「網路安全」

委辦單位：教育部顧問室資通安全聯盟

執行單位：成功大學電機系

課程模組大綱(一)

- Module 1：網路安全導論
- Module 2：密碼學基礎
- Module 3：金鑰管理
- Module 4：X.509
- Module 5：鑑別技術
- Module 6：Kerberos
- Module 7：電子郵件安全

課程模組大綱(二)

- Module 8：防火牆
- Module 9：虛擬私有網路(VPN)
- Module 10：IP安全機制
- Module 11：Web安全機制
- Module 12：網路安全架構
- Module 13：入侵偵測
- Module 14：無線網路安全

Module 1：網路安全導論

學習目的

1. 近年來網際網路已成為資訊快速交換的媒介，伴隨著網路應用及複雜性的增加，網路資訊系統的漏洞層出不窮，其中網路蠕蟲與電腦病毒、木馬、側錄或間諜等惡意程式相互結合所衍生的混合式攻擊更是增加了防禦的難度，本課程模組將引導學生了解網路安全的威脅及相關的防護機制。
2. 同時我們將介紹一些常見的網路安全問題與目前大家所使用的安全模型，也會談到一般的網路安全評估方法與一些數位系統概念。

學習目的

3. 本模組共有六個小節包括(1)前言 (2)安全威脅 (3)安全防護 (4) OSI安全架構 (5)安全模型 (6)結論，共須三個鐘點。

Module 1：網路安全導論

- Module 1-1：前言(*)
- Module 1-2：安全威脅(*)
- Module 1-3：安全防護(*)
- Module 1-4：OSI安全架構(*)
- Module 1-5：安全模型(**)
- Module 1-6：結論(*)
- Module 1-7：專案實作(**)

* 初級(basic):基礎性教材內容
**中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容
***高級(advanced):適用於深入研究的內容

Module 1-1：前言(*)

前言

『如果沒有網路、安全就容易許多』

網路安全的議題

- 網路安全的定義
- 網路安全的方法
- 網路安全衍生的問題

網路安全環境的構成

- 個人電腦
- 作業系統
- 使用者
- 防火牆
- 組織政策

課程模組介紹

- 網路安全的威脅
- 相關的防護機制
- 網路安全問題
- 安全模型
- 網路安全評估方法

Module 1-2：安全威脅(*)

