電腦、網路與行動服務安全實務

The Security of Computer · Network and Mobile Service in Practice — Applying to High-tech Society

網路時代的優勢在於知識的無界限傳遞，創造無限的想像空間與人類生活的全新商機，藉此亦改變人類原有的生活文明發展，面智慧型手機的應用越發成長，滿足使用者更多元的需求，不論網路安全亦或資訊安全的橫呼皆表示數位科技在安全的絕對必然性，因為唯有安全才能保障資料於網路傳遞的正確性，資料於數位電腦儲存的完整性，並可抵禦所有可能人為／自然的破壞，想當然爾，能夠達成安全的基礎即是密碼的理論基礎與悠久的內涵發展，在這樣的需求下，此本書的突出亦應而生，藉由安全機制的認識，才能實現PKI網路世界的人/事/物的信賴，也能享受科技帶來的高度文明成果。

本書分四大部分，「資訊安全基礎」介紹建構資訊安全與應用所需的基礎知識與概念及資訊犯罪所面對的法律規範與議題；「資訊安全應用」探討各項資訊安全設定的應用，如瀏覽、通訊以及社交網路…等廣為大眾所使用的科技應用與加強安全性；「資訊安全實務」討論目前網路安全應用與解決之道並佐以實務上的應用，如：PGP資料加密、網路安全交易SET/SSL、電腦病毒、惡駭系統安全防護、Snort與Nessus網路安全工具等，「資訊安全進階學習」則為稍較艱深、繁雜的數學公式與相關應用程式，並收錄於CD中提供讀者學習。

光碟內附 本書範例程式檔

博碩文化股份有限公司
DrMaster Press Co.,Ltd.
www.drmaster.com.tw

電腦、網路與行動服務安全實務
The Security of Computer · Network and Mobile Service in Practice — Applying to High-tech Society
王旭正、楊中皇、李榮三 著

博碩文化
EU31221

電腦、網路與行動服務安全實務
The Security of Computer · Network and Mobile Service in Practice — Applying to High-tech Society

王旭正、楊中皇、李榮三 著

作者簡介 About Writer

王旭正 *Shuh-Jeng Wang*

國立台灣大學電機工程學博士，研究興趣為資訊安全與管理、資訊鑑識與數位證據、密碼學、資料建構工程。

作者為資訊密碼與建構實驗室(Information Cryptology and Construction Lab., ICCL, http://hera.im.cpu.edu.tw)主持教授，作者定期為資訊科技類雜誌撰寫專欄(http://www.netadmin.com.tw/PCuSER)，作者並為國際訪問學者，分別於2002年、2004-2005年、2007年、2010-2011年造訪Florida State University(美,FSU)、CarnegieMellon University (美, CMU)、University of Florida (美, UF) 進行持續性學術研究工作，作者亦兼任中華民國資訊安全學會理事(2000-2012)與副理事長(JULY 2012-)，協助學會各項學術/研究/產學座務推動。

楊中皇 *Chung-Huang Yang*

美國路易斯安那大學電腦工程博士，目前為國立高雄師範大學資訊教育研究所教授兼中華民國資訊安全學會理事長，曾任國立高雄師範大學資訊教育研究所所長、國立高雄第一科技大學資訊管理系主任、中華電信研究所「資訊安全與密碼技術」計畫主持人，日本電信電話公司博士後研究員、美國RSA Data Security, Inc.軟體研發工程師。作者並分別於2001年、2004年與2006年造訪日本電信電話公司橫須賀研究中心、美國University of Louisiana at Lafayette與日本九州大學，進行國際學術交流合作。

李榮三 *Jung-San Lee*

國立中正大學資訊工程博士，研究興趣為資訊安全、密碼學、無線通訊、數位浮水印技術。作者在所屬研究領域已發表六十餘篇相關論文，於2008-2012年期間擔任電腦學刊執行編輯，並曾任電腦學刊以及資訊安全通訊客座編輯。目前為逢甲大學資訊工程學系助理教授兼研發處校務企劃組組長，同時亦擔任中華民國資訊安全學會監事。

電腦、網路與行動服務安全實務

The Security of Computer、Network and Mobile Service in Practice-

Applying to High-tech Society

王旭正 楊中皇 李榮三

目錄

- **CH11 電腦病毒**
- **CH12 網路駭客攻擊及防制策略**
- **CH13 數位鑑識**
- **CH14 網路安全綜合解決方案**

Part IV 資訊安全進階學習(收錄在 CD)

