MSN 應用感知會談鑑識系統之設計與實作

蘇暉凱*、胡勝雄、黃國城
國立虎尾科技大學電機工程系
hksu@nfu.edu.tw*

摘要 — 網際網路應用大多數以會談 (Session) 爲基礎，在資料通訊之前先建立會談關係，之後再實際交換使用者資料；大部分會談應用的特性都是在通訊期間才決定動態資料通道，因此已經無法從單純的網路層與傳輸層標頭資訊來判斷網路封包類別。本論文研究與設計 MSN 應用感知會談鑑識系統，以應用感知關鍵技術，追蹤與記錄使用者會談狀態與行爲，以提供網路安全鑑識與網路安全決策的重要參考資料。

關鍵詞：MSN、應用感知、網路鑑識、會談分類、網路安全。

一、 前言

隨著網際網路的普及，網際網路應用服務成長快速且多樣化；然而，網際網路應用大部分皆以會談(Session)爲基礎，在資料通訊之前先建立會談關係，最後再實際交換使用者資料。從早期傳統 Client/Server 應用，延伸至點對點 (Peer-to-Peer) 與點對多點 (Point-to-Multipoint)，如：Client/Server FTP、點對點 SIP Phone 與點對多點都是以會談方式進行 IPTV 等網際網路應用。然而，大部分會談應用的特性都是在通訊期間才決定動態資料通道 (Date Channel)，因此網路封包已經無法從單純的 IP Address 與 TCP/UDP Port 來判斷網路封包類別；除此之外，使用者隨著生活或工作需要而常常更換上網地點，並且使用不同的電腦來連結網路，一旦使用者狀態改變將可能造成當前的網路安全策略失效。

因此，網路鑑識逐漸成爲目前新興的資安話題，如何追蹤與記錄使用者會談行爲，並且如何在發生安全事件後能夠快速找出問題點，這些都凸顯網路鑑識的重要性。網路鑑識不像入侵偵測一般，有所謂的特徵值來進行比對，必須藉由人的經驗再加上工具的輔助，網路鑑識不如入侵偵測般可以做事件的預防或即時防止，因爲入侵偵測有所謂特徵資料庫可以進行比對以達到即時性的防禦，而鑑識卻是沒有特徵資料庫，必須要靠事後的行爲分析來找出問題，因此鑑識的目的是針對事後的分析沒有辦法達到即時性的防禦。

本篇論文以 MSN (MicroSoft Network) Messenger 會談鑑識爲案例，研究與設計 MSN 應用感知會談鑑識系統；應用感知技術乃根據不同網際網路應用，給予不同層級之協定分析，以進行網路鑑識。本論文以 MSN 的應用感知 (Application-Aware) 關鍵技術，並且以人爲出發點，追蹤與記錄使用者友好關係與會談行爲，判斷封包傳送行爲之合法性，以及資料封包之即時性與非即時性，提供高精確之網路鑑識資料。除此之外，本論文於 IXP465 嵌入式發展平台實現 MSN 應用感知會談鑑識系統，分析應用層狀態封包，並且將分析之後的資料記錄到 MySQL 資料庫系統，作爲鑑識的重要參考資料。

[1] 本研究由國科會贊助，計畫編號 NSC-98-2218-E-150-006。

二、 背景

2.1 網路鑑識相關技術

網路鑑識是運用各種網路協定技術分析網路封包，透過收集、分析、過濾、比對等方法找出可疑的封包，或是隱藏在正常行爲模式中的異常行爲，用以察覺、預防與還原某一時間的網路行爲及內容, 以防止進一步的危害事件發生。網路鑑識工具，繼防火牆和網路入侵檢測之後，爲網路提供第三層安全保護，用以提升網路安全整體防禦能力，且提高安全管理員對網路安全警告的分析和回應能力；它同時也收集和保留所有網路原始資料，並可以進行歷史資訊檢索等功能。

一般網路鑑識基本會採用封包擷取的方式，讓所有流過的封包都完整的記錄並複份至系統，這些儲存的資料有些系統會直接進行加密並且進行雜湊的動作，這動作的目的是在於保證這些資料不會在過程中被更改或是刪除，更不會被其它人看到裡面的內容，再接下就會進行分析及檢驗的過程。

