Chap11 網路安全

高中資訊科技概論

松崗圖書公司

本章目錄

11-1 網路安全問題

一、電腦病毒

二、駭客

三、間諜軟體

四、網路釣魚

五、網路蠕蟲

六、垃圾郵件處理

11-2 網路安全防護

一、防毒軟體

二、防火牆

三、資料備份

四、資料加密

五、無線網路的安全性

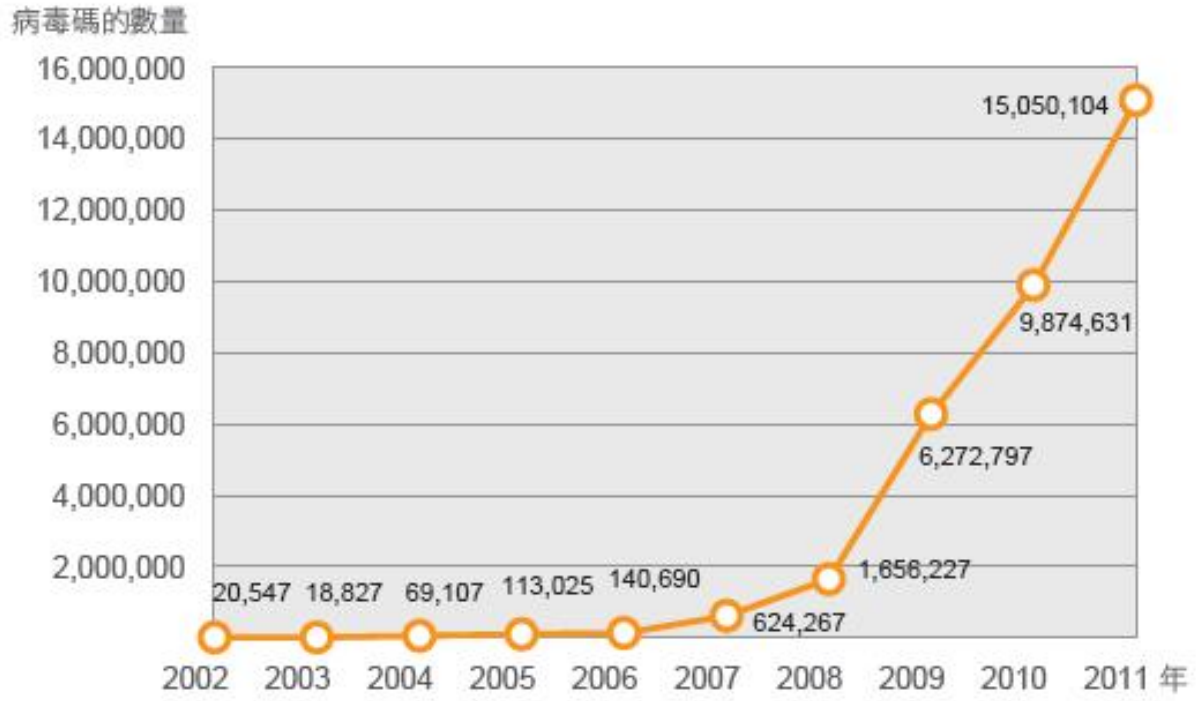
11-1 網路安全問題

11-1 網路安全問題

- 網路使生活更便利，但我們常忽略這些科技所潛藏的**安全問題**
- 例如**病毒**、**駭客**、**木馬程式**等**惡意程式** (Malware) 常造成很大損失
- 如何提升網路的安全性，避免資料被竊取、篡改、僞造，是資訊時代的當務之急

一、電腦病毒 (Virus)

- 電腦病毒常位居網路安全問題的第一位，由防毒軟體的病毒碼數量可以發現，病毒的成長速度越來越快



防毒軟體病毒碼的趨勢圖 (來源：Symantec 網站)

一、電腦病毒

特性

1. 會將自己複製到正常檔案或開機區
2. 一個檔案中毒，該台電腦其他檔案可能也會被感染
3. 有些只是惡作劇；有些可能會造成電腦資料的損毀，甚至破壞硬碟
4. 有些會快速且大量散佈，造成網路癱瘓