- **Ch02 密碼系統-基本數論**
- **Ch03 對稱式金鑰系統-AES 實務**
- **Ch07 資訊隱藏-NC 與 TAF 之計算**
- **程式碼**
  - **01-Ch02 密碼系統-RSA**
  - **02-Ch03 對稱式金鑰系統-AES**
  - **03-Ch03 對稱式金鑰系統-DES**
  - **04-Ch07-資訊隱藏-Visual Cryptography**

電腦、網路與行動服務安全實務

The Security of Computer、Network and Mobile Service in Practice-

Applying to High-tech Society

出版序

本書**電腦、網路與行動服務安全實務**為電腦、網際網路與行動服務安全的相關理論與實務上所涉及的概念作介紹。在本書中，共分成四大部分，「**資訊安全基礎**」、「**資訊安全應用**」與「**資訊安全實務**」，以及收錄在 CD 中的「**資訊安全進階學習**」。由最原始的安全概念直至近來 Internet 上最新主題/應用/趨勢皆囊括於其中。

在第一部分「**資訊安全基礎**」 中，說明人類秘密的根源並介紹資訊安全這門學問的基礎與發展，直至最新密碼系統(Cryptography)的發展。撰寫時，Simon Singh 的著書：The Code Book：The Science of Secrecy from Ancient Egypt to Quantum Cryptography (1999)，Rudolf Kippenhahn 的著書: The Code Breaking: A History and Exploration (1999)，與相關的附錄文獻，給了相當有趣/玩味/深入的觀點，在參閱之下亦豐富了本部分的撰寫工作。在此對於各式秘密通訊與資訊安全的研究學者/作者抱以誠摯的尊崇。這一部分我們介紹資訊安全基礎概念，使讀者能具備數與密碼學習的基礎 ，藉此得以對秘密背後所隱藏真相的探索更具備紮實基礎。密文的解析與瞭解不再是如此的陌生與遙不可及的夢，紮實的基礎不但可窺見了別人宣稱的秘密，當然也可創造/鞏固自己的秘密。

第二部分裡 我們安排「**資訊安全應用**」。內容則泛談在現代網際網路的世界中所應具備的安全概念與應用並討論諸如 IDS/IPS/HONEYPOT 的攻擊/防禦議題。藉由相關範例的導入了解密碼學不再只是理論，而是可以應用在我們生活上各個方面。並且討論在各方面的應用上，會有哪些安全性的議題以及該如何防範，如雲端、手機以及社交平台等。第二部分，我們亦介紹資訊隱藏的議題，另

類的秘密通訊。資訊隱藏早存在我們活動空間，然在近十年有了新形式的詮釋。

第三部分「**資訊安全實務**」。此部分主要討論目前網路安全實務與解決之道。有鑑於現今電腦網路使用率的普及且網路安全的相關議題日漸受到重視，因而本書介紹與大家生活息息相關實務上網路安全議題，如：PGP 資料加密、網路安全交易 SET/SSL、電腦病毒、電腦系統安全防護、Snort 與 Nessus 網路安全工具等。面臨當前多變且難以預測的資訊安全威脅，讀者可利用本部分所介紹的工具做為系統縱深防護的一部分，從而降低外來攻擊所可能造成的損失。並藉由數位鑑識來從中取得數位證據，本部分除了具體點出資訊安全相關議題的潛藏危機，亦從實務的角度解說建立資訊安全系統的防護方法與解決之道。讀者可了解安全電子交易機制、入侵偵測系統的架設、資料加密軟體的使用等實用性的防護方法，以及數位鑑識的觀念，進而提昇系統安全性，強化自我系統的防護。

第四部分「**資訊安全進階學習**」。為了方便讀者在閱讀本書時，能夠較有效率地瞭解文中所欲表達的含意。而將一些過於艱深、難懂的數學公式從書上移除。還有為了不讓整本書篇幅過多，而將一些資訊安全技術的應用與實務擷取下來。但是我們仍然認為這些資訊是對讀者有幫助的，所以將這些資料與相關加密的程式碼一起收錄在 CD 中。有意更加學習、了解這些內容的讀者可自行 DIY。

