目錄

第一篇　認識問題

Chapter 1　資訊安全概論

1.1 資訊安全問題的演進 1-2
1.2 推動資訊安全應有的觀念 1-3
　資訊安全是一種取捨 1-4
　資訊安全是管理議題 1-4
1.3 資訊安全的範圍與目標 1-5
　資訊安全的三元素 1-6
　資訊安全的目標 1-7
1.4 基本的存取控制 1-8
　身分認證的方法 1-8
　較先進的身分認證協定 1-10
1.5 基本的網路安全 1-11
　制定安全設計目標 1-12
　切割安全區域 1-12
　融入新科技 1-13
　管理資訊風險 1-15
　建立多層次防禦 1-16
自我評量 1-18

Chapter 2　資訊法律與事件處理

2.1 網路的罪與罰 2-2
　電腦在犯案中的角色 2-3
　電腦犯罪的種類 2-4

2.2 資訊的所有權 2-5
2.3 個人資料保護法與資訊安全 2-7
2.4 資訊安全事件的處理方法 2-8
問題分類 2-9
問題調查 2-10
問題隔離 2-11
問題分析 2-11
復原與紀錄 2-12
自我評量 2-13

Chapter 3 資訊安全威脅

3.1 資訊安全威脅的目的 3-2
以侵入為目的 3-2
以竄改或否認為目的 3-3
以拒絕服務為目的 3-4
3.2 認識一般的攻擊 3-4
攻擊通關密碼 3-4
利用後門 3-5
攔截與偽裝 3-5
3.3 認識軟體弱點的利用 3-7
3.4 認識惡意程式 3-7
認識病毒 3-8
認識蠕蟲 3-9
認識木馬與邏輯炸彈 3-9
3.5 認識網路攻擊 3-10
認識 TCP/IP 協定 3-11
有關 TCP/IP 的攻擊手法 3-13
3.6 認識社交工程 3-15
自我評量 3-16

Chapter 4　駭客手法研究

4.1 攻擊網站 4-2
網站的掃描、分析、與攻擊 4-3
4.2 攻擊網頁 4-6
混淆攻擊法與 XSS 4-6
資料隱碼攻擊法 4-7
搜尋引擎攻擊法 4-10
隱藏欄位攻擊法 4-12
4.3 攻擊身分認證 4-13
通關密碼破解法 4-13
輸入截取攻擊法 4-15
4.4 攻擊無線網路 4-16
WEP 的安全問題 4-17
無線網路的竊聽攻擊 4-17
欺騙的無線基地台 4-18
無線網路的拒絕服務攻擊 4-18
自我評量 4-20

第二篇　安全架構

Chapter 5　認證、授權與存取控制

5.1 存取控制的主要概念 5-2
存取控制的類別 5-2
存取控制的威脅 5-3
5.2 身分與身分認證 5-4
單點登錄 5-6
身分認證元件 5-7
智慧卡 5-8
生物特徵 5-11
身分管理 5-13

5.3 資料存取控制 5-13
5.4 入侵偵測與入侵測試 5-16
自我評量 5-18

Chapter 6 資訊安全架構與設計

6.1 國際標準管理系統 6-2
全面品質管理 – TQM 6-2
資訊安全管理系統 – ISMS 6-3
資訊技術服務管理 – ITSM 6-4
能力成熟度模型整合 – CMMI 6-4
6.2 安全等級與評估準則 6-5
可信任的運算基礎 – TCB 6-7
產品安全性的評估準則 6-8
6.3 正式的安全模型 6-10
狀態機模型 6-10
Bell-LaPadula 模型 6-11
Biba 模型 6-12
Bell-LaPadula & Biba 聯合模型 6-14
Clark-Wilson 模型 6-14
存取控制矩陣 6-16
不干擾模型 6-17
Brewer & Nash 模型 6-17
6.4 安全模式 6-18
自我評量 6-20

