VoIP攻擊分析與數位證據鑑識機制之研究

林宜隆
國立中央警察大學資訊管理學系

顏雲生
佛光大學資訊應用學系

吳柏霖
佛光大學資訊應用學系

蕭勝方
佛光大學資訊應用學系

摘要

網路電話（VoIP）具有高隱匿性、移動性、低成本性，目前已經成為詐騙集團最佳的犯罪工具之一，本文首先探討網路電話的安全威脅，再針對所有的威脅逐一分析，研究出各種威脅的因應之道，並提出網路電話數位證據鑑識標準作業程序，來解決數位證據易修改的問題，以確保原始資料及所擷取的證據之完整性。最後進行網路電話數位證據鑑識機制的驗證，以供鑑識資通犯罪人員提供未來偵查的原則、方向和準則。

關鍵字：VoIP、攻擊、數位鑑識

A Study on VoIP Attack Analysis and Digital Evidence Forensic Mechanism

I-Long Lin
Department of Information Management, National Central Police University

Yun-Sheng Yen
Department of Applied Informatics, Fo Guang University

Bo-Lin Wu
Department of Applied Informatics, Fo Guang University

Sheng-Fang Siao
Department of Applied Informatics, Fo Guang University

Abstract

The development of the Internet is fuelled by numerous commercial intentions; it is no longer simple information delivery. Moreover, many criminals try to earn profit through the Internet. Thus, the use of the internet should be under the protection of information security in order to assure honest users. The main problems today include Internet phone fraud and internet phone attacks; therefore, in addition to the analysis and management of Internet security vulnerabilities, penetration testing should be added to test the security in a practical Internet environment. This paper consults the related works of DEFSOP and correlative digital evidence from different scholars and develops a higher quality and more suitable DEFSOP. In addition, this paper discusses the security problems faced by the VoIP, lists prevention policies and designs a VoIP DEFSOP to help forensics operators. This paper shows how VoIP DEFSOP works in the operation stage through experiments in order to provide investigators with suggestions for the future.

Key words: VoIP, Attack, Digital Forensics

壹、緒論

網路電話成為“次世代電話”（next generation phone）而倍受矚目的原因，是因為網路電話不同於傳統電話的壟斷、封閉的環境。正因為如此，網路電話技術將成為未來的電話技術。然而資通訊科技（ICT, Informational Communication Technology）的快速發展為我們的生活帶來許多好處，人們為了將通訊成本降低而開始發展網路電話（VoIP, Voice over IP）（賴薇如等2007），如此新興的發展的另一面正訴說著不確定的安全性。

所以許多VoIP設備具有基於Web-based的管理功能，因此用戶（client）還必須監測（sniff）和修補（patch）基於Web-based管理功能的隱患與安全漏洞（security vulnerabilities）才能降低危險性。此外，VoIP還具有很多其他弱點和安全隱患（David et al. 2007）。因此，安全性問題（security problem）是VoIP中急需解決的關鍵問題，同時也影響VoIP的進一步發展。目前，隨著VoIP的廣泛應用，對其安全問題的研究日益受到重視。因此，應進一步加強VoIP網路安全（VoIP Network Security）研究，並結合VoIP通信應用的特點，不斷完善VoIP應用安全體系，才能使VoIP的發展再向前推進，而數位證據鑑識（digital evidence forensics）將變得特別重要。

穆齊（Antonio Meucci）自1860年發明電話（electric telephone）後，帶給人類極便利的通訊方式，隨著世界的進步、繁榮，電話成為人類生活的重要溝通工具，也因此電話衍生成為不法犯罪工具（crime tools），其中以欺騙的方式來謀取利益本文稱之為電話詐欺（phone fraud）。使用電腦及網路的犯罪者，犯罪行為不容易被發現，就算使用者發現異常，一般使用者也莫可耐何，甚至有些情況如駭客入侵盜取被害者電腦存放之資料、窺視資料夾、植入木馬程式、病毒等，被害者常已遭侵害仍不自知，此因網路做為犯罪工具具有不限時間、空間、匿名（anonymous）等特性，又使用電腦及相關設備所產生之數位資料（digital data）因其本身特性，無法簡單辨識，故確定犯罪者身份及蒐證對象為偵查此等犯罪首先面對的問題（謝開平 民92）。然而發現犯罪者並蒐集相關證據資料後，因數位資料（digital data）可以輕易的不著痕跡進行更改，且數位資料之原本不易確定，偵查機關與司法審判機關對此等數位證據應有如何之認知，如何適用證據法則，如何以數位證據（digital evidence）證明犯罪事實，因數位證據之構成涉及高度電腦技術而成為難題。

貳、文獻探討

一、VoIP簡介

VoIP的英文全名是“Voice over Internet Protocol”。VoIP是一種以IP為基底所進行的網路語音傳輸機制，因此VoIP又常被通俗地稱為“網路電話”。這是一種技術創新的通信服務業務，它把語音壓縮（voice compression）、編碼（coding）、封包分組（packet

assembly）、分配路由（routing assignment）、存儲交換（stored forward switching）、封包解壓等交換處理在網際網路上來實現語音通信（林宜隆等 2009）。促進網路資源利用，降低語音業務成本，因此VoIP在全球範圍內得到了迅速的發展，可以說是目前世界上發展最快、普及最快的一門應用服務技術之一，也是電腦網路界關注的焦點。

在網路電話和傳統電話在架構上有著明顯的不同（林宜隆等 2009），傳統電話是透過公用交換電話網（PSTN, Public Switched Telephone Network）的電路切換式網路來提供聲音，網路電話是利用閘道（Gateway）技術將語音封包透過IP網路進行傳送，並對每一個封包都進行加密（encryption）。附有目的地位址（destination address）的這些封包，到達目的地時會重組後再轉換成一般的通話聲音。

歷經五年的發展後，網路電話成為資訊技術進步帶來的一項新型電話業務在全世界發展，並對傳統電話業務形成越來越大的威脅。網路電話從當初的PC to PC發展到今天的PC to Phone、Phone to Phone等多種業務形式，但不論是現在還是將來，Phone to Phone的應用將擁有最大的市場。因此，網路電話/傳真就是通過IP網路傳送的電話/傳真業務。