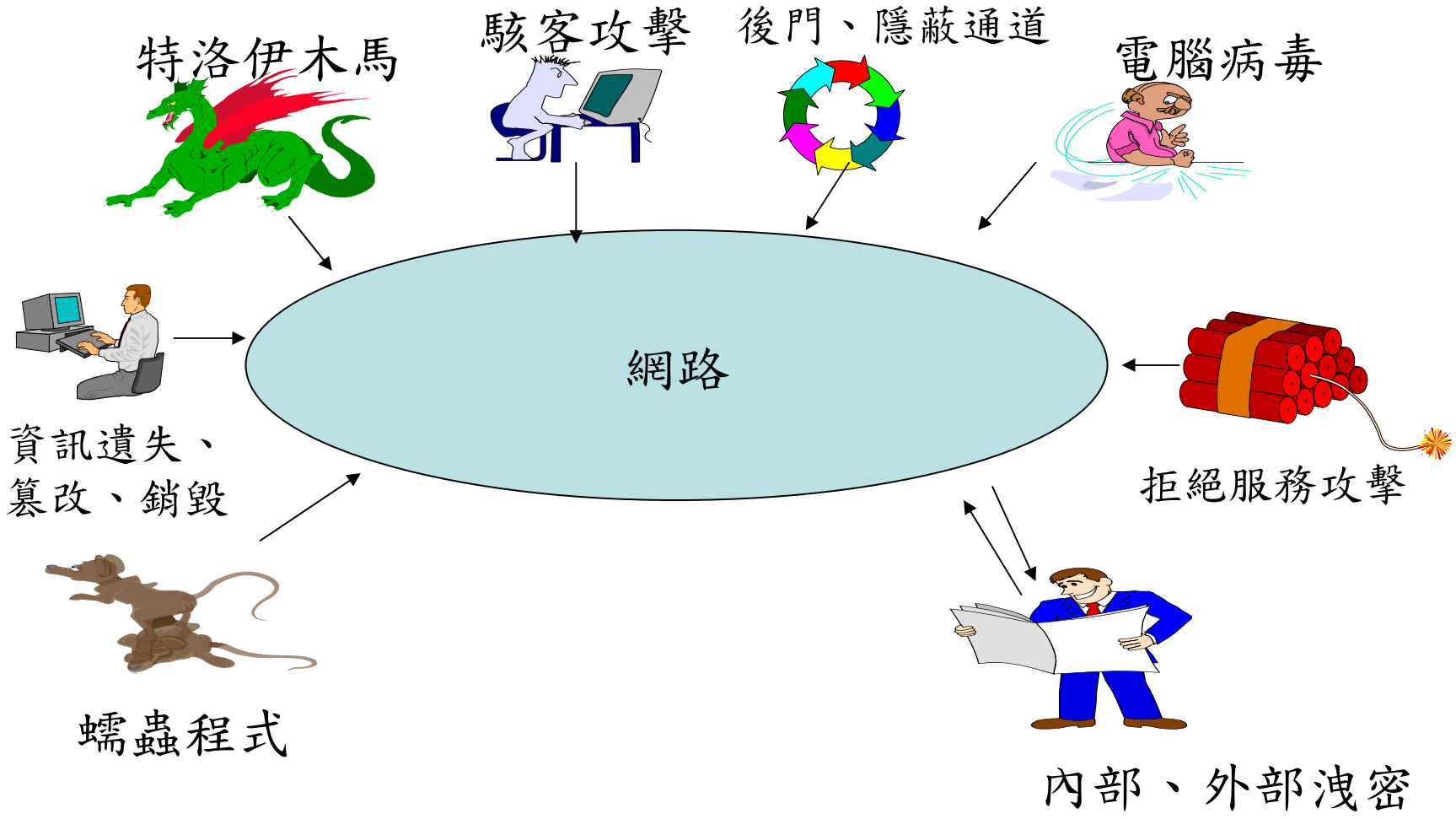
安全威脅

網路所存在的安全威脅幾乎涵蓋了以ISO/OSI 所定義的TCP/IP七層架構中的每一層。

安全威脅類型

- 資訊蒐集
- 竊聽
- 欺騙
- 連線劫持
- 拒絕服務

電腦網路安全所面臨威脅



資料來源：摘自卿斯漢，網路安全縱橫談。

威脅種類

1. 資訊蒐集(reconnaissance)

威脅種類

2. 竊聽(Sniffer)

威脅種類

3. 欺騙(Spoofing)

威脅種類

4. 連線劫持(Session Hijacking)

威脅種類

5. 拒絕服務(Denial of Service)

威脅成因(弱點)

1. 資訊蒐集
- TCP/IP通訊協定固有的不安全性
- 系統所提供的服務資訊(BANNER)
- 應該封鎖的暴露服務
- 個人資訊的暴露

威脅成因(弱點)

2. 竊聽
   - 安全性不足的實體安全性
   - 傳送機密資料時缺乏加密
   - 以純文字或安全性不足的加密或雜湊演算法來傳輸重要資訊

威脅成因(弱點)

3. 欺騙

- TCP/IP通訊協定固有的不安全性
- 缺乏連線來源與目的篩選限制
- 不安全的使用者身份辨識方法

威脅成因(弱點)

4. 連線劫持

- 實體的安全性不足
- TCP/IP通訊協定固有的不安全性
- 未加密的通訊
- 未鑑別的連線

威脅成因(弱點)

5. 拒絕服務

- TCP/IP通訊協定固有的不安全性
- 安全性不足的路由器及交換器設定
- 未加密的通訊
- 服務軟體的錯誤

威脅方式(攻擊手段)

1. 資訊蒐集
- Tracert
- Telnet
- 掃瞄
- 廣播要求
- 代理程式

威脅方式(攻擊手段)

2. 竊聽
   - 攻擊者將封包竊聽工具放在目標網路上，以擷取所有資料傳輸

威脅方式(攻擊手段)

3. 欺騙
   - 修改封包
   - 偽冒使用者

威脅方式(攻擊手段)

4. 連線劫持
   - 攻擊者使用工具來結合欺騙、路由變更及封包處理。

威脅方式(攻擊手段)

5. 拒絕服務

- 暴力式封包溢流
- SYN 溢流攻擊
- 服務剝削
- 蠕蟲、病毒、木馬

Module 1-3：安全防護(*)

安全防護(防禦方式)

1. 資訊蒐集防護

- 使用一般性的設定資訊來發送服務訊息(BANNER)
- 使用防火牆來限制不應該公開揭示的服務
- 人員正確的危險認知(警覺)

2. 竊聽防護

- 增強實體安全性
- 防止惡意裝置、程式的安裝
- 區隔限制網路封包廣播範圍
- 加密透過網路傳送的資料
- 強固的網路設備管理權限控管
- 使用工具協助偵測竊聽裝置

3. 欺騙防護

- 在路由、交換器上限制篩選網路連線的來源及目的位址
- 固定的網路及網卡位址對應關係
- 安全可靠的使用者身份辨識

4. 連線劫持防護

- 對工作階段加密
- 在防火牆設定對連線狀況的檢查

5. 拒絕服務防護

- 限制篩選廣播要求
- 限制篩選網際網路控制訊息通訊協定(ICMP)要求
- 修補及更新服務軟體
- 使用防毒(木馬)系統

Module 1-4：OSI安全架構(*)

OSI安全架構

X.800 OSI安全架構
(X.800,Security Architecture for OSI)

OSI安全架構的三個角度

- 安全攻擊：任何洩漏組織資訊安全的行為。
- 安全服務：能夠加強資訊安全的服務，這些服務是由數種安全機制提供。
- 安全機制：用來偵測或預防安全攻擊，或者能夠復原安全攻擊的機制。

安全攻擊

1. 主動式攻擊：
   - 偽裝
   - 修改訊息內容
   - 重送
   - 阻絕服務
   - 主動式攻擊偵測

安全攻擊

2. 被動式攻擊

- 被動式攻擊的重點
- 被動式攻擊偵測

安全服務

- 安全服務的目的
- 安全服務定義

安全服務

安全服務五種類別：

1. 鑑別
2. 存取控制
3. 資料完整性
4. 不可否認性
5. 資料隱密性

安全機制

- 特定安全機制
- 一般安全機制

安全機制

一般安全機制：

- 受信任的功能
- 安全標籤
- 事件偵測
- 安全稽核追蹤
- 安全復原

安全機制

特定安全機制：

- 加密
- 數位簽章
- 存取控制
- 資料完整性
- 驗證交換
- 路由控制
- 公證

安全服務項目 (Service)	對付的威脅 (Threat)	使用的安全機制 (Mechanism)
資料隱密性	截聽洩漏	運用SSL及S/MIME加密 資料加密 (DES , RSA)
資料完整性	篡改、重送、遺失	運用雜湊函數確保資料的完整性 數位信封 (RSA 及 DES)
資料來源鑑別	偽冒傳送假資料	運用公鑰／私鑰技術 訊息押碼 (MAC), 數位簽章 (RSA)
不可否認性	否認已收、送資料	使用數位簽章技術 數位簽章 (RSA)
存取控制	非法、冒名存取	使用權限伺服器 交互式身份驗證

