- 本書由密碼學基礎開始，進入應用密碼學、電子商務安全、乃至私有網路安全，完整且有序列的介紹相關安全技術。
- 詳述 DES、3DES、RC5、IDEA、AES、RSA、Diffie-Hellman、MD4、MD5、SHA-1、密碼演算法。
- 解說 MAC-DES、HMAC、RSA、DSS、X.509、Kerberos、PKI、資訊安全技術。
- 分析與實例探討防火牆、入侵偵測、網路病毒、IPSec 安全網路的架設原理。
- 隨書光碟備有各種演算法的程式範例，與 OpenSSL 安全程式開發套件。
- 描述 SSL/TLS、S/MIME、PGP、電子商務安全技術。

光碟內附 本書範例程式、OpenSSL套件、DevC++套件

Security

資訊與網路安全技術

And

Information and Network Security Techniques

第二版

粘添壽 著

旗標出版股份有限公司

資訊與網路安全技術

第二版

資訊與網路安全技術

And

Information and Network Security Technology

第二版

感謝您購買旗標書，記得到旗標網站

www.flag.com.tw

更多的加值內容等著您…

1. 建議您訂閱「旗標電子報」：精選書摘、實用電腦知識搶鮮讀; 第一手新書資訊、優惠情報自動報到。

2.「補充下載」與「更正啓事」專區：提供您本書補充資料的下載服務，以及最新的勘誤資訊。

3.「線上購書」專區：提供優惠購書服務，您不用出門就可選購旗標書!

買書也可以擁有售後服務，您不用道聽塗說，可以直接和我們連絡喔！

我們所提供的售後服務範圍僅限於書籍本身或內容表達不清楚的地方，至於軟硬體的問題，請直接連絡廠商。

- 如您對本書內容有不明瞭或建議改進之處，請連上旗標網站 www.flag.com.tw，點選首頁的 **讀者服務**，然後再按左側 **讀者留言版**，依格式留言，我們得到您的資料後，將由專家爲您解答。註明書名(或書號)及頁次的讀者，我們將優先爲您解答。

旗標網站：www.flag.com.tw

學生團體 訂購專線：(02)2396-3257 轉 361,362
傳眞專線：(02)2321-1205

經銷商 服務專線：(02)2396-3257 轉 314,331
將派專人拜訪
傳眞專線：(02)2321-2545

國家圖書館出版品預行編目資料

資訊與網路安全技術 / 粘添壽著. -- 第二版.
-- 臺北市：旗標, 2008.11 面； 公分
參考書目：面 含索引
ISBN 978-957-442-674-4 (平裝)
1. 資訊安全 2. 電腦網路
312.76 97021497

作　　者／粘添壽
發 行 人／施威銘
發 行 所／旗標出版股份有限公司
台北市杭州南路一段 15-1 號 19 樓
電　　話／(02)2396-3257(代表號)
傳　　真／(02)2321-2545
劃撥帳號／1332727-9
帳　　戶／旗標出版股份有限公司
總 監 製／施威銘
行銷企劃／張慧卿
監　　製／陳煥章
執行企劃／黃昕暐
執行編輯／黃昕暐
美術編輯／林美麗
封面設計／古鴻杰
校　　對／粘添壽．黃昕暐
校對次數／7 次

新台幣售價： 720 元
西元 2008 年 11 月出版
行政院新聞局核准登記 - 局版台業字第 4512 號
ISBN 978-957-442-674-4

序

隨著資訊網路的風行，如何增加它的安全性，已成爲時下最重要的課題。本書整合資訊與網路安全的相關技術，略盡微薄之力，望能使讀者在研習資訊系統安全方面有所幫助。作者已將本書所有演算法程式範例與相關論文彙集於隨書光碟內。另外，爲了方便學校授課，也將書本內重點製作成 PowerPoint 檔，以及輔助教材張貼於教學網站(www.tsnien.idv.tw)，有興趣的讀者可自行下載參考使用（或向旗標公司索取）。

本書適合大學三、四年級授課，也可作爲研究所研習網路安全用書，更是一般專業訓練不可或缺的好教材。本書共計 17 章，劃分爲四大篇，各篇大綱如下：

- **第一篇 密碼學基礎**：本篇利用五個章節分別針對秘密金鑰系統、公開金鑰系統、雜湊與亂數演算法做深入淺出的介紹，無論是專門研習密碼學或資訊安全技術，本篇都給予一個既完整且基礎性的概念。
- **第二篇 資訊安全技術**：本篇介紹如何將密碼學運用到資訊安全領域的相關技術，內容包含訊息確認、數位簽章、數位憑證、認證系統與公鑰基礎架構等五個章節；瞭解這些技術是進入資訊與網路安全的必備門檻。
- **第三篇 電子商務安全技術**：具備資訊安全技術之後，本篇繼續使用二個章節介紹建構安全網頁與安全電子郵件系統等相關技術。
- **第四篇 私有網路安全技術**：固定位置之私有網路的架設防火牆與入侵偵測系統，以及整合建構遍佈全球各地的分屬機構之虛擬私有網路，本篇以五個章節分別介紹相關的安全技術。

