網路安全與密碼學概論

Cryptography and Network Security

Behrouz A. Forouzan◎原著
李南逸、王智弘、林峻立、張智超、溫翔安、葉禾田◎翻譯

美商麥格羅・希爾
資訊科學　系列叢書

滄海書局
Tsang Hai Book Publishing Co.

國家圖書館出版品預行編目資料

網路安全與密碼學概論 / Behrouz A. Forouzan
作 ; 李南逸等翻譯. -- 初版. -- 臺北市 :
麥格羅希爾, 2008.08
面 ; 公分. -- (資訊科學叢書 ; CI013)
參考書目:面
含索引
譯自 : Cryptography and network security
ISBN 978-986-157-478-3(平裝)

1. 資訊安全 2. 密碼學

312.76 97009803

資訊科學叢書 CI013

網路安全與密碼學概論

作　　者　Behrouz A. Forouzan
翻　　譯　李南逸 溫翔安 葉禾田 張智超 林峻立 王智弘
業務行銷　林妙秋 曾時杏 黃永傑 李本鈞
出版經理　張景怡
企劃編輯　朱紋寬
教科書編輯　林芸郁
特約編輯　張文惠

出 版 者　美商麥格羅・希爾國際股份有限公司 台灣分公司
地　　址　台北市 100 中正區博愛路 53 號 7 樓
網　　址　http://www.mcgraw-hill.com.tw
讀者服務　E-mail: tw_edu_service@mcgraw-hill.com
TEL: (02) 2311-3000　FAX: (02) 2388-8822
法律顧問　惇安法律事務所盧偉銘律師、蔡嘉政律師及江宜蔚律師
總經銷(台灣)滄海書局
地　　址　台中市西屯區 407 台中港路二段 122-19 號 11 樓
TEL: (04) 2708-8787　FAX: (04) 2708-7799
劃撥帳號: 00263458
E-mail: thbook@tsanghai.com.tw

出版日期　2008 年 8 月（初版一刷）

Original: Cryptography and Network Security, 1e　ISBN: 978-007-287022-0

ISBN：978-986-157-478-3

尊重智慧財產權！

譯序

翻譯本書起始於鳳凰花開時，由於麥格羅•希爾公司的朱紋寬小姐慧眼識英雄，也虧所有譯者本著愚公移山的精神，所以決定集合眾人之力接下翻譯的工作，雖為所有譯者的處女秀，但一絲不苟的態度與敬業的精神，相信絕對不會輸給專業的翻譯人員。

本書可說是Behrouz A. Forouzan博士正式跨足網路安全的第一本大作，雖然Behrouz A. Forouzan博士早已在通訊網路領域享有盛名，但本書深入闡述密碼學及網路安全的議題，詳細閱讀後對其精闢的見解感動不已，因此有幸可以與其他譯者合作翻譯本書，實在受益匪淺，也更堅定希望翻譯本書讓更多學子得以一窺奧妙的信念。

然過程的辛苦實不足為人道之，所幸有智超建置網站解決一致性問題，多次會議共同解決深奧的基礎原理，數不清的E-MAIL與交互校稿，最後才能讓初稿出爐。在此也要特別感謝麥格羅•希爾公司的林芸郁小姐，若沒有經驗豐富的她不辭辛勞、逐字校對，本書絕對無法付梓。此外，若沒有譯者家裡妻小的寬宏大量，更不可能有此譯本，在此要特別感謝他們的體諒。

雖然窮眾人之力希望能完整傳達本書的理念與內容，然唯恐譯本中仍有疏漏，因此期望各位專家學者不吝指教，全體譯者必將虛心接受，再次感謝。

李南逸

暨全體譯者

2008年鳳凰花開時

前言

網際網路是一個遍及全球的通信網路，已經用很多方式改變了我們的日常生活。一個新的商業範例允許個人在線上商店進行消費。全球資訊網（WWW）允許人們分享資訊，電子郵件技術則把人們從全世界各個遼闊的角落連結起來，此一不可避免的進展也讓我們對網際網路產生了依賴性。

