序文

本書**電腦與網路安全實務**為電腦與網際網路安全的相關理論與實務上所涉及的概念作介紹。在本書中，共分成三大部分，「**資訊安全篇**」、「**網路安全與應用篇**」與「**系統安全篇**」。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「**資訊安全篇**」 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，得以窺探密碼之妙與神奇。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密碼學的研究學者/作者抱以誠摯的尊崇。第一部分的安排裡亦介紹資訊安全的相關技術/原理/發展與應用的討論，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「**網路安全與應用篇**」。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基礎運作並討論諸如 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，而是可以用簡潔的方式表現，並藉此來拉近我們生活上的實務操作，使讀者能確實融入資訊安全所學與現代網際網路的實務操作的距離。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「**系統安全篇**」。此部分主要討論目前網路安全應用與解決之道。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的網路安全議題，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。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，進而提昇系統安全性，強化自我系統的防護。

吾人一直以 Team Work 為研究/討論/決策的主軸。再次地這本書的完成，依然是群策群力的工作模式。ICCL (Information Cryptology & Construction Lab.) 的伙伴/研究人員為此本書的付出之心力，吾人銘記在心。尤其學生之一柯宏叡對本書重要章節的繆力整理，更是舒緩不少我在本書付梓時間上的壓力。我在辦公室/研究室門上擺滿了許多的鐘/錶/計時器，其一之意是提醒時間的珍貴，一天雖僅有 24 小時，卻應如何發揮至 24n， n>0 的工作效能，保握每一分/秒時間如同電腦的分時與分工(Time Sharing and Multi-task)機制！對於宏叡的努力與對此書的表白，在以下的兩段的自序文中可看出端倪。

近幾年來電腦與網路的快速發展，從得資訊相關領域也跟著蓬勃發展。然而，隨著以往所強調的方便、快速等，到現在更加強調的是安全。如同早期製作網頁者，多是以美工排版、內容、互動性為主要考量，安全被視為末節。而如今，在追求建立優良網站時，就一定也要重視到資訊安全。否則，辛苦的成果可能就會在片刻間遭人摧毀殆盡。

每個人的看法或同或不同，都有賴每個人對事物所具備知識與想法而定。這本書提供了一個有關資訊安全領域中的廣泛介紹，也提供了我們的看法與想法，乃至於我們所認為可行對策。這可能是我們的洞見，也可能是我們的一廂情願。實情為何，都是需要大家共同去思考，並不吝於提供建議，方能使我們所提出解決方案更為完備。此次，能有機會在研究教授群的指導之下，能夠將所知、

所學化為文字，成為篇章，在資訊安全這個領域的推展上，略盡棉力，在此對吾師致上衷心的感謝。

本書章節的編撰，是結合中央警察大學數位鑑識研究工作室(ICCL)與高雄師範大學資訊教育研究所**楊中皇教授**與台灣大學電機工程學系所**雷欽隆教授**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 張晃瑜、蔡維宸、林立群、張淯閎的全力參與，使得本書得以順利附梓。另外，ICCL 副主任黃嘉宏的網路安全技術的實驗編入，適時地對本書的發揮事半功倍的效果。藉此對 ICCL 及研究群所有人員的努力表達深摯的感謝。

最後我們以網站裡(http://hera.im.cpu.edu.tw)對生活的期許與讀者分享：

「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」。

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、雷欽隆 謹識

Mid-July 2009