一、電腦病毒 (Virus)

- 病毒分類
  - 開機型病毒 (Boot-type Virus)
    - 會感染硬碟的開機區
    - 電腦一開機，病毒便會被載入記憶體，伺機感染其他檔案
  - 檔案型病毒 (File-type Virus)
    - 會感染電腦的可執行檔
    - 當這些檔案被執行時，病毒就會被執行

一、電腦病毒 (Virus)

- 電腦病毒的分類
  - 複合型病毒 (Multi-partite Virus)
    - 兼具開機型與檔案型病毒的特性
    - 例如台灣曾經大流行的 Hammer 病毒、歐洲流行的 Flip 病毒皆屬此類型
  - 千面人病毒 (Polymorphic / Mutation Virus)
    - 每次都會以不同的病毒碼傳染出去
    - 例如 Whale 病毒的病毒碼幾乎都不相同；Flip 病毒只有 2 Bytes 的共同病毒碼

一、電腦病毒 (Virus)

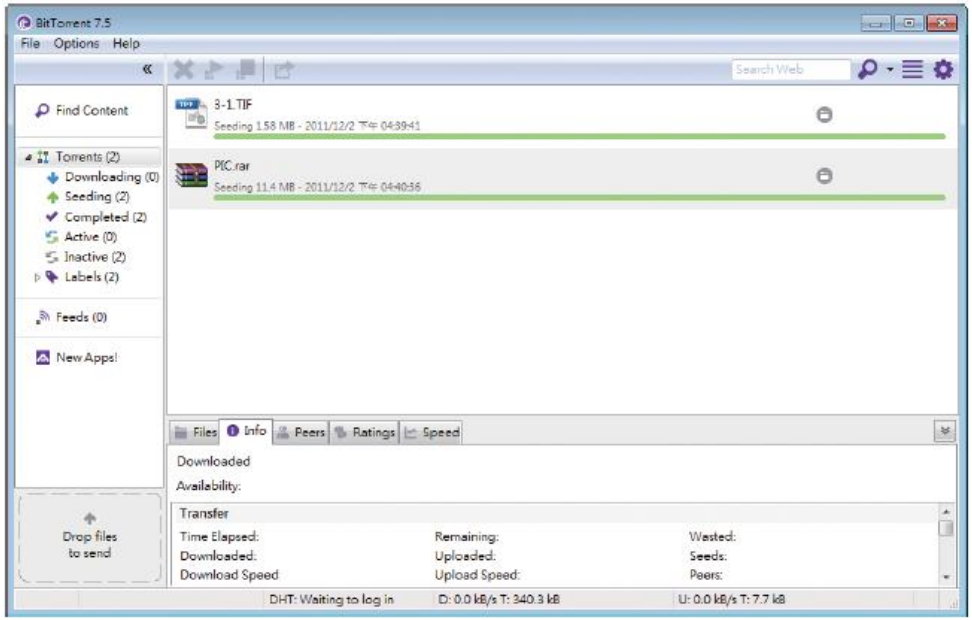
- 電腦病毒的分類
  - 網頁型病毒
    - 網際網路已成爲病毒最佳的傳播者
    - 使用者只要瀏覽含有網頁型病毒的網頁，可能不知不覺就會受到感染
    - 此類型病毒寄生於網際網路上，防範更爲困難

二、駭客 (Hacker)

- 起初是指一群熱衷寫程式的人，藉由撰寫自由軟體，促進資訊的交流與分享
- 現在駭客帶有負面的意涵，主要是源自於被稱爲破網者或鬼客的 Cracker，是指一群未經許可，透過網路擅入電腦系統的人
- 駭客通常具有特殊目的，如竊取商業機密、挖掘個人隱私、竄改重要資料、更改網站首頁、破壞系統與檔案、或阻斷服務等。
- 駭客行爲會**觸犯法律**，如**隱私權**、**智慧財產權**等

二、駭客 (Hacker)

