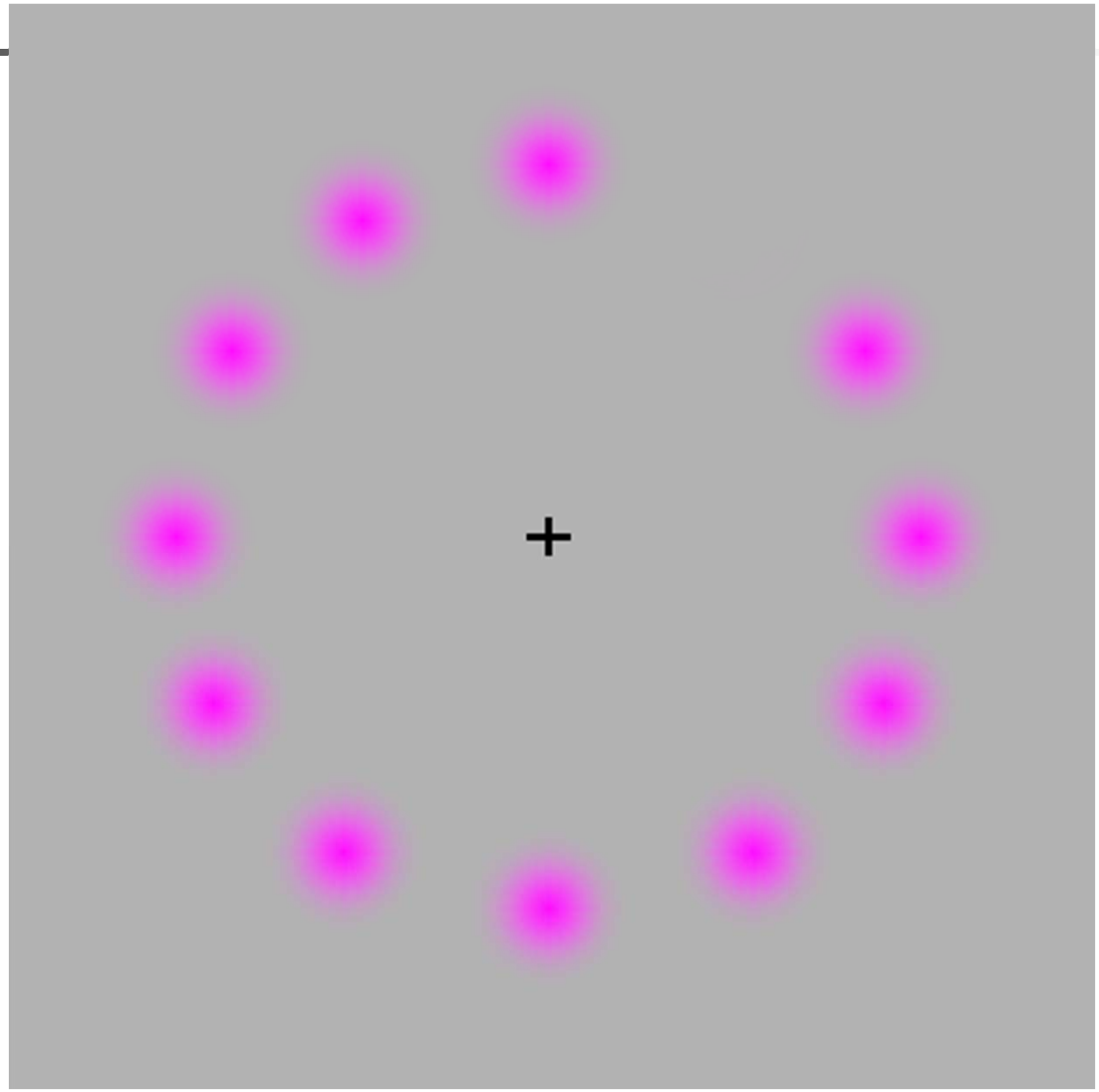
科技安全認知與作為

DOP Shiuh-Jeng **WANG** /王旭正

- 中央警察大學 資訊管理系
- 中華民國資訊安全學會 (www.ccisa.org.tw, 理事 (2000-2012)
- 中華民國資訊安全學會 副理事長 (www.ccisa.org.tw, 2012-)
- Visiting Scholars at FSU and UF in USA, 2002, 2004, 2010.
- Academic tour for International Project Inspection at CMU in USA, 2007
- Columnists of Domestic Information-tech Magazines, http://www.netadmin.com.tw/ 網路通訊/iThome/網管人雜誌, 2002-2006, 2007-至今
- Director of ICCL, http://hera.im.cpu.edu.tw (Information Cryptology and Construction Lab.)
- sjwang@mail.cpu.edu.tw, http://www.wretch.cc/blog/icclsjwang