然而，網路鑑識技術目前遭受到阻礙有：(1) 高速網路的普及造成日常網路流量增加導致網路鑑識速度也必須加快，負載也相對變重；(2) 資料量大同時也意味著較長的鑑識分析時間，無法有效率的檢視出攻擊來源，資料越複雜干擾越多，非攻擊的網路資料將會增加網路鑑識的困難度；(3) 攻擊手法翻新，隱匿性攻擊將可潛伏一段時間而不被發現，因此網路鑑識機制要能夠紀錄與儲存大量的網路資料。

2.2 會談分類

一般封包分類方法可分爲兩種類型，非狀態式分類與狀態式分類。非狀態式分類典型的作法是多欄位分類 (Multi-Field Classification)，多欄位分類是根據封包的目的位址、來源位址、目的埠、來源埠和通訊協定類別等欄位來進行分類封包[6][7][8]。狀態式分類是根據封包前後關聯，進行封包分類，會談分類是狀態分類的一種。會談分類是監測控制通道 (Data channel) 而得知傳輸地址的數據通道 (Data channel)，進行該會談相關封包分類，因此，會談分類必須管理每一會談狀態，並可以準確識別出會談控制與資料所有封包[5]。

由於會談分類必須處理與管理所有會談狀態，對於骨

幹高速網路來說，可能會造成傳輸瓶頸，因此，如何運用網路結構與分類機制優化是一大課題。

2.3 MSN 協定

MSN Messenger 爲 Microsoft 所開發的一套即時通訊系統[2]，它是以 Windows Message 爲發展起點，接著在開發出大眾所知的 MSN 即時通訊，至今 MSN 已推出了多種通用版本，但是核心的控制協定是不變的。

由於 MSN Protocol 是 Microsoft 自訂且非公開化的通訊協定，因此無標準文件說明協定細部內容。MSN 是一種以即時訊息 (Instant Messaging) 爲主，多媒體加值通訊爲輔之應用服務。MSN 以 MSNP (MSN Protocol) 作爲通訊協定，並且於 MSNP15 以後，開始使用 SSO (Single Sign-On) 認證機制；MSNP 最新版本是 MSNP18，目前被使用於 Windows Live Messenger 2009 (9.0)。

MSN Messenger Protocol 的內定埠號爲 1863。首先，它會先辨別 Client 端之版本，再評估是否可以與 Server 端版本相容，經判斷後如果可以與 Server 版本相容，則會給予連結。連結成功後，MSN Messenger Protocol 會先連線至 NS (Notification Server)，此時 NS 再依據 Client 端來決定要將連線導向其地方之 SBS (Switchboard Server)，連結上 SBS 後，連線就算完成。因此，監控通訊埠 1863，並解析 MSN Messenger Protocol，我們可以得到每一個 MSN 使用者的狀態與訊息交換內容。

三、 需求分析

3.1 使用案例

圖 1 爲使用案例說明，使用者對白可分爲 MSN 使用者與網路管理者，MSN 使用者需先有上網行爲，才能做 MSN 應用，及上網聊天等應用；系統透過封包擷取技術將網路封包複份至 MSN 應用感知會談鑑識系統，以供網路管理者處理 MSN 協定分析與狀態記錄。