- 經過正常管道入侵
  - 例如透過合法下載的程式，直接入侵使用者的電腦等。
  - 進入別人電腦分享的目錄，進行破壞，如網路芳鄰或 P2P 的分享目錄等

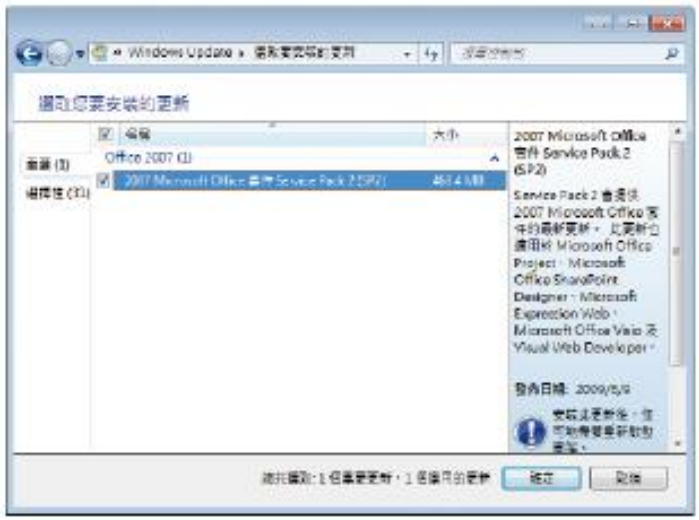


二、駭客 (Hacker)

- 利用系統漏洞
  - 駭客最常利用作業系統或應用軟體的安全漏洞，作爲入侵的管道
  - 系統或軟體都應隨時修補漏洞或更新



Windows 作業系統 Update



Microsoft Office 升級套件

作業系統或應用軟體修補漏洞

二、駭客 (Hacker)

- 木馬程式 (Trojan)

  隱藏在合法電腦程式內，安裝到電腦後，會危害電腦系統的安全。

  是目前最常見的入侵的手法，也是最不容易防範的。

  常見木馬的種類：

  - 破壞型

    會破壞並且刪除電腦重要的檔案，如 .exe 等類型檔案

二、駭客 (Hacker)

- 木馬程式 (Trojan)
  - 密碼發送型

    會將電腦裏隱藏的**密碼**轉送到網路指定的位置

    尤其許多使用者登錄網站時，爲了避免重新輸入密碼，常使用**記憶密碼**的功能，但許多木馬程式都可以找到並破解這些密碼資料

二、駭客 (Hacker)