二、VoIP與PSTN的使用差異

和傳統的基於電路交換機制的公眾語音通信網路（PSTN）相比，IP-based網路最大的不同是在傳輸層（fransport layer）使用了封包交換（packet-switch）的機制，由此帶來的好處是頻寬更高，頻寬的使用率（utilityrate）也更高。網路電話透過IP-based網路比透過電路切換式（circuit-switch network）網路所傳輸的資料多很多。一條傳統電話的語音頻道（voice channel）需要64Kbps，然而網路電話每一語音頻道依據使用的壓縮技術（compression technology）最多只使用10-15Kbps之頻寬（bandwidth），而且可以和其他資料共同使用同一條線路，可以降低成本及提高線路的使用率。

三、VoIP電話詐欺分析

（一）VoIP電話詐欺

VoIP電話詐欺是利用網路電話為媒介，靠著多重轉接的方式，撥打詐騙電話。可大量節省電話詐欺成本以及逃避警方追緝。VoIP電話詐欺是近年來興起的犯罪型態。電話詐欺集團也研發出更多新穎的VoIP電話多重轉接的方式，提高警方的偵辦難度。

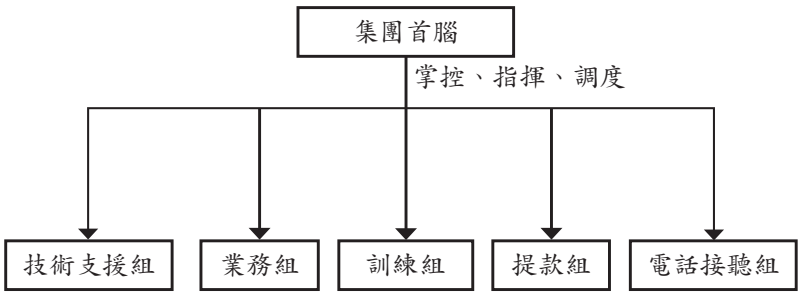
（二）VoIP電話詐欺犯罪組織結構

電話詐欺犯罪集團組織本文分析除集團首腦（chief）外主要分為五組（teams）（如圖1所示）（林宜隆等 2008）。

1. 集團首腦（Group chief）：掌控、指揮、調度各組織協調聯絡事宜，提供資金購買詐騙集團需要的設備，如手機、SIM卡、固網電話、人頭帳戶、傳真機、電腦網路等設備、租借犯罪場所、刊登報紙廣告等費用及負責分配詐欺贓款給所有詐欺集團成員。
2. 訓練組（Training）：負責新成員招募，訓練分組成為提款組、業務組、電話接聽

組、技術支援組，安排詐欺技巧訓練，編輯教戰準則、安排人員實地參與詐欺集團詐欺實務。

3. 提款組（Withdrawal）：負責在ATM附近待命，接受集團首腦電話指令負責提款。業務組負責刊登報紙或網路廣告，以收購金融帳戶或電話號碼人頭，前往銀行等金融機構申請銀行人頭帳戶，以供集團從事匯款洗錢，利用人頭門號申請手機，以供集團首腦與各組織聯絡的用途。
4. 電話接聽組（Answering）：負責第一線電話詐財的執行，要熟記詐騙教戰守則內容，每一個接聽組成員有其固定的職位姓名及專屬轉接電話，各自分工其職，記錄被害人匯款進度，匯款金額，以及匯入帳號以提供提款組成員進行領款或轉帳事宜。
5. 技術支援組（Technology Support）：負責建置多重電話轉接管道的，以避免警方追緝，維護網路電話詐騙公司軟硬體系統建置以及維護，台灣各種機房設置。
6. 業務組（Affair）：負責刊登報紙或網路廣告，以收購金融帳戶或電話號碼人頭與前往銀行等金融機構申請銀行人頭帳戶，以供集團從事匯款洗錢。



圖：VoIP電話詐欺犯罪集團組織圖

四、數位鑑識（Digital Forensics）

電腦鑑識（computer forensics）是關於如何在電腦內找到得在法庭上用以證明待證事實之證據資料之技術，電腦鑑識亦為關於電腦鑑識分析、數位證據發掘、數位資料回復、數位資料搜尋、電腦分析和檢查等工作，經由專家（expert）完整地處理、分析，重建電腦特定使用者在電腦上之歷史活動，也就是將電腦內的相關數位資料加以保存（preservation）、識別（identification）、擷取（extraction）以及文件化（documentation）之過程，透過嚴謹的鑑識程序（forensic procedure），可使數位證據具備證據能力，進而提高證據證明力。進而言之，電腦鑑識研究目的，在於避免偵查人員當面對電腦設備遭受外來惡意攻擊（malicious attack（hacker/virus）的破壞、竊取或更動電腦資料時，因為欠缺電腦鑑識之基本觀念、訓練與技術，未能遵循證物處理程序，導致所得的證據不具證據能力，並使得承審法官不願將所蒐集（acquisition）之數位證據（digital evidence）作為認定事實之依據，如此在案件偵辦上將會面臨無法補救之窘境。

換言之，電腦鑑識（computer forensics）之目的在於如何在蒐證的過程中，確保數位

證據之不可否認性（non-repudiation）與完整（integrity）性，使數位證據具有證據能力而能採為呈堂證據。

參、VoIP 安全威脅與弱點分析

一、VoIP安全議題

VoIP 和無線網路（Wireless network）技術的融合，讓廠商能以具成本效益的方式，解決與延遲（delay jitter）和即時（real-time）語音封包資料流程優先權（priority）等問題有關的服務品質（QoS）挑戰，為新型電信應用開啟了大門。這兩種核心技術的緊密結合，使得在不受網路類型或實際位置限制條件下部署可靠的點對點（point-to-point）成為可行的。不幸的是，VoIP連接也因此受到無線網路所帶來的大量安全威脅。

二、VoIP被攻擊類型

由於VoIP建立於IP-based Network之上，因此無法避免遭受來自各方的攻擊，所以本文下將針對網路電話所容易受到的攻擊行為加以分類。

（一）阻斷服務攻擊（DOS and DDOS）：是指故意的攻擊網路通訊協定的缺陷或直接耗盡被攻擊物件的資源，目的是讓目的電腦或網路無法提供正常的服務或資源訪問，使目標系統服務系統停止回應甚至崩潰。

（二）監聽和竊聽（Eavesdropping and Sniffing on Conversations）：因為攔截VoIP通信確實不難，駭客（hacker/cracker）的手段也很多，駭客必須從大量的二進位（Binary）資料中重建實際的語音通話，因此監聽VoIP通話與監聽傳統PSTN電話相比還是多了一些難度。目前網上有很多免費的駭客工具可以完成捕獲，重建和播放VoIP通話內容等全套工作。駭客可以利用這些工具不經驗證就獲取VoIP通話內容。