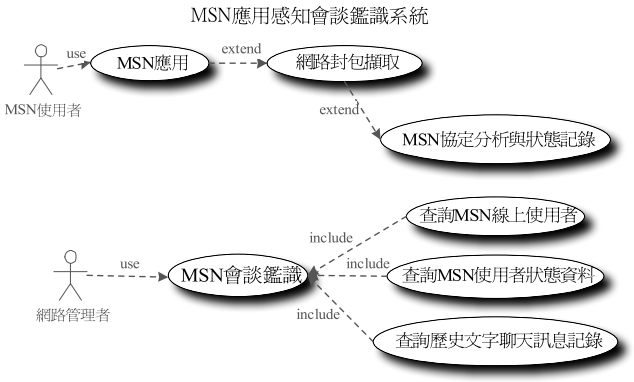

圖1 使用者操作介面

網路管理者可藉由 MSN 協定分析與狀態記錄作爲 MSN 會談鑑識，可由查詢線上使用者列表查詢使用者登錄資料，如：何時上線、暱稱、國家等；同時，管理者可藉由使用者狀態資料查詢使用者登錄情形、IP 位址、及上線狀態等，也可以查詢使用者狀態記錄，如：爲線上、忙碌、離開等等，可藉此確認在線與離線之清單，此外，還可以好友列表，觀察使用者好友關係、登錄情形等，還可以查詢好友狀態記錄，觀察使用者的好友狀態變更情形；資料查詢可提供管理者查詢使用者過去的一些會談記錄等。

3.2 功能需求

3.2.1 使用者介面需求

本系統使用者介面範本如圖 2 所示，使用對象爲網路管理者，網路管理者可以透過使用者介面範本來查詢關於網路使用者的 MSN 應用資料，資料包括：

1. 線上使用者：可以查詢線上使用者與好友的關係及使用者的暱稱、IP 位址等。
2. 使用者狀態資料：可提供查詢使用者的好友狀態變更情形。
3. 歷史訊息紀錄：可提供使用者過去的一些會談紀錄等。

圖2 使用者介面範本

3.2.2 系統功能性需求

爲了滿足網路鑑識需求，本論文規劃以下功能性需求：

1. 封包監聽器：
   a. 擷取特定介面進出的封包 。
   b. 具封包偵測功能。
2. 會談分類：
   a. 根據 IP 與 TCP/IP 資料，分類出特定類別之封包。
   b. 丟棄非特定類別之封包。
3. 會談協定分析器：
   a. 具分析 MSN 封包之功能。
   b. 具管理封包資料的功能。
4. 會談管理：
   a. 管理使用者會談資料。
   b. 儲存使用者會談資料至資料庫系統。
5. 資料收集：
   a. 儲存使用者通訊或語音之資料。
   b. 儲存 MySQL 資料庫系統資料。

3.2.3 系統非功能性需求

本系統爲符合在小型企業網路或家庭網路實際應用，所以定義以下非功能性需求：

1. 系統資料準確率必須達到 99%以上。
2. MSN 協定分析時間必須小於 10 毫秒，平均每秒處理 100 以上個 MSN 封包，以滿足家庭網路與小型企業網路需求。

四、 系統架構

圖 3 爲 MSN 應用感知會談鑑識系統環境圖，MSN 使用者位於區域性企業網路 (Enterprise Network) 或家庭網路 (Home Network)，MSN 應用感知會談鑑識系統 (MSN Session Forensic System) 可以佈置於企業/家庭閘道器對外出口之網路設備；企業閘道器除了轉送網路封包外，必須分析所有 MSN 相關封包，並且將分析結果儲存於 MSN 應用感知會談鑑識系統資料庫，提供網管人員進行鑑識作業。

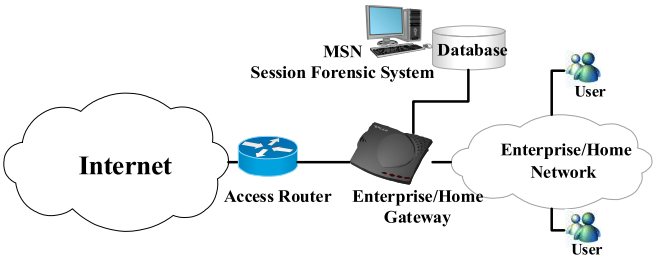

圖3 MSN 應用感知會談鑑識系統架構圖

MSN 應用感知會談鑑識系統是一種狀態式 (Stateful) 封包分析器，在不影響正常封包傳送的情況下，依應用類別分析與管理每一會談狀態 (Session State)，其中包含：