資料來源：參考自ISO 7498-2, Security Architecture, 1989

入侵

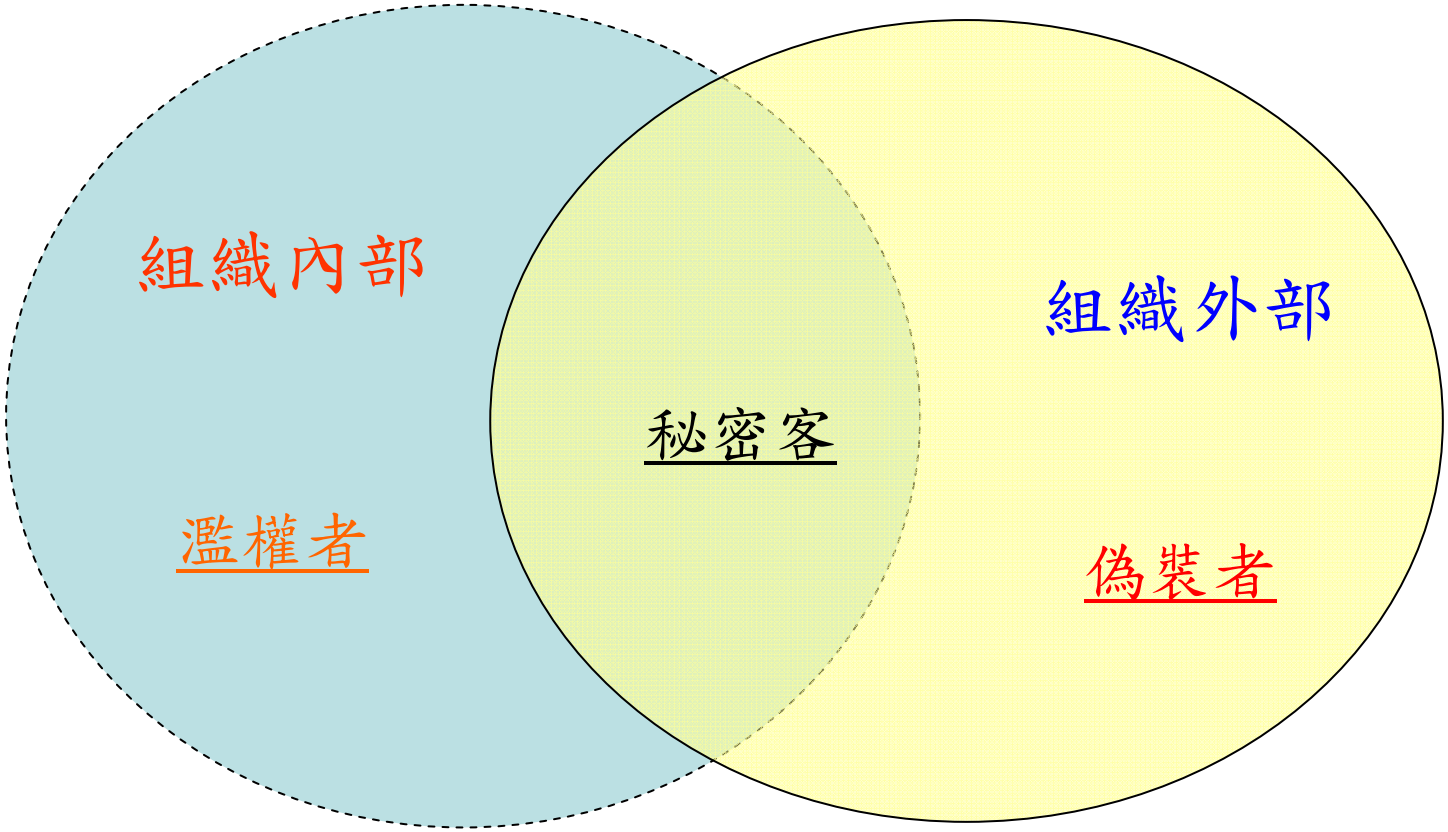
- 入侵(intrusion)的定義

三種等級的入侵者

1.偽裝者(Masquerader)

2.濫權者(Misfeasor)