（三）層級間欺騙（Spoofing on Different Layers）：在不同的網路傳輸層級中實施欺騙

（四）中間人攻擊（Man-in-the-middle attack, MITM）：在通訊過程中實施攻擊，將通話攔截、阻絕、篡改或竊聽。

（五）連線截取（Session Hijacking）：這是一種在入侵者（intruder）當使用者登入（login）主機完成後，進行連線截取，讓合法者與主機斷線，由入侵者取代之。如此，入侵者不必破解密碼就可登入主機。

（六）改變聲音的流向：這是一種，在二個對話中的人，做中間人攻擊，也就是收話者聽到的不是發話者的內容，而是其他內容，但由於人類對話的無法預性，所以發生機率比較小，但有一種例外，例如：只需要回答yes或no的這種問題，就可以很容易的成功。

（七）盜取通信費：這種盜取通信費的方法有二種，第一種是讓一支電話打很多次到付費開頭的號碼，產生高話費。第二種是，攻擊者仿造一支電話，欺騙電話系統，讓電話系統認為攻擊者是是合法的的電話。

（八）帳單數據運用：攻擊者可以利用帳單資料來分析出一些資訊。例如：一家公司的執行者打電話給另一家公司的執行者，攻擊者可以分析二家公司是否要合併。攻擊者若有能力更改帳單資料，那麼他就可以避免支付帳單，或是其他更嚴重的犯罪行為。

肆、VoIP數位證據鑑識標準作業程序（VoIP DEFSOP）

一、數位鑑識計算（Digital Forensic Computing）

數位鑑識計算（digital forensic computing）是一門能夠幫助解決資通安全事件或資通犯罪中數位證據難題的科學。故「數位鑑識科學」其定義為（林宜隆等 2002）：「以周延的方法及程序保存、識別、抽取、記載及解讀電腦及網路系統媒體證據與分析其所成之科學」。而澳州數位鑑識專家Jill Slay（2007）在cyberspace 2007研討會演講中，提出了4P's模型，分別是以傳統資通訊安全相關的Prevnetion-預防、Protection-防護和與數位鑑識相關的Preservation-保全、Presentation-呈現等四個構面，由黃志龍（2006）提出的數位證據鑑識標準作業程序（Digital Evidence Forensics Standard Operating Procedure, DEFSOP ）包括概念階段、準備階段、操作階段、報告階段與澳州數位鑑識專家Jill Slay結合，如圖2所示，四階段分析如下（林宜隆&藍添興民2003; 黃志龍民2006）：

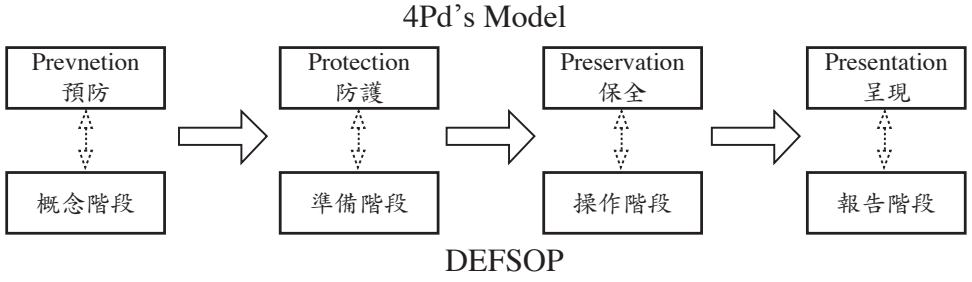


圖2：4P's model與DEFSOP之對應關係圖

（一）概念階段

數位證據（digital evidence）的取得要遵循合法、真實的原則，當事人不得以非法侵入他人電腦資訊系統的方法獲取證據；證據取得的途徑必須以立法的形式規定取得數位證據的程序及許可權如。主要原則有以下七點（林宜隆&藍添興民2003；藍添興2003）：

1. 儘早蒐集證據，並保證其沒有受到任何破壞，即在處理時，必須確保電腦或其它儲存媒體上的資料保持在原始的狀態，內容不得修改。
2. 必須保證「證據的連續性」，即在證據被正式提交給法庭時，必須能夠說明在證據從最初的獲取狀態到法庭上出現狀態之間的任何變化，當然最好是沒有任何變化。

3. 對於數位證據的任何稽核資料、紀錄或分析的處理過程，應建立處理方法、紀錄與保留結果，就算委由公正第三方進行相同的處理程序，其所得結果應相同。
4. 在特殊情況下，如果需存取原始數位證據的資料，則必需由有能力處理的專家，進行存取的動作，並對其處理的動作予以說明及適當解釋。
5. 應當全程紀錄及拍攝蒐集、分析及鑑識等過程。
6. 存放和使用存有拷貝證據的軟碟（floppy disk）、光碟（compact disk）、磁帶（magnetic tape）、硬碟（hard disk）、隨身碟（flash disk）、儲存卡（storage card）等時應當注意安全，並遠離強磁場、水、火等，使用時應注意病毒的檢測。
7.使用證據複製品進行分析、調查及鑑識的工作。

（二）準備階段：

本階段的主要工作是做一些鑑識前的準備工作，並蒐集相關資料，是為操作階段各程序執行的預作準備，以下為其 驟（林宜隆&藍添興2003；藍添興 2003）：

1. 蒐集犯罪對象基本資料：根據犯罪的類型，並利用已掌握的情況分析可能作案的人員，若案情需要也可訪談相關人員，並規劃鑑識執行的策略。決定搜索地點、對象與時間根據犯罪的類型，並利用已掌握的情況分析可能作案人員，若案情需要也可訪談相關人員，另外再決定搜索地點、對象與時間，依據蒐集嫌犯資料後，決定搜索地點和時間。
2. 工具的準備：必需準備電腦軟硬體規格的參考手冊（manual）、犯罪工具程式的參考手冊及破解電腦。
3. 人員的專業性：對於一些鑑識工具的使用，鑑識人員必須具備專業性，也就鑑識人員應該考取相關鑑識證照或認可，才不致於在鑑識過程中遺漏寶貴的數位證據，甚至是破壞掉數位證據。
4. 技術勤前教育：在每次出任務前，必須針對鑑識人員進行進一步的說明，說明搜索任務、項目，並檢查軟硬體及工具是否準備齊全，以避免一些意外狀況發生。