Chapter 7 基礎密碼學

7.1 密碼學的演進 7-2
位移加密法 7-2
替換加密法 7-3
頻率分析法 7-3
多重字母替換加密法 7-4

7.2 電子時代的新挑戰 7-5
連續金鑰加密 7-6
成功的密碼機器：「謎」 7-7
另類的加密法 7-8
現代電腦密碼學 7-9
7.3 對稱式加密法 7-10
DES 加密法 7-11
AES 加密法 7-12
對稱式加密法的優缺點 7-13
7.4 非對稱式加密法 7-13
RSA 加密法 7-16
其它非對稱式加密算法 7-17
非對稱式加密法的優缺點 7-17
7.5 雜湊、簽章與複合式系統 7-17
複合式系統 7-19
7.6 對稱式加密的模式 7-20
ECB 模式 7-21
CBC 模式 7-22
CFB 模式 7-23
OFB 模式 7-23
CTR 模式 7-24
Triple DES 7-25
7.7 加密法的應用 7-26
PKI 應用範例 7-27
瞭解 X.509 7-27
瞭解 SSL 與 TLS 7-28
瞭解 CMP 與 S/MIME 7-29
瞭解 SET 7-29
瞭解 SSH 7-30
瞭解 PGP 7-31
瞭解 HTTPS、S-HTTP 與 IPSEC 7-31

7-8 金鑰管理 7-32
金鑰的產生 7-32
金鑰的儲存與配送 7-33
金鑰的託管 7-33
金鑰的過期、收回、與中止 7-34
金鑰的歸檔與重新取出 7-34
金鑰的更新與銷毀 7-34
7.9 密碼系統的攻擊 7-35
密碼算法的攻擊案例 7-36
自我評量 7-37

Chapter 8 資訊系統與網路模型

8.1 電腦系統架構 8-2
作業系統的基本功能 8-3
中央處理器架構 8-3
8.2 記憶體與外掛元件 8-4
記憶體管理 8-5
記憶體映像 8-6
記憶體滲漏 8-6
虛擬記憶體 8-7
外掛儲存元件 8-7
輸入輸出元件 8-8
8.3 作業系統的程式執行 8-9
保護圈 8-10
虛擬機器 8-10
8.4 網路的組件 8-11
網路連結組件 8-12
防火牆與 IDS 8-13
數據機 8-14
PBX 系統 8-14
伺服器與個人電腦 8-15
無線通訊系統 8-15

網路線 8-16
8.5 OSI 網路模型 8-18
OSI 模型的七個階層 8-18
實體層（L1） 8-20
資料連結層（L2） 8-21
網路層（L3） 8-23
傳輸層（L4） 8-26
會談層（L5） 8-27
展現層（L6） 8-27
應用層（L7） 8-28
8.6 封包攔截與分析工具 8-28
攔截通關密碼實例 8-29
攔截網路通訊實例 8-30
重組網路通訊實例 8-31
自我評量 8-32

第三篇　縱深防禦

Chapter 9　防火牆與使用政策

9.1 防火牆概論 9-2
9.2 防火牆的種類 9-3
封包過濾防火牆 9-3
狀態檢查防火牆 9-5
應用代理閘道防火牆 9-6
個人防火牆 9-7
9.3 建立防火牆環境 9-10
DMZ 9-11
VPN 9-11
9.4 防火牆的安全政策 9-12
防火牆管理 9-13
自我評量 9-15

Chapter 10　入侵偵測與防禦系統

10.1 IDPS 概論 10-2
入侵偵測的方法 10-2
偵測的準確性與調節 10-4
入侵防禦的方法 10-4
10.2 IDPS 的種類 10-5
網路為基礎的 IDPS 10-6
無線 IDPS 10-8
網路行為分析 IDPS 10-9
主機為基礎的 IDPS 10-10
10.3 IDPS 範例與整合技術 10-11
與 IDPS 相關的技術 10-12
自我評量 10-14

Chapter 11　惡意程式與防毒

11.1 惡意程式的種類 11-2
病毒 11-2
蠕蟲 11-4
木馬 11-4
惡意行動碼 11-5
追蹤 Cookies 11-6
攻擊工具 11-6
網路釣魚 11-7
11.2 惡意程式的防禦 11-9
安全政策與教育訓練 11-9
弱點補強 11-10
防毒軟體 11-10
11.3 惡意程式事件的處理 11-11
惡意程式隔離 11-12
瞭解受感染的主機 11-13

CH 7

基礎密碼學

本章概要

7.1 密碼學的演進

7.2 電子時代的新挑戰

7.3 對稱式加密法

7.4 非對稱式加密法

7.5 雜湊、簽章與複合式系統

7.6 對稱式加密的模式

7.7 加密法的應用

7-8 金鑰管理

7.9 密碼系統的攻擊

以今日觀之，「密碼學（cryptography）」乃高深之數學與複雜的運算，然而密碼學並非電腦時代的新產物，數千年來許多人創造秘密通訊的方法，也有許多人鑽研破解之道。本章我們將從密碼學的演進切入，從西元前的簡易混淆手法介紹到電腦時代各種複雜的加解密運算，並討論從密碼學衍生的安全通訊協定。由於本章為基礎密碼學，我們將儘量避免深奧的數學，而以建立觀念與實用為主。

