分散式網路事件分析紀錄系統之研製

張以磊、柯開維*、吳和庭
國立台北科技大學資訊工程學系

摘要 —本論文設計並實作一套標準化之分散式架構設計，用於網際網路上的分散式網路事件分析紀錄系統，攔截網路封包、解析網路活動並讀取封包內容進行檔案還原紀錄。

此系統由擷取紀錄子系統、資料庫子系統、分析子系統構成，透過網路連線合作達成明確的分工並可依通訊監察的需求組合出不同之監察網路，達成可彈性佈建的目標及高可擴充性及可維護性。並實作 FTP、HTTP、SIP、H.323 通訊協定分析紀錄及網路異常行為偵測之功能，驗證此系統設計的可用性。[1]

一、 緒論

近根據台灣網路資訊中心截至 101 年 3 月之最新統計結果，台灣上網人口已達 1593 萬人，隨著網路普及率和速度的提升，人們透過網路進行更多工作或日常生活上的資訊交換。在人們依賴網路作為生活上不可或缺之工具的同時，亦有眾多的犯罪行為在網路上發生，或間接由網路作為犯罪者間溝通之工具，藉由網路服務之隱匿性，取代傳統之會面、書信、電話等已有相對完善之監察機制、高暴露風險之通信方式。由此趨勢不難察覺網路通訊監察之迫切必要性。另外，公司行號、政府機關等，亦大量使用網路作為組織間通訊的媒介，基於對組織內部機敏資料的保護，亦需要一有效的網路通訊監察機制作為必要時的偵察輔助之用。

比較市面上較知名具有網路通訊監察能力之產品，Wireshark[1]雖具有豐富的協定分析之能力，但僅能針對封包做儲存，並且不是為長時間監察所設計；ClearSight Analyzer[2]功能與 Wireshark 類似，且價格昂貴；E-Detective System[3]雖具有通訊協定傳輸內容還原及長時間監察的能力，但不具有即時監聽與音傳送之功能，且價格昂貴並須要專屬硬體。

本論文以 Java 語言開發，將實作一套由擷取紀錄子系統、資料庫子系統、分析子系統構成之標準化的「分散式網路事件分析紀錄系統」。用於網際網路上的分散式網路事件分析紀錄系統，攔截網路封包、解析網路活動並讀取封包內容進行檔案還原紀錄，並實作 FTP[4]、HTTP[5]、SIP[6][7]、H.323[8][9][10]通訊協定分析紀錄及網路異常行為偵測功能，驗證此系統設計的可用性。透過網路連線合作達成明確的分工並可依通訊監察的需求組合出不同之監察網路，達成可彈性佈建的目標及高可擴充性及可維護性。

[1] 本研究由國科會贊助，計畫編號 NSC102-2218-E-027-004。

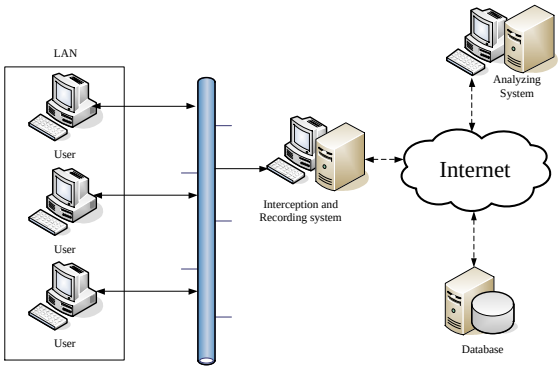
Corresponding author:kwk@csie.ntut.edu.tw
DOI:10.6159/IJSE.2014.(4-2).11

二、 分散式網路事件分析紀錄系統

本論文提出之系統主要分成資料庫系統、擷取與紀錄系統(Interception and Recording System, IRS)與分析系統(Analyzing System, AS)。確定要分析紀錄的通訊協定後，先以人工方式操作相關通訊協定，例如進行 FTP 的上傳、下載動作；接著以 Wireshark 擷取並篩選出相關封包並加以紀錄保存；觀察封包紀錄，從關聯性判斷、執行、結束判斷、結束四個階段需進行的動作，尋找封包中存在可供程式進行判斷與分析的特徵；接著使用這些特徵撰寫用以紀錄該通訊協定網路事件的程式碼；最後，透過 Colasoft Packet Builder 播放封包檔案或以手動方式再次產生網路事件，進行程式的除錯與驗證工作