（三）操作階段：

進行此一階段需小心謹慎，否則將影響法庭的判決-：

1. 蒐集程序：在蒐集資料這個階段，本文將數位資料分為三個部分，分別為變動性數位資料、固定性數位資料及檔案系統數位資料，在各個部分整理出何種數位資料該用何種工具來蒐集。
2. 分析程序：在分析資料這個階段，本文將分析資料分為五個部分，分別為檔案、記錄檔（log）、Windows登入檔、判別惡意程式碼及其他，在各個部分整理出何種數位資料該用何種工具。
3. 鑑定程序：在鑑定這個階段，本文將鑑定分為四個部分，分別為資料萃取、比對及個化、重建犯罪現場，在比對及個化整理出數位資料（digital data）該用何種工具來進行鑑識。

（四）報告階段：

法院審判需要的相關資料如下說明：

1. 撰寫及呈現：鑑識報告是必須給法官、被告及偵辦人員等相關人員閱讀，因此內容需淺顯易懂，真實呈現。原則上可提供證據的物品皆應作為呈堂證供，即具有證據能力及證明力之證物都要呈現及報告於法庭之上。
2. 驗證鑑識結果：鑑識結果的正確性，除遵守相關之原則外，其操作手冊及相關表格建立與鑑識工具的使用說明在電腦鑑識領域中是相當重要的一環。鑑識（forensic scientists）人員必須撰寫鑑識流程（forensicprocedure）及使用工具（utilities），以便日後第三人或機關檢驗或複驗以求其正確性及公信力。
3. 法庭準備：數位證據鑑識應分類、說明符合證據監管之流程，做好法庭交互結問的準備工作，以最專業及最真實的呈現給法官裁判
4. 案件建檔及學習：由於數位證據鑑識是不斷進步的科技及技術，每件案件應依案件類型分類，建立每件案件的卷宗及經驗、技術分享，最好建立專家知識庫，提供下次他人偵辦案件參考。

二、VoIP 數位證據鑑識標準作業程序（VoIP DEFSOP）

由於數位証鑑識依案件不同，所以會有不同的鑑識工具與流程，其中分別以暫時性資料與永久性資料的鑑識方式有極大差別，且在難易度與可鑑識性差異甚大，本文將針對VoIP DEFSOP中的操作階段作深入探討，在VoIP的搜集、分析、鑑定三階段過程（如圖3所示），如下說明。

（一）搜集階段：

VoIP因為有即時性的特性，所以除非VoIP的Server端與Client裝有IDS或是蜜罐（Honeypot）能夠留下攻擊記錄，攻擊記錄只能儲存在記憶體中或是暫存器，因此VoIP DEFSOP在本階段必需注重在於變動性的數位資料。蒐集程序需考量數位資料的類型並選擇適當的工具來加以蒐集，其中需特別注意到變動性數位資料有封包（packets）的來源網路位址（source IP）與目地網路位址（destination IP）、封包類型、封包內容、網域名稱（domain name）等，而固定性數位資料有要求輸入帳號與密碼。

（二）分析階段：

駭客對電腦產生的所有行為都會存在硬碟和記憶體，所以鑑識就是要找出駭客所留下來的痕跡，但由於VoIP在網路上傳送資料有即時性的特性，駭客不會在硬碟上留下資料，也不會在電腦上運行程式，因此無法在硬碟上找到VoIP運作正常與異常之間的差異性來當作證據，所以在VoIP的分析階段最佳的情況就是必需在電腦運作的情況下找出駭客攻擊的封包。但仍可分析侵入到作業系統內的（系統）記錄/稽核檔、各種日誌（系統日誌、事件日誌和安全日誌）及其他（如檔案建立時間、修改時間和存取時間，帳號登入網站之起訖時間及使用時間等遭到非法使用記錄），分析程序需針對不同資料類型選擇適當的分析工具。

（三）鑑定階段：

這個階段分別為資料萃取、比對及個化、重建犯罪現場。其中比對及個化將整理出數位資料並決定該用何種工具來進行鑑識（通常需透過重建網路電話入侵現場、重建網站伺服器漏洞等，再進一步觀察電腦使用者登入程序、身份認證程序，或是顯示出來的等訊息）。在前面的分析階段找出駭客攻擊的封包後，開始萃取封包資料，萃取的內容有封包的協定、服務類型、TTL值…等資訊，再從封包資料內容比對出攻擊樣態。

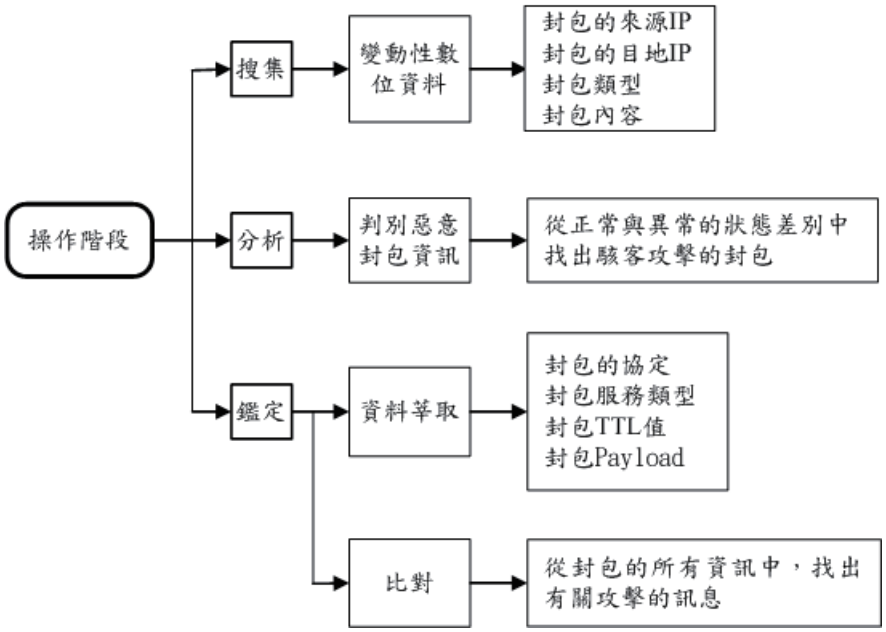


圖3：VoIP DEFSOP操作階段圖

伍、系統實作與案例驗證

一、實驗環境架構

本實驗將所有機器接在同一路由器上，並給予固定的虛擬IP位址。電腦A除了在Windows XP下安裝軟體電話外也安裝了VMware軟體來將BackTrack4建立起來。電腦B是在Windows 7下安裝軟體電話。電腦C安裝VMware軟體後，再在VMware上安裝Windows XP再安裝SIP Server（Rosenberg et al. 2002），此作法是因為VMware有容易複製的特性，所以在攻擊實驗當中若使SIP Server失靈後仍有備份可以使用。如此可以將上述三台實體電腦架構成一實驗平台如圖4所示。

