc. of the IEEE ISI 2008 Workshops, LNCS 5075, pp. 260-271, 2008.

[12] H.-M. Hsu, Y. S. Sun and M.-C. Chen, "Collaborative Scheme for VoIP Traceback," Digi. Investig. (2011) Vol. 7, issues 3-4, pp. 185-195, doi:10.1016/j.diin.2010.10.003.

[13] D. Cooper et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, IETF Network Working Group, 2008. Available: http://www.ietf.org/rfc/rfc5280.txt.

[14] J. Postel, "TCP: Transmission Control Protocol," RFC 0793, IETF Network Working Group, 1981. Available: http://www.ietf.org/rfc/rfc0793.txt.

[15] M. Roesch, "Snort-Lightweight Intrusion Detection for networks," In Proc. of USINIX LISA'99, November 1999.

[16] V. Jacobson, G. Leres, and S. McCanne, "libpcap," Lawrence Berkeley National Laboratory, 1994. Available: http://www-nrg.ee.lbl.gov/.

[17] J. Yu, Y.V. R. Reddy, S. Selliah and S. Reddy, "TRINETR: An architecture for collaborative intrusion detection and knowledge-based alert evaluation," Advance Engineering Informatics, 2005. pp. 93-101.

[18] Y. Xie, V. Sekar, M.K. Reiter and H. Zhang, "Forensic Analysis for Epidemic Attacks in Federated Networks," In Proc. of the 14th IEEE ICNP, 2006.

[19] H. Khurana, J. Basney, M. Bakht, M. Freemon, V. Welch, and R. Butler, "Palantir: A Framework for Collaborative Incident Response and Investigation," In Proc. of the 8th symposium on Identity and Trust on the Internet, 2009.

[20] E. S. Pilli, R.C. Joshi and R. Niyogi, "Network Forensic frameworks: Survey and Research Challenges," Digit. Investig. (2010) Vol. 7, issues 1-2, pp. 14-27, doi: 10.1016/ j.diin.2010.02.003.

[21] M. Handley and V. Jacobson, "SDP: Session Description Protocol," RFC 2327, IETF Network Working Group, 1998. Available: http://www.ietf.org/rfc/rfc2327.txt.

[22] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-time Applications," RFC 3550, IETF Network Working Group, 2003. Available: http://www.ietf.org/rfc/rfc3550.txt.

[23] J. F. Kurose and K. W. Ross, "Computer Network," Published by Addison Wesley, 3th Edition, 2005.

[24] G. J. Holzmann, "Design and Validation of Computer Protocols," Published by Prentice-Hall, 1991.

[25] W. Stallings, "Cryptography and Network Security-Principles and Practices," Published by Pearson Education International, 4th Edition, 2006.

Hsien-Ming Hsu was born in Kaohsiung, Taiwan, in 1963. He received B.S. degree from Chinese Naval Academy in 1985, and M.S.E.E. degree from the Department of Electrical and Computer Engineering, Naval Postgraduate School, Monterey, California, U. S. A., in 1996. Currently, he is working towards the Ph.D. degree in the Department of Information Management, National Taiwan University. His research interests include network security, Geo-profile and communication systems.

Feng-Yu Lin was born in Taipei, Taiwan, in 1968. He received B.S. degree in Law from Central Police University in 1990, and M.S. and the first Ph.D. degrees in Department of Transportation Management, National Chiao-Tung University, in 2000 and 2004, respectively. Currently, he is working towards the second Ph.D. degree in the Department of Information Management, National Taiwan University. His research interests include spectrum management, network security, Geo-profile and communication systems.

Yeali Sunny Sun received her B.S. from the Computer Science and Information Engineering department of National Taiwan University in 1982, and M.S. and Ph.D. degrees in Computer Science from the University of California, Los Angeles (UCLA) in 1984 and 1988, respectively. From 1988 to 1993, she was with Bell Communications Research Inc. (Bellcore; now Telcordia). In August 1993, she jointed National Taiwan University and is currently a professor of the Department of Information Management, and the chief director of the Computer and Information Networking Center of National Taiwan University. Her research interests are in the area of wireless networks, Quality of Service (QoS) and pricing, Internet security and forensics, scalable resource management and business model in cloud services and performance modeling and evaluation.

Meng Chang Chen received his B.S. and M.S. degrees in Computer Science from National Chiao-Tung University, Taiwan, in1979 and 1981, respectively, and the Ph.D. degree in Computer Science from the University of California, Los Angeles, in 1989. He was with AT&T Bell Labs from 1989 to1992. He is a Research Fellow of Institute of Information Science, Academia Sinica, Taiwan and have served as Deputy Director of the institute for 5 five years. His current research interests include wireless access network, QoS networking, computer and network security, information retrieval, and data and knowledge engineering.