Visiting Scholar at FSU/UF in USA

- 醞釀 -

資訊安全偵防與入侵之數位證據鑑識研究

王旭正

Visits at
1. Computer Science Department, Florida State University (**FSU**), Florida, USA

2. Computer and Information Science and Engineering Dept., University of Florida (**UF**), Florida, USA

Aug.2004- Feb. 2005

摘要

資訊安全與鑑識問題，不單單是執法機關才會面臨的問題，是整個社會都有可能面對的困擾。只不過大部分的人員(包含資訊專業人員)在面對這些問題時往往因欠缺相關常識、不知所措而隨性處理。對各大組織或執法機關而言，培養具備資訊鑑識人員的需求已刻不容緩。本進修計畫研究即是具此需求赴美進修，尋求新的思路，與了解國際的研究狀況。並進而研究更可行的解決與因應之道 。本次六個月的計畫成果豐碩，期間投諸心力，所收錄的發表研究/專題討論等資料計有 JOURNAL PAPER 二篇(SCI)， PROCEEDINGS PAPER 一篇， CONFERENCE PAPERS 四篇與二處參訪研究大學的專題研究演講報告，使得進修之目的獲得實質的效益 。未來的國外進修計畫盼能投諸更多的時間，專心研究工作，使得學/研/教/授能充分發揮與更豐富成果回饋。

關鍵字: 資訊安全，電子商務管理與安全，

電腦與網路鑑識， 數位證據 ，資訊犯罪偵查技術

第一節　背景與任務

科技發明的突飛猛進，電腦、資訊機具設備的大眾化、平價化，加上網際網路的平民化、普及化，使得大量的資訊漸漸融入於我們的生活中，在不知不覺中改變了人們原有的生活模式，這看似簡單易懂的數據〞“0”與“1”經由科技技術的演進，可存於電腦資訊設備中，傳輸於網際網路通訊設備中。一連串“0”與“1”的組合模式—數位化，亦漸漸成為現代社會訊息表達、溝通的主要方式之一。資訊化社會為人們帶來了無法想像的快速與便捷，即所謂的電子商務時代的來臨。但是，當我們在享受、應用這數以百萬計的科學家、工程師，日以繼夜所研究發明的成果時，也應該要用點心思於電腦、資訊網路環境安全維護上。因為從古自今，犯罪行為從未消失，甚而在電腦出現之後，媒體與電腦、資訊網路通信(C&C)成為人類生活的新寵，使得加諸於電腦、資訊的犯罪行為，亦因之油然而生。

資訊安全乃是指如何達到資訊的秘密性，鑑定性的科學。其運作方式乃透過密碼系統來達成並能使傳送方和接收方達到秘密分享或數位簽章的系統。因此，在一個密碼系統中，有發送方、接收方、攻擊者等三種主要的角色，發送方將訊息加密後傳送至接收方，接收方受到訊息後解密得到明文。而攻擊者則試圖在雙方傳送的過程中截取加密後的明文，利用任何方法來求取明文，或假冒發送方送一偽造訊息讓接收方誤以為真。一個密碼系統應應提供以下四項基本功能:秘密性, 鑑定性, 完整性與不可否認性等來因應攻擊與相關的資訊犯罪問題叢生。

所謂電腦、資訊犯罪可定義為凡是以電腦、資訊網路及其周邊設備為工具，從事非法之犯罪行為。在過去許多相關的文獻中亦有依法律、安全技術等觀點來探討電腦犯罪的特質、類型與手法。而在內政部警政署的電腦犯罪報告資料中亦針對電腦犯罪從偵查觀點將電腦犯罪的類型區分為電腦存取、電腦濫用、電腦盜用及電腦網路等四類型，但在這些報告中，雖對電腦資訊犯罪事件做了相當的歸納，然而在證據的探討以定位犯罪嫌疑人的涉案程度，卻仍然未有較深入的討論。資訊鑑識處理為電腦證據的保存與保護，如何在處理程序中採用合宜步驟與措施是相當的重要，而沒有經過適當訓練的世界頂級電腦專家，也可能在證據採集過程中犯下過錯，如同其他科學一樣，資訊鑑識科學亦有其專業性。在許多案件中，鑑識人員可能會漏失有效證據的採集(如取得未關機前的電腦暫存資料)，造成電磁證據的輕易流失。基於這樣的理由，處理電腦證據採集的人員必須經過妥適的訓練與培養，而電腦證據的採集過程亦需事先作一規範，以期有效保全證據。在本次的研究中 即朝向二大方向進行研究: 研究課題 I：資訊安全(Information Security)協定設計與偵防技術; 研究課題 III：電腦與網路鑑識(Computer and Network Forensics) 研究。

