Jan. 2006

序文

本書**資訊與網路安全**-**秘密通訊與數位鑑識新技法**(***Information and Network Security: Eyes of Secret –State of the Art on Internet Security and Digital Forensics***)為古往今來秘密通訊、密碼學(Cryptography)與網際網路安全(Internet Security)的相關理論與實務上所涉及的概念作介紹。在本書中，共分成五大部分(Five Parts)，開始於第一部分(PART I)的 **“人類的秘密”** 結束於第五部分(PART V)的 **“新興網路犯罪與電腦鑑識科學”**。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 **“人類的秘密”** 中，說明人類秘密的根源並介紹密碼學這門學問的基礎與發展，直至最新量子電腦/密碼(Quantum Computer/Cryptography)的發展。在撰寫此第一重點時，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。

第二部分則為 **“密碼學的基礎、技術與應用”**。此部分的安排部分為密碼學與資訊安全的相關技術/原理/發展與應用的討論，使讀者能具備密碼學基礎 ，藉此得以對秘密背後所隱藏真相的探索更具備理論基礎 。密文的解析與瞭解不再是如此的陌生與遙不可及的夢，紮實的基礎將不但窺見了別人宣稱的秘密，當然也可創造/鞏固自己的秘密。

第三部分裡 我們安排 **“網際網路安全與實務”**。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。

接著第四部分 **“資訊隱藏的玄機”**，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。最後第五部分 **“新興網路犯罪與電腦鑑識科學”** 為資訊科技社會所得面臨的資訊安全危機/事件/應用問題，諸如 CYBER-CRIME：詐欺/賭博/洗錢/…等新興網路犯罪的資訊安全議題，進行深入/實務的討論。另外，本部分進一步討論了未來的資訊安全偵查趨勢的電腦/網路下電腦鑑識/數位證據觀念(Computer forensics/Digital Evidence)的/技術/法律等主題。在資安危機意識逐漸高漲的時代，如何建立一套標準的證據鑑定程序，並與資訊安全所發展的技術結合，實為一門有趣且值得深入探究的新領域學問。

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 H.J. Ke 對本書後半章節的繆力整理，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 H.J. Ke 的努力與對此書的表白，在以下的兩段的 H.J. Ke 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，能有機會在吾師的指導之下，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。

在此，ICCL 的副座(副主任, Deputy)J.H. Huang 給我許多的研究理論與實務工作協助，使我無慮於 ICCL 的工作推廣。此本書的完成，亦犧牲他許多假期與休息時間，感謝他為 ICCL 的努力與付出。我們的陣容有了副座 J.H. Huang 的協同作戰而更加堅強，也有了他，當我在對 ICCL 研究人員在研究工作與相關的庶務未達成既定目標而藉口發飆的時候，為場面緩頰。本書的 IDS 章節亦是副座提供最真實系統實驗的精華數據，藉此感謝副座為 ICCL 的付出。

努力的背後，Family 絕對是最重要的支柱，In Particular for **Rebecca/G.Y./G.R.**， my wife, my kids, my loves with them。 最後吾人以經常對 ICCL/生活的期許(禪語)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」。

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-資訊密碼暨建構實驗室
http://hera.im.cpu.edu.tw

http://163.25.10.166

王旭正, Jan. 2006

謹致

Jan. 2006

Preface

Information and Network Security: ***Eyes of Secret –State of the Art on Internet Security and Digital Forensics*** is an introduction to concepts dealing with related theories and practices on past and present cryptography and internet security. This book is comprised of five parts, beginning with “The Secrets of Mankind” (PART I) and concluding with “Newly Emerging Internet Crimes and Computer Forensics Science” (PART V). This book covers topics ranging from the most primitive concepts of safety to the most recent issues, applications, and trends on the Internet.

In the first section, “**The Secrets of Mankind**”, we describe the roots of mankind’s secrets and introduce the foundations and development of cryptography, up to the most recent evolution in quantum computers and cryptography. As we illustrate this first major point, Simon Singh’s *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (1999), Rudolf Kippenhahn’s *The Code Breaking: A History and Exploration* (1999) and related literatures provide comparatively interesting, provocative, and thorough insights, so that we can scrutinize the mystery and wonder of the secrets. Reference to this literature also enriches the writing of this section. We would like to show our deep and sincere respect to those researchers and writers who have undertaken research on various types of secret information and cryptography.

