資訊安全
(Information Security)

電腦網路犯罪與安全

電腦網路犯罪與安全

- 你用網路銀行嗎?
  - 28%的美國消費者每週至少有3次是透過電話、網路或分行以存取其網路銀行報告書。
  - *冒用銀行名義所發出的電子郵件要求更新網路銀行密碼及資料*
  - *“網路詐騙的集團，專門製作「與知名網站幾可亂真的假網站」，或假借中國信託名義發送eMAIL收集客戶個人機密資料。”* ~資料來源：中國信託~

電腦網路犯罪與安全 (Cont.)

- 你利用網路買東西嗎?
  - 美國商務部報告，網路零售銷售量從2000年2730萬美金到2004年增加325%接近8820萬美金。
  - *“...假賣場，「盜用帳號」成為新的犯案手段，更有惡質騙徒以假帳號截標...”~資料來源：花蓮縣警局~*
  - *“歹徒以「資料拼圖」手法，將已蒐集而來的會員帳號與密碼，不斷以人工登入方式，企圖測試每一組帳號與密碼所歸屬的網站”~資料來源：內湖分局~*

電腦網路犯罪與安全 (Cont.)

- 打成績自己來
  - *“美國加州橙縣18歲高中生康恩（Omar Khan）涉嫌夜闖校園，再駭進學校電腦竄改自己的成績，案發後被以多項罪名移送法辦，若罪名全部成立，最重可處38年徒刑。”~資料來源：聯合報2008/06/20~*
  - *“台北縣板橋重慶國中傳出了駭客入侵學校電腦系統，竄改學生成績的事件...一位老師進入學校電腦資料庫準備輸入學生成績的時候，發現成績有誤，一開始她以為是系統的問題，沒想到後來學校資訊人員上網查看，竟然發現二、三年級所有學生的第一次段考成績，全都被改成85分。”~資料來源：東森NowNews 2002/10/30~*

電腦網路犯罪與安全 (Cont.)

- 資通安全注重的三種資料類型
  - **機密資料**
    - 只允許經授權的人存取，禁止非經授權者存取或閱讀。
    - 例如軍事、情報以及有關國家安全的資料。
  - **敏感資料**
    - 政府、機構及企業等具敏感性之資料。(e.g. 戶政資料)
  - **正確資料**
    - 保護該資料的正確性及有效性，禁止該資料被破壞、偽造以及篡改。(e.g. 交易資料, 學籍資料)

電腦網路犯罪與安全 (Cont.)

- 我們周遭的電腦系統與網路
  - 網路銀行
  - 自動化的超級市場結帳系統
  - 網路課程
  - 網路購物
  - 網路旅遊資源

電腦網路犯罪與安全 (Cont.)

- 這些系統有哪些漏洞？
- 應該採取哪些步驟來確保這些系統的安全？
- 如何保護這些個人資訊？

電腦網路犯罪與安全 (Cont.)

- 網路安全很嚴重嗎?
  - “沒有人可以緊跟我的電腦。”
  - “天快塌了！”
  - 中庸

電腦網路犯罪與安全 (Cont.)

- 安全性威脅的形態
  - 惡意軟體 – **MAL**icious soft**WARE**
    - Trojan hourses、間諜軟體
  - 入侵
    - 未經授權進行系統資料存取
  - 阻斷服務攻擊（DoS） – **D**enial **o**f **S**ervice attacks
    - 癱瘓系統，使系統無法提供服務

電腦網路犯罪與安全 (Cont.)

- 惡意軟體– 具有惡意目地的軟體
  - 病毒

    - 通常是藉由電子郵件散布
    - 消耗系統資源而造成網路變慢或停止
    - *“駭客用來竊取網際網路用戶金融及個人資料的「Downadup」(或稱「Conflicker」、「Kido」)蠕蟲病毒，過去四天來入侵全球各地的聯網電腦”* ~資料來源：中時電子報~
    - *“微軟公司2009/02/12宣布懸賞25 萬美元，要捉拿製造或釋出電腦病毒Conficker的元凶。”* ~資料來源：聯合新聞網~

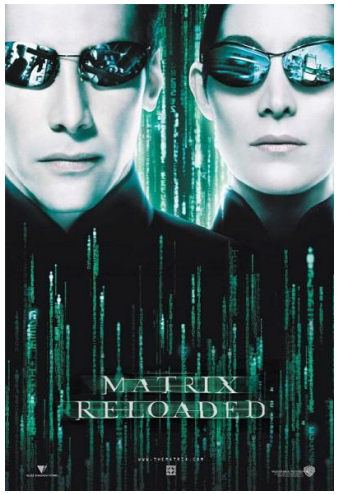
電腦網路犯罪與安全 (Cont.)