2.1 系統架構

本系統主要分成資料庫子系統、擷取與紀錄子系統(Interception and Recording System, IRS)與分析子系統(Analyzing System, AS)。如圖一所示。

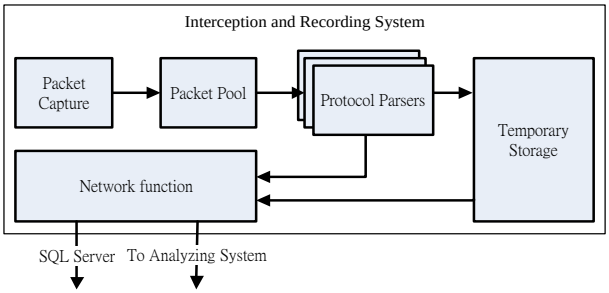


圖一：分散式網路事件分析紀錄系統架構

2.2 子系統架構

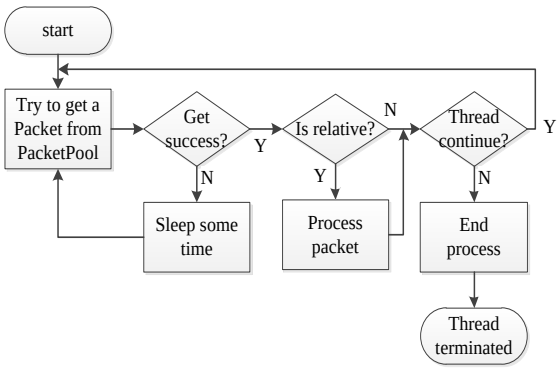
各子系統所負責功能則如下列所述。

(1) 擷取與紀錄系統：負責項目有擷取封包、判斷封包是否屬於目標通訊協定、追蹤相關連線，如 FTP 協定額外開啟之資料傳輸連線和語音通話的 RTP 連線追蹤、紀錄原始資料，即未經分析、解碼、還原，僅做初步排序與分段整理之數據串流、產生網路事件紀錄條目上傳至資料庫，以便 AS 進行查詢、接受 AS 的請求，上傳原始資料至 AS、接受 AS 的請求，即時轉送語音資料至 AS。架構如下圖二所示。



圖二：擷取與紀錄系統架構

其中，Protocol Parser 程式流程如圖三所示。



圖三：Protocol Parser 程式流程

本論文實作下列 Protocol Parser 完成網路監聽功能：

a. FTP Protocol Parser：
發現 FTP 命令連線並將連線交由 FTP Command Protocol Parser 處理。

b. FTP Command Protocol Parser：
負責對單一 FTP 命令連線的內容作解析，當發現 FTP 開啟資料連線並傳送檔案時，將資料連線交由 FTP Recorder Protocol Parser 進行紀錄。

c. FTP Recorder Protocol Parser：
對單一 FTP 資料連線進行檔案紀錄的動作。根據 FTP Command Protocol Parser 找到的 FTP 資料連線，取出每一 FTP 檔案封包之內容並加以重新排序組合成為完整的檔案。

d. HTTP Protocol Parser：
發現 HTTP 請求並將連線交由 HTTP Recorder Protocol Parser 進行整個請求及回應的紀錄。

e. HTTP Recorder Protocol Parser：
針對單一 HTTP 連線上的所有請求及回應，紀錄其標頭與訊息內容，並分別存檔紀錄。

f. RTP Protocol Parser：
負責紀錄單一 RTP 連線通訊內容，並視需求轉送由 SIP Protocol Parser 或 H.323 Protocol Parser 偵測，並經 AS 指定欲及時監聽之特定 RTP 連線之封包至 AS 提供即時監聽。

g. SIP Protocol Parser：
追蹤 SIP 通話，確認 RTP 音訊通道後建立 RTP Protocol Parser 紀錄音訊。

h. H.323 Protocol Parser：
發現通話控制訊號並分析取得 H.245 連線交由 H.245 Protocol Parser 分析取得 RTP 語音通道。

i. H.245 Protocol Parser：
追蹤特定 H.245 連線，取得 RTP 通道交由 RTP Protocol Parser 擷取紀錄音訊內容。