1. 註冊狀態。
2. 閒置狀態。
3. 會談初始化狀態。
4. 會談已建立狀態。
5. 會談中斷狀態。

我們將在使用者 Session 註冊過程中，擷取使用者資訊 (User Profile)，獲得使用者上線 IP Address；並且透過使用者與使用者間會談頻率，以及使用者資訊中好友清單，來定義使用者間之友好關係；在會談初始化過程中，我們將擷取會談初始化所協議出來的動態資料頻道 (Data Channel) 資訊，針對該 Data Channel 進行相關鑑識資料記錄。

在高速網路環境中，MSN 應用感知會談鑑識系統可能是整個系統的瓶頸，不當之設計將影響 Session 分析結果之準確性，反而讓系統更不安全。因此，我們規畫以高效能電腦進行 MSN 應用感知會談鑑識系統系統軟體發展；最後轉移到 IXP 465 嵌入式發展平台發展，測試與驗證系統產品化之可行性，並且針對分析效能進行最佳化設計與改善。

五、 系統元件設計

5.1 元件功能設計

圖 4 爲 MSN 應用感知會談鑑識系統功能方塊圖，元件功能包括：

1. 封包監聽器：擷取特定介面進出的封包。
2. 會談分類：依據 IP 與 TCP/UDP 資訊分類出特定封包以及丟棄非特定封包。
3. 會談協定分析器：分析並管理 MSN 封包資料之功能)。
4. 資料收集器：儲存使用者通訊資料。

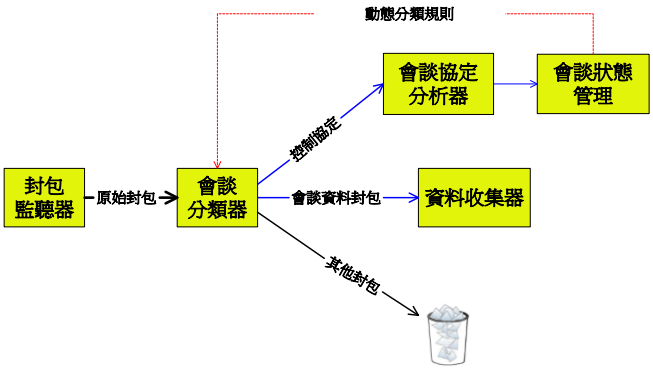

圖4 MSN 應用感知會談鑑識系統功能方塊圖

系統透過 MSN 封包監聽器擷取網路中所有 MSN 封包，並交由 MSN 會談分類，分類之後的封包由會談協定分析器分析，分析完畢後立即存入資料庫供其他元件使用。

其中 MSN 會談協定分析器分析資訊如下：

1. 使用者資訊：使用者帳號、使用者暱稱。
2. 使用者好友資訊：好友帳號、類型 (是否爲封鎖對象)、好友狀態 (上線、離線、忙碌等等)。
3. 使用者登入資訊：使用者上線時間、使用者在線時間、IP 位址。
4. 交談訊息記錄：使用者與好友之交談記錄。
5. 檔案傳遞記錄：使用者與好友之檔案傳遞記錄。
6. 多媒體訊息記錄：使用者與好友之多媒體訊息記錄（語音、視訊…等等）。

5.2 IXP 465 嵌入式開發平台設計

圖 5 爲系統軟體堆疊圖，由於 IXP 465 嵌入式系統軟硬體的限制，因此以 Embadded Linux 爲核心作業系統，進行開發 MSN 應用感知會談鑑識系統。