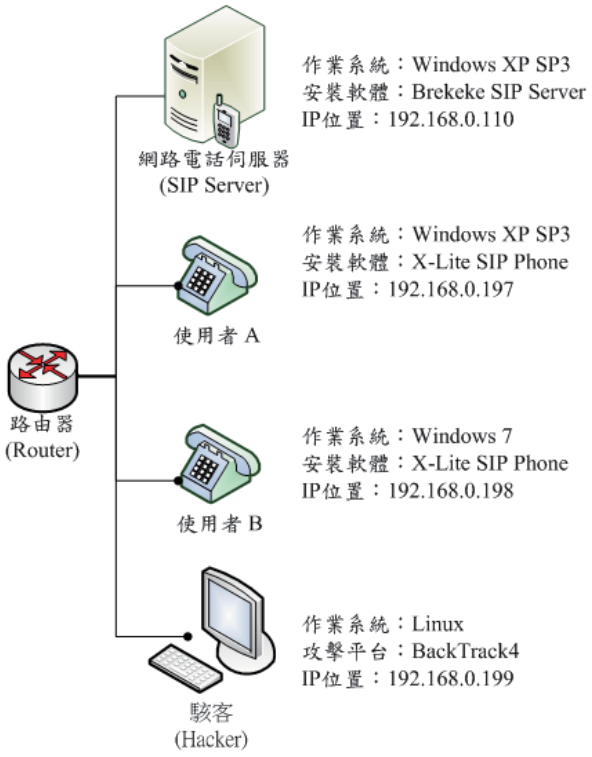


圖4：實驗環境圖

二、實驗方法與模擬案例

本實驗將驗証VoIP DEFSOP當中操作階段的蒐集、分析、鑑定，首先將SIP Server架設完成後，再安裝SIP Phone在二台電腦上，使SIP Phone能夠向SIP Server註冊並且可以相互撥打電話，再利用BrackTrack4攻擊平台向SIP Server進行攻擊。

攻擊影響分類如下：

（一）經駭客攻擊後，目標電腦無反應

經由駭客發動攻擊後，因目標電腦有防火牆或其它安全設定，使得攻擊不成功，User端與Server依然連線正常。

（二）經駭客攻擊後，目標電腦受影響不嚴重

經由駭客發動攻擊後，因攻擊設定錯誤或攻擊能量不足以影響VoIP運作。

（三）經駭客攻擊後，目標電腦受影響嚴重：

經由駭客發動攻擊後，User端與Server端會發生連線中斷與無法連線的情形，若再次要求連線時則無法連線。

本實驗以SIP Server經駭客攻擊後仍可正常運作為主要研究。其實驗步驟與程序如下所示，且因為本實驗VoIP的特性，所以只能在記憶體（RAM）中作鑑定，因此必需是在

電腦開機的情形下進行，而目前的鑑識工具絕大多數都屬於硬碟鑑定所以都不適用。而鑑識人員最重要的一件事情就是等待，蒐集需要長時間的等待，如此接下來的分析階段與鑑定階段才能夠有正確的結果。本實驗完成SIP Server建置後，使用者 A與使用者B能夠建立連線，再由hacker端對SIP Server進行buffer overflow攻擊。

模擬案例（一）：台北某科技公司員工對同業B公司進行VoIP設備進行攻擊，預備入侵同業電腦竊取商業機密，犯罪內容如下：

（1）犯罪時間：2009年1月

（2）犯罪地點：台北縣

（3）犯罪事實：○○科技公司張○○利用公司辦公處，以公司申請的網路及公司電腦下載駭客攻擊平台對同業B公司進行入侵攻擊。

（4）犯罪者剖析：①張嫌利用公司電腦及網路下載駭客攻擊平台②張嫌利用公司電腦安裝駭客攻擊平台並對同業B公司網路電話設備進行攻擊。

（5）犯罪損害：張嫌攻擊成功，但未造成損害。

（6）起訴移送：刑法第358條、第359條、第360條，妨害電腦使用罪。

（7）犯罪流程：利用BackTrack4攻擊平台畫面，以下簡稱bt4，如圖5所示為bt4攻擊模式，首先使用bt4之前必需先更新bt4攻擊資料庫來增加攻擊測試的樣本，隨後後開啟bt4的攻擊畫面。

在圖6中輸入欲攻擊的類型或協定後會出現可以攻擊的種類，接著輸入B公司SIP Server的IP位置192.168.0.110和Port 5060後送出會出現攻擊方式與攻擊目標的確認方塊，攻擊完成後會顯示目前攻擊的狀態如圖7所示攻擊第3次與攻擊的模式。