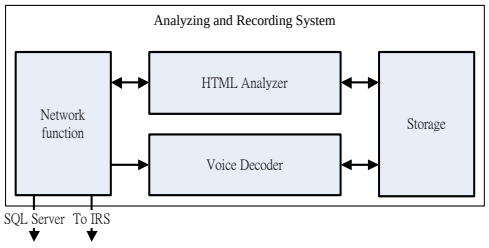
j. 而異常行為偵測則分別偵測三種異常行為，過量 Ping、ARP 欺騙、ARP 衝突及 SYN Flood 攻擊為目標 使用下列三個 Protocol Parser。

i. Ping Protocol Parser：
藉由計數每個 IP 收到 ICMP Echo request 封包的次數偵測 ICMP Ping 異常。

ii. ARP Protocol Parser：
透過追蹤 ARP 封包、建立 ARP 表格及計數各網路位置的 ARP 請求、回應封包數量偵測 ARP 欺騙及 IP 衝突。

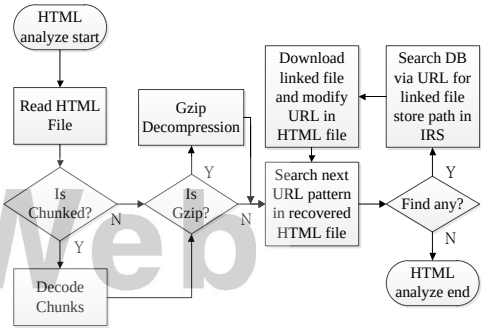
iii. SYN Protocol Parser：
透過計數各網路位置到的 SYN 封包及完成 TCP 三向交握的數量偵測 SYN flood。

(2) 分析系統：提供功能有連結資料庫取得網路事件紀錄條目、整理條目呈現給使用者，並提供數種呈現及查詢方式供使用者使用、從 IRS 下載原始資料並還原為檔案、網頁還原功能、語音數據串流解碼功能、即時解碼及播放 IRS 轉送之語音原始資料。架構如圖四所示。



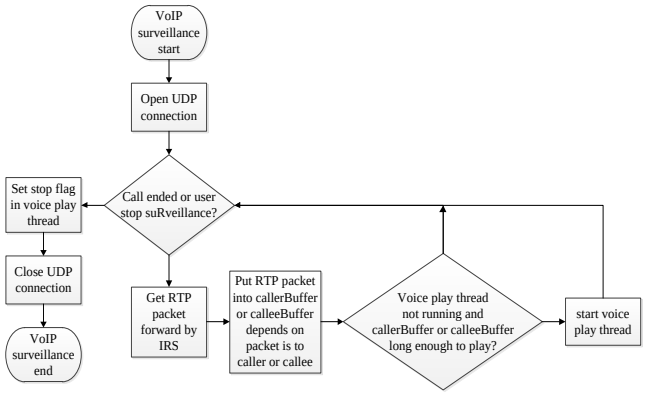
圖四：擷取與紀錄系統架構

下圖五、圖六為 HTML 分析還原流程及即時語音監聽流程。



圖五：HTML 分析還原流程

整個實作系統中資料庫系統須有能夠接受 IRS 及 AS 連線的網路存取能力；IRS 需要安裝有 Java 執行環境 (Java Runtime Environment, JRE)、Jpcap 及 WinPcap 或 libpcap，並有連線至資料庫系統及接受 AS 連線之網路存取能力的主機；AS 則僅需安裝有 JRE 及具連線至資料庫系統及 IRS 之網路存取能力的主機即可。本論文考量整體系統以 Java 語言開發，選擇了對 Java 相容性相當高的 MySQL Database Server，做為儲存網路事件紀錄、各 IRS 名稱-IP 位置對應及服務狀態等資訊的儲存體。



圖六：即時語音監聽流程

2.3 系統實作與開發環境

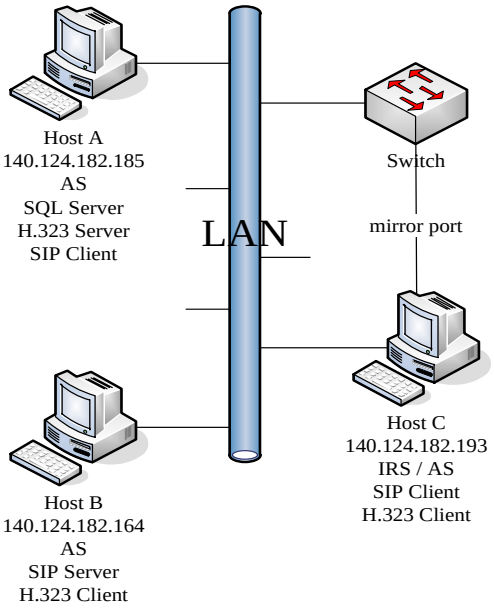
表 I
系統開發環境與工具

Language Platform	Java 6 update 45
Database Server	MySQL v5.6
Operating System	Windows 7
Develop tools	Jpcap 0.7 WinPcap 4.1.3(Win series) or libpcap 1.3.0(Unix-like)

