Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 1632 – 1636

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

A Real-time Crime Detection System Based on Lawful Interception - A Case Study of MSN Messenger

Chi-Hua Chen[a,*] , Wan-Jia Chen[a,b], Ya-Fen Wang[a], Chi-Chun Lo[a]

[a]*Institute of Information Management, National Chiao-Tung University, Taiwan, R.O.C.*
[b]*Computer Center, National Changhua University of Education, Taiwan, R.O.C.*

Abstract

In recent years, the number of online crimes (e.g., the various emerging scams and criminal schemes) has increased. Online crime suspects utilize the anonymous nature of web to disguise their identity through various methods and evade detection and surveillance from law enforcement agencies. This study proposes an effective lawful interception system, *Real-time Crime Detection System* (RCDS), which includes *Criminal Investigation Bureau* (CIB), *Internet Service Providers* (ISP), and *Network Interception Server* (NIS) to establish a legally sanctioned lawful interception process which can collect and store evidence for criminal detection in real time. We provide a case study of MSN Messenger to describe the *MSN Protocol* (MSNP), information flow process, and lawful interception methodologies. The RCDS can provide criminal detection and surveillance services for MSN to obtain criminal communication records in turn reducing online criminal activities.

Selection and/or peer-review under responsibility of [CEIS 2011]

Keywords: Crime Detection; Lawful Interception; MSN Messenger.

1. Introduction

In recent years, the number of online crimes (e.g., the various emerging scams and criminal schemes) has increased. Online crime suspects utilize the anonymous nature of web to disguise their identity through various methods and evade detection and surveillance from law enforcement agencies. The crime suspect's communication methods and identifying numbers are hard to be verified under the electronic surveillance warrant for the *Law Enforcement Monitoring Facilities* (LEMF). In comparison with traditional telephone and mobile phone communication records, the online communication is more uncertain to be tracked. For example, crime suspects can make online crime in the different locations of

* Corresponding author. Tel.: +886-975292259
E-mail address: chihua0826@gmail.com

doi:10.1016/j.proeng.2011.08.304

the different internet cafés where they engage in criminal communications and utilize special computer technology to avoid the law enforcement interception on the specific network node. Therefore, the choice of network nodes for interception is uncertain and complicating difficulty of surveillance [1-3].

In this paper, we propose the *Real-time Crime Detection System* (RCDS) based on lawful interception system for online criminal detection. The RCDS includes *Criminal Investigation Bureau* (CIB), *Internet Service Providers* (ISP), and *Network Interception Server* (NIS) to establish a legally sanctioned lawful interception process which can collect and store evidence for criminal detection in real time.

The remainder of this paper is broken down into 4 sections. Section 2 shows system architecture and functions which are combined with the lawful interception processes. Section 3 presents a case study of MSN Messenger to describe the *MSN Protocol* (MSNP) [4], information flow process, and lawful interception methodologies. The last section provides the conclusions and future work.

2. System Architecture

The RCDS which is based the lawful interception system works with CIB and ISP. The NIS can be built in the providers' network systems. Figure 1 shows the architecture of the RCDS. Law Enforcement agents can use the web site on the CIB to send the criminal investigation requests to ISP, and the NIS which obtains the related interfaces (e.g., *Handover Information* (HI)) for ISP interconnection [1-3]. Moreover, the NIS can capture and analyze the network packets to save the crime information into the *Intercept Related Information* (IRI) files and *Contents of Communication* (CC) files which are sent to CIB for lawful interception.

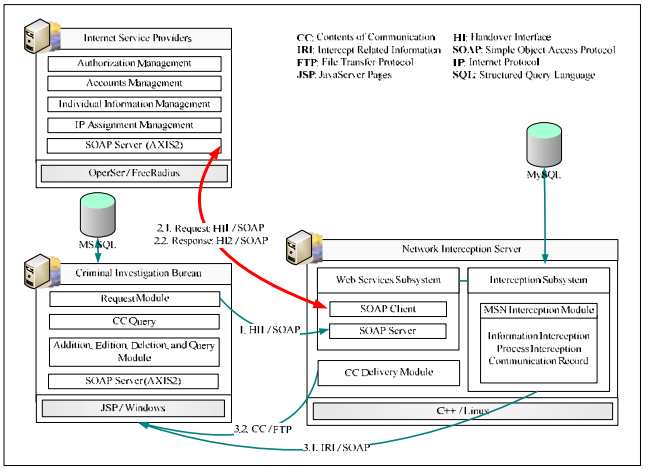

Fig. 1. System Architecture of the RCDS

The RCDS which connects all the switches and hubs duplicates and sents all the packet passing through these switches and hubs to NIS for the effective surveillance. The NIS can to perform packet capture and filtering according to a suspect list for lawful interception. Therefore, NIS requires the ability to support the analysis of all communication protocols (e.g., MSNP) and retrieve the *Internet Protocol* (IP) addresses and communication contents from each conversation. This system can maintain the quality of communication and make user unaware when the user communication is intercepted, as well as be able to perform crime detection without adding loading in the ISP network.