本書第一版原是由兩位作者協力完成，但吳順裕博士忙於其它研究，無暇修正本書，則將此重任交付作者獨自完成，也感謝他繼續提供許多寶貴意見與研究成果。最後對於旗標公司的協助潤筆與修飾，並允諾出版本書致最高的謝意。

本書並非經典之作，僅就自己所學將過去工作經驗彙集成書，書中難免有遺珠之憾，望讀者 / 教師給予不吝指教。

粘添壽 謹識

2008 年 9 月 28 日 於高雄

如何研讀本書

- **隨書光碟**：包含本書程式範例與 OpenSSL 套件。每一目錄下包含該演算法程式範例，以及相關規格書或論文。程式範例內有註明與書本相對應的章節或圖表，任何 C 編譯器都可以編譯執行（Windows 或 Linux 皆可）。也請讀者詳閱規格文件，這對了解該演算法很有幫助。

- **程式範例**：各演算法範例皆是最基本程式架構，讀者可將其擴充其他功能。譬如 DES 程式可擴充成 DES-CBC 、 3DES 或 MAC-DES 程式。

- **實習環境**：本書採用 OpenSSL 公用程式作爲密碼系統的實習環境，包含各種對稱密碼系統、公開密碼系統、安全郵件、以及憑證發行與認證等等，這對我們學習資訊安全很有幫助，請讀者依照書本介紹方法，儘速將該系統安裝完成，並實際演練。

- **教學範圍**：不分學系，第一、二篇是必備的入門課程，其中三、四兩章，因涉及較複雜的密碼學，授課老師可依學生學習狀況斟酌。就管理學系而言，作者建議教學範圍以第三篇爲主，第四篇爲輔；反觀就工程學系而言，則需偏重四篇。當然，一切還是依授課老師爲主，作者的建議僅供參考。

- **電子書**：爲了減少本書篇幅，不得已將第十六章與十七章內容，製作成 PDF 檔案，儲存於隨書光碟 PDF資料夾內，請讀者自行列印閱讀。深感歉意！！

- **RFC 網站**：本書共參考八十幾篇 RFC 規範（附錄 B），讀者若有需要更進一步瞭解的話，請到 RFC 網站下載原版規範(www.rfc-edit.org)。

- **教學網站**：爲使授課老師方便教學，作者已完成 PowerPoint 簡報檔製作（請向旗標公司索取），並陸續蒐錄其他輔助教材、論文、規範、或新增程式範例，張貼於作者教學網站，歡迎讀者多加利用。

編後語

記得，剛進入中山大學電研所就讀碩士班時，實驗室裡總放置一部謝文雄教授所組裝的收音機，每天不斷播放著中廣音樂網，吵得讓我無法專心看書（謝老師一向很節儉捨不得買音響）。每當謝老師離開實驗室，我就將收音機關掉；但當他回來時，他又隨即打開收音機，每天就這樣反反覆覆經過數年。十幾年過後的今天，自己當上了老師，每天陪伴著我雖然不是中廣音樂網 （我組裝的收音機更不能聽），但已由鄧麗君懷念歌曲、台灣懷念老歌、古箏佛讚，進步到目前的霹靂布袋戲原聲帶。此時的我，終於頓悟，原本當老師是多麼孤單、作研究又是那麼無聊，唯有此道，足以讓自己得到這麼一點點的成就。在此向全國所有老師致最高敬意，由於您們默默無聞的努力奉獻，培養出衆多優秀學生，使能有效提昇台灣的技術水準，進而擠身國際高科技列強之中。半路出家的我，必須好好向您們學習。

contents 目錄

第 0 章　OpenSSL 實習環境建置

contents

第一篇　密碼學基礎

第 1 章　安全性資訊系統簡介

第 2 章　傳統秘密金鑰系統

contents 目錄

第 4 章 現代公開金鑰系統

contents 目錄

第 5 章 雜湊與亂數演算法

第二篇 資訊安全技術

第 6 章 訊息確認

第 7 章 數位簽章與數位憑證

contents 目錄

contents 目錄