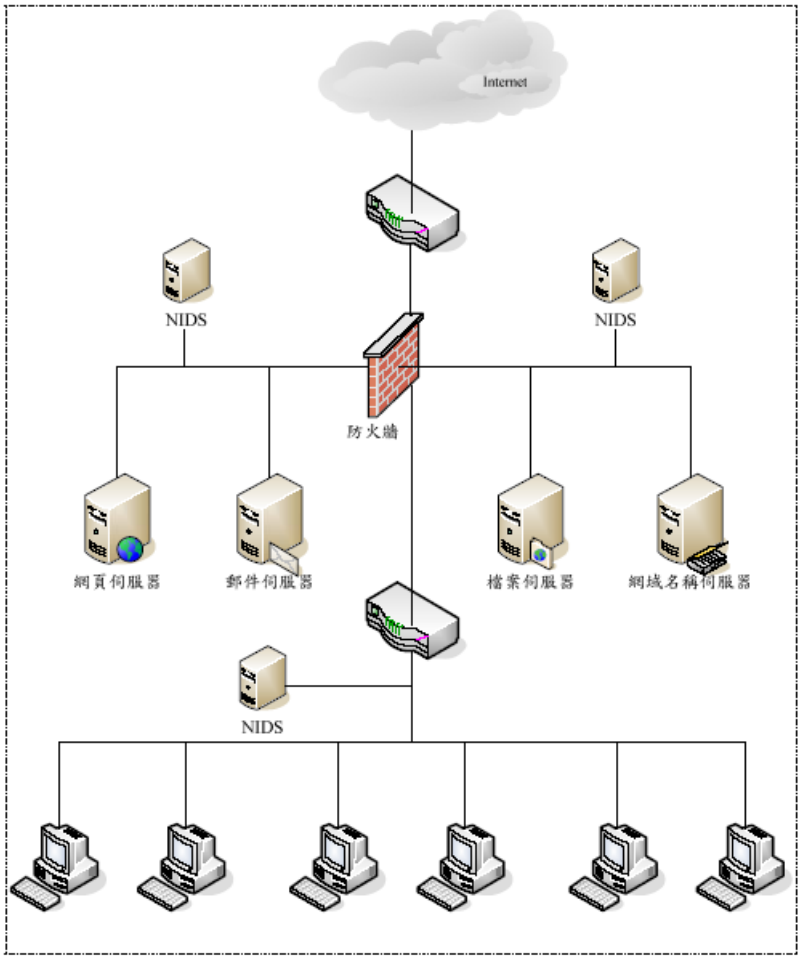
3.秘密客(Clandestine user)


