一個基於合法監聽的即時犯罪偵測系統－以 MSN Messenger 為例

程鼎元[1]　陳志華[2]　郭庭歡[3]　吳哲一[4,*]
[1]華夏科技大學資訊管理系
[2]中華電信研究院智慧聯網研究所
[3]國立中山大學資訊工程學系
[4]國立屏東科技大學電子計算機中心
[*]joey@mail.npust.edu.tw

摘要

近年來網路網路犯罪越來越盛行，各式各樣的犯罪方式也層出不窮。通訊監察的對象很容易利用各種方式隱匿自己的存在，逃避司法機關的偵查。而且，網路通訊監察有別於傳統電信監察方式，還具有普遍性和第三人被侵害性兩個特色。因為，在網路犯罪的監察和偵測上深具困難度。本研究有鑑於網路犯罪偵測的重要性，提出一套有效的合法監聽系統—實作一個基於合法監聽的即時犯罪偵測系統(Real-time Crime Detection System, RCDS)，主要包含有通訊監察中心端、網際網路服務提供者(Internet Service Provider, ISP)業者端、以及網路監察伺服器，以建立合法監聽流程，並即時偵測犯罪行為的產生和儲存犯罪紀錄。在本研究中，我們將以 Case Study 方式，以 MSN Messenger 為例，描述 MSN 資料結構、訊息流程、以及監聽方式。RCDS 將可提供 MSN Messenger 犯罪偵測，有效的取得犯罪通聯紀錄，以減少未來的犯罪率。

關鍵詞：合法監聽、犯罪偵測、犯罪通聯紀錄、MSN Messenger。

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.

Keywords: Lawful Interception, Crime Detection, Criminal Communication Records, MSN Messenger.

1. 前言

近年來網路網路犯罪越來越盛行，各式各樣的犯罪方式也層出不窮。其中，網路犯罪中被通訊監察的對象將可能利用各種方式隱匿自己的存在，以躲避司法機關和警政單位的偵查。此外，由於網路電話的興起，相較於傳統電話將更讓執法者難以進行偵查動作，增加偵測的困難度。

然而，網路通訊監察有別於傳統電信監察方式，還具有普遍性和第三人被侵害性兩個特色。(1) 普遍性：由於許多網際網路服務將可能由傳統電信業者，許多網際網路服務提供者(Internet Service Provider, ISP)業者、網路內容服務提供者(Internet Content Provider)等網際網路業所提供，不再像傳統電信偵測那樣只由由中華電信公司等傳統電信業者獨占。因此，與執法機關配合的通訊監察者將依網際網路應用服務的不同而異。(2) 第三人被侵害性：由於傳統電話網路是以點對點的方式進行傳播，但網路電話則是以封包交換系統的方式處理許多使用者的封包。因此，在網路監聽的環境下，應設置過濾程式，以取得被監察對象的相關資訊，並避免無辜第三人被到監察[1-3]。

本研究有鑑於網路犯罪偵測的重要性，提出一套有效的合法監聽系統—實作一個基於合法監聽的即時犯罪偵測系統(Real-time Crime Detection System, RCDS)，主要包含有通訊監察中心端、ISP 業者端、以及網路監察伺服器(Network Interception Server, NIS)，以建立合法監聽流程，並即時偵測犯罪行為的產生和儲存犯罪紀錄。

此論文以下分為五個章節，在第二節分析說明系統架構與功能設計，並描述合法監聽流程。第三節將以 Case Study 方式，以 MSN Messenger 為例，描述 MSN 資料結構、訊息流程[4]、以及監聽方式。最後一章則說明此論文之結論與未來研究方向。

2. 系統架構

一個基於合法監聽的即時犯罪偵測系統主要

與各個網際網路服務提供者(Internet Service Provider, ISP)業者和 VoIP 業者合作，於其機房架設網路監察伺服器(Network Interception Server, NIS)，該系統架構如圖 1 所示。監察人員可於通訊監察中心端對監察對象進行投單，NIS 再與 ISP 業者取得監察對象之相關資訊[1-3]，並針對其封包之封包擷取和分析技術進行實作和監聽，最後再將通聯紀錄回傳予通訊監察中心。