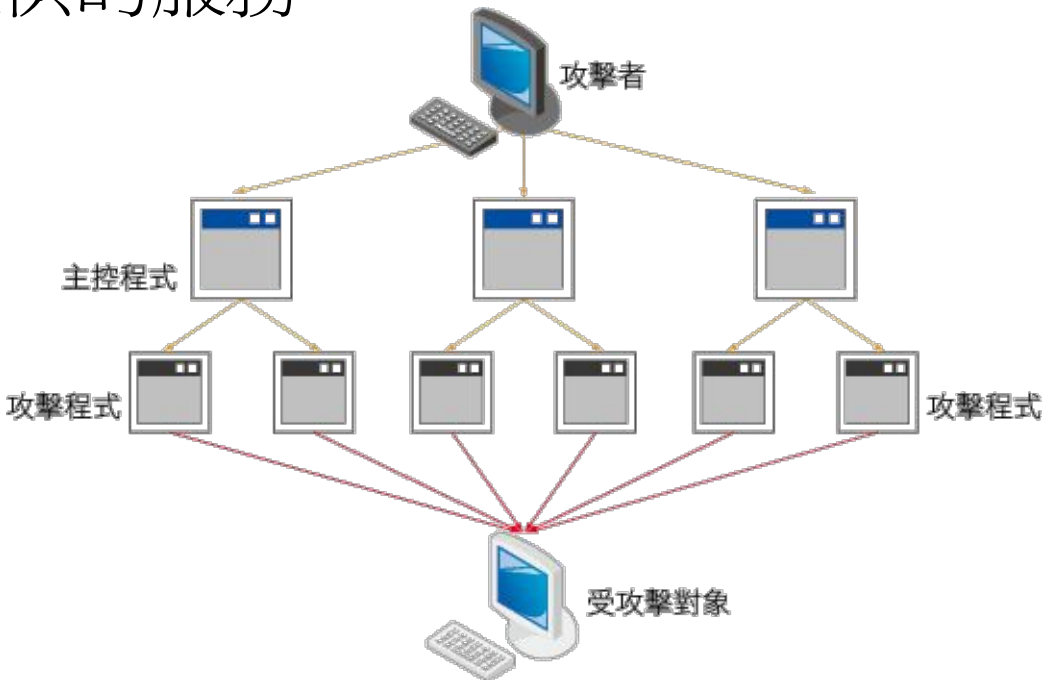
- 木馬程式 (Trojan)
  - 遠端存取型

    只要使用者執行**遠端服務程式**，木馬程式就可以知道服務端的 IP 位址、帳號與密碼，進而進行遠端控制
  - 鍵盤記錄型

    使用者按下鍵盤的任何按鍵，都會被木馬程式記錄，再從記錄中找到帳號密碼等重要資料

二、駭客 (Hacker)

- 木馬程式 (Trojan)
  - 阻斷服務 DoS (Denial of Service, DoS) 攻擊型
    - 是指利用程式瞬間產生**大量的網路封包**，癱瘓網路和主機，讓使用者無法獲得網路或主機提供的服務



二、駭客 (Hacker)

- 木馬程式 (Trojan)
  - 駭客入侵到有安全漏洞的伺服器後，會在原網頁加入一段 HTML，其他使用者瀏覽此網頁，紅色標示的 HTML 就會自動下載**惡意程式**，植入使用者的電腦中



二、駭客 (Hacker)

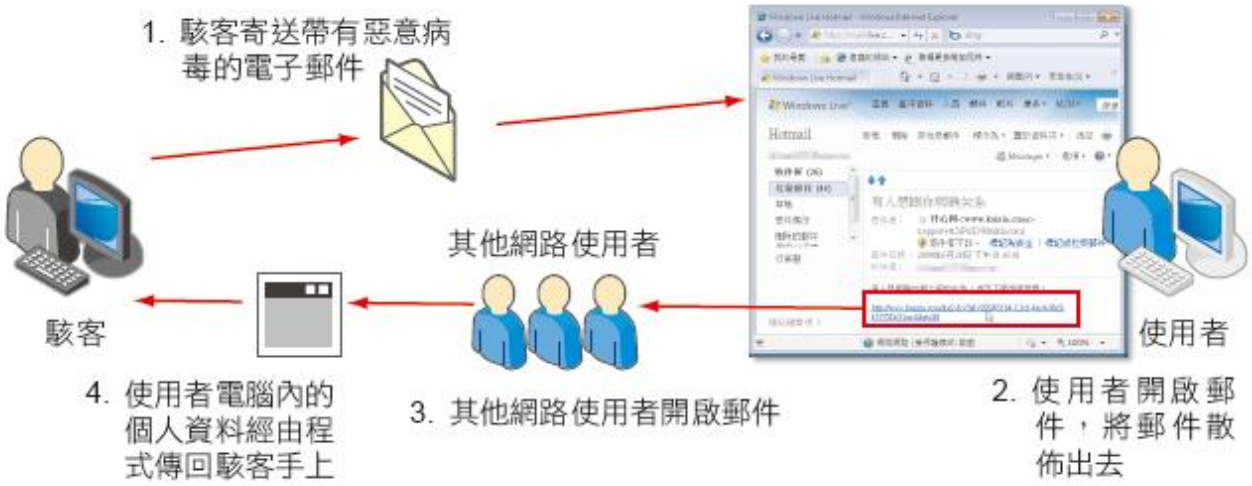
- 木馬程式 (Trojan)
  - 設計網頁資料庫程式時，若有安全漏洞，可能會讓駭客取得管理者的帳號密碼。駭客就可以在伺服器裏建立、竄改、或刪除資料庫的重要資料