組織內部
濫權者
秘密客
組織外部
偽裝者

入侵偵測

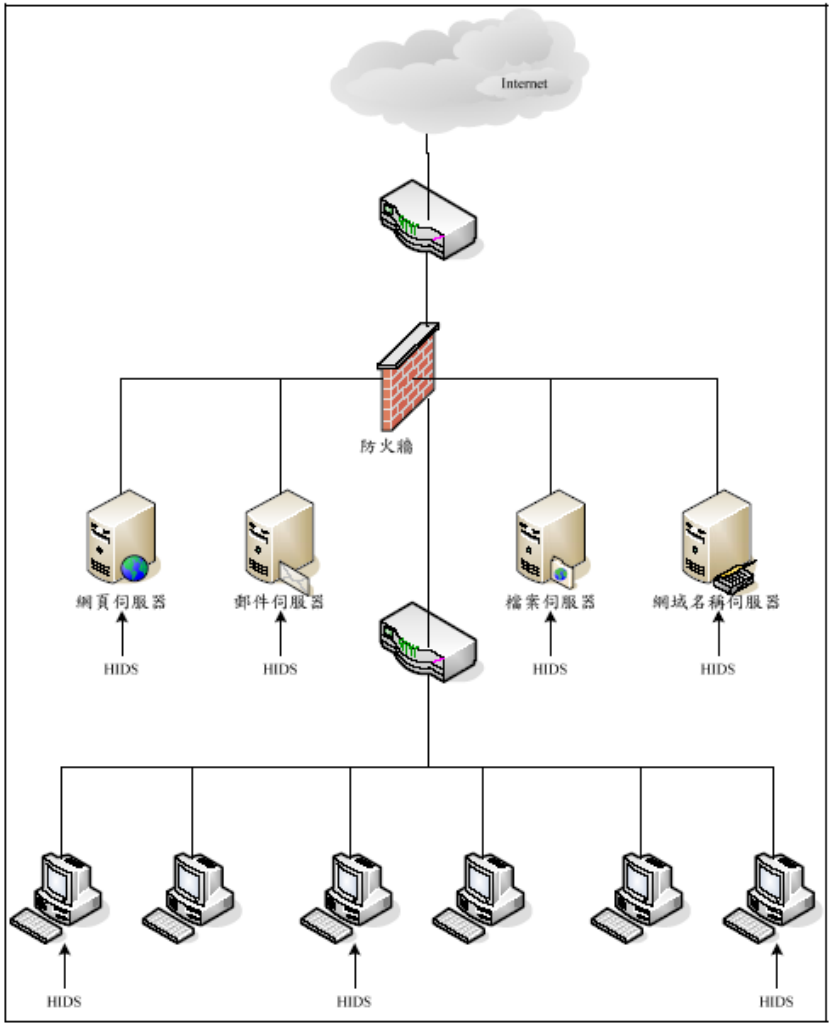
- 入侵偵測的定義
- 入侵偵測的作用
- 入侵偵測的技術
- 入侵偵測的類型

網路型入侵偵測系統架構



資料來源：摘自黃志雄，智慧型網路安全防衛系統之設計與實作。

主機型入侵偵測系統架構

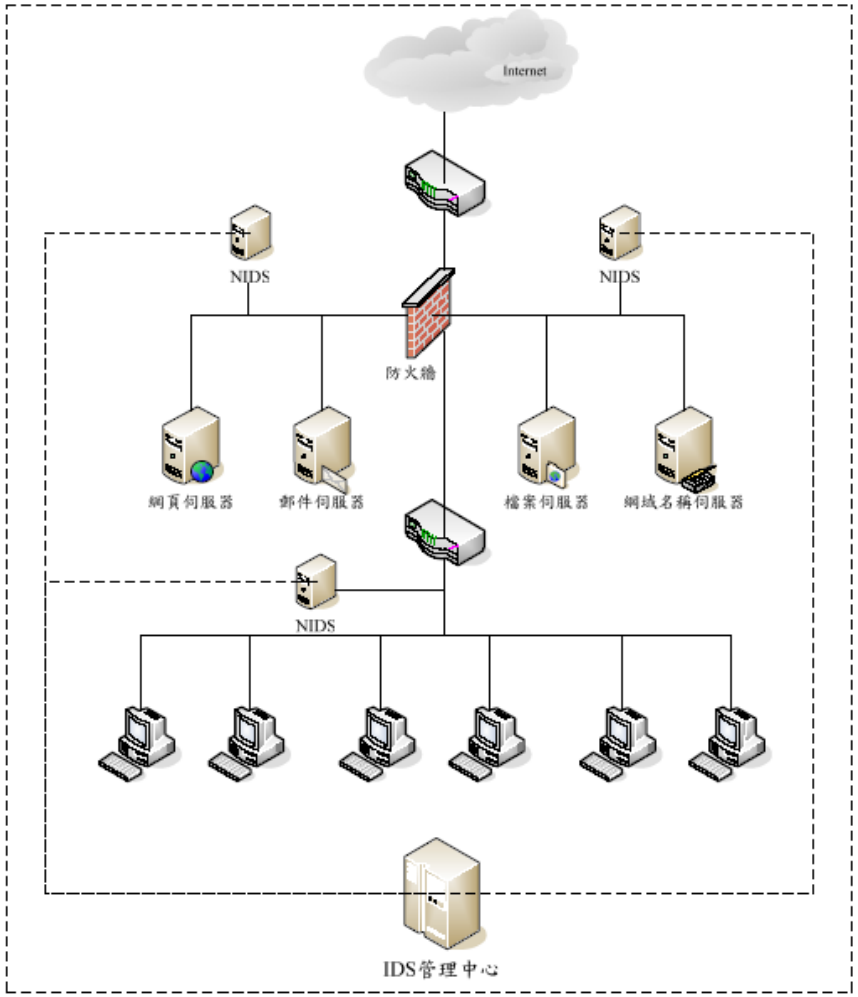


資料來源：摘自黃志雄，智慧型網路安全防衛系統之設計與實作。

分散式入侵偵測(Distributed Intrusion Detection)

- 集中架構
- 分散架構

分散式入侵偵測系統架構



資料來源：摘自黃志雄，智慧型網路安全防衛系統之設計與實作。

誘捕系統(Honeypots)

- 誘捕系統定義
- 誘捕系統作用

Module 1-5：安全模型(**)

安全模型

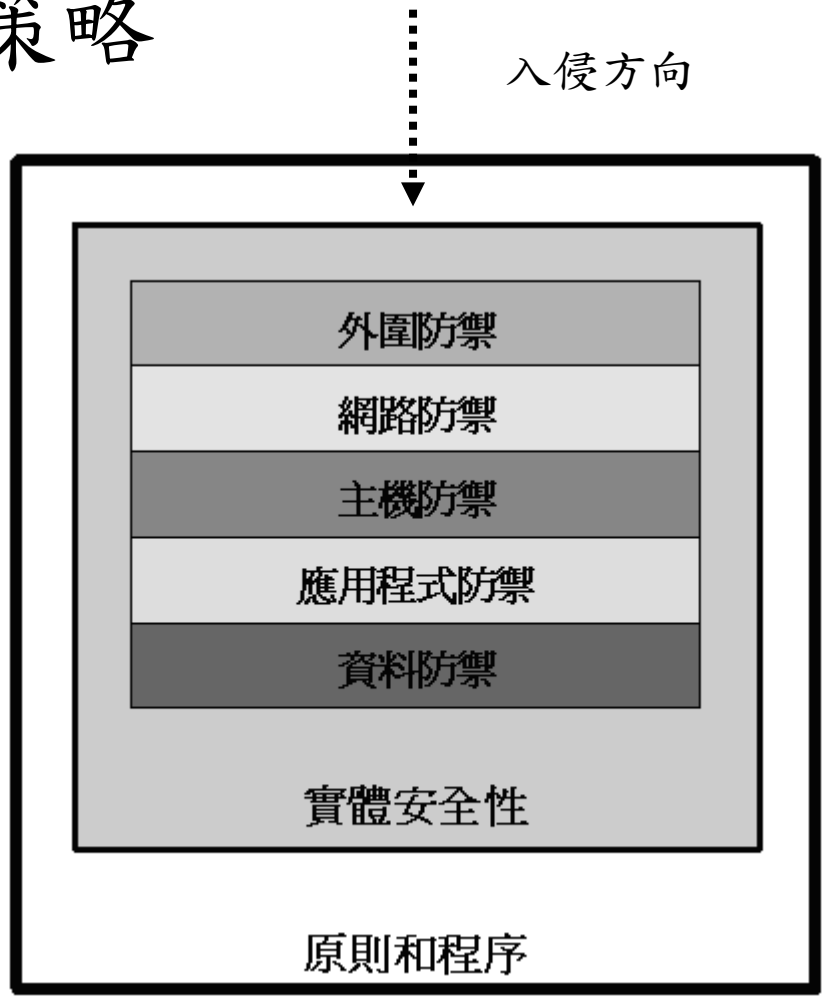
『網路是應用程式的進入點』

微軟_縱深(深度)防禦概念 (Defence in Depth)