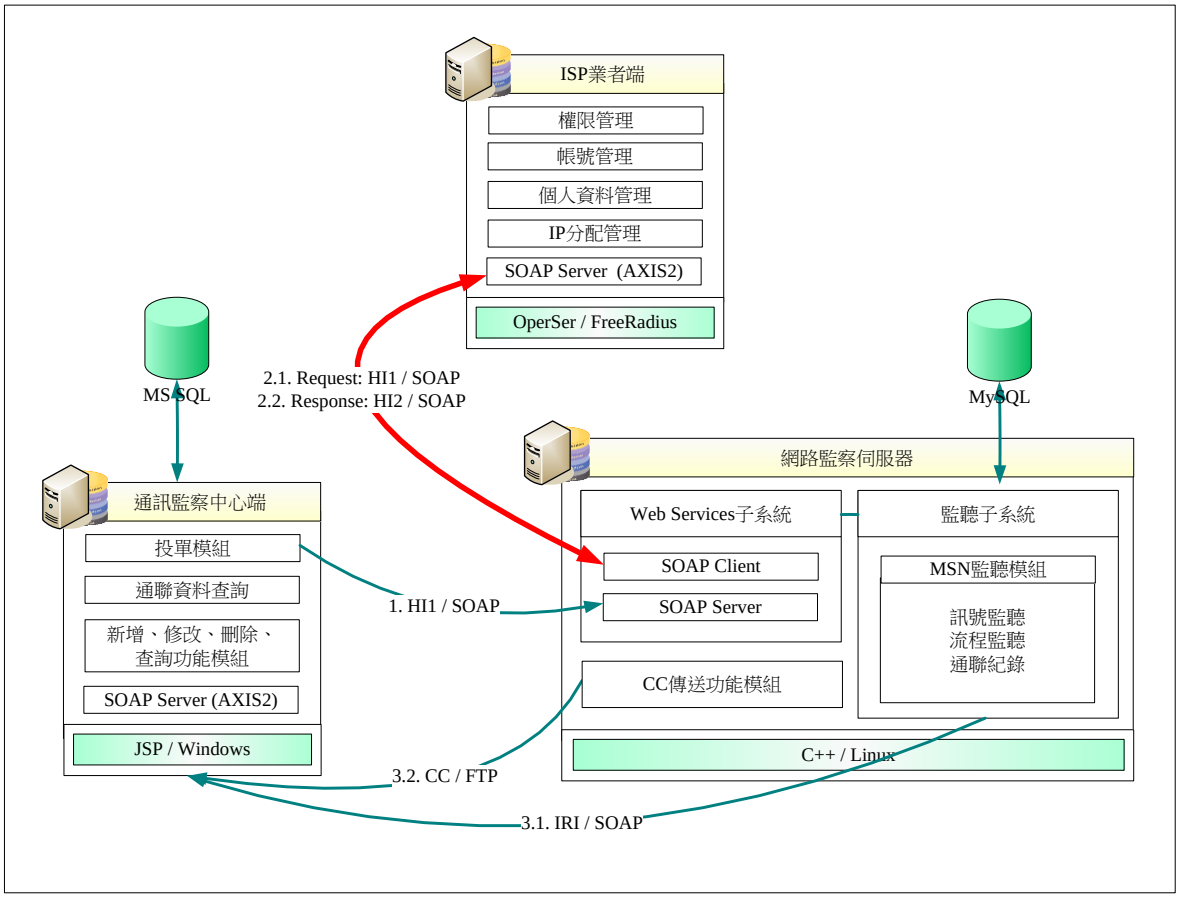

圖 1 合法監聽的即時犯罪偵測系統之系統架構圖

3. MSN Messenger 監聽

3.1 MSN 通訊機制

MSN Messenger 是一個基於 MSNP 協定的 Instant Messenger (IM)通訊系統。它提供了登錄、認證、授權的全面服務框架(Framework)。從網路拓撲(Topology)的角度來說，MSN Messenger 分為服務層、連結層和客戶層三層，客戶層的主要功能是接收用戶指令，如發出登錄請求、改變使用者狀態、發送文字訊息請求和發送檔案請求等，並 Request 給相應的伺服器群。連結層提供了一個客戶層到服務層的網路通路。

MSN 使用 TCP 傳輸協定，除了檔案傳輸和語音聊天是直接 P2P 通信之外，其他所有的情形全部透過 C/S 進行。服務層有三種類型的伺服器[4]：

(1). 派遣伺服器(Dispatch Server, DS)：DS 是使用者和伺服器建立連結的初始伺服器，它的主要功能是協商協定版本和向使用者發送可用的通知伺服器(Notification Server, NS) IP 和 Port，並且在使用者收到 NS 的 IP 及 Port 並發回確認(ACK)後，DS 切斷與使用者的連結。它的域名是 messenger.hotmail.com，標準伺服器 Port 是 1863。