網際網路是一個開放論壇，但產生一些安全問題。因此，機密性、完整性和確認性有其必要。人們需要確信他們的網際網路通訊是機密的。在線上購物時，他們需要確信那些商店能經過確認。當他們將交易要求送到銀行時，則想要確信訊息的完整性是被保護的。

網路安全是允許我們舒服地使用網際網路的一套協定，而無須擔心安全攻擊。提供網路安全最常見的工具是密碼學，那是一種重新流行且適用於網路安全的老技術。這本書首先向讀者介紹密碼學的原理，然後運用那些原理來描述網路安全協定。

本書特色

本書特色是設計來讓讀者特別容易理解密碼學和網路安全。

架構

本書使用一種累增的方法來教導密碼學和網路安全。它假設讀者沒有特別的數學知識，例如數論或抽象代數。但是，因為密碼學和網路安全不能在沒有這些數學領域的背景下被討論，因此這些主題將在第二章、第四章和第九章介紹。熟悉這些數學領域的讀者可以跳過這些章節。第一到十五章討論密碼學，第十六到十八章討論網路安全。

視覺方法

本書使用對比的文字和圖表來表示非常技術性的主題內容，且沒有複雜的公式。超過400個圖表提供了一個視覺和直覺的機會來理解內容。圖表在解釋艱難的密碼學概念和複雜的網路安全協定的過程中特別重要。

演算法

演算法在教導密碼學中扮演了一個重要角色。為了讓描述在各種電腦程式語言中變得獨立，演算法是以一種現代程式語言容易撰寫出來的虛擬碼呈現。在本書的教科書資源網可以下載相對應的程式。

重點

重要的概念會以方塊特別強調，以做為快速的參考和及時注意。

範例

每一章提供許多範例以探討該章的概念。部分範例僅用來顯示立即使用概念和公式；部分範例用來顯示密碼法的實際輸入／輸出關係；其他範例則對一些困難的想法提供較佳的理解。

推薦讀物

在每一章的最後，讀者將找到一個書籍的目錄以進行更進一步的閱讀。

關鍵詞彙

關鍵詞彙以粗體方式出現在各章內文中，且每一章的最後面也會列出關鍵詞彙的清單。所有的關鍵詞彙會在本書最後的詞彙表中定義。

重點摘要

各章以內容摘要來做結束。它提供各章重點的簡短概述。

練習集

在每一章的最後，學生可以發現一個練習集，用來加深和應用那些凸顯的概念。練習集由兩個部分組成：問題回顧和習題。問題回顧是為了測試讀者對本章內容的初階理解，習題則需要對內容有更深的理解。

附錄

附錄提供快速的參考內容，或者對本書討論需要理解的概念回顧。一些數學主題的討論也在附錄裡提出，以避免已經熟悉這些內容的讀者分心。

證明

在章節中的數學事實並沒有證明，而是強調運用這些事實的結果。對那些證明感興趣的讀者可以參考附錄Q。

重要詞彙

在本文的最後，讀者將找到一個擴展的重要詞彙。

本書內容

在第一章前言之後，本書被分成四個部分：

第一篇：對稱式金鑰加密技術

第一篇介紹對稱式金鑰密碼學，包括傳統和現代。此篇的章節強調使用對稱式密碼學以提供機密性。第一篇包括第二章到第八章。

第二篇：非對稱式金鑰加密技術

第二篇討論非對稱式金鑰密碼學。此篇的章節介紹非對稱式密碼學如何提供安全性。第二篇包括第九章和第十章。

第三篇：完整性、確認性與金鑰管理

第三篇介紹密碼學的雜湊函數如何能提供其他安全服務，例如訊息完整性和確認性。此篇的章節也介紹非對稱式金鑰和對稱式金鑰密碼學如何能彼此搭配。第三篇包括第十一章到第十五章。