大綱

1. 資訊安全與電腦犯罪
2. 鑑識與鑑定
3. 資訊安全-PKI與自然人憑證
4. 軟體安全-常見軟體攻擊
5. 網路詐騙
6. 結論

何謂資訊安全

- 資訊對組織而言就是一種資產。
  - 知識經濟時代的來臨。
  - 3M, …。
- 資訊安全：「為了保護企業(機關)資訊不受任何威脅，降低風險的發生機率並採取措施保證業務不會因風險的發生而中斷，確保業務營運或將損失降至最低。」

何謂資訊安全

- 資訊對組織而言就是一種資產。
  - 知識經濟時代的來臨。
  - 3-M, 知識管理(KM)、資料倉儲(WHM)與資料探勘(DM)的崛起。
- 資訊安全：「為了保護企業(機關)資訊不受任何威脅，降低風險的發生機率並採取措施保證業務不會因風險的發生而中斷，確保業務營運或將損失降至最低。」

資訊安全所面臨的問題

天災

- 地震
- 水災
- 火災
- 風災

人禍

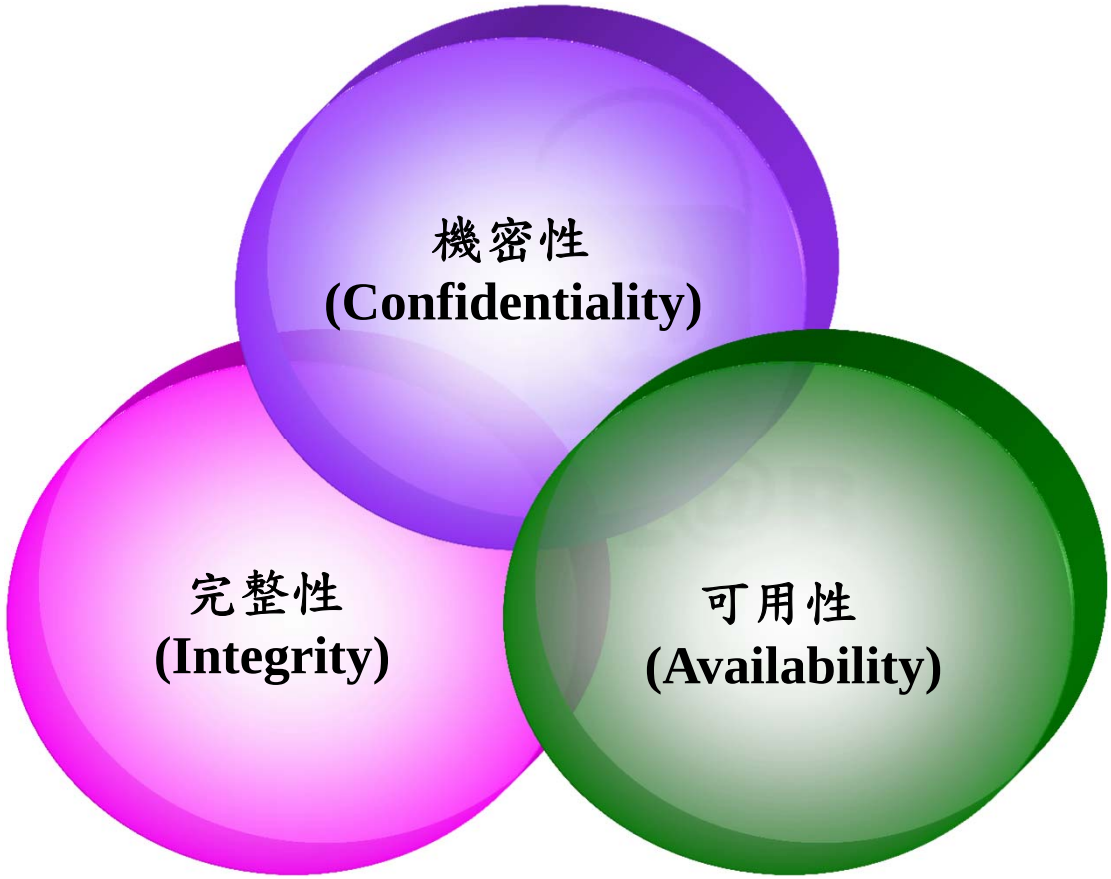
外賊與內鬼

- 病毒
- 駭客
- 操作失當
- 設定不當
- 人為惡意

資訊安全範圍

- 在資訊安全管理中，首先必需瞭解資訊安全的範圍，大致可分為下列四個領域： 軟體與硬體
  - 一、人員安全：防止人為的疏忽、濫用或誤用資訊及設備。
  - 二、資料安全：防止資料遭未經授權之存取及誤用並保護資料的機密性、完整性及可用性。
  - 三、環境安全：防止環境的問題所造成資訊及設備的傷害。
  - 四、實體設備安全：防止設備因不當的安裝、設定及使用，造成的資訊安全事件。

資訊安全的目標(C.I.A)



Managements & Sensitive

"TIME":

- **T:**
- **I:**
- **M:**
- **E:**

How about C.I.A.