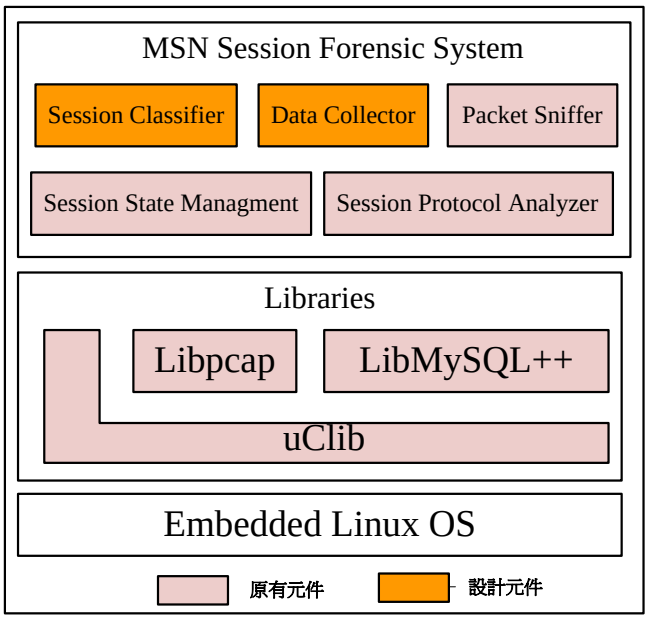

圖5 於 IXP 465 系統軟體堆疊圖

本系統使用 Open Source 「imsniff」 作爲 MSN 應用感知會談鑑識系統基礎，其中使用到 libpcap、libMySQL++ 以及 uClib 等函式庫，Packet Sniffer、Session Protocol Analyzer、Session State Management 之元件功能基本上是採用 imsniff 原始功能，本論文額外增加 Session Classifier 與 Data Collector 功能，以進行會談分類，並且利用 libMySQL++ 函式庫將鑑識相關資料儲存於 MySQL 資料庫系統。

在系統硬體平台部份，我們採用 IXP465 嵌入式開發平台，並且作爲企業網路或家庭網路對外之網際網路接取設備，如：Enterprise Gateway 或 Home Gateway。本論文將 MSN 應用感知會談鑑識系統植入 Enterprise/Home Gateway，讓網際網路存取設備具有基本 MSN 鑑識功能。

圖 6 爲 IXP 465 硬體架構圖，IXP465 嵌入式開發平台包含了許多部份，其中重要硬體元件有 XScale Core、SDRAM (128MB)、FlashRAM (64MB) 以及 NPEB (IXP0、IXP1) 乙太網路介面等。

因爲 IXP1 的 4 個 port 是利用 KS8995M Ethernet Switch 晶片串接在一起，因此可以獨立提供 Ethernet Switch 功能，Ethernet 訊框交換不會經過 CPU 處理。因此，爲實現 MSN 會談協定分類與分析，我們必須將 IXP0 與 IXP1 橋接起來 (bridge) 成 br0，作爲 MSN 應用感知會談鑑識系統之網路介面，以處理流經 IXP465 之所有封包。