三、系統運作與分析

3.1 系統運作環境

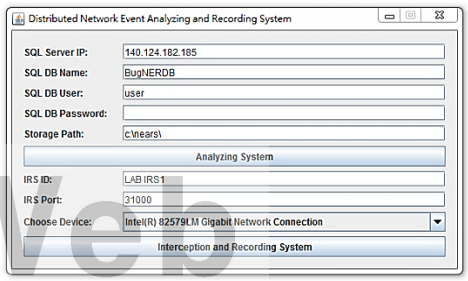
圖七為本系統在實體網路上的運作環境，在實驗室區網內，由主機 A、B 及其它實驗室電腦做為被監查之對象，主機 C 執行 IRS，並安裝兩張網路卡，其中一張用來存取網際網路，另一張則配合使用交換器(Switch)之 Mirror port 功能，將所有通過交換器之封包轉發至主機 C 進行監察。資料庫系統則由 A 主機執行，而 AS 可執行於任意執行於裝有 JRE 的系統。網路電話環境則使用三台電腦扮演網路電話之伺服器與發受話端，其中相同協定之網路電話，因為伺服器與發受話端在同一主機上執行會造成網路電話無法正確運作(port 衝突及無法正確進行通話允許等)，故相同協定之網路電話伺服器與發受話端必須放置於不同主機，本測試環境以 A 主機執行 H.323 伺服器及 SIP 客戶端而 B 主機執行 SIP 伺服器及 H.323 客戶端，為了節省使用電腦的數量，兩種網路電話之另一客戶端由執行 IRS 的 C 主機執行。非網路電話之通訊協定流量(FTP、HTTP、異常行為封包)，則由此網路內任意主機產生並透過 Mirror port 轉發至主機 C 進行監察統。



圖七：系統運作環境

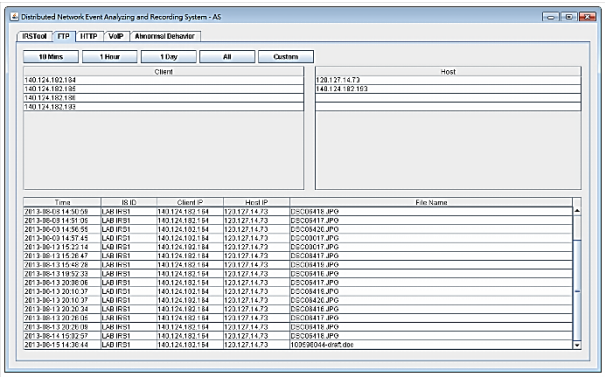
3.2 系統操作

當系統啟動後，使用者可以看到如圖八所示之系統啟動畫面，需輸入資料庫系統的 IP 位置、資料庫名稱、帳號及密碼讓系統可以正確從曲資料庫系統以寫入紀錄條目或從資料庫系統讀取需要的資訊，另外需輸入讓系統用來儲存資料的檔案系統路徑，若要啟動 IRS 系統則須輸入 IRS 系統使用的 ID 及用以接收 AS 命令之 port 號並選擇擷取介面，而 Analyzing System 及 Interception and Recording System 兩按鈕則分別可以啟動 IRS 進行截取或啟動 AS 進行監察資料的調閱及分析還原。

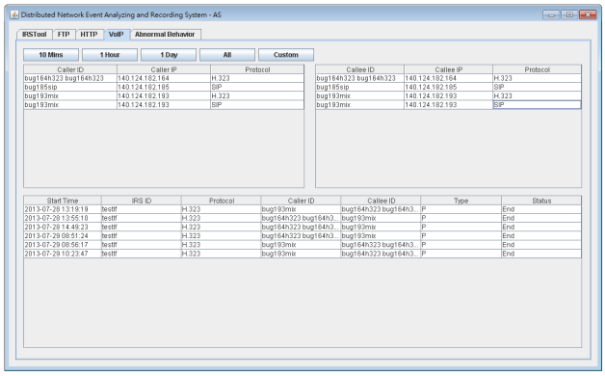


圖八：系統初始化設定

當按下 IRS 按鈕後，系統即開啟 IRS 開始擷取網路封包進行分析、追蹤及紀錄的動作。而按下 AS 按鈕後，系統則會開啟 AS 提供使用者查看事件紀錄及還原通訊內容之功能，圖九是以 FTP 為例的事件瀏覽功能畫面，圖十則是 VoIP 事件瀏覽功能畫面。