- 機密性
- 完整性
- 可用性

Managements & Sensitive

"TIME":

- **T:** Target
- **I:** Instruction
- **M:** Management
- **E:** Execution

何謂資訊安全

- 只從密碼學、駭客入侵、網路漏洞、防火牆、防毒與入侵偵測系統的角度看資訊安全是不夠的。
- 「人員管理」的議題最重要但最常被忽略。
- 資訊安全的觀念需要「管理」與 「技術」的結合。
- 錯誤觀念!!
  - 國內對資安的認知，大部份還是停留在防毒、防垃圾郵件及防火牆這些只能防範外部的攻擊。
  - 資安是只是資訊部門的事，資訊部門做的好，企業(機關)就沒有資安的問題。

電腦犯罪

- 電腦犯罪日漸嚴重(調查報告)
  - 調查報告美國在西元兩千年因電腦犯罪所產生的財產損失即增加43%，由 $US265 million 增加為 $US378 million (FBI案件統計)
  - 美國85% 的企業及政府機構曾偵測到計算機系統遭到入侵
- 資料來源:http://www.smh.com.au/icon/0105/02/news4.html.

六何分析

六何(5W1H)要件	概要	內容
如何 How	犯罪手段	電子郵件、假網站、惡意程式。
	獲利方式	網路銀行、信用卡。
	操作方式	社交工程、駭客工具、系統漏洞等。
何人 Who	犯罪主體 嫌疑人	Phisher(個人/組織)
	被害人	被害者(持卡人，帳號使用者)
	關係人	銀行、網站所有人(個人/組織)、ISP、安全組織(CERT/公司)政府機關
何事What	犯罪類型	詐欺罪、竊盜罪、防害電腦使用罪、電腦處理個人資料保護法、洗錢防制法等。
何時When	犯罪時間	檔案的「建立日期」、「存取日期」、「修改日期」
	出入時間	帳號登入網站之「起訖時間」及「使用時間」
何地Where	犯罪地點	連線詐騙網站IP 位址 電子郵件 相關入侵工具軟體
為何 Why	犯罪動機與目的	信用資料的疑義與金融需求的必要。

網路安全的三層面

- 第一層（實體）：保護網路架構、以及應用系統防止入侵
  - 如：機房進出安全控管、終端機安全控管
- 第二層（傳輸）：保護資訊在網路傳輸時安全
  - 如：防火牆、VPN、加密系統、認證系統
- 第三層（使用者，應用）：保護並管理網路使用者
  - 如：內容安全管理

內容安全管理的範圍

- 網站網頁內容安全管理
  - 將網際網路分成數十種分類網站，對於不同組織與環境需求進行過濾與管理、統計
- 電子郵件內容安全管理
  - Come in：過濾垃圾郵件、病毒郵件
  - Go out：過濾重要文件與關鍵內容
- 即時通訊內容安全管理
  - 防止洩密以及消耗生產力

網際網路濫用的風險

- 每十台電腦便有九台感染了間諜軟體
- 全球曾有超過兩百萬台伺服器和 PC 互相感染了 Nimda 病毒
- 44% 的員工在工作時間內執行網路媒體應用程式消耗公司頻寬
- 45% 的企業偵測到有內部員工進行未獲授權之存取

即時通訊(IM)軟體 vs 電子郵件

- 皆是網際網路發達後所產生的通訊工具
  - 即時與非即時
  - 即時傳訊息與文字簡訊的效率高，更方便且快速得到回應
  - 專家指出，通訊趨於簡化的趨勢使溝通愈來愈非人性化。「不想跟某人見面？那就打電話。不想打電話？那就寄電子郵件。不想費力寫正式書信？那就傳個簡訊。」