- 惡意軟體– 具有惡意目地的軟體
  - 特洛依木馬(Trojan horses)
    - 以古老的木馬屠城故事而命名
    - *“敘利亞第一夫人阿絲瑪的個人電腦被以色列軍情人員侵入，竊取敘利亞總統巴夏爾的情報。以色列軍情人員使用「特洛依木馬」程式記錄她的電腦訊息，包括她跟巴夏爾的電郵往返和網上聊天內容全都被駭。”* ~資料來源：聯合新聞網 2005/06/06~
    - “企業防毒及反垃圾郵件軟體廠商 Sophos 指出有一種特洛伊木馬病毒 LegMir-Y，專門竊取多人網路遊戲《天堂》的使用者名稱及密碼...”~資料來源：數位之牆~

電腦網路犯罪與安全 (Cont.)

- 惡意軟體– 具有惡意目地的軟體
  - 間諜軟體
    - 你的一舉一動都被監視了
    - Cookies
    - Key logger (鍵盤側錄程式)

電腦網路犯罪與安全 (Cont.)



- 入侵
  - Hacking or cracking
  - 入侵系統以取得系統資源的攻擊
  - 一定要透過電腦攻擊才能入侵嗎?
    - 社交工程
    - *某人向一家公司會計部門宣稱自己是公司的技術支援人員，其宣稱受到系統管理者的指示進行系統維修，請其提供使用者帳號與密碼。*
  - 撥號攻擊(war-dialing)
  - 駕駛攻擊(war-driving)

電腦網路犯罪與安全 (Cont.)

- 阻斷服務攻擊（DoS） – **D**enial **o**f **S**ervice attacks
  - 得不到你的心，讓你無法愛別人
  - 攻擊者沒有要存取系統，只是阻擋合法使用者存取系統

電腦網路犯罪與安全 (Cont.)

- 網路上常見的攻擊
  - 病毒
    - 全新與變種的病毒
  - 未經授權的系統存取
    - DoS 攻擊
    - 入侵
    - 員工的誤用

電腦網路犯罪與安全 (Cont.)

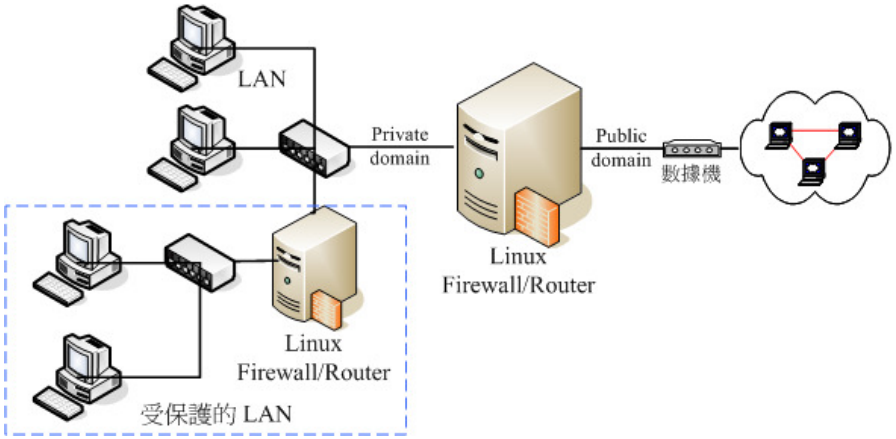
- 基本的資訊安全術語
  - 人物
    - 駭客
      - 白帽駭客
      - 黑帽駭客(怪客)
      - 灰帽駭客
    - 腳本小子（Script kiddies）
    - 有道德的駭客

(尋找系統錯誤是學習該系統的最佳途徑)

肉腳級的駭客

電腦網路犯罪與安全 (Cont.)