第四篇：網路安全

第四篇介紹在第一篇到第三篇討論的密碼學如何能用來產生在三層網際網路模型中的網路安全協定。第四篇包括第十六章到第十八章。

如何使用這本書

這本書是為學術和專業讀者而寫的。有興趣的專業人士能使用它來做為自我學習與研究。做為一本教科書，它可當作一個學期或者一季的課程。下列是一些指南。

強烈建議第一篇到第三篇

如果課程需要超越密碼學以外並且進入網路安全的範疇，則建議閱讀第四篇。在讀第四篇前需先讀過一門網路課程。

線上學習中心

麥格羅・希爾線上學習中心包含許多與密碼學和網路安全有關的額外內容。讀者可以連線到www.mhhe.com/forouzan網站。教授和學生能存取課程內容，如投影片等。網站上為學生提供解決古怪問題的方法，且教授能使用一組密碼以存取完整的解法。此外，麥格羅・希爾使用一種敝公司專有的產品（稱為PageOut），讓建置一個課程網站易於上手。您並不需要HTML的相關知識、不需花長時間，也不需要設計技術，PageOut 提供一系列的樣版，您只需要將課程訊息填入樣版並且點擊16種設計之一，不用一個小時，您就能建置一個專業設計的網站。雖然PageOut提供「立即」的發展，但完成的網站將提供強而有力的特色。一份交互式的課程大綱可讓您發表與課程相符的內容，因此當學生造訪此一PageOut 網站時，您的課程大綱將指引他們去Forouzan的線上學習中心，或者您自己所提供的特定內容。

Behrouz A. Forouzan

目次

網路安全與密碼學概論

Cryptography and Network Security

Behrouz A. Forouzan
DeAnza College

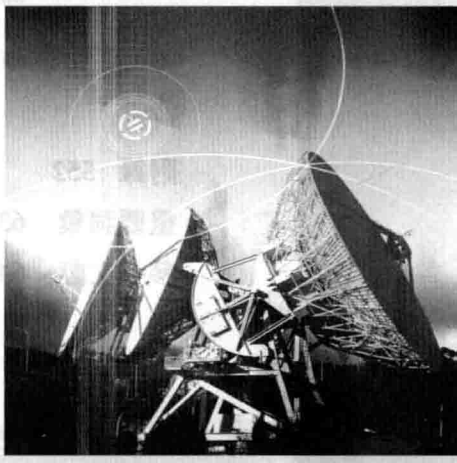
王智弘 李南逸 林峻立 張智超 溫翔安 葉禾田 翻譯
（以上按姓氏筆劃排序）

Mc Graw Hill Education

US Boston Burr Ridge, IL Dubuque, IA Madison, WI New York San Francisco St. Louis
International Bangkok Bogotá Caracas Kuala Lumpur Lisbon London Madrid Mexico City Milan Montreal New Delhi Santiago Seoul Singapore Sydney Taipei Toronto

CHAPTER 1

導論



學習目標

本章的學習目標包括：

- 定義三個安全目標。
- 定義威脅安全目標的安全攻擊。
- 定義安全服務及它們與安全目標的關係。
- 定義提供安全服務的安全機制。
- 介紹設計安全機制的兩種技術：密碼學與隱藏學。

生活在資訊時代裡，我們需要保存與自己生活有關的每個訊息，換句話說，資訊就像任何其他資產一樣是有其價值的。既然是資產，資訊就需要避免攻擊且被安全地保護起來。

為了保護資訊，資訊需要被隱藏且避免未授權的存取（機密性）、避免未授權的更改（完整性），以及讓授權的個體在需要時得以使用（可使用性）。

直到幾十年前，由組織所蒐集的資訊才被儲存在實體的檔案內。檔案的機密性乃藉由限制授權予信任的人才能存取來達成；同樣地，只有被授權的人才被允許修改檔案的內容。可使用性則由指明至少一人在任何時候都能存取檔案來達成。

由於電腦時代的來臨，資訊的儲存變成電子化，不是儲存在實體媒介上，而是儲存在電腦裡。不過，資訊的三個安全需求自始至終都沒有改變。檔案儲存在電腦裡仍然需要機密性、完整性與可使用性，只不過這些安全需求的設計不同，且更富挑戰性。

在過去二十年裡，電腦網路在資訊使用上產生了革命性的改變。現在的資訊是分散式的，被授權者可從遠端使用電腦網路來傳送與接收資訊。雖然上述的三個需求（機密性、完整性和可使用性）沒有改變，但它們現在有了一些新的特點。當資訊被儲存在一台電腦裡時，應該不僅是機密的，而且當它被從一台電腦傳送到另一台電腦時，也應該維持其機密性。

