

資訊與網路安全技術

第一章 安全性資訊系統概論

1-1 安全性資訊系統要件

1-2 安全性工具

1-3 訊息的安全性

1-4 系統的安全性

1-5 網路的安全性

1-6 電子商務的安全性

第二章 傳統秘密鑰匙系統

2-1 密碼學簡介

2-2 傳統密碼學的基本原理

2-3 換位加密法

2-4 取代加密法

2-5 數位資料加密原理 – 區塊加密

2-6 Feistel 密碼演算法

2-7 傳統密碼系統的摘要

2-8 DES 密碼系統

2-9 AES 密碼系統

2-10 Triple DES 密碼系統

2-11 密碼系統的安全性

第三章 現代公開鑰匙系統

3-1 公開鑰匙系統簡介

3-2 公開鑰匙的數學基礎

3-3 公開鑰匙的同餘算數

3-4 RSA 演算法

3-5 RSA 參數與安全性

3-6 Diffie-Hellman 鑰匙交換法

3-7 公開鑰匙系統之應用

第四章 雜湊與亂數演算法

4-1 雜湊演算法簡介

4-2 簡單的雜湊函數

4-3 MD5 訊息摘要

4-4 SHA-1 演算法

4-5 破解雜湊函數

4-6 亂數產生器

第五章 密碼系統的實習環境 – Open_SSL

5-1 OpenSSL 簡介

5-2 OpenSSL 管理工具

5-3 OpenSSL 命令語法

5-4 傳統密碼系統操作

5-5 公開鑰匙演算法操作

5-6 DH 公鑰演算法操作

5-7 DSA 公鑰演算法操作

5-8 訊息摘要操作

第六章 訊息確認

6-1 訊息確認簡介

6-2 完整性檢查碼 -ICV

6-3 訊息確認碼 - MAC

6-4 MAC-DES 演算法

6-5 HMAC 演算法

6-6 MAC 操作方式

第七章 數位簽章與數位憑證

7-1 數位簽章簡介

7-2 RSA 數位簽章

7-3 DSS 數位簽章

7-4 數位憑證

7-5 憑證與私鑰的儲存

7-6 憑證認證的運作

7-7 憑證授權中心

7-8 數位簽章的仲裁

7-9 範例：電子投標系統

第八章 安全性網頁系統

8-1 安全網頁系統架構

8-2 SSL 安全協定

8-3 SSL 握手協定

8-4 SSL 主密鑰產生

8-5 SSL 會議鑰匙的計算

第九章 安全性電子郵件

9-1 安全性電子郵件簡介

9-2 Secure E-Mail 安全郵件

9-3 MIME 郵件標準

9-4 Secure-MIME 安全郵件

第十章 防火牆

10-1 私有網路安全簡介

10-2 防火牆簡介

10-3 防火牆架構

10-4 封包過濾器

10-5 IP 封包過濾

10-6 IP/TCP 封包過濾

10-7 IP/UDP 封包過濾

10-8 IP/ICMP 封包過濾

10-9 代理系統

10-10 網路位址轉譯 - NAT

第十一章 入侵偵測與網路病毒

11-1 入侵偵測系統簡介

11-2 入侵偵測與防火牆架設

11-3 駭客身份

11-4 入侵步驟與技巧

11-5 入侵技巧

11-6 入侵偵測系統

11-7 入侵偵測技術

11-8 主機型入侵偵測系統

11-9 網路型入侵偵測系統

11-10 誘捕型防禦系統

11-11 網路病毒

第十二章 虛擬私有網路 – IPSec

12-1 虛擬私有網路簡介

12-2 VPN 網路型態

12-3 IP 安全協定

12-4 IPSec AH 協定

12-5 IPSec ESP 協定

12-6 安全關聯

第十三章 用戶認證與協定

13-1 用戶認證簡介

13-2 用戶帳號/密碼

13-3 單向認證協定

13-4 相互認證協定

13-5 集中式用戶認證

第十四章 Kerberos 認證系統

14-1 認證協定與認證系統

14-2 Needham-Schroeder 認證協定

14-3 公開鑰匙認證協定

14-4 Kerberos V4 認證系統

14-5 Kerberos V5 認證系統