The second section is “**Foundations, Methodologies, and Applications of Cryptography**.” The layout of this section is a discussion of the related methodologies, principles, development, and applications of cryptography and information security. This section will enable the reader to grasp the fundamentals of cryptography, by which they can acquire a more theoretical basis to investigate the hidden truth behind secrets. The analysis and comprehension of codes is not a strange and unattainable dream anymore. Solid foundations will not only decipher the secrets claimed by others, but also create and consolidate one's own secrets.

In the third section we have laid out "**Internet Security and Practice**." In this section, security concepts and fundamentals demanded by the modern Internet world are briefly illustrated. We also discuss issues such as hacking/anti-hacking of IDS/IPS/HONEYPOT. With the use of relevant examples, understanding cryptography is no longer just about theory, but rather can be presented in a simple way such that readers will be able to shorten the distance between communication security theory and real world applications of the modern internet.

Following afterwards is the fourth section, "**The Abstruse Mechanisms of Hiding Information**" – secret information of other forms. Information secrecy has long existed in our area of activity, and it has undergone a whole new interpretation within the past ten years. Finally, the fifth section, "**Newly Emerging Internet Crimes and Computer Forensics Science**" has an in-depth and practical discussion of the topics of information security crises, events, and applications faced by the entire information and technology community, such as cyber-crime (fraud, gambling, money laundering, etc.). Moreover, this section further discusses major technical and legal issues on the Computer Forensics/Digital Evidence of future information security investigations. In an age when people are becoming more and more aware of information security crises, how to establish a standardized verification/identification procedure and combine it with the technology of information security development is an interesting field of study that deserves in-depth investigation.

I have always regarded teamwork as pivotal to research, discussion, and decision-making, and the completion of the second edition of this book was the result of a team effort. I will always remember the efforts and energy partners and researchers at ICCL (Information Cryptology & Construction Lab) put into this work. I would also like to thank one of my students, H.J. Ke, for his sorting and organizing of the last half of this book, which reduced the pressure of time constraints. I set up many clocks, watches, and timers all over my office and lab doors; one reason I did this step was to remind myself of the value of time. Even though we only have twenty-four hours in a day, how one expands it to the function of 24n (n>0) and takes full advantage of every minute is the same as the time sharing and multi-tasking system in a computer! H.J. Ke's efforts on this book can be seen in his forward below.

With the rapid development of the computer and Internet in recent years, related information fields have also developed rather quickly. However, unlike the past, when speed and convenience were emphasized, today it is security that is emphasized more. Early web-page designers were primarily concerned with aesthetics, content, and interaction; security was largely neglected. However, today, when attempting to set up a successful website, one must pay attention to information security. Otherwise, all one's hard work might be completely destroyed by others in a matter of moments.

People may or may not have the same idea; it all depends on the knowledge and ideas people have on different issues. This book has provided a broad introduction to the field of information security, our viewpoints and ideas, and our proposed solutions. The contents in this book are probably just our own narrow perspective, and possibly our bias. We would like everyone to think about the truth and freely offer advice; only through this effort can we make our solutions complete. This time, under the instruction of my advisor, I was able to translate what I know and what I have learned into words and a book, and contribute to the development of the field of information security. I hereby express my deep gratitude to him.

The deputy dean of ICCL, J.H Huang, has provided much assistance on both theoretical and practical work, allowing me to not have to worry about other work for ICCL. He also sacrificed a lot of vacation time and rest for the completion of this book, and I am very grateful for the efforts he has given to ICCL. Our team became stronger with J.H. Huang's assistance. When I was angered at members of the research team at ICCL who could not make significant progress to fit in with the ICCL requirements, it was J.H. Huang who eased the situation. He also provided the most accurate and systematic data for the chapter on IDS. I therefore express my gratitude to him for all he has done for ICCL.

Family is absolutely the most important pillar of support behind hard work, in particular Rebecca, G.Y., G.R., my wife, and my children – my love is with all of them. Finally, I would like to share with readers my expectations of ICCL/Life:

"Think ***why*** *you are here".*

"Find ***where*** *you are interested in here".*

"Marry ***whom*** *you look for here".*

"Get ***what*** *you want to have here".*

"Honor here ***when*** *you own something special with knowledge".*

I hope this book can be used as a preliminary attempt for the literature of technology development/research, and a reference for related fields.

ICCLAB

(ICCL –Information Cryptology and Construction Lab.)
http://hera.im.cpu.edu.tw
http://163.25.10.166

Wang

Shiuh-Jeng Wang