駭客於伺服器資料庫內植入資料

三、間諜軟體

- 指未經使用者同意，在電腦進行特定工作的軟體
- 不會大量繁殖，也不會破壞系統；可能會**竊取**使用者的資料或**綁架**網頁；或將使用者的 email 加入**垃圾信件名單**中；或竊取即時通訊的資料等



三、間諜軟體 (Spyware)

- 被植入間諜軟體的電腦常有以下特徵：

1.瀏覽器自動跳出**廣告視窗**，無法移除

2.瀏覽器**首頁**被改成其他網站，且無法改回原設定值

3.瀏覽器自動被啓動到**特定網頁**上

4.遊戲寶物或網路帳號密碼被盜用

5.上網速度**變慢**或著會自動**當機**

6.反間諜軟體或防毒軟體**無法正常運作**

四、網路釣魚 (Phishing)

- 網路釣魚就是以網路爲媒介，利用僞造的電子郵件或網站作爲誘餌，讓使用者洩漏機密資料
- 例如設計仿真的假網站，讓使用者誤以爲是真實網站，便進行刷卡消費，詐取他人財物
- 根據統計，網路釣魚有愈來愈多的趨勢

四、網路釣魚 (Phishing)

- 常見的手法
  - 寄發**假郵件**
    - 例如僞造銀行寄發的郵件，要求確認帳號與密碼，連線至假的網路銀行
  - 利用**假網域名稱**
    - 註冊類似的網域名稱，只要使用者瀏覽這些假網頁，就可能被植入木馬程式
  - 利用網頁的**假連結**
    - 在使用者信賴的網站，設計一個連結，讓使用者以爲是在真的網站內，實際上已被連結到別的地方，藉此欺騙使用者輸入重要資料

四、網路釣魚 (Phishing)

- 防範方法
  - 開啓連結網址時，先**複製**網址，**貼到**瀏覽器測試正確性，如果是詐騙的網路釣魚，使用的網址大多是假的
  - 注意瀏覽器的狀態，含有安全性資料內容的正常網頁，如網路銀行的網頁等，瀏覽器右下角會有「鎖頭」圖示；如果沒有，表示沒有加上**加密協定**，可能是危險的網頁

五、網路蠕蟲 (Worm)

- 是一種獨立的**程式**，會自我**複製或變形**後，透過網路連線傳播。會使電腦當機，占用網路頻寬，使網路**阻塞**
- 具有**大量複製**的能力，被感染的電腦，有時會自動傳 email 給通訊錄的每個人。若收件者的電腦也感染，會重複相同的動作，形成龐大的流量，癱瘓網路
- 常利用 OS 的**安全漏洞**，進行散佈；有時會合併其他惡意程式攻擊電腦；型態轉變相當快，常讓防毒軟體來不及因應

六、垃圾郵件處理

- Email 中，常常夾雜許多**不請自來**的**沒用**信件，如廣告信、色情資訊等
- 這些未經收件人**允許**，就大量寄出的郵件，就是**垃圾郵件 (Spam)**