微軟的深度防禦模型

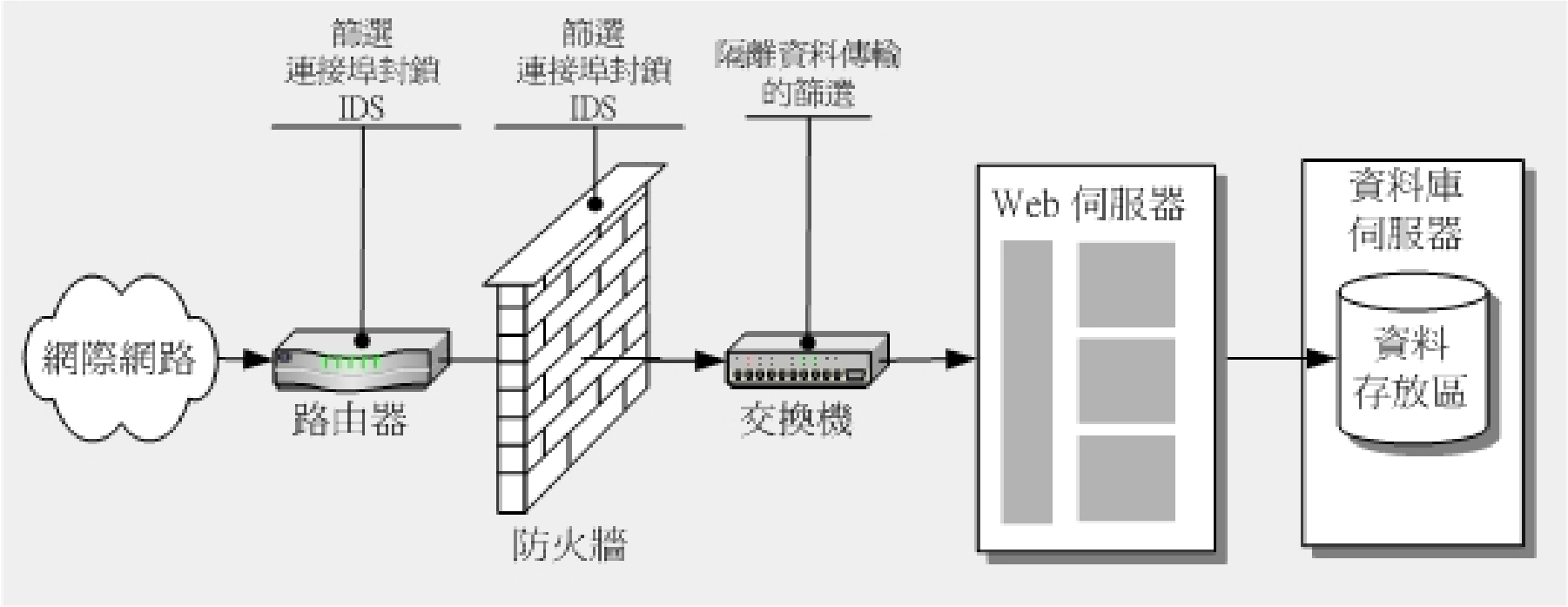
資料來源：摘自微軟TechNet網站，安全性風險管理指南。

微軟深度防禦策略



資料來源：摘自微軟TechNet網站，Windows 2000 Server 安全性指南。

典型的網路應用系統架構



資料來源：摘自微軟MSDN網站，保障網路的安全。

安全模型評估範例

評估對象：客戶線上訂購系統存取點一

1. 位置：網際網路至路由器。
2. 來源：主要為由外至內。

安全模型評估範例

3. 威脅：
   a. 實體破壞(線路)
   b. 資訊蒐集
   c. 竊聽
   d. 欺騙
   e. 阻斷服務
   f. 實體環境(高溫、火災、無備用電源)等

安全模型評估範例

4. 弱點：
   a. 無良好防護的線路
   b. 路由器軟體版本有安全性缺陷
   c. 網路通訊未加密
   d. 客戶僅以帳號及密碼辨識
   f. 路由器是放置在不具備環境控制的非安全的場所