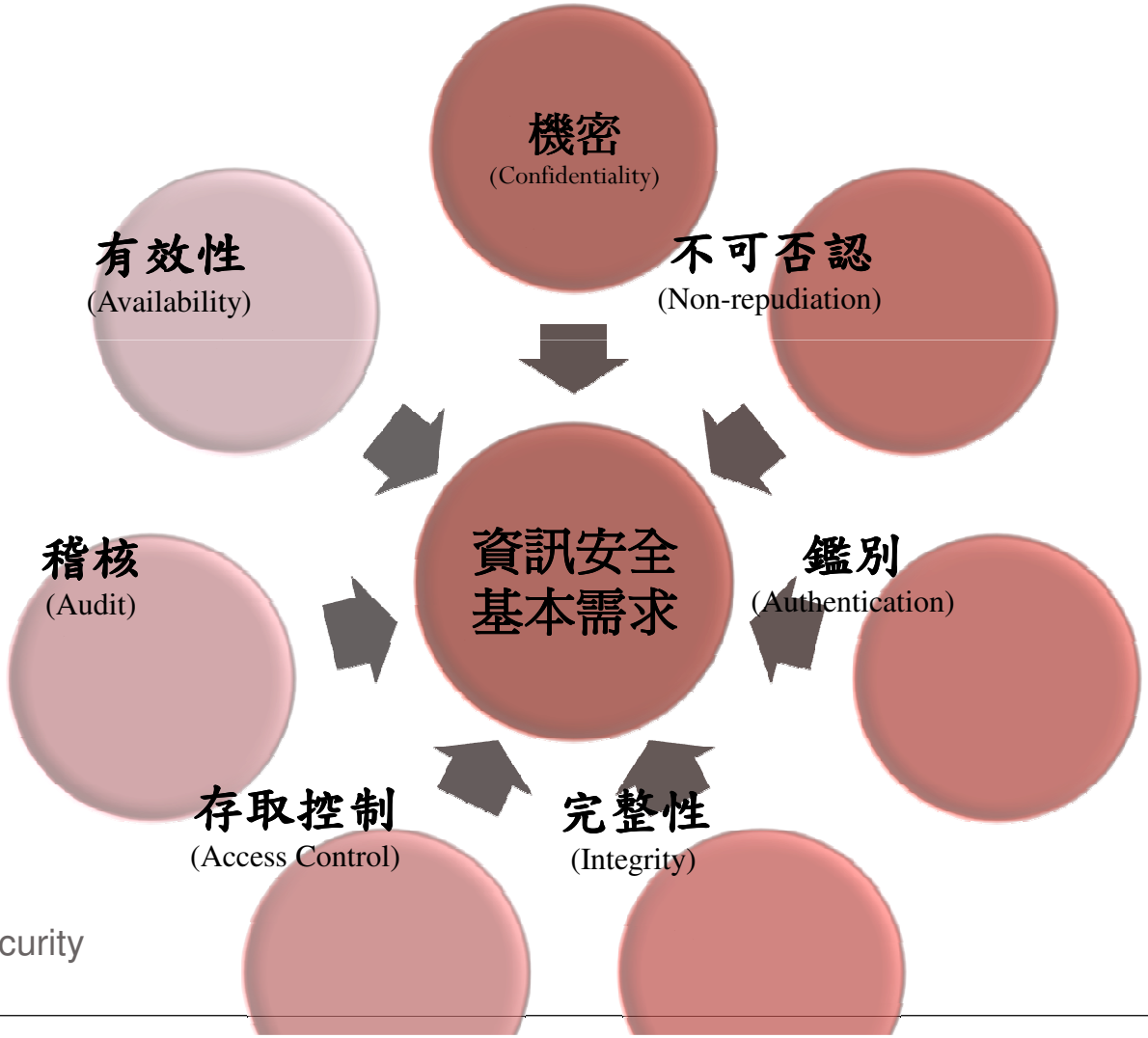
- 基本的資訊安全術語
  - 裝置
    - 防火牆
      - 過濾網路訊務
    - 代理伺服器（Proxy server）
      - 隱藏內部主機的 IP 位址
    - 入侵偵測系統（Intrusion Detection System）
      - 監視訊務以找出攻擊意圖



電腦網路犯罪與安全 (Cont.)