廣告垃圾郵件

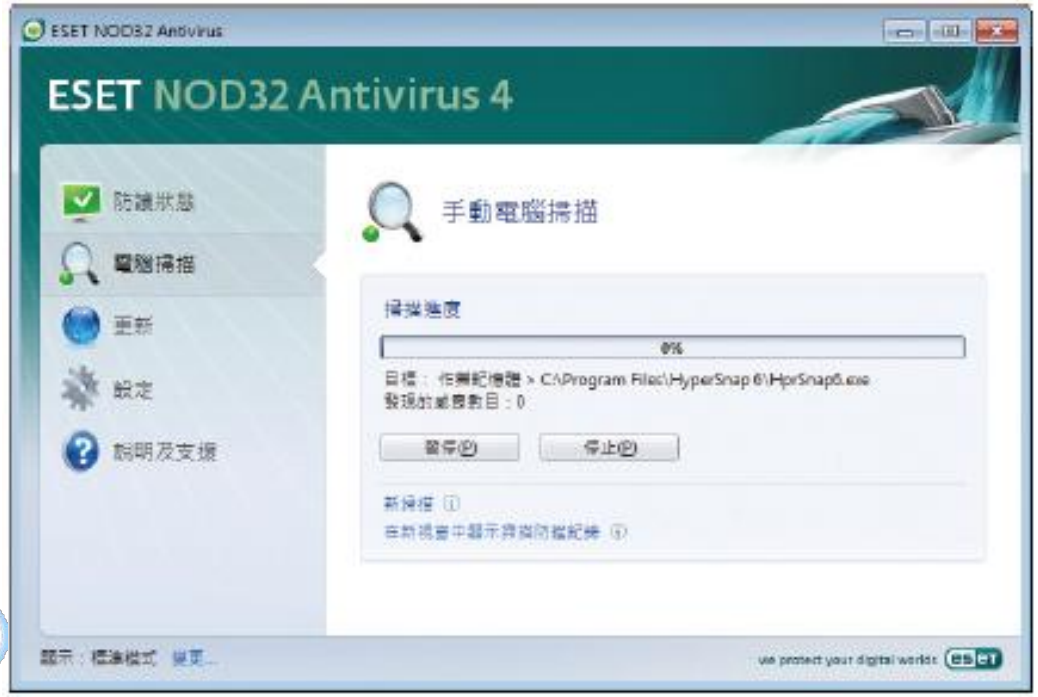
六、垃圾郵件處理

- 防範方法
  - **不隨意留下**電子郵件
    - 垃圾郵件常透過註冊網站時留下的 email 資料發送；一定要，可填較少使用的信箱
  - **不回覆**來歷不明的信件
    - 有些垃圾郵件會要求回覆，以確定 email 是否使用，回覆可能會收到更多垃圾郵件
  - 善用郵件的**密件副本**
    - 密件副本寄信，可將其他收件人的 email 隱藏起來，避免大家的信箱都被傳送出去

11-2 網路安全防護

一、防毒軟體

- 可清除或阻絕惡意軟體的應用軟體
- 具有監控、識別、病毒掃瞄和清除、自動升級和下載病毒碼等功能
- 是電腦的防禦系統，也是每台電腦必安裝的軟體



一、防毒軟體

- 電腦中毒處理步驟
  - 拔掉網路線，以免波及到其他電腦
  - 重新開機，按 **F8 鍵**進入**安全模式**
  - 使用防毒軟體刪除或修復中毒的檔案
  - 如要求慎重，可再次執行步驟 2 和 3，或使用**不同**掃毒工具再掃瞄一次
  - 接上網路線，重開新機，正常啓動OS
  - **更新系統**與防毒軟體的**病毒碼**
  - 使用已更新的防毒軟體再次掃瞄

一、防毒軟體

- 常見的防毒軟體

軟體名稱	Windows	Mac OS	Linux	免費
AOL Active Virus Shield	V			V
Avast! Home Edition	V		V	V
PC Tools AntiVirus Free Edition	V	V		V
PC-cillin 趨勢科技	V			
Avast! Professional Edition	V	V	V	
Kaspersky Anti-Virus	V	V	V	
McAfee VirusScan	V	V	V	
NOD32	V		V	
Norton AntiVirus 賽門鐵克	V	V	V	