安全模型評估範例

5. 可能攻擊行動：

   攻擊者以路由器已知的出廠預設後門密碼，入侵路由器後取得最高控制權限。

6. 安全防護機制：

   在路由器上設定限制對路由器的可連線登入存取網址。

安全模型評估範例

7. 風險等級：

   路由器經防護限制後仍有安全顧慮，其風險等級為中等。

8. 可能損害：

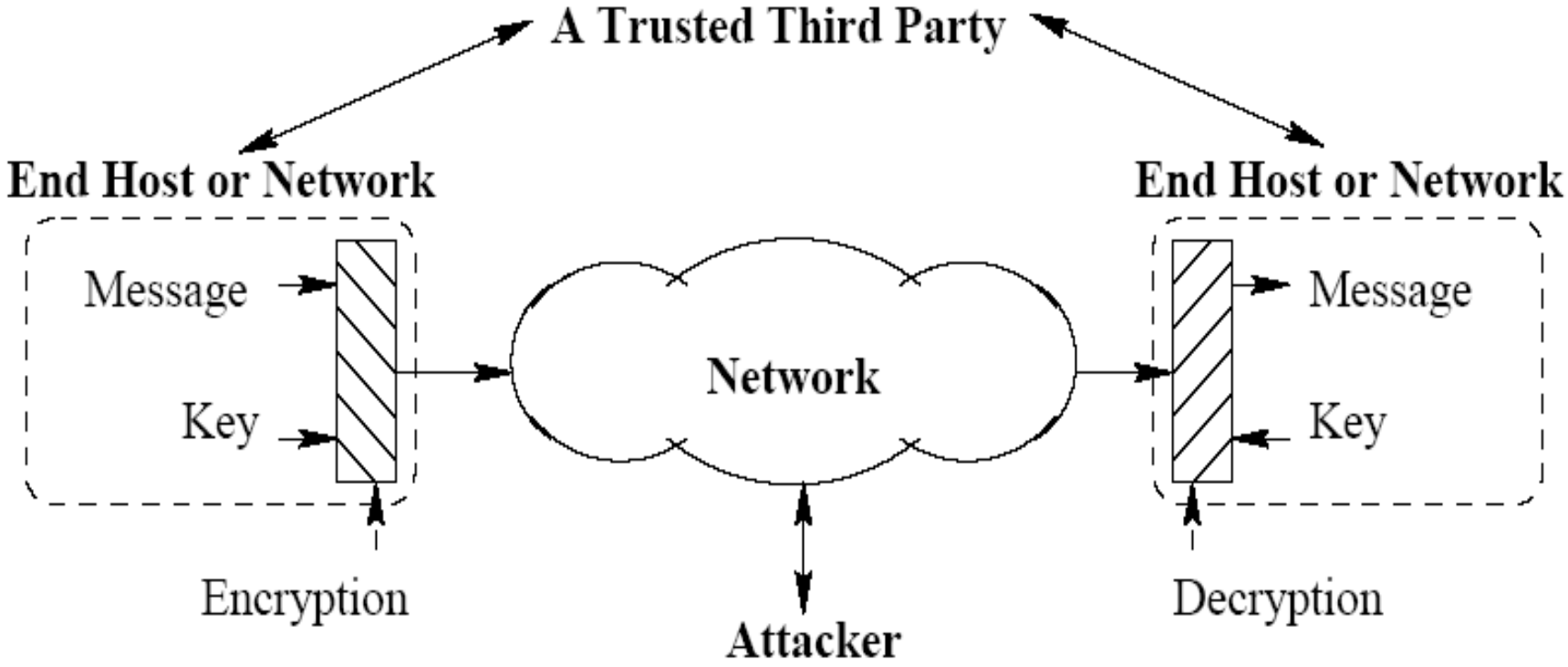
   對外網路連線中斷，客戶無法線上訂購產品，估計每小時損失……。

安全模型評估範例

9. 修復及災難復原成本：

因路由器軟體版本已無法更新，需新購XX廠牌XX型路由器乙部所需經費…。

網路安全模型

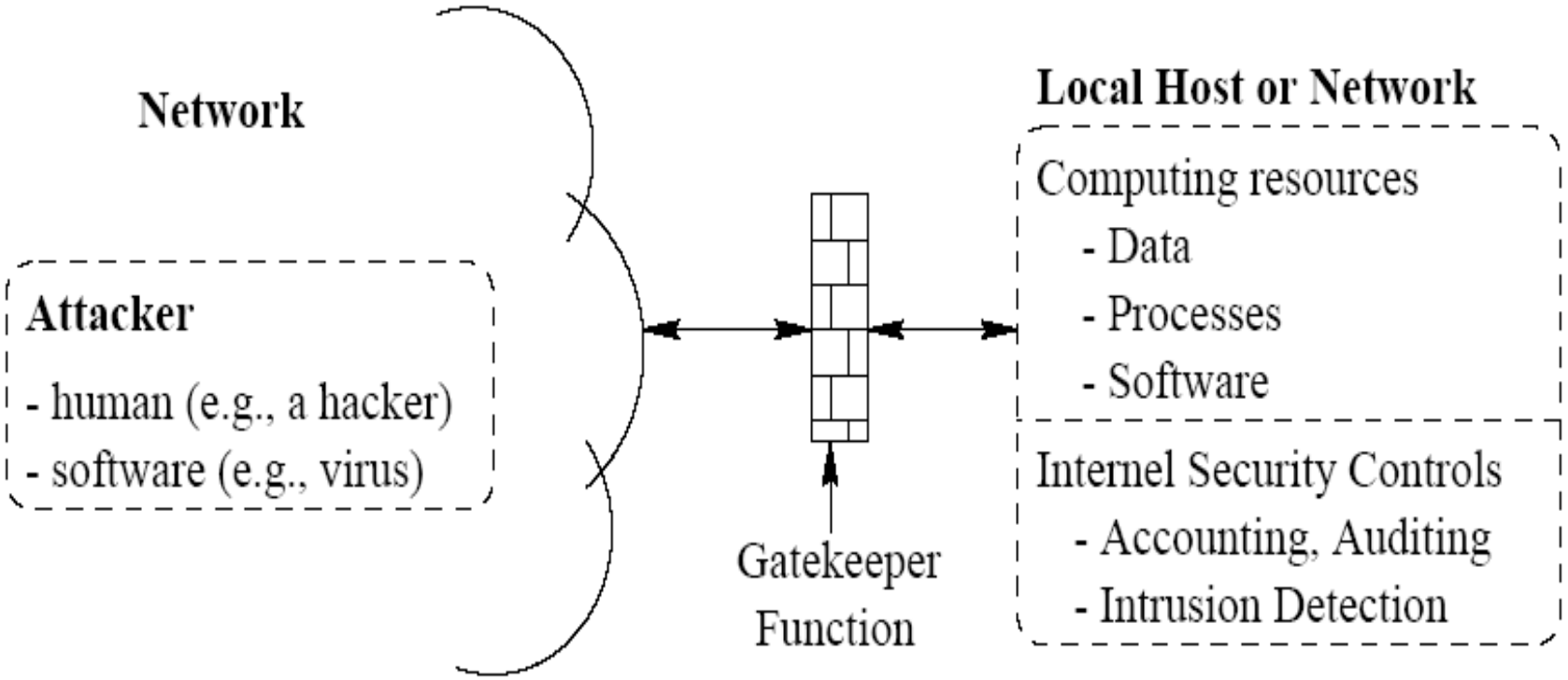


資料來源：摘自**Panwar, Mao, Ryoo, Li: TCP/IP Essentials**。

網路安全的四個基本任務

1. 設計安全的資訊轉換演算法。
2. 產生秘密金鑰。
3. 設計傳送與分享金鑰的方法。
4. 指定使用的協定

網路存取安全模型



資料來源：摘自**Panwar, Mao, Ryoo, Li: TCP/IP Essentials**。

使用網路存取安全模型的注意事項

1. 選取適當的守門人函數來辨識使用者。
2. 實作安全控管，確保唯有獲授權的使用者才能存取特定的訊息或資源。
3. 利用受信任的電腦系統來實作這個模型。

Module 1-6：結論(*)

結論

『網路本身並沒有危險性』

影響網路安全的幾個因素：

	技術層面	社會層面（使用者）
無心之過	軟體設計不良、 當機、病毒	忘記密碼、人為疏忽
惡意為之	密碼破解、病毒、 木馬	駭客、職員故意破壞

資料來源：摘自國家圖書館網站，網路安全。

網路安全新興威脅七大特徵：

1.歷史悠久的惡意程式自我防禦技術
2.令人眼花撩亂的龐大變種惡意程式
3.亂”件”齊發的垃圾郵件
4.難以抗拒的誘惑-社交工程
5.有洞就鑽
6.就是要你消受不起-DDoS
7.陸海空聯合大進擊-混合式攻擊

資料來源：摘自宋紅偉，展望網路安全 新興安全威脅七大特徵。

本課程暫時摒除使用者的因素，針對當前的網路安全威脅，在後續的課程模組中逐一的介紹相關主要的防護因應機制，期望能對開始接觸網路安全知識的學習者有所助益。

習 題

習題一

- 假設您是組織的資訊安全人員，請針對個人電腦的防護草擬一份電腦網路連線的安全政策，以提供資訊安全長訂定組織政策的參考。

習題二

- 請參考OSI/ISO 的所定義的TCP/IP七層架構，分別針對每一層目前已知的安全性威脅手法(案例)，加以蒐集資料並分別列表(例如2003年發生的疾風蠕蟲MSBlast.A 是屬於在網路層拒絕服務的一種)。

習題三

- 請參考投投影片第1-16頁，針對圖中目前電腦網路安全所面臨的各種威脅，自網路上搜尋最近二年來所發生的相關案例，每種至少列舉出三則，並請註明資料來源。

習題四

- 請就網路上提供的FTP、MAIL、WEB等資訊服務，進行資料蒐集，針對其所提供的服務資訊(BANNER)嘗試蒐集系統之種類、版本等相關資訊(每類服務至少各舉出三個以上的站台)。