(2). 通知伺服器(Notification Server, NS)：當在 MSN 會話(Session)期間時，客戶端會一直保持與 NS 連結，並且當在狀態改變時將會與 NS 進行通訊，其動作包括有登錄、改變狀態、獲取使用者列表、修改使用者訊息，發起聊天、郵件通知和退出等。而 NS 伺服器 Port 也是 1863。

(3). 中轉伺服器(Switchboard Server, SS)：SS 主要負責轉送使用者之間聊天的訊息內容。當每開一個聊天視窗時，使用者與伺服器就建立一個 TCP 連線，並且當使用者之間進行檔案傳輸或語音聊天時，將會發送系統訊息，以及建立 P2P 會話通道(可能轉為使用 UDP)。而當需要 P2P 通訊使用的 Port 由使用者自動協商決

定，如檔案傳輸通常使用 6891 Port。而 SS 伺服器 Port 也是 1863。

3.2 MSN 傳輸信令內容

要實現與 MSN 使用者的即時通訊，對 MSN 協定的解析是非常關鍵而重要的一個環節。而對於 MSN 信令的解析是十分重要的，可以透過相對應信令的解析，做出不同的處理，表 1 列出了 MSN 主要命令和說明。

以 MSN 使用者傳送訊息為例，其流程如圖 2 所示。訊息的 Payload Command 將會以 MSG 開頭，其中資料部分又分為 Header 和 Body。不同類型的訊息有不同的 Header，對即時訊息來說，比較重要的是 Content-Type 與 X-MMS-IM-Format，分別指定了訊息類型/編碼(通常是 UTF-8 編碼)與格式資訊。Body 與 Header 之間以一個空行分隔，內容是 UTF-8 編碼格式的訊息內容。例如：接收的即時訊息是以如下形式由 SB 服務器發送到本機的"網路"字串，其封包內容如圖 3 所示。關於 X-MMS-IM-Format 中的各項參數如下：

- FN=Font，字體，要經過 URL 編碼。如"網路"是 %E7%B6%B2%E8%B7%AF。
- EF=Effects，字體特效，粗體或傾斜等，每種以一個字元標識，不區分順序。
- CO=Color，顏色，16 進制 RGB 組合，如紅色是 ff0000。
- CS=Character Set，字元集，預設為 UTF-8。
- PF=Pitch and Family，與字元間距相關的一些格式設定。

3.3 訊息監控的環境部署

基於即時通訊軟體的通訊架構，要實現對即時通訊訊息的監控，對於不同網路環境，分別有不同的部署。對於集線器(Hub)連結的網路，如果機器 A 需要與其他機器進行網路通訊，A 發出資料封包會被同時複制到集線器的所有其他 Port 上。換言之，用集線器連結的網路，網路內任何一台機器均能夠"聽到"其他機器的通訊，當然也能夠將這些通訊資料封包抓取下來。所以在集線器網路中，任何一台機器均可部署，實現訊息的獲取。

交換器(Layer 3 Switch)與集線器不同在於通訊資料封包不再複製到其他所有 Port，而是精確發送到目標機器所在的 Port，其他機器就無法"聽到"這種目的性較強的通訊，因此就無法實現資料封包的抓取了。具體情況如下：

(1) 如果是透過代理伺服器(Proxy)上網，只要在代理伺服器上部署即可。

(2) 如果區域網路的 Gateway 是伺服器電腦，則可在此 Gateway 伺服器電腦上部署。

(3) 如果區域網路的 Gateway 不是伺服器電腦，而是路由器(Router)，可在交換器和路由器之間加裝一個集線器，將網管機器接在集線器上，從而在網管機器上實現部署。

(4) 對於部分可網管的交換器，可以透過對交換器的配署，對所有 Port 的資料通訊映射到某一個 Port，並在此 Port 相連的機器上部署。

3.3.1 側錄模組

在以上部署好的環境中，首先利用 Libpcap 函式庫編寫一個網路側錄程式，抓取網路資料封包。Libpcap 的英文意思是 Packet Capture library，即資料封包捕獲函數庫[5]。該函式庫提供的 C 函數介面可用於需要捕獲經過網路介面(通過將網卡設置為混雜模式，可以捕獲所有經過該介面的資料封包，目標位址不一定為本機)資料封包的系統開發上。著名的 TCPDUMP 就是在 Libpcap 的基礎上開發而成的。Libpcap 提供的介面函數主要實現和封裝了與資料包截獲有關的過程。這個函式庫為不同的平台提供了一致的程式介面，在安裝了 Libpcap 的平台上，以 Libpcap 為介面寫的程式，能夠自由的跨平台使用。在 Linux 系統下，Libpcap 可以使用 BPF (Berkeley Packet Filter)分組捕獲機制來獲得很高的性能。