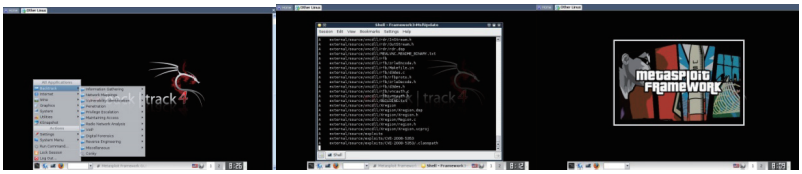


圖5：BackTrack4攻擊種類、更新攻擊資料、GUI介面攻擊模式

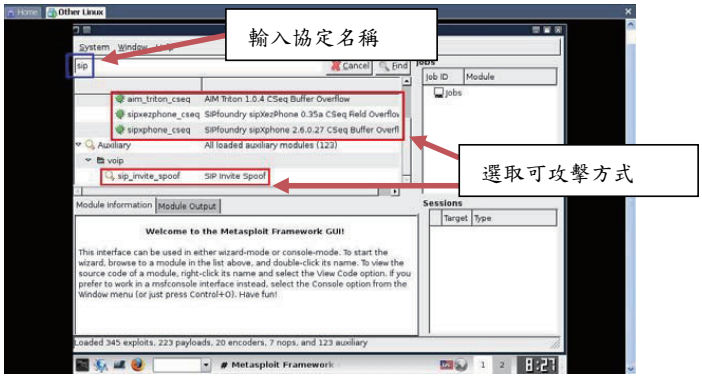


圖6：BackTrack4 GUI介面攻擊模式

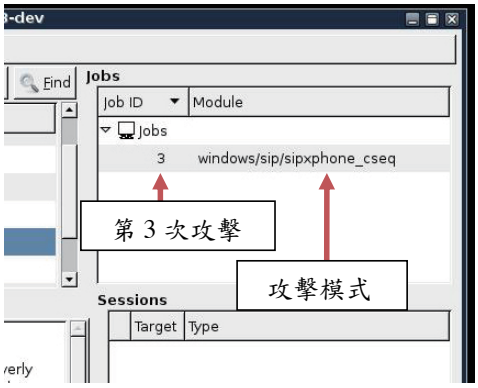


圖7：模擬案例（一）現階段攻擊狀態圖

模擬案例（二）：桃園某電信公司員工對同業B公司進行VoIP設備進行攻擊，預備癱瘓同業電信設備，犯罪內容如下：

（1）犯罪時間：2009年2月

（2）犯罪地點：桃園縣

（3）犯罪事實：○○電信公司李○○利用公司辦公處，以公司申請的網路及公司電腦下載駭客攻擊平台對同業B公司進行DOS攻擊。

（4）犯罪者剖析：①李嫌利用公司電腦及網路下載駭客攻擊平台 ②李嫌利用公司電腦安裝駭客攻擊平台並對同業B公司網路電話設備進行攻擊。

（5）犯罪損害：李嫌攻擊成功，但未造成損害。

（6）起訴移送：刑法第358條、第359條、第360條，妨害電腦使用罪。

（7）犯罪流程：如圖8所示為bt4所有攻擊模式。首先更新bt4攻擊資料庫增加攻擊測試的樣本，隨後後開啟bt4的攻擊GUI介面以利攻擊者操作。輸入欲攻擊的類型或協定後會出現可以攻擊的種類，選定攻擊方式後會出現確認方塊，在輸入B公司SIP Server的IP位置192.168.0.110和Port 5060後送出會出現攻擊方式與攻擊目標的確認方塊，攻擊完成後會顯示目前攻擊的狀態如圖9所示攻擊第50次與攻擊的模式。

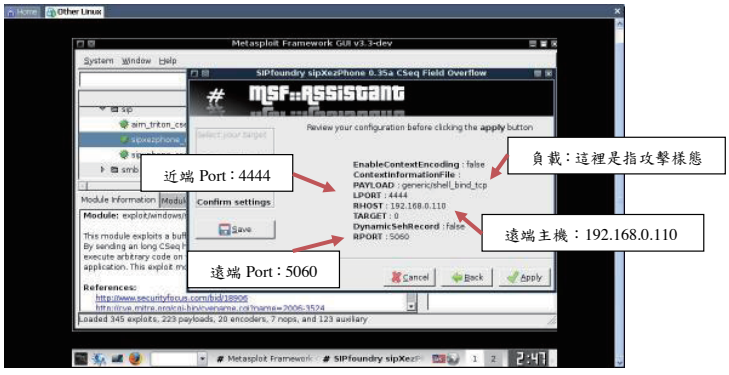


圖8：模擬案例（二）封包搜集與分析圖

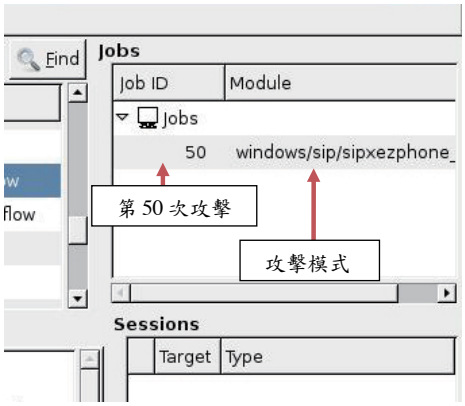


圖9：模擬案例（二） 現階段攻擊狀態圖

三、實驗結果與案例驗證

案例（一）進行案例驗証：

（1）偵查流程：①B公司定期修補VoIP軟體與作業系統漏洞時發現遭到攻擊。②鑑識人員利用鑑識工具尋找攻擊封包。③發現攻擊來源IP。④發現IP使用者。

（2）查獲贓證物：桌上型電腦、隨身碟、駭客程式

（3）鑑識流程：如圖10所示，為VoIP DEFSOP中的搜集與分析階段，在此鑑識人員用Wireshark來進行搜集封包，從圖中可以看到在最左邊的箭頭指的是欲搜集的協定，在此輸入SIP來找到有關VoIP的協定資料，而中間箭頭指的是可選取欲查看的封包，因此分析階段必需在這裡找到可能是攻擊的封包，最後在最右邊的箭頭指的是發現異常的封包，但並不一定所有的攻擊都會在此出現異常的訊息，所以鑑識人員必需逐一檢視封包內容進行分析，才不會遺漏攻擊的封包，而此異常訊息只是加速鑑識人員分析判斷。

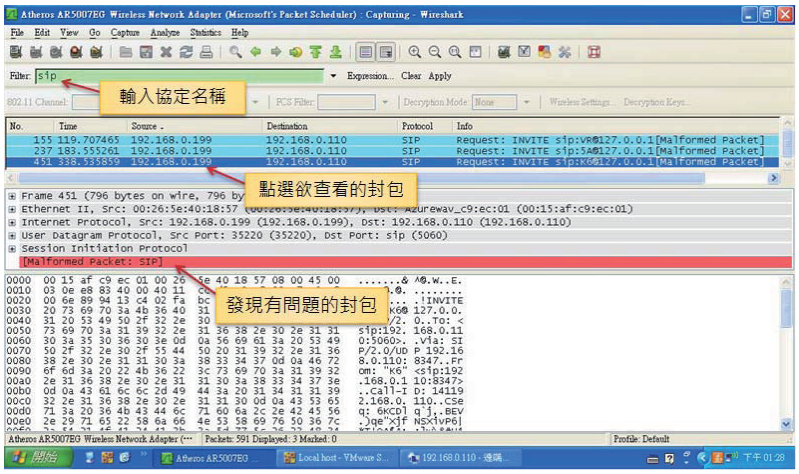


圖10：模擬案例（一）封包搜集與分析圖

如圖11所示，鑑識人員發現了這是一個緩衝區溢位（buffer overflow）攻擊，而buffer overflow就是嘗試在電腦的記憶體上加入過多的資訊，讓駭客可以在目標電腦上執行任何命令，簡單來說，程式需要回復return address，並且執行完畢後要回復到上一個呼叫的程序狀態，在這的堆疊區段中儲存了上一個呼叫這個程序的位址，在執行完畢後會將return address的值取出，並且跳回該位址，如果程式設計者在設計讀取輸入值時忽略了檢查輸入值的長度。在一般的程式設計下這些輸入的緩衝區是一個固定長度的資料，如果程式設計者不小心允許使用者輸入大於緩衝區長度的資料時，就會產生所謂的buffer overflow，當然在沒有複蓋到 return address 時倒還不至於造成嚴重的安全問題，可是問題出現在駭客可以經過一連串的設計來複蓋return address，將它指向一段惡意的程式碼。