- 基本的資訊安全術語
  - 活動
    - 飛客入侵（Phreaking, 盜撥）
      - 利用惡意且大多是違法的方式來躲避為通訊帳單、訂單、轉帳、或其它服務付費。(Raymond, 2003)
    - 認證(Authentication)
      - 站住、口令、誰?
    - 稽核（Auditing）
      - 查看log file 看看你做了什麼

資訊安全的基本需求


機密
(Confidentiality)
有效性
(Availability)
不可否認
(Non-repudiation)
資訊安全
基本需求
稽核
(Audit)
鑑別
(Authentication)
存取控制
(Access Control)
完整性
(Integrity)

保密性或機密性

- 確保資訊的機密，防止機密資訊洩漏給未經授權的使用者。機密性資料內容不能被未經授權者所竊知，僅能被授權者所存取。
- 存取包括讀出、瀏覽及列印。另外「資料是否存在於系統」也是一項很重要資訊。
- 可透過資料加密程序來達到資料的保密性或機密性。

完整性

- 資料內容僅能被合法授權者更改，不能被未經授權者篡改或偽造。
- 資料完整性必須確保資料傳輸時不會遭受篡改，以保證資料傳輸內容之完整性。
- 數位簽章可用來確保資料傳輸過程中，不會被駭客篡改及偽造，以確保資料之完整性。

鑑別性 (Authentication)

- 包括身分鑑別(Entity Authentication)及資料（或訊息）來源鑑別(Data or Message Authentication)。
  - 訊息來源的鑑別
    - 是要能確認資料訊息之傳輸來源，以避免惡意的傳送者假冒原始傳送者傳送不安全的訊息內容。
    - 一般利用數位簽章或資料加密等方式來解決訊息的來源鑑別問題。
  - 身分鑑別
    - 使用者身分的識別是要能快速且正確地驗證使用者身分。
    - 為了預防暴力攻擊的惡意侵犯，對於使用者身分鑑別的時效性比起訊息驗證要來得嚴謹。

可用性 (Availability)

- 確保資訊系統運作過程的正確性，以防止惡意行為導致資訊系統毀壞(Destroy)或延遲(Prolong)。

不可否認性 (Non-Repudiation)

- 在資訊安全需求中，對於傳送方或接收方，都不能否認曾進行資料傳輸、接收
- 數位簽章及公開金鑰基礎架構（Public Key Infrastructure，簡稱PKI）對使用者***身分***及***訊息***來源做身分鑑別及資料來源鑑別，並可再與使用者在系統上的活動進行連結，以達權責歸屬及不可否認性。

存取控制

- 資訊系統內每位使用者依其服務等級而有不同之使用權限。服務等級愈高者其權限愈大；相反地，服務等級愈小者其權限愈小。
- 存取控制主要是根據系統的授權策略，對使用者做授權驗證，以確認是否為合法授權者，防止未授權者存取電腦系統及網路資源。

稽核

- 資訊系統不可能達到絕對安全（百分之百）。
- 我們必須藉由稽核紀錄(Audit Log)來追蹤非法使用者，一旦發生入侵攻擊事件，可以盡快找到發生事件之原因，讓回復系統(Recovery)及未來能偵測此類入侵的手法，防止系統再一次被入侵。

電腦網路犯罪與安全 (Cont.)

- 達到網路安全的形式
  - 周圍式安全方法
    - 小公司、資料重要性較低的環境適用
    - Firewall, Proxy server, IDS
  - 階層式安全方法
    - 周圍安全+每一系統安全
  - 主動與被動
  - 混合式安全性方法

電腦網路犯罪與安全 (Cont.)

- 中華民國《電腦處理個人資料保護法》
  - 《民法》第195條則揭示「隱私」為人格權的一種，當「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。…」
  - 1995年8月11日公布施行的《電腦處理個人資料保護法》
  - 1999年7月14日公布施行的《通訊保障及監察法》第6條明訂：「凡個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍」。
- 資料來源：~徐振雄，《網際網路法》第七章~

電腦網路犯罪與安全 (Cont.)