練習

- 利用線上免費偵測資源，檢查自己的電腦是否有木馬程式

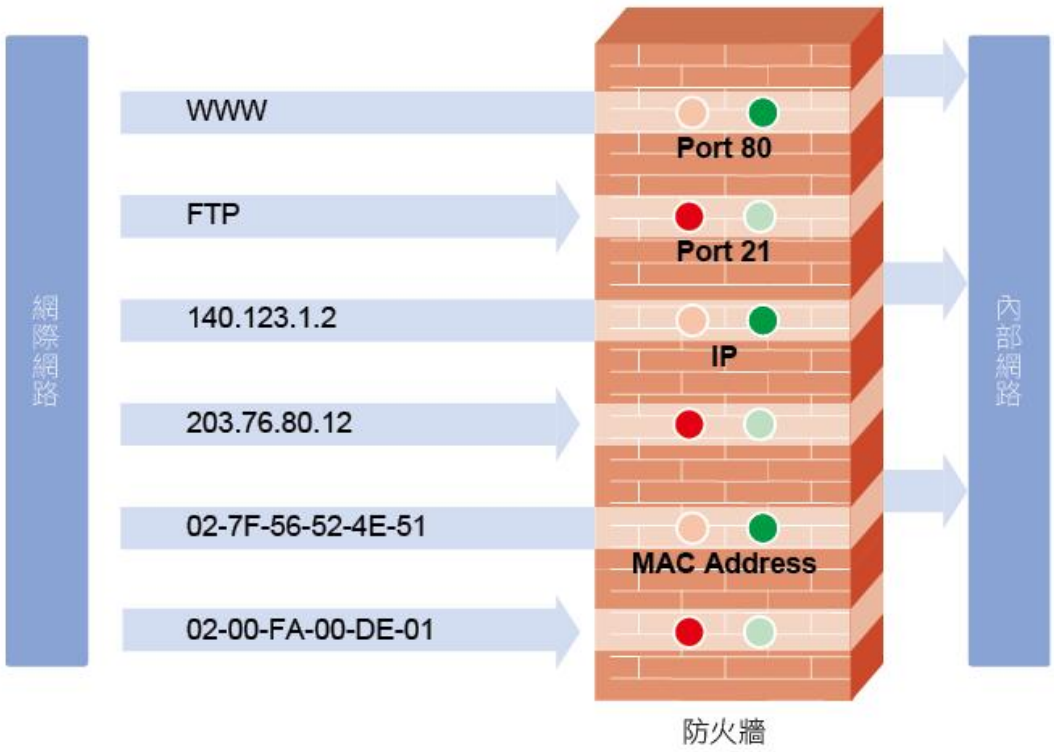
- 免費線上掃毒

二、防火牆

- 像門禁一樣，可以有效管制進入**內部網路**的封包
- 將內部網路和外部網路、或網際網路互相**隔離**，保護內部網路或主機
- **硬體式**防火牆使用獨立運作之硬體作爲防火牆，只做防火牆的功能，速度與效率較佳
- **軟體式**防火牆是在電腦安裝防火牆軟體，除了防火牆功能，也提供其他的服務

二、防火牆 (Firewall)

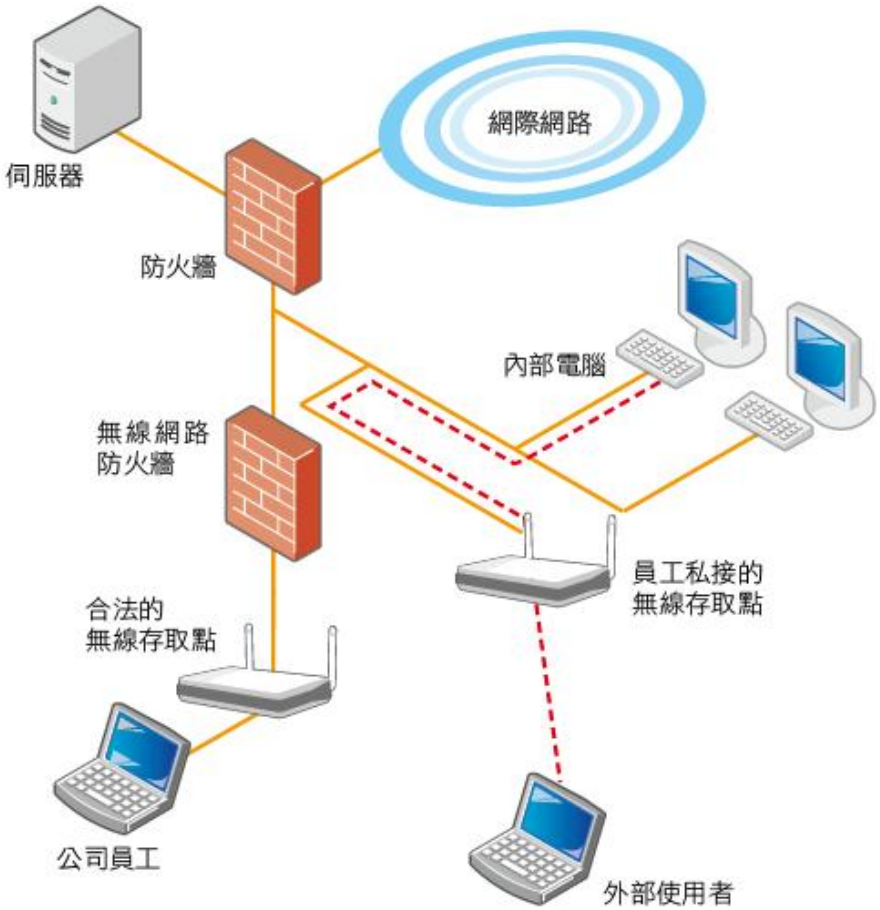
- 防火牆會過濾分析CP/IP的封包，例如 IP 來源、Port 號碼、MAC Address 等，判斷該封包是否能夠進入內部網路