所以鑑識人員可以從圖11第一部分中看到這是一個很大的資料，而第二部分指的就是這些資料內容是無義意的，從第三部分中可以發現buffer overflow攻擊將位址指向127.0.0.1，並且port是8374，所以鑑識人員鑑定這是一個惡意的攻擊。

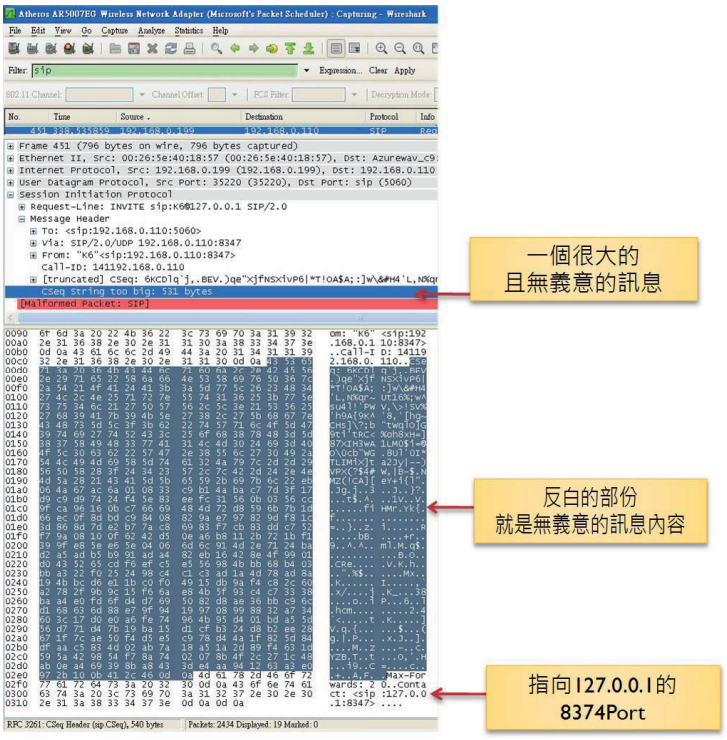


圖11：模擬案例（一）封包鑑定圖

VoIP DEFSOP 操作階段實驗結果如下並整理如圖12所示：

（1）變動性資料：

來源IP：192.168.0.199

目的IP：192.168.0.199

封包類型：SIP

（2）判別惡意封包資訊：

異常訊息：Malformed packet：SIP

（3）資料萃取：

封包的協定：SIP，RFC3261（J. Rosenberg 2002）

封包服務類型：語音

封包TTL值：64

（4）比對：

攻擊的資訊：如圖13所示

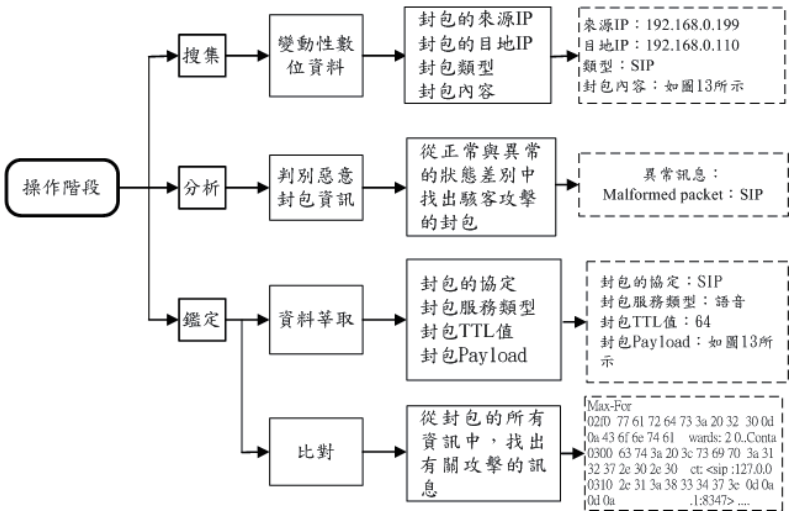


圖12：模擬案例（一）VoIP DEFSOP操作階段結果圖

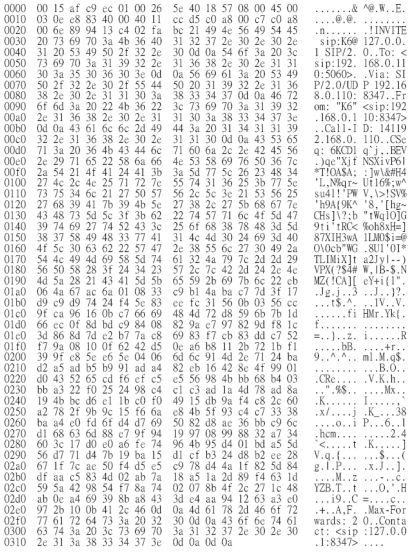


圖13：模擬案例（一）攻擊封包全部內容圖

案例（二）進行案例驗証：

（1）偵查流程：①B公司發現遭到攻擊。②鑑識人員利用鑑識工具尋找攻擊封包。③發現攻擊來源IP。④發現IP使用者。

（2）查獲贓證物：桌上型電腦、隨身碟、駭客程式

（3）鑑識流程：如圖14所示，在此鑑識人員使用Wireshark輸入SIP通訊協定來找到有關VoIP的協定資料進行搜集封包，模擬案例（二）發現為數不少的異常封包，但並不一定所有的攻擊都會在此出現異常的訊息，所以鑑識人員必需逐一檢視封包內容進行分析，才不會遺漏攻擊的封包，而此異常訊息只是加速鑑識人員分析判斷。

