

# 序文

本書**資訊安全-網際網路安全與數位鑑識科學**(*Information Security: Eyes of Privacy-State of the Art on Internet Security and Digital Forensics*)為現代二十一世紀重要的資訊安全/網際網路安全與科技犯罪/**鑑識與證據**的相關理論與實務上所涉及的概念作介紹。為何她(資訊安全)會重要，想像一部高科技下的性能房車，是否得再配備安全無虞的保護機制/系統，才得以登峰造極、完美出眾、自由自在。面對高科技時代各式新興產品(尤其網際網路的應用)的需求、創新(Innovation)、刺激與脈動，這就是「她」的必然與必要性的意境了。

這本書的撰寫就像一件工程般的進度規劃。沒有一群專業工作者，當然也就成就不了一個既定目標的工程。撰寫「資訊安全」這本書，我僅只是一群工作者的督促者，雖然「資訊安全/數位鑑識/證據分析」(“Information Security/Digital Forensics/Evidence Investigation”)是我研究上的興趣之一，但「學無止境，教學相長」，這句哲言確實讓我受並匪淺。

從心得交換/討論中，我將我的 ICCL (Information Crypto & Construction Lab.) 研究人員分成三個研究層次，分別為基礎研究(Fundamental Study)、主要研究(Major Study)與卓越研究(Power Study)。這些成員提供了我諸多的資安/數理邏輯思考的研究空間想像。這群研究人員包括了過去式下雖已單飛但仍念念不忘的「老鳥」(Senior Guys)，現在式下正要畢業的「菜鳥」(Junior Guys)與未來式裡準備嗷嗷待哺/魔鬼訓練的「新鮮人」(Fresh Members)。所有的 ICCL Members 皆為 Lab 的永續經營盡最大的努力並留下難以抹滅的「菜鳥」回憶。

事實上，一項工程來自一群專業的工作者，這群資 ICCL 的伙伴/老老小小確實認真地完成了這項工作，這是一本屬於所有努力者的書。希能導引對有興趣的讀者感受 E/D(Electronic/Digital)時代裡「她」的魅力。

在整個撰寫過程中，ICCL 研究人員之一，高大宇 (Da-Yu Kao)，對本書的資料提供與編輯整理貢獻尤多，以下為高大宇為讀者在品嚐本書時，所提供的金玉良言：

本書撰寫內容，原則上以協助讀者面對電腦世界中種種資訊犯罪所衍生的問題為出發點，期望讀者能從別人錯誤的失敗案例中，學得一些經驗。所舉範例多為根據國內外文獻或報載內容，加些故事性虛構情節的模擬範例，為避免點名相關當事人或機構均以「化名」表示，相關圖、表、範例中，可識別相關身份的 IP 位址、帳號、次數、日期、時間或地點等資訊，也作了些許變化處理，以方便進行學術性之中立分析論述，也沒有任何攻訐任何單位或人員的意圖。任何個別實際案例之真實情節，只有老天爺與當事者最為清楚，即使是負責偵查（或審理）該案的檢警調執法人員，也只能就相關發現事證作一判斷分析。但因任何犯罪事件不見得均有完整證據會被察覺、發現，這使得部分案件會在有限認知與不足證據下，做出分析判斷，而相關審判結論，亦可能與真正事實間存在落差！但盡職的執法人員總會盡可能地尋求「最接近事實真相」的訴訟效果。另外

另外，個別範例的事件分析為作者針對虛構個案範例內容的學術看法與感想，又個案訴訟過程細節內容之不相同，也經常衍生不同的判決結果。任何個案情節如有雷同，純屬巧合，對於任何「對號入座」之特定對象或內容臆測，概與本書無關，也希望本書陳述意見可以提供讀者一些資訊安全方面的省思參考，不必過渡拘泥於範例事件之真實與否。本書設定的主要讀者為具有資訊背景的大專生/研究人員或從業人員，除可定位為有關資訊安全的犯罪訴訟基礎書籍外，亦可作為參考工具書。

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@B**

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, Aug. 2006

謹致

## Forewords

This book, ***Information Security: Eyes of Privacy – State of the Art in Internet Security and Digital Forensics***, is an introduction to the theory and application of 21<sup>st</sup> century information/Internet security and high-tech crime forensics. Why is information security important? Imagine a high-tech, performance automobile: shouldn't it be equipped with a security system of the highest quality in order to ensure that no damage is done to it and that it will continue to perform at its best? Security is inevitable and necessary in this high-tech era to face the need, innovation, stimulation, and timing of various new products, particularly in the world of Internet applications.

This book is akin to a progress plan for an engineering project. Without involving a group of professionals, the preset goals of a project will never be completed. During the writing of *Information Security*, I was only the superintendent of a group of professionals. Although information security/digital forensics/evidence investigation is one of my research interests, I found the saying to be true that knowledge is infinite, one learns by teaching. From discussions and exchange of ideas, I divided my researchers in my Information Crypto & Construction Lab (ICCL) into three research levels: Fundamental Study, Major Study, and Power Study. These groups provided me with many research ideas regarding information security and mathematical and logical deliberation. The researchers included the Senior Guys, past graduates who left but never forgotten; the Junior Guys, current students preparing to graduate; and Fresh Members, future graduates ready to learn and train. All ICCL members worked hard on the continual operation of the lab and were left with unforgettable memories.

A completed project results not from a single mind but from a group of specialized workers, and all the colleagues from ICCL, young and old, worked together

to complete this work. This book belongs to all of those hard workers. We hope that it will demonstrate to interested readers the attraction of Internet security in this electronic, digital era.

Throughout the writing process, one of the ICCL researchers, Da-Yu Kao, who is also my student, contributed the most in providing materials and editing. What follows is the valuable advice to the readers from **Da-Yu Kao**:

The content of this book is basically meant to help readers become familiar with the various problems resulting from high-tech crimes, with the hope that the readers can learn from the mistakes others have made. Most examples are based on articles from domestic and international publication, while some are simulated, fictional cases. In order to protect the privacy of the litigant or organization, all names are assumed and all IP addresses, account numbers, frequencies, dates, times, and locations are altered; in this way, a neutral technical analysis can be discussed with no intention of criticizing any organization or individual. Only God and the concerned parties know the realities of any one particular; even the law enforcement officials in charge of the investigation (or attempted investigation) of the case may only have been able to provide analysis from the discovered evidence. Since not all of the evidence of any given crime can be discovered or obtained, analysis can only be carried out based on limited knowledge and insufficient evidence. And the result of a trial may be far from the truth. But most devoted law enforcement officials will do whatever they can to ensure that they know as much of the truth as is possible to know.

Some individual case discussions are the personal opinions and feelings of the author toward a fictional situation. Moreover, the differences in the details of legal processes often yield differing results. Any similarities to any actual events are purely coincidental, and this book is completely irrelevant to any speculation on any specific individual or case.

We hope the ideas discussed in this book can provide references to the readers about information security. The book assumes its main readers to be college students, researchers, or working professionals with backgrounds in information technology, and in addition to being the basic manuscript for legal issues in information security crimes, this book can also be used as a reference manual.

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.



**(ICCL –Information Cryptology and Construction Lab.)**

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

<http://163.25.10.166>

A handwritten signature in black ink, appearing to read "Shiuh-Jeng Wang".

**Shiuh-Jeng Wang**