3. MSN Messenger Interception

In this section, we describe the MSNP and discuss the deployment and implementation of NIS for MSN Message Interception.

3.1. MSNP

MSN Messenger is an *Instant Messenger* (IM) which is built on MSNP. MSNP provides complete framework for sign-in, verification and authorization services. Base on network topology, MSNP includes three tiers which are service tier, connection tier, and user tier. User tier mainly receives and transmits user requests (e.g., sign-in requests, state change requests, text message requests and file transmission requests) to relevant servers through connection tier [4].

3.1.1. MSN Architecture

MSNP is based on *Transmission Control Protocol* (TCP) to build socket and transfer packets. In MSNP, the file transmission and voice chats are through *Peer-to-Peer* (P2P) connection, and other transmissions are through *Client/Server* (C/S) connection. In service tier, there are three types of servers which are described as follows [4].

(1) *Dispatch Server* (DS): In the initial connection establishment, user will open a TCP socket and connect to DS (i.e., messenger.hotmail.com) port 1863. The DS provides negotiation between user and *Notification Server* (NS). DS will send the available IP and port of NS to users. When the user receives IP and port from DS and returns with **ACK** command, the DS will remove the connection with the user.

(2) NS: During a MSN session, users maintain connection with NS for task establishment (e.g., sign-in, state change, friend list update, message transmission, chat requests, email notification, and sign-out). The server port is also 1863 mostly.

(3) *Switchboard Server* (SS): SS provides the gateway for chats between users. When a new chat is established, a new TCP session will be built between user and SS. The server port is mostly 1863. When file or voice transmission is required, SS will send a command to sender and receiver for P2P establishment. The transmission port which is usually automatically negotiated by users is usually 6891.

3.1.2. MSN Commands

To provide instant messaging for MSN users, it is critical to abide to protocols in MSNP. Decoding the commands is an important issue to provide the different processes according to the MSNP commands. Using an example of user messaging, the process of MSN messaging is shown in Figure 2. The message packet contains the Header and Body information, and the **MSG** command information is stored in the Header of the packet. Different message types contain their particular command information in the Header. In the case of instant messages, Content-Type and X-MMS-IM-Format which are more important denote the messages encoded in UTF-8.

3.2. MSN Message Interception Deployment

For MSN message interception deployment, the interception system are required the different designs and deployments according to the different network environments. In star-topology (i.e., Hub-based platform) environment, when a device needs to make connections with other devices, the packet which is sent by the device will be simultaneously duplicated to all the ports in the Hub. This means that any devices in the Hub-based platform can listen all communications of all devices in the star-topology and use the packet capture module and packet composition module to capture the packets. Therefore, the NIS can deploy on any device to intercept information. The various deployment environments are described as follows.