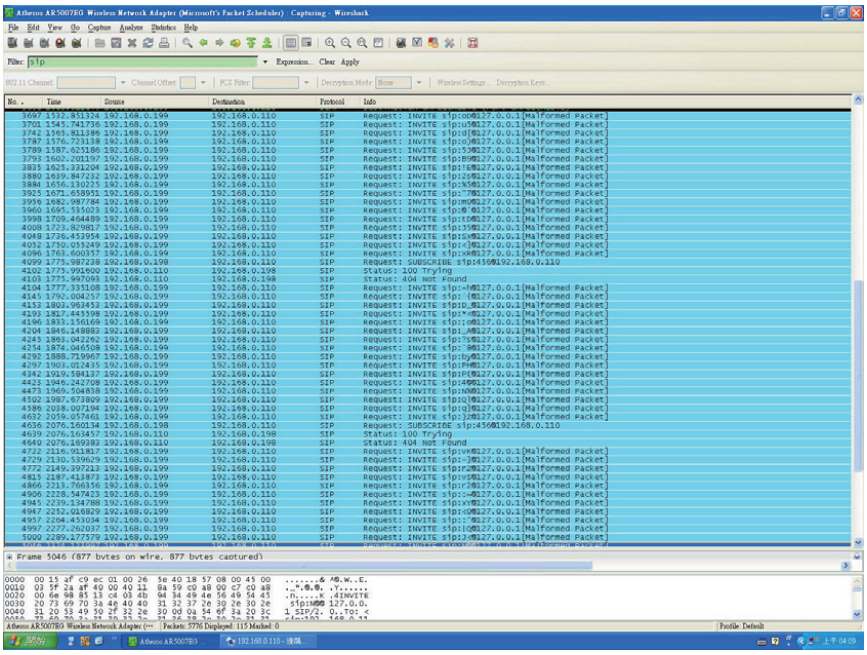


圖14：模擬案例（二）封包搜集與分析圖

鑑識人員發現了這是一個緩衝區溢位攻擊，而且有50次之多，企圖癱瘓SIP Server，如圖15所示，攻擊將位址指向127.0.0.1，並且Port是64479，所以鑑識人員鑑定這是一個惡意的攻擊。VoIP DEFSOP 操作階段實驗結果如下：

（1）變動性資料：

來源IP：192.168.0.199

目的IP：192.168.0.199

封包類型：SIP

（2）判別惡意封包資訊：

異常訊息：Malformed packet：SIP

（3）資料萃取：

封包的協定：SIP，RFC3261[52]

封包服務類型：語音

封包TTL值：64

（4）比對：

攻擊的資訊：如圖15所示

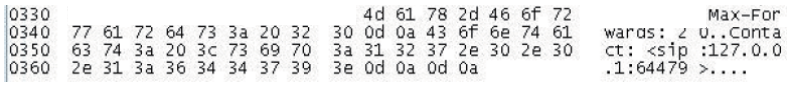


圖15：模擬案例（二）攻擊封包攻擊內容圖

陸、結論

網際網路發展至今而存在著許多商業行為，而不在只是單存的發佈資訊而以，其中還伴隨著心懷不詭的歹徒費盡心思的想在網際網路中獲得利益，所以網際網路必需是在資訊訊安全的保護之下才能夠使人們無畏的使用。數位證據需經過特殊媒介始可顯現，它可被輕易地複製、竄改，並且不易個化。因此，建立足以獲得信賴之數位鑑識程序，將是辦案人員所蒐集之數位證據能否證明待證事實之重要關鍵。目前電腦內之數位資料，都有特定資通設備可顯示資料內容，因此在資料檢視、編輯、匯出或保存上已獲得改善。電腦取證方面，網路電話都有其特定的數位證據，了解網路電話的各種可能特徵或形式後，便能進一步縮小取證的範圍。

本文參考蒐集國內、外相關學者的數位證據鑑識作業程序及規範及相關數位證據的文獻探討，並提出高品質且合宜的數位證據鑑識標準作業程序及規範。除此之外，特別針對網路電話所遭受的安全問題進行探討，並整理出網路電話的攻擊防治方法與設計網路電話數位證據鑑識標準作業程序（VoIP DEFSOP）來協助鑑識人員的需求。最後以實驗的方式說明在操作階段將如何進行，提供未來鑑識人員的一個參考方向。由於電腦科技日新月異，各式各樣的網路電話諸多犯罪型態和手法也不斷翻新，鑑識人員需經常性地加強相關的鑑識技能，才能合法而又有效地遏止不法。如果電腦使用者也能具備數位鑑識的基本知識，當遭受網路電話攻擊或詐騙時，便能發現並能保存重要數位證物，以利警方還原數位證據顯現的原始真相取得先機，作為日後指控嫌疑犯的有利證據和作為訴訟行為中的重要佐證。

參考文獻

1. 林宜隆、顏雲生、吳柏霖，2009，『VoIP安全威脅弱點分析與攻擊防治方法之初探』，資訊科技與實務研討會，銘傳大學主辦。
2. 林宜隆、顏雲生、吳柏霖，2008，『電話詐欺及網路詐欺之犯罪偵查與防制對策之

研究』，國際資訊管理學術研討會，暨南大學主辦。
3. 林宜隆、楊鴻正、王俊雄，2002，『資通安全鑑識相關技術之研究』，「網際空間：資訊、法律與社會」學術研究暨實務研討會，中央警察大學資訊管理學系。
4. 林宜隆、藍添興，2003，『數位證據蒐證程序之初探』，資訊管理學術暨警政資訊實務研討會, 中央警察大學主辦。
5. 黃志龍，2006，建構數位證據鑑識標準作業程序規範之研究，中央警察大學碩士論文。
6. 藍添興，2003，數位證據標準作業程序之研究，中央警察大學碩士論文。
7. 賴薇如、逄愛君、江為國、張林煌、陳懷恩，2007，網路電話系統與應用，台北：維科圖書有限公司。
8. 謝開平，2003，電腦詐欺在比較刑法上之研究，國立台北大學法學研究所博士論文。
9. Jill Slay，2007，『major research issues in Forensic Computing』，「網際空間：資訊、法律與社會」學術研究暨實務研討會，行政院海岸巡防署、中央警察大學、中華民國資訊管理學會共同主辦。
10. David, B., Xiangyang, L., and Jinhua, G.“Security Challenge and Defense in VoIP Infrastructures,”*IEEE Transactions on Consumer Electronics* (37:6), November 2007.
11. Rosenberg, J., Schulzrinne, H., and Camarillo, G.“SIP: Session Initiation Protocol,”*RFC3261*, June 2002.