網路防火牆的功能

二、防火牆 (Firewall)

- 防火牆**管不到繞過它的連線**
  - 例如內部網路有人利用有線網路，私接 AP 時，外部使用者，連上該台 AP，就可以完全不受防火牆管控



私接無線存取點可能會形成網路安全的漏洞

二、防火牆 (Firewall)

- 防火牆無法管控**合法**進入的惡意程式
  - 例如以**網頁**方式下載的惡意程式，透過 port **80** 進入內部網路，防火牆無法分辨它和網頁的封包，所以無法攔截
- 防火牆無法防範**病毒**
  - 傳統的防火牆不具防毒功能。現在有些防火牆也內建**防毒**、**反入侵**、和**過濾網頁**的功能，這就是所謂的**防毒牆**

- Windows 防火牆
  開啓防火牆功能
  新增例外網站

三、資料備份

- **資料備份**是最重要的資訊安全工作
- 要**定期備份**，還要在不同的位置**異地備份**
- 重要資料不要只存放在**隨身碟**中





四、資料加密

- 加密 (Encryption)
  - 就是將原始的資料，根據事先定義好的方法，轉換成無法被他人解讀的資料，避免原始的訊息，讓他人知道
  - 資料加密後，收件者收到資料後，必須進行解密 (Decryption)，將資料轉換成原始的樣子，才能閱讀

四、資料加密

- 明文 (Plaintext)：加密前的資料
- 密文 (Ciphertext)：加密後所得的資料
- 金鑰 (Key) ：加密或解密的方法常使用金鑰，金鑰一般可分成私密金鑰 (Private Key) 和公開金鑰 (Public Key)



練習

- 使用 MD5 進行加密

五、無線網路的安全性

- 無線網路以**電磁波**作爲傳遞資訊的媒介，傳輸的資料很容易被竊取
- 例如曾經發生過歹徒截取無線網路的電磁波，入侵網路銀行，竊取信用卡資料，造成銀行及用戶的財物損失
- 無線網路的安全性很重要，購買 AP 後，應立即進行**安全設定**，以免危害網路安全

五、無線網路的安全性

更改及隱藏 SSID

使用加密 **WPA-PSK**



設定存取控制清單


無線 - 存取控制
「存取控制」（Access Control）讓您可以封鎖來自某些無線基地台的存取，或僅略過來自某些無線基地台的存取。在「接受」（Accept）模式下，WL530g僅可接受來自控制清單中所列含有MAC位址之基地台的無線存取。在「拒絕」（Reject）模式下，WL530g將會拒絕來自控制清單中所有含有MAC位址之基地台的無線存取。
MAC存取模式：
Accept
存取控制清單
新增
刪除
MAC位址
還原
儲存
套用
還原:
清除上述設定值並還原有效設定值。
儲存:
現在確認所有設定值並重新啟動WL530g。
套用:
確認上述設定值並繼續。

牛刀小試

- 網路安全簡介
- 電腦木馬程式基本概念
- 電腦病毒
- 防火牆的原理與應用
- 電腦檔案備份操作練習
- 備份檔案還原操作練習
- 資料的加密與解密
- 垃圾郵件的防治

本章內容結束