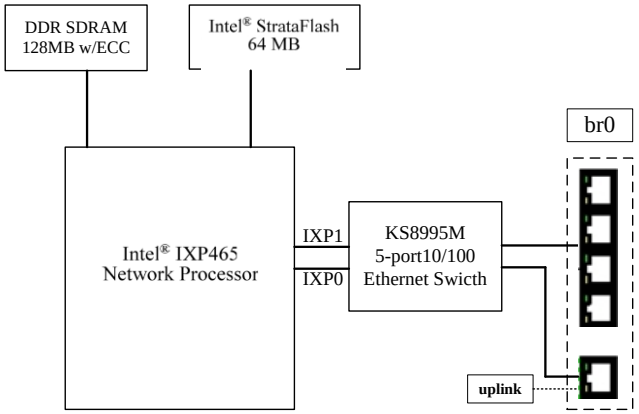

圖6 IXP 465 硬體架構圖

六、 功能驗證與結果

本章節以 MSN 訊息時序圖，說明 MSN 通訊與本系統互動關係。

6.1 MSN 登入案例

圖 7 爲 MSN 登入訊息序列圖，圖中分爲認證與狀態機換兩個流程，使用者在登入時透過 XFR 命令由通知客戶端轉向連接指定的 NS，再透過 USR 命令來鑑識使用者身分資料，與 NS 進行連接作認證動作，使用者先與 NS 協商 MSN Messenger 協議版本，發出客戶端的 OS、語言、MSN Messenger 版本等訊息，確認版本之後接下來向客戶端分配 NS，通知客戶端轉向連接指定的 NS；認證完成之後，根據 CAL 命令來建立連接聊天的請求，返回建立聊天請求的應答之後，使用者連接到 DS，由 ADL 命令爲客戶端告知 DS 會員身分資料，告知 DS 客戶端允許哪些人與之對話，哪些人當客戶端狀態改變時請 NS 也要通 知他，DS 做認證動作後確定使用者正常連線，即透過 NS 回傳給使用者，通知使用者重新連接到該 NS，並且由 UUX 命令來像 DS 設定自己的個人狀態訊息資料，接下來 DS 通知客戶端好友上現貨狀態改變，如：NLN、FLN…等狀態改變。資料包括好友資料、離線狀態訊息等。MSN 應用感知會談鑑識系統將在不影響正常封包傳送的情況下，擷取所有經過的封包至 MSN 應用感知會談鑑識系統，包括好友資料、狀態訊息等資料。

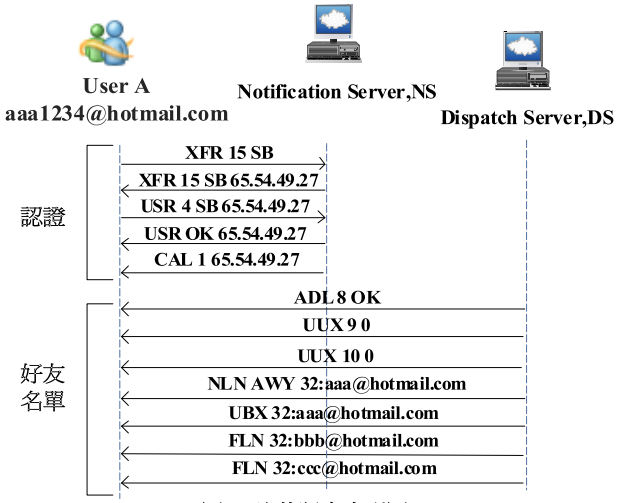

圖7 登錄訊息序列圖

6.2 文字聊天案例

圖 8 爲 MSN 聊天訊息序列圖，圖中分爲認證和訊息交換兩個流程，一般聊天時，使用者間的聊天訊息不會直接送到對方，而是先將訊息送給 SB，再由 SB 送給對方。對話開始時，使用者 A 會先跟 SB 建立聊天，透過 XFR 命令由 SB 通知客戶端轉向連接指定的 NS，接下來 SB 提供政策和機制給使用者，USR 命令來鑑識使用者身分資料，根據政策和機制與自己的密碼做認證動作；認證之後使用者根據 CAL 命令來建立連接聊天的請求，返回建立聊天請求的應答之後，聊天即成立；在不影響正常封包傳送的情況下，MSN 應用感知會談鑑識系統將擷取所有經過的封包至 MSN 應用感知會談鑑識系統，包括聊天記錄等資料。

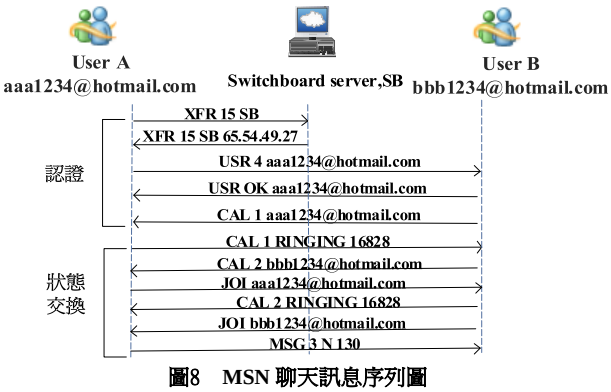

圖8 MSN 聊天訊息序列圖

6.3 實作成果

6.3.1 IXP 465 - MSN 應用感知會談鑑識系統

本論文採用個人電腦 (PC-Based Linux Bridge) 與 IXP 465 嵌入式發展平台作爲 MSN 應用感知會談鑑識系統開發平台，目前我們已於 PC-Based Linux Bridge 完成完整功能發展，並且將 MSN 應用感知會談鑑識系統植入 IXP 465 發展平台進行功能驗證與測試，如圖 9 爲 IXP 465 嵌入式發展平台發展。