資訊科技為我們帶來更多元、更便利、更富足的社會。現在我們不單單只著眼於資訊科技會為我們帶來哪些好處，更應該要瞭解到資訊科技所引發的另類省思。由於科技進步，利用資訊科技從事犯罪的案例不斷成長。而且手法跟造成的損害也不斷精進與增加。所以資訊安全已結合資訊科技成為極重要的一環與基礎知識。

本次改版，我們將所有章節重新整合。並且因應近年來科技的發展，加入了許多相關章節。諸如雲端運算、行動裝置…等。本書章節的編撰，藉由中央警察大學數位鑑識研究工作室(ICCL, http://hera.im.cpu.edu.tw)與高雄師範大學資

訊教育研究所**楊中皇教授**與逢甲大學資訊工程學系所**李榮三教授**的研究群之合作結果。在群策群力、積極規劃與共同合作下終得呈現給讀者。也要感謝 ICCL 的伙伴/研究人員: 陳家儂、張淯閎及吳敏豪的全力參與，使得本書得以順利附梓。藉此對 ICCL 及研究群所有人員的努力表達深摯的感謝。

ICCL 網站裡(http://hera.im.cpu.edu.tw/sjw_2006/) 標以一則想法與讀者共勉-

「學習 as well as 忘」;「研究 as well as 痴」;「做事 as well as 心」;「生活 as well as 混」;

「情感 as well as 容」;「持處 as well as 后」;「成就 as well as 慟」;

玩味其間。並盼此書得以為科技發展/研究之文獻做粗淺整理，以為此相關領域的參酌。

&

ICCL –FROG

http://hera.im.cpu.edu.tw

王旭正、楊中皇、李榮三 謹識

JUNE, 2012

電腦、網路與行動服務安全實務

The Security of Computer 、Network and Mobile Service in Practice-

Applying to High-tech Society

導 讀

緣起

電腦、網路與行動服務安全實務(*The Security of Computer、Network and Mobile Service in Practice- Applying to High-tech Society*)技術的基礎是密碼學(Cryptography)。雖說密碼是一門古老的學問，然却老葉新枝地在現代科技導向的數位資訊時代迅速竄紅。在目前 PKI 時代裡，電腦、網路以及行動安全已成重點發展與必然的趨勢。網路時代的優勢在於知識的無界限傳遞，創造無限的想像空間與人類生活的全新商機，藉此亦改變人類原有的生活文明發展。而智慧型手機的應用越發成長，滿足使用者更多元的需求。不論網路安全亦或資訊安全的稱呼皆表示數位科技在安全的絕對必然性。因為唯有安全才能保障資料於網路傳遞的正確性，資料於數位電腦儲存的完整性，並可抵禦所有可能人為／自然的破壞。想當然爾，能夠達成安全的基礎即是密碼的理論基礎與悠久的內涵發展。在這樣的需求下，此本書的來由亦因應而生。藉由安全機制的認識，才能實現 PKI 網路世界的人/事/物的信賴，也能享受科技帶來的高度文明成果。

架構：

本書**電腦、網路與行動服務安全實務**共分四大部分，「**資訊安全基礎**」、「**資訊安全應用**」、「**資訊安全實務**」與、「**資訊安全進階學習**」。全文以十四章加以編寫，分別如下：

- **第一章：安全系統概論**

近二十年來藉由電子商務的掘起，世界各國家/社會/單位，諸如金融商業、網路通訊、國防軍事、 皆會受其影響而有所牽動。並引發資料在傳輸/儲存期間相關安全問題的深切思考/研究。倘使資訊安全措施出現問題使系統遭受破壞，所損失亦往往可擴至全球性的災害。許多文獻/報導的事實歷歷在眼前，由此可深刻感受**系統**安全的重要性。

- **第二章：密碼系統**

現階段的著名資訊與網路安全演算法所使用的密碼機制則大都以數論為安全理論的基礎，至今公開金鑰系統更被廣泛應用在安全上。密碼系統的運作原理及著名的演算法：DH、RSA。發展至今，亦有許多的相關的發展/延伸/變化，諸如數位簽章/橢圓曲線系統/Elgamal 系統等。以上都在本章做介紹及一密碼系統 CSP 之應用。

- **第三章：對稱式金鑰系統**

典型/傳統的密碼系統中，只有合法的發送雙方知道加/解密金鑰，此種系統稱為對稱金鑰/秘密金鑰/單一金鑰密碼系統。本章介紹對稱金鑰密碼系統與 DES 的演算機制以及其進階的加密標準 AES，並輔以實例來實際執行加/解密過程。

