電腦安全的硬體與軟體

- 社會新聞(報稅)
- 病毒掃瞄器
  - 目的：避免電腦遭受病毒感染
  - 搜尋已知病毒的特徵
    - 特徵比對
    - 行為比對
  - 特徵比對
    - 所有已知病毒檔案的清單
    - 存放在一個副檔名為 .dat 的檔案裡

電腦安全的硬體與軟體 (Cont.)

  - 病毒碼更新 → 更新上述 .dat 檔案
  - 防毒軟體可掃瞄個人電腦、網路與收到的電子郵件是否中毒
- 行為比對
  - 意圖對開機磁區 (硬碟的第 0 軌) 進行寫入的動件
  - 企圖改變檔案系統
  - 自動化電子郵件軟體
  - 自我繁殖
- 病毒典型行為模式

電腦安全的硬體與軟體 (Cont.)

- 防毒軟體運作時機
  - 背景病毒掃瞄器 (Ongoing virus scanners)
    - 持續在背景執行掃瞄動作
  - 隨選病毒掃瞄器 (On-demand virus scanners)
    - 使用者啟動時才會運作
  - 目前大部份病毒掃瞄器均提供上述兩項功能
- 電子郵件及附件掃瞄
  - 在伺服器上進行掃瞄
  - 電子郵件下載到個人電腦時先通過病毒掃瞄，再交給電子郵件軟體

電腦安全的硬體與軟體 (Cont.)

- 下載掃瞄
  - 針對下載檔案進行掃瞄
- 檔案掃瞄
  - 定期掃電腦上的檔案
- 智慧型行為模式掃瞄 (Heuristic scanning)
  - 新一代的病毒掃瞄方式
  - 利用『規則』來判斷檔案或程式的行為是否與病毒相同
  - 有利於找出未知型態之新式病毒

電腦安全的硬體與軟體 (Cont.)

- 缺點是會造成誤判，即沒中毒的檔案被懷疑已中毒，真正的病毒卻沒有發現出來
- 主動式程式掃瞄
  - Java applets 、 ActiveX 及特別吸引人的視覺效果可能潛藏著病毒，應予以掃瞄
- 常見防毒軟體
  - McAfee
  - Norton
  - Pc Cllin
  - Abast http://www.avast.com/index_cns.html

電腦安全的硬體與軟體 (Cont.)

- 防火牆
  - 介於內部網路及外部網路間的屏障
  - 檢查下列參數以過濾封包
    - 封包大小
    - 來源端 IP 位址
    - 通訊協定
    - 目的端位址
  - 可以是硬體或軟體
  - 架設在可信任及不可信任的網路之間

電腦安全的硬體與軟體 (Cont.)

- 防火牆種類
  - 屏障式防火牆 (Screening firewall)
  - 應用程式閘道器 (Application gateway)
  - 電路層閘道器 (Circult-level gateway)
- 屏障式防火牆
  - 最基本的種類
  - 封包過濾器
  - 依所訂定的規則檢查封包以判斷是否放行
  - 無法檢查狀態
  - 提供有限服務 (又稱堡壘主機 bastion host)

電腦安全的硬體與軟體 (Cont.)

- 應用程式閘道器或代理伺服器
  - 代理伺服器：客戶端提出需求時，先向代理伺服器查詢，如代理伺服器無法提供所需服務再向真正伺服器提出要求
  - 代理伺服器會代種客戶端與外界的伺服主機進行連線
  - 可將客戶端隱蔽起來
- 電路層閘道器
  - 功能與代理伺服器雷同，但更安全
  - 不對通訊協定進行額外處理或過濾
  - 在使用者完成認證後建立虛擬 『電路』
  - 部份應用上不適合，如電子商務網站

電腦安全的硬體與軟體 (Cont.)

  - 不支援 URL 的過濾功能
  - 稽核能力有限
- 防火牆檢查封包的方式
  - 狀態封包偵測 (Stateful packet inspection, SPI)
    - 可根據目前封包的檢查結果或先前檢查封包的結果判斷後續封包是否應了放行
    - 知道前後封包之間的關係
    - SPI 可以分辨封包是連線的一部份或是企圖入侵的假造封包

電腦安全的硬體與軟體 (Cont.)

- 無狀態封包偵測 (Stateless packet inspection
  - 不會檢查封包內容
  - 不會分析前後封包間的關係
  - 容易遭受下列攻擊
    - Ping 洪泛
    - SYN 洪泛
    - DoS 攻擊
- 網路主機式防火牆
  - 在現行作業系統主機上安裝軟體
  - 弱點：依附在現行作業系統上

電腦安全的硬體與軟體 (Cont.)

- 防火牆日誌
  - 防火牆所有的活動均會被記錄
  - 日誌可提供有用的資訊以協助偵測入侵行為
  - 判斷攻擊來源
  - 阻止日後相同技術攻擊
  - 網管應定期檢查防火牆日誌

電腦安全的硬體與軟體 (Cont.)

- 反間諜軟體
  - 掃瞄並檢查電腦裡是否有間諜軟體
  - 檢查是否有已知的間諜軟體
  - 避免從網路下載來路不明的軟體或檔案
  - 使用合法防護軟體
- 入侵偵測軟體
  - 檢查通訊埠的流入與流出行為 (例：海關)
  - 找尋可能具有入侵意圖的模式