7.1 密碼學的演進

密碼學是永無止盡的攻防，自古到今許多極聰明的人創造加解密的算法，卻又有極聰明的人找出破解之道。西元前第五世紀斯巴達人將訊息寫於細長皮革，纏繞在多角形的木杖上。例如「MEET ME AT NINE ...」（斯巴達人當然不會用英文，這只是舉例），當皮革解開時上面的信息卻是「MTAI..EMTN..EENE」。收信人將皮革纏上相同尺寸的木杖之後，原信息得以重現，請見圖 7-1（左）。

凱撒大帝在西元前第一世紀以當時簡單又有效的方式為自己傳出的信息加密：他將每一個字母移動三位。如圖 7-1（右）所示，M 移三位成為 P，E 成為 H，而 T 成為 W。加密之後，就不容易再從字面上讀懂含意。

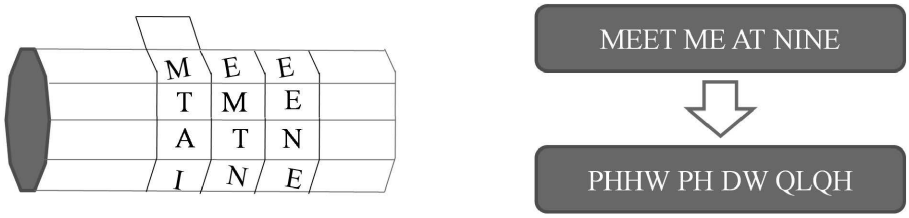

圖 7-1 斯巴達人的密碼木杖（左）與凱撒的字母替換（右）

位移加密法

前述斯巴達人的木杖使用簡單的「位移加密法（transposition ciphers）」，它重新調整資訊的字母或位元順序，藉以隱藏機密。圖 7-2 是一個例子，我們橫向地讀就是明碼：「小明今天早上把收集幾個月的蠶寶寶以每隻十塊錢價格賣給他的鄰居。」縱向地讀就是密文：「小上個寶塊給明把月以錢他今收的每價的天

集蠶隻格鄰早幾寶十賣居。」這樣的密文很難一眼看懂，但若仔細觀察，就可以找到破解位移加密法的規律性。

小	明	今	天	早
上	把	收	集	幾
個	月	的	蠶	寶
寶	以	每	隻	十
塊	錢	價	格	賣
給	他	的	鄰	居

圖 7-2 位移加密法範例

替換加密法

凱撒使用簡單的「替換加密法（substitution ciphers）」，它直接做字母位移。圖 7-3（左）的範例僅只簡單地移動三位，比較容易觀察到規律性。若使用攪亂（但固定）的替換表加密，就更難找出規律性，圖 7-3（右）的範例就採用替換表。

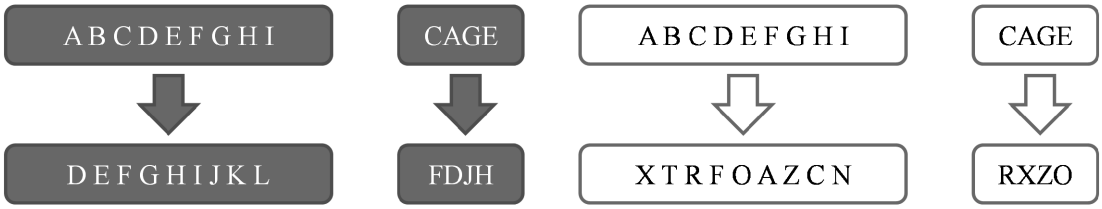

圖 7-3 替換加密法範例一（左）與範例二（右）

頻率分析法

阿拉伯人在第九世紀已享有極高的文明，他們的經文學者發現有些字母出現的頻率遠高於其它。因此，一篇以替換法加密過的密文，可以用字母出現的頻率反推出原文。圖 7-4 是英文字母在文章中出現的機率統計表，出現機率最高的字母依序為 E, T, A, O, I 等。假如我們仔細統計密文中出現頻率最高的字母依序為 O, K, X, M, N，就能找出可能的替換表對應關係。歐洲等到文藝復興時期才發展出類似破解法，因此阿拉伯人在秘密通訊上佔有數個世紀的優勢。