在本章中，我們首先探討資訊安全的三個主要目標，然後介紹資訊攻擊如何威脅這三個目標，接著討論安全服務與安全目標的關係，最後，我們定義提供安全服務的機制，並且介紹能用來實現這些機制的技術。

1.1 安全目標

首先，讓我們來探討三個**安全目標（security goal）**：機密性、完整性與可使用性（圖1.1）。

圖 1.1 安全目標的分類

機密性

機密性（confidentiality）或許是資訊安全中最常見的特點。我們需要保護自己的機密資訊，因此一個組織需要防衛那些可能會危害訊息機密性的惡意行動。在軍隊中，隱藏敏感性資訊是最重要的。企業中，對競爭者隱藏一些資訊對組織的營運也很重要。至於銀行業，客戶的帳戶同樣需要被保密。

在本章後面，我們將介紹機密性不僅適用於資訊的儲存，也適用於資訊的傳播。當傳送或接收遠端電腦的部分訊息時，我們需要在輸送過程中想辦法隱藏它。

完整性

資訊經常需要改變。在銀行內，當顧客存款或提款時，他們的帳號餘額就需要改變。**完整性（integrity）**是表示改變只能由授權的人或透過授權的機制來進行。違背完整性並不必然是惡意行為的結果，系統的中斷（例如電力劇烈變化）也可能造成一些資訊不預期的變化。

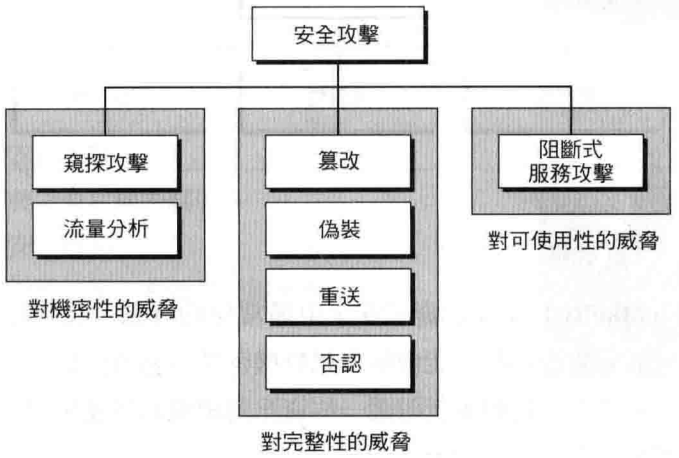
可使用性

資訊安全的第三個組成要素是**可使用性（availability）**。一個組織產生或儲存的資訊要能讓被授權者可以使用，如果它無法使用，則此資訊就沒有用處。資訊經常需要改變，這表示它必須讓被授權者存取。在組織內，資訊不能被利用就好像缺乏機密性或完整性一樣有害。想像在一家銀行裡，如果客戶不能存取他們的帳戶並進行交易，將會發生什麼事。

1.2 攻擊

我們的三個安全目標（機密性、完整性和可使用性）會被**安全攻擊（security attack）**所威脅。雖然文獻上使用不同的方法來區分攻擊種類，但我們首先可將它們與安全目標的關係做區分；接著，再根據它們對系統的影響分成兩大類。 圖1.2顯示第一種分類法。

圖 1.2 與安全目標有關的攻擊分類法



威脅機密性的攻擊

一般來說，威脅機密性的攻擊有兩種型態：**窺探攻擊（snooping attack）**與**流量分析（traffic analysis）**。

窺探攻擊

窺探攻擊是一種對資料的非法存取或攔截。例如，一個透過網際網路傳送的資料可能包含祕密的資訊。一個未被授權的實體有可能會攔截此資料，並且把資料內容用於有益自己的地方。為了防止窺探攻擊，可以透過本書所討論的加密技術，讓攔截者無法看到資料的實際內容。

流量分析

雖然對資料加密可讓攔截者無法看到資料的實際內容，但他們卻能透過監控網路上傳輸的資料，來獲得其他類型的資訊。例如，他們能找到發送者或接收者的電子位址（例如電子郵件信箱位址）。或者，他們能蒐集請求和回應資料，而推測出交易的性質。