本報告的組織編排分別為第二節的研究成果 。第三節為專題演講與參觀訪問資料。 第四節為本次進修研究的結語。 另外，亦附錄相關的證明文件表述此行的目的與實質的收益酌予參考。

第二節 研究成果

I. "Accelerating VQ-based Codeword Search on the Basis of Partial Search Strategy," International Journal Computer Standards & Interfaces, accepted in **Dec.** 2004 and published in Vol. 28, No. 2, pp. 231-240, 2005. (SCI)

II. "Anonymous Wireless Authentication on a Portable Cellular Mobile System, IEEE Transactions on Computers, Vol. 53, No. 10, **Oct.,** pp. 1317-1329, 2004.(SCI)

III. 具角色基礎的階層式存取控制架構," Communications of the CCISA, Vol. 10, No. 4, **Oct.,** 2004.

IV. **"**Strategies to Combat the Invasion of Cyberspace from Within," presented in the Conference of Crime Investigation and Forensic Sciences, Taiwan, **Nov.** 2004.

V. "Multicasting Secret Images using a Knapsack-like Cipher System," to be presented in 17th International Conference on Computer Applications in Industry and Engineering (CAINE-2004), Orlando, Florida, USA, **Nov.** 2004. (INPEC)

VI. "Gathering Digital Evidence in Response to Information Security Incidents," studied in **Fall** 2004 and presented in IEEE International Conference on Intelligence and Security Informatics (IEEE ISI-2005),

Lecture Notes in Computer Science (LNCS), Atlanta, Georgia, USA, May, 2005. (SCI Extended)

VII. "Survey of Cyber-security and a Fundamental of Geometric Common Key Agreement in MANETs," studied in **Fall** 2004 and presented in the IASTED International Conference on Networks and Communication Systems (NCS 2006), ISBN: 0-88986-590-6, March, Thailand, 2006. (ACTA Press)

第三節 專題演講與參觀訪問

I. 吾人分別於 Oct. 1, Oct. 10, 2004 於 Computer Science Dept., Florida State University (FSU) 的資訊安全研討課程 (由 Prof. Mike Burmester 主持) 對最新的研究主題 "Authentication and Cryptography on Wireless Communication Systems," 進行共 100 分鐘的專題講演。

II. 吾人並定期至另一所研究大學, Computer and Information Science and Engineering Dept. of University of Florida (UF), 作學術 Seminar 研究討論(由 Prof. Shigang Chen 主持). 並受邀於 Nov. 1,

2004 以 FSU 的討論延伸進行共 90 分鐘的專題講演，資料形式同上。並進一步，延伸至 Ad-hoc 的安全機制與應用(酌附研究論文摘要)。

第四節 結語

在本次計劃中，前往的研究拜訪科系以 Florida State University (FSU), Computer Science Department, 為主要機構。並以 Security and Assurance in Information Technology Laboratory 為訪問之研究中心，該研究中心近年積極從事資安理論 、應用與資訊鑑識、 資安危機事件等課題上多方的研究 ， 亦為該校 Florida State University 所大力投注發展的重點。除此外， 吾人亦訪問 Computer and Information Science and Engineering Dept. of University of Florida (UF) 。 該校在資訊學門的發展為全美的重要研究大學, 藉此亦收集到完整的資料, 以利研究的進行。綜合此行的研究計畫目標皆能囊括其中， 並專心研究， 實為成功的進修經驗 。亦藉此報告的繳交， 綜合所有的進修論文的研究， 以為學界參酌。

附 錄 Ⅰ

I. Invitation letter of FSU

II. Academic certificate of Prof. Mike Burmester at FSU

III. Invitation letter of UF

IV. Academic certificate of Dr. Shigang Chen at UF

附 錄 **II**

Ⅰ. 參訪期間所發表論文， 並至二所大學 FSU 與 UF 演講資料

II. **S.J. Wang**, “Anonymous Wireless Authentication on a Portable Cellular Mobile System, IEEE Transactions on Computers, Vol. 53, No. 10, Oct., pp. 1317-1329, 2004.(SCI)