3.3.2 資料重組模組

根據捕獲到的資料封包，首先將資料封包的基本協定解析出來，把從資料鏈結層抓取到的資料封包解析成協定資料的格式，分辨各個協定的標頭和負載，將不是 IP 協定的資料封包過濾掉，解析出 TCP 層的資料。由於同一個訊息 Segment 資料不一定在同一個封包(Packet)中傳輸，須進行 TCP 重組，要對同一個 TCP 連結的資料採用 Libnids 函式庫進行重組。Libnids 的主要功能包括擷取網路資料包、IP 碎片重組、TCP 資料流程重組及 Port 掃描攻擊測試和異常資料包測試等[6]。Libnids 使用了 Libpcap 捕獲資料封包的功能，可以設定過濾規則，指定捕獲感興趣的資料封包。

當封包由 Libpcap 進入，收到封包後進入 Libnids 的 ip 重組引擎，模組的 input 為 IP 結構。從 Libnids 接到 IP 封包結構之後，進行應用層的分析呼叫 process_MSNPacket 為起點作為 Libnids 的 callback function。為剖析 MSN 命令類型呼叫 analyze_packet 判斷 msn 命令類型。並轉呼叫對應的函式進行 msn 連線資訊維護。主要與測錄即時訊息的函式為 handler_msn_msg。handler_msg_joi 為 switch board 連線建立前的通知，詳細指令邏輯與背後意義可參考 MSN 協定分析的指令列表，如表 1 所示。handler_msn_msg 亦會呼叫對應的函式作 parsing 的細部內容，以將嫌疑犯的通話內容進行側錄，製成通聯紀錄匯出予通訊監察中心，流程如圖 4 所示。

表 1　MSN 主要信令一覽表[4]

命令	來源	去向	說明	備註
ACK	SS	Client	確認，做出肯定回答	acknowledgement
ADD	Client	NS	發出添加新聯絡人到列表的請求	add user
	NS	Client	返回添加新聯絡人到列表的回應	
CHG	Client	NS	發出改變狀態的請求	change state
	NS	Client	返回改變狀態的回應	
FLN	NS	Client	通知有聯絡人列表中的使用者下線	off-line
ILN	NS	Client	當使用者端登錄或添加聯絡人到列表時，通知聯絡人狀態	initial online state
LST	Client	NS	發出獲取聯絡人列表的請求	list
	NS	Client	返回獲取聯絡人列表的回應	
MSG	Client	SS	發送訊息到其他使用者(聊天對象)	message
	NS	Client	傳遞伺服器(系統)的訊息到使用者	
	SS	Client	傳遞其他使用者(聊天對象)的訊息到使用者端	
NLN	NS	Client	通知使用者端聯絡人上線或改變狀態	on-line
REA	Client	NS	發出修改使用者暱稱的請求	rename nickname
	NS	Client	返回修改使用者暱稱的回應	
VER	Client	DS	協商 MSN Messenger 協定版本	version
	Client	NS		
	DS	Client		
	NS	Client		