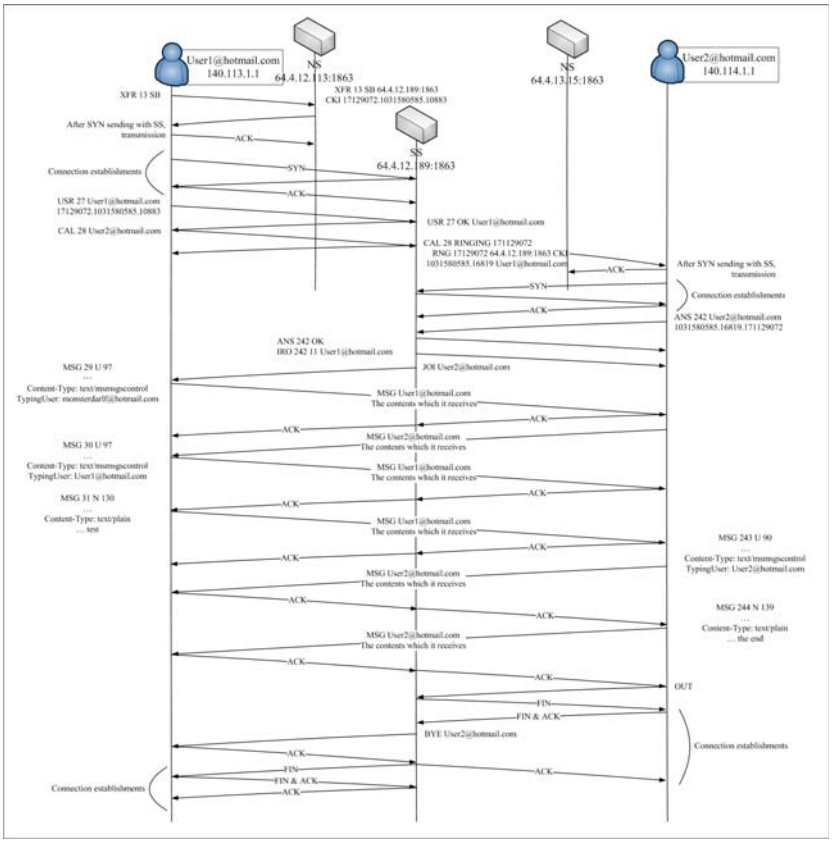

Fig. 2. The Process of MSN Messaging

(1) If all connections of network access are through a Proxy, the NIS can only deploy on the Proxy.
(2) If the Gateway on *Local Area Network* (LAN) is a server, the NIS can deploy on the Gateway server.
(3) If the Gateway on LAN is not a server but a Router, the NIS can deploy on a Hub which is installed between Layer 3 Switch and Router.
(4) If the Layer 3 Switch can support network management configuration, the NIS can deploy on this Layer 3 Switch.

3.2.1. Packet Capture Module

In the deployment environments described above, a packet capture module based on the Libpcap library is written for packet capture. The Libpcap library stands for packet capture library which provides a portable framework for low-level network monitoring [5]. The C/C++ library provides a high level interface for packet capture systems which is able to capture packets going through network interface. The well known TCPDUMP is based on Libpcap. Libpcap provides an interface library with mechanisms to realize and encapsulate the packets through packet capturing process for various system platforms. Therefore, the programs which are written with Libpcap can be used in the heterogeneous platforms. Under Linux, Libpcap can use *Berkeley Packet Filter* (BPF) to perform group capture for higher performance.

3.2.2. Packet Composition Module

After packet capture, packet composition is required because all the message segments are not always contained within a single packet. Libnids can support packet capture, fragment composition, packet composition, segment composition, port scan test, and abnormal packet detection [6]. Libnids uses the packet capture functions of Libpcap to set up the filtering rules and identify the target packets for capturing. The composition functions which are important functions of Libnids refer the packet composition process in Linux Kernel. Libnids is more advance than Lipcap to provide the segment composition. Therefore, Libnids can capture and analyze each application program based on TCP.

The packets will be composited and transform to IP packet structure by Libnids when they are captured by Libpcap. The callback function of Libnids, process_packet function, which will analyze the application layer information of packet when the Libnids receives IP packets. To decipher MSN command types, analyze_packet function is used to analyze command types and call up corresponding function to provide MSN connection information. For example, the handler_msg_joi funtion can analyze the notification before SN establishes the connection. The handler_msn_msg function is the main real-time interception function to analyze and produce the communication records for sending to LEMF. The process of MSN packet capture and composition is shown in Figure 3.

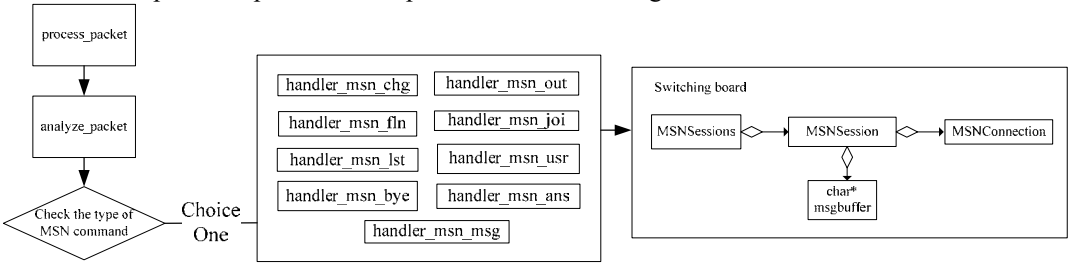

Fig. 3. The Process of MSN Packet Capture and Composition

4. Conclusions and Future Work

This study proposes an effective lawful interception system, RCDS, which includes CIB, ISP, and NIS to establish a legally sanctioned lawful interception process which can collect and store evidence for criminal detection in real time. In the case study of MSN Messenger, we describe the MSNP, information flow process, and lawful interception methodologies. The RCDS can provide criminal detection and surveillance services for MSN to obtain criminal communication records in turn reducing online criminal activities. In the future, the RCDS can be applied to detect various online crimes based on various protocols (e.g., *Hypertext Transfer Protocol* (HTTP) and *Voice over Internet Protocol* (VoIP)) for lawful interception.

References

[1] ETSI, “Lawful Interception (LI); Requirements of Law Enforcement Agencies”, ETSI TS 101 331, Version 1.3.1, 2009.

[2] ETSI, “Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture”, ETSI TS 101 943, Version 2.1.1, 2004.

[3] ETSI, “Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic”, ETSI TS 101 671, Version 3.3.1, 2008.

[4] M. Mintz, “MSN Messenger Protocol”, 2011. Available at: http://www.hypothetic.org/docs/msn/

[5] L. MartinGarcia, “TCPDUMP and Libpcap”, 2011. Available at: http://www.tcpdump.org

[6] R. Wojtczuk, “Libnids”, 2011. Available at: http://libnids.sourceforge.net/