- 電腦處理個人資料保護法
  - 簡稱「個資法」。
  - 所謂電腦處理個人資料，係指自然人之姓名、出生年月日、特徵、指紋、婚姻、身份證編號、職業、財務等「足資識別該個人」的資料
  - 本法的重點如下 ：
    - 不論公務或非公務機關，對於個人資料的蒐集、利用都必須尊重當事人的權益，並不得逾越特定目的之必要範圍。
    - 資料處理時，除應與蒐集之特定目的相符外，當事人有請求維護資料的正確性、停止利用或刪除該資料的權利。
    - 保有個人資料檔案者，有指定專人負責防止個人資料被竊取、竄改、毀損、滅失或洩漏的義務，違反者，當事人得對其提出損害賠償訴訟。

電腦網路犯罪與安全 (Cont.)

- 隱私權
  - 未通知當事人並取得其同意之前，資料持有者不得將當事人為特定目的所提供的資料運用在另一個目的上

電腦網路犯罪與安全 (Cont.)

- 全球許多國家已制定反垃圾郵件法
  - 日本2002年「特定電子郵件法」及「反垃圾郵件法」
  - 歐盟2003年「隱私電子通訊法」
  - 美國2003年底「垃圾郵件管制法案」等等
  - 臺灣則於2004年底由國家通訊傳播委員會（NCC）擬發「防止濫發商業電子郵件管理條例」法案，並即將宣佈實施。
    - 該法案規定，業者在未經使用者同意下，不得濫發電子郵件，否則最高可罰個人新臺幣2000元、企業2000萬元 。
- 與垃圾郵件可能相關者，還有隱私權。
  - 隱私權乃不受他人任意干擾之權利
  - 電子郵件信箱的住址

電腦網路犯罪與安全 (Cont.)

- 妨害電腦使用罪
- 法務部決定在刑法增列「妨害電腦使用罪」章
  - 其中最重的是屬於公訴罪性質的「製作供妨害電腦使用之程式」罪
  - 電腦犯罪專章列在刑法增列第卅六章「妨害電腦使用罪」
    - 刪除電磁記錄擬制為動產之規定。
    - 修正提高不正利用自動付款設備最之刑度。
    - 修正刪除干擾電磁記錄規定。
    - 增訂妨害電腦使用罪章。
    - 增訂無故入侵電腦罪。
    - 增訂保護電磁記錄之規定。
    - 增訂干擾電腦系統及相關設備罪。
    - 增訂製作專供電腦犯罪用之程式罪。
    - 增訂部分條文告訴乃論之規定。

電腦網路犯罪與安全 (Cont.)

- 刑法:
  - 第358條規定：「無故輸入他人電腦密碼、破解保護措施者，處三年以下有期徒刑，得併科十萬元以下罰金」。
  - 第359條規定：「無故變更、取得或刪除他人電磁紀錄者；處五年以下有期徒刑、拘役得併科廿萬元以下罰金」。
  - 第360條規定：「干擾電腦程式或相關設備者，處三年以下有期徒刑，得併科十萬元以下罰金」。
  - 第361條規定：「製作專供妨害電腦使用之電腦程式即電腦病毒者，處七年以下有期徒刑」。

電腦網路犯罪與安全 (Cont.)

- 虛擬寶物與貨幣竊盜刑責
  - 2002 年八月，臺北地方法院針對虛擬寶物竊盜的案例，首度作出判決。該被告除依刑法觸犯竊盜罪外，並觸犯詐欺得利罪，判處罰金 2500 元、緩刑二年，得易服勞役。
    - 因被告竊取之電磁記錄（虛擬寶物、裝備及貨幣），必須利用遊戲伺服器所虛擬之空間，方能支配使用，無法經由單機複製，故被告藉由遊戲伺服器將被害人所持有支配之上述電磁記錄取為己有行為。依刑法第 323 條及第 320 條第 1 項，即成立竊盜罪。
    - 在本案當中，被告未經被害人同意即輸入其帳號密碼，使遊戲公司誤以為是被害人上線而提供服務之行為。依刑法第 339 條第 2 項，則成立詐欺得利罪。

電腦網路犯罪與安全 (Cont.)

- 網路安全是一個持續發展的領域
- 你將需要三個層級的知識
  - 第一，選修課程充實自己基本的技術
  - 第二，詳細地學習所使用的系統，包含系統所有的優點與缺點
  - 最後，保持處於持續發展之威脅與漏洞的最新狀態