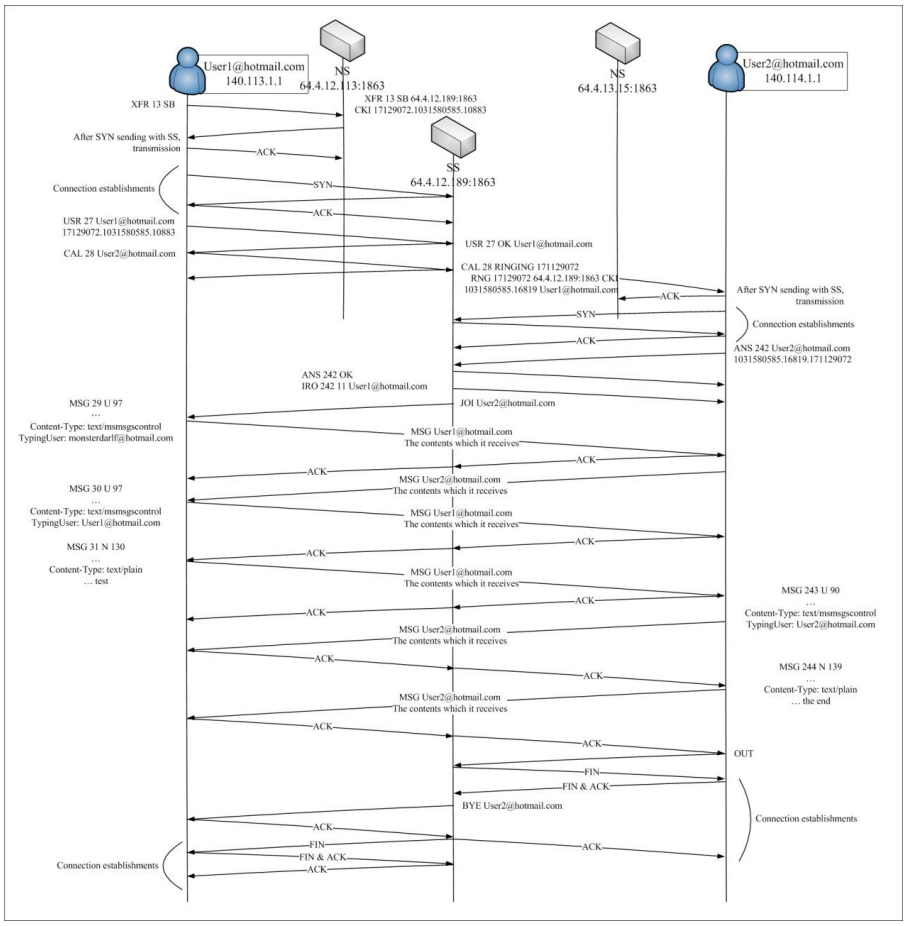

圖 2　MSN 使用者傳送訊息流程[4]

MSG SenderEmail SendName Length\r\n
MIME-Version: 1.0\r\n
Content-Type: text/plain; charset=UTF-8\r\n
X-MMS-IM-Format: FN=...; EF=...; CO=...; CS=...; PF=...\r\n
\r\n
Message

圖 3 MSN 訊息流程內容[4]

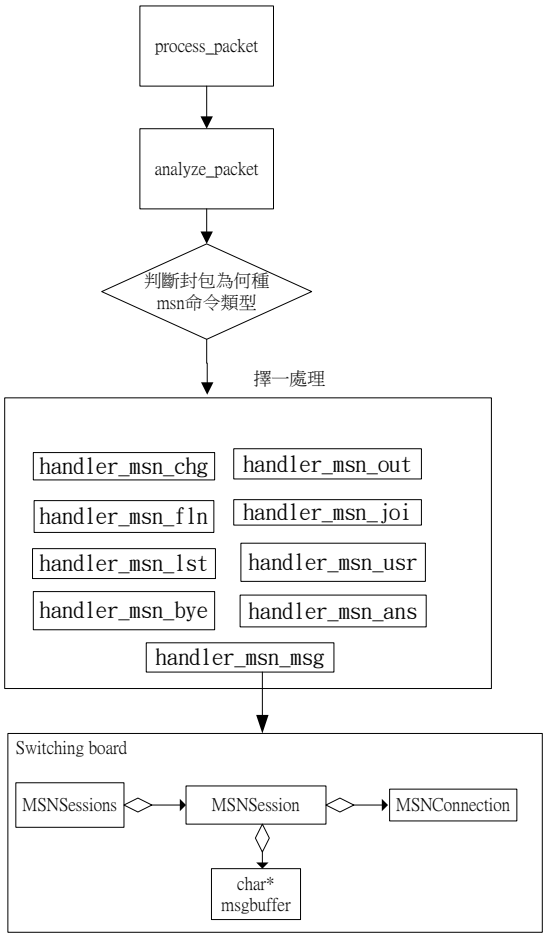

圖 4 監察模組與流程

4. 結論

本研究主要提出一套有效的合法監聽系統—實作一個基於合法監聽的即時犯罪偵測系統，主要包含有通訊監察中心端、ISP 業者端、以及網路監察伺服器，以建立合法監聽流程，並即時偵測犯罪行為的產生和儲存犯罪紀錄。並且，以 MSN Messenger 為例，描述 MSN 資料結構、訊息流程、以及監聽方式。RCDS 將可提供 MSN Messenger 犯罪偵測，有效的取得犯罪通聯紀錄，以減少未來的犯罪率。未來可考慮將此架構應用於不同的網路犯罪行為偵測上，於網路監察伺服器中加入各種網路 Protocol 之監聽與封包解析，例如：VoIP、HTTP、FTP、YMSG、Telnet、SMTP、POP3 等。

參考文獻

[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/