圖九：FTP 事件瀏覽功能畫面



圖十：VoIP 事件瀏覽功能畫面

3.3 系統特色與類似系統之比較

本系統相關技術特色，包含了使用 Java 開發具跨平台特性、以分散式架構增加監察網路佈建之靈活性、具備 SIP、H.323 網路電話之即時監聽功能及 FTP 傳輸檔案還原和 HTTP 頁面重現功能。表 II 為本論文實作系統與其它市面上較常見、功能類似之商業化系統及開放原始碼系統作比較。

表 II
類似系統比較表

	本系統	Wireshark	ClearSight Analyzer
系統特性比較			
使用者介面	簡易	複雜	複雜
開放原始碼	是	是	否
擴充性	易	易	不易
價格	開放原始碼	開放原始碼	昂貴
系統功能比較			
分散式架構	有	無	無
FTP 檔案側錄	完整檔案還原	只儲存封包	只儲存封包
HTTP 頁面側錄	重現存取時畫面	只儲存封包	只儲存封包
VoIP 即時監聽	有	無	無
異常行為偵測	有	無	無
可分析之協定	較少	多	多
適合長時間監察	適合	不適合	不適合

四、結論

本本論文設計並實作一具有高佈建靈活性與高協定可擴充性之分散式網路事件分析紀錄系統。

在靈活佈建方面，擷取與紀錄子系統負責擷取封包、通訊協定連線追蹤與儲存原始資料；分析子系統負責整理並呈現網路事件紀錄於使用者，並根據使用者需求調閱、解析、還原原始資料；資料庫子系統負責網路事件條目之紀錄與查詢動作，並紀錄系統成員的網路位置與服務狀態。三種子系統可依需求以不同數量、不同位置互相搭配，形成多變的網路事件監測網，合作完成網路事件之監聽、協定分析、資料還原與紀錄工作。

在可擴充性方面，本論文設計一標準化四階段之流程對通訊協定進行分析，並依此分析流程對 FTP、HTTP、SIP、H.323 通訊協定及網路異常行為進行分析並實作個通訊協定之協定分析程式，證明本系統可以依據需求透過標準化流程對各種不同通訊協定進行分析與擴充。

本論文以 Java 語言配合 Jpcap 函式庫實作前述系統設計以證明其可用性，實作完成之系統具有 FTP 檔案還原、HTTP 網頁還原、SIP、H.323 通話還原之能力，並且能透過使用者介面以數種方式供使用者作友善之搜尋及操作。最後以真實實驗室網路環境長時間監測及透過 Colasoft Packet Builder 大量產生網路事件測試系統，證明其具有長時間運作及應付瞬間大流量之穩定性。

五、參考文獻

[1] Wireshark, URL: http://www.wireshark.org
[2] ClearSight Analyzer, URL: http://www.flukenetworks.com/enterprise-network/network-monitoring/ClearSight-Analyzer
[3] E-Detective, URL: http://www.internet-recordor.com.tw/internet-recordor/Wired%20System%20App.html
[4] J. Postel, and J. Reynolds, "File transfer protocol," Internet Engineering Task Force, RFC 959, October 1985.
[5] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," Internet Engineering Task Force, RFC 2616, June 1999.
[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP:Session Initiation Protocol," Internet Engineering Task Force, RFC 3261, June 2002.
[7] 王謙志著，「以 SIP Phone 為基礎之跨平台側錄監聽與分析系統」，碩士論文，國立台北科技大學資訊工程系碩士班，台北，2010。
[8] International Telecommunication Union, "Packet-based Multimedia Communications Systems," Recommendation H.323, Telecommunication Standardization Sector of ITU, December 2009.
[9] 黃威穎著，「H.323 網路電話音訊監控與錄製系統之研製」，碩士論文，國立台北科技大學資訊工程系碩士班，台北，2008。
[10] 蔡家瑞著，「客製化 H.323 協定之至慧型網路電話監控語錄音系統」，碩士論文，國立台北科技大學資訊工程系碩士班，台北，2009。