- **第四章：資訊犯罪與資安規範**

電腦科技的浩瀚寬廣，衍生各類犯罪行為亦相對變化莫測，資訊犯罪過程中幾乎不必花費昂貴成本，便能達到施行犯罪行為的目的，這使得面對如此低成本，破壞層度高的犯罪形式，每位電腦使用者得省思了解這種犯罪的危險性與因應之道。事實上，良好的密碼機制使用與搭配恰當的資安政策都將有利於防範資訊犯罪的持續發生。

上述四章為本書的第一部分：「資訊安全基礎」。本書在前三章，安全系統概論、密碼系統及對稱式金鑰系統，向讀者介紹建構資訊安全與應用所需的基礎知識與概念。在後續的章節，有許多的應用都是基於此三章的基礎而衍生。並且在第四

章說明資訊犯罪所面對的法律規範與議題。以較有趣的說法，前四章可謂本書之基礎建設。

- **第五章：網路安全協定**

現階段的著名資訊與網路安全演算法所使用的密碼機制則大都以數論為安全理論的基礎，尤其是公開金鑰系統。公開金鑰系統已是現在 Internet 公開金鑰基礎建設發展中的重要核心之一，值得讀者探索並加以推廣應用。

- **第六章：公開金鑰基礎建設**

公開金鑰基礎建設（Public Key Infrastructure，PKI）是由管理電子憑證的機構所組成，其中最重要的組成元素即為憑證中心。本章針對 PKI 需求、IC 卡應用方式及與政府部門在公開金鑰基礎建設上的運作加以介紹，藉以引發 PKI 注入新科技時代的必然需要。

- **第七章：資訊隱藏**

資訊隱藏其實已有數百年歷史了，但是大多在軍事通訊方面較為常見，由於近幾年電腦與網路的快速發展，網際網路幾乎成為最重要的資訊傳輸管道，而網際網路是個開放的大環境，如何在開放的網際網路中傳送機密且重要的資訊給對方，又讓別人看不出來，透過資訊隱藏即可以達到這樣的目的。

- **第八章：雲端運算安全**

近年來因網際網路及寬頻網路的普及化，推動「雲端運算」時代的來臨。雲端運算具資源整合、降低初期投資及提升效能利用率等優勢，預期未來「雲端運算」將成為產業界爭相投入發展的重要技術。然而，在發展雲端科技及創新應用之際，以「網路」為核心的雲端運算技術，同樣面臨安全性的威脅，因此，如何達成相關「安全」的目標及取得雲端使用者對於技術的信賴，將是未來雲端科技產業發展的關鍵因素。

- **第九章：行動裝置安全**

隨著手機科技的創新發展，新世代的智慧型手機不再僅侷限於通話功能，而是因

應使用者的需求趨向多元化的發展。人們對手機的依賴愈來愈重，隨時透過行動網路存取相關網路資源，但相對的個人資料亦曝露在極高的洩露風險中。因此，與手機相關的行動裝置「安全性」議題，逐漸受到重視。本章共分為以下參部分：第一部分將介紹行動裝置。第二部分將智慧型手機作業系統。在第三部分將提出行動裝置目前面臨的安全威脅，及提供安全防護建議。

- **第十章：社交網路服務安全**

社交網路服務（SNS，Social Network Service），這項服務是基於網際網路，為使用者提供相互聯繫的管道。然而在享受社交網路服務所帶來好處的同時，在其中也隱藏了相當大的資訊安全危害。隱密訊息的發佈，如果權限設定不當，就會使其暴露在公開場合。犯罪者也能創立秘密社團，在其中討論違法議題。在本章將會為大家介紹社交網路服務的觀念、應用即其安全性議題，並教導大家又該如何防範。

以上六章為本書的第二部分：「資訊安全應用」。第五、六章是基於前四章的觀念去做衍生，探討在各項資訊安全設定上的應用為何。如在第五章網路安全協定，其就是應用對稱及非對稱加密的技術，結合 HASH 技術落實其安全性。第七章開始，是依據各項資訊應用面上的安全議題去做探討。如雲端、通訊以及社交網路，等近期廣為大眾所接觸與使用的科技應用。除將為大家介紹定義、應用，還加入安全性議題，教導大家如何加強在各方面的安全性。