習題五

- 請簡單比較主動式攻擊和被動式攻擊有何不同 。

習題六

- 請說明安全服務的五種類別和其意義 。

習題七

- 請說明安全服務所要應付的威脅和其所採用的安全機制為何 。

習題八

- 請簡單比較分散式入侵偵測之集中架構與分散架構有何優缺點。

習題九

- 請簡單說明誘捕系統的作用。

習題十

請說明網路安全的四個基本任務。

Module 1-7:專案實作(**)

專案目的

- 本專案以學校的線上選課系統為對象，進行安全模型評估。
- 利用實際操作的方式讓同學了解安全模型評估。

專案描述

- 請參考Module 1-5安全模型評估範例，並以學校的線上選課系統為對象，進行安全模型評估。

參考文獻

1.陳富國，網路安全精要應用與標準，弘光大學資管系簡報。

2.網路安全，國定圖書館網站，http://infotrip.ncl.edu.tw/law/security.html。

3.保障網路的安全。Microsoft MSDN網站，
http://www.microsoft.com/taiwan/msdn/secmod/html/secmod88.mspx

4.賴榮樞，企業資安防護的重要觀念，Microsoft TechNet網站，
http://www.microsoft.com/taiwan/technet/columns/profwin/
15-security_enterprise.mspx

5. Shivendra Panwar, Shiwen Mao Jeong-dong Ryoo, and Yihan Li，
TCP/IP Essentials ，
http://assets.cambridge.org/052195049X/full_version/052195049X_pub.pdf

6. William Stallings，Cryptography and Network Security Third Edition，
http://williamstallings.com/Crypto3e.html

7.宋紅偉，展望網路安全 新興安全威脅七大特徵，天極Blog。
http://www.5dmail.net/html/2006-1-26/2006126100433.htm

8.黃志雄，民94，智慧型網路安全防衛系統之設計與實作，
東海大學資科所碩士論文。

9. 安全性風險管理指南， Microsoft TechNet網站，
http://www.microsoft.com/taiwan/technet/security/topics/complianceandpolicies/secrisk/srsgch04.mspx
10. Windows 2000 Server 安全性指南， Microsoft TechNet網站，
http://www.microsoft.com/taiwan/technet/Security/prodtech/win2000/staysecure/secops02.aspx