圖9 IXP 465 - MSN 應用感知會談鑑識系統

6.3.2 鑑識結果

表 I
MSN 聊天訊息資料

編號	發訊者	收訊者	聊天訊息	時間
1	aa@live.com	bb@ live.com	23226Efef272i	2010-06-01 09:25:39
2	bb@ live.com	aa@ live.com	2ee2e822ul2	2010-07-10 20:40:26
3	aa@ live.com	bb@ live.com	3e115o36e87yj	2010-07-10 20:41:11
4	bb@ live.com	aa@ live.com	4e326ee54er2	2010-08-03 14:32:13

本系統建置實驗室對外網路上，MSN 使用者約 5~8 人，表 I 爲實際執行之 MSN 聊天訊息之鑑識資料，由於文字聊天內容具有個人隱私性，因此本系統將相關敏感性資料進行雜湊或加密。

除了功能性驗證外，在系統效能測試部份，本論文定義系統處理時間爲擷取到一個封包至儲存該鑑識資料到資料庫的時間，其中包含協定分析、資料處理與資料儲存時間。在個人電腦雛形平台部份，測試電腦硬體規格爲：Intel E8400 3.0GHz CPU、4GB RAM、Ubuntu 10.04 Desktop I386 作業系統，量測 100 筆 MSN 封包，平均系統處理時間爲 0. 071 毫秒 (ms)，標準差爲 0.083 毫秒 (ms)，而 IXP 465 嵌入式發展平台部分，量測 100 筆 MSN 封包，平均系統處理時間爲 4.3 毫秒 (ms)，標準差爲 2.7 毫秒 (ms)，測量結果說明，本系統符合在小型企業網路或家庭網路實際應用需求。

七、 結論

本論文設計與實作 MSN 應用感知會談鑑識系統，並且以人爲出發點，追蹤與記錄使用者友好關係與會談行爲，提供精確之網路會談應用鑑識資料。本論文完成個人電腦雛形平台與 IXP 465 嵌入式發展平台之實作，並且完成功能性測試，從個人電腦雛形平台的效能測試數據我們可以發現，MSN 應用感知會談鑑識系統可以滿足一般小型企業網路或家庭網路之網路鑑識需求；最後，此鑑識結果可以作爲阻擋攻擊行爲或進行網路安全策略制定之重要參考數據。此外，在系統資源有限的狀況下，如何進行效能優化，以因應更複雜之網路環境，將是未來可以繼續努力的方向。

參考文獻

[1] 鐘國麟, “分散式會談起始協定分析器的設計與實作(The Design and Implementation of Distributed SIP Analyzer)”, 國立中正大學碩士論文, 2004.

[2] MSN Messenger Protocol, http://en.wikipedia.org/wiki/Microsoft_Notification_Protocol.

[3] H, Sengar, D. Wijesekera, H. Wang, S. Jajodia, “VoIP Intrusion Detection Through Interacting Protocol State Machines,” International Conference on Dependable Systems and Networks (DSN 2006), pp. 393-402, 25-28 June 2006.

[4] 洪丞緯, 歐育智, 張凱翔, 蔡志汶, 蘇暉凱, "以 MSN 即時通訊朋友關係爲基礎校園網路安全監控系統之設計與實作," 2008年台灣網際網路研討會 (TANET2008), 義守大學, Oct 20-22, 2008.

[5] Hui-Kai Su, Cheng-Shong Wu and Kim-Joan Chen, "Session Classification for Traffic Aggregation," IEEE International Conference on Communications 2004 (ICC 2004), June 23, 2004.

[6] M. Uga and K. Shiomoto, “High speed policy based packet forwarding using efficient multi-dimensinal range maching,” in Proc. ACM SIGCOMM, Vancouver, Canada, Sept. 1998.

[7] P. Gupta and N. McKeown, “Algorithms for packet classification,” IEEE Network, vol. 15, pp. 24–32, March/April 2001.

[8] M. Uga and K. Shiomoto, “A modular approach to packet classification: Algorithms and results,” in Proc. INFOCOM, Israel, Mar. 2000.