- **第十一章：電腦病毒**

電腦病毒原是一段小程式，它常寄存在可執行檔，不論是用組合語言或巨集功能，感染電腦檔案，透過主動式複製、感染、傳播及發作等特徵，造成電腦系統之操作失靈、故障破壞、磁碟毀損或資料遺失。在網際網路日益興盛之後，病毒傳染的速度加快、範圍也擴大，損失也愈嚴重，成本也有所遞增，寫病毒程式的人不僅精明，更嘗試寫出複雜、難偵測和解毒的電腦病毒。舉凡下載檔案、瀏覽

網頁、讀取信件，幾乎都可能會導致中毒事件發生，電腦病毒在結合網際網路後成為一種惡意程式，更結合木馬、網蟲及攻擊程式的特性，已成為不可忽視之全球性問題，更有形成如同網路瘟疫般地令人注意警戒。

- **第十二章：網路駭客攻擊及防制策略**

資訊網路科技的快速普及雖然帶給人類莫大的助益，卻也帶來不少的犯罪問題，而資訊犯罪已隱然成為未來社會棘手的問題。資訊犯罪並不單純只是電腦的問題，亦包括公約、倫理、道德及法律層面等問題。其中，又以網路駭客入侵問題最具神秘性且防制困難度較高。

- **第十三章：數位鑑識**

資訊安全『information security』扮演了非常重要的角色。儘管資訊犯罪案件日益遽增，但『凡走過必留下痕跡』。從事資訊犯罪所留下的痕跡是以數位的資訊，此時就需要『數位鑑識 digital forensics』。數位鑑識最主要的工作，就是利用數位鑑識工具，設法從資訊犯罪過程中，擷取出具備證明能力以在法庭上做佐證，足以證明嫌犯的犯罪事實之數位證據的作業程序。在上述提及之數位證據、數位鑑識與鑑識工具以及反鑑識之議題，都將在本章為各位做說明。

- **第十四章：網路安全綜合解決方案**

目前最廣為熟知的幾個軟體與協定分別為 PGP、SET&SSL 與防火牆。由於電子郵件在傳送上安全的重要性與日俱增，且內容格式愈趨多樣化，已非單純的文字檔，更加入影音、影像等許多檔案形式增強電子郵件功能，於是製定一套通訊協定標準整合各項通訊格式，並顧及傳輸上的安全性，已成為政府機關、研究組織的研究目標。

上述四章為本書的第三部份: 「資訊安全實務」。本篇主要討論目前網路安全應用與解決之道並佐以實務上的應用。有鑑於現今電腦網路使用率的普及且網路安全的相關議題日漸受到重視，因而本書介紹與大家生活息息相關的網路安全實務

議題，如：PGP 資料加密、網路安全交易 SET/SSL、電腦病毒、電腦系統安全防護、Snort 與 Nessus 網路安全工具等。

本書的第四部分：「資訊安全進階學習」。是在改版本書時，為了方便讀者更易閱讀本書，我們將一些較艱深、繁雜的數學公式以及為了篇幅關係而有部分實務上的應用從書中擷取下來。雖然如此，但是我們認為這些擷取下來的資訊，仍是對讀者有幫助的。所以將其收錄在 CD 中，讓有興趣、想瞭解進階知識的讀者能夠學習。並且在書中提及到的相關程式應用，都由我們的團隊親自撰寫而來。為了幫助讀者親自操作與應用這些程式，我們也將這些程式碼整理之後一併收錄在 CD 中。

編撰:

事實上本書的編寫採循序漸進的故事架構為起始，並輔以基礎理論、網路安全、實務需求、商業應用、新數位時代的多媒體技術、資訊社會的安全應用與如何抵禦犯罪行為的資安事件等多項實際生活問題做編撰。本書所有的編排皆一氣呵成，使讀者從過去經驗，直到現在的社會應用，有最深刻的科技安全奧妙與豐富的學習/探索之旅。

對象:

對於本書的編排，除了適合一般大專/技術學院/大學的學生上課教材使用外，亦為相關研究所的資訊安全、網路安全與行動通訊安全等論文研究基礎。

ICCL-資訊密碼暨建構實驗室
(Information Cryptology and Construction Lab.)
(http://hera.im.cpu.edu.tw)