電子郵件內容管理的問題

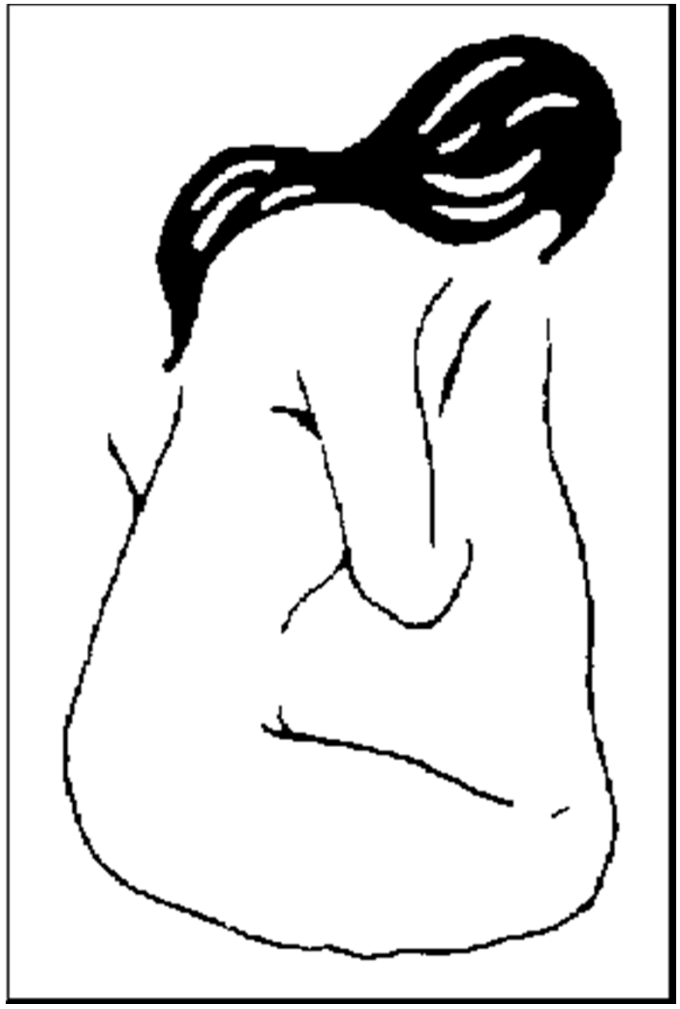
- 垃圾郵件佔電子郵件流量50%以上
- 54%的使用者每天收到一到五封垃圾郵件、37%的使用者每天收到五到二十封垃圾郵件
  …
- 垃圾郵件裡病毒郵件的比率最高達47%
- 超過百分之五十的員工認為企業應該裝設反制垃圾郵件系統
- 電子郵件是最容易洩密的管道

即時通訊內容管理的分析

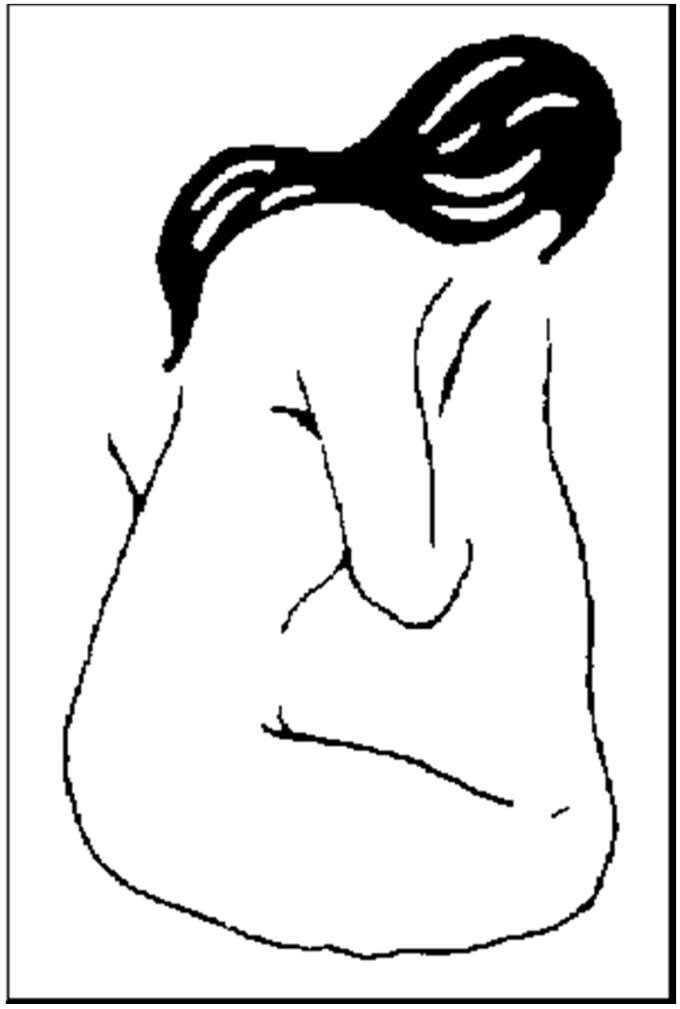
- 全球已有超過四分之三的網路人口在使用即時通訊軟體
- 即時通訊:…MSN, …
- 有82%的使用者認為網路即時通訊可以快速解決工作上溝通的問題
- 所有企業中，已有超過80%的企業員工使用即時通訊軟體，有23%的企業是採用全開或全關，少於1%的企業對即時通訊做細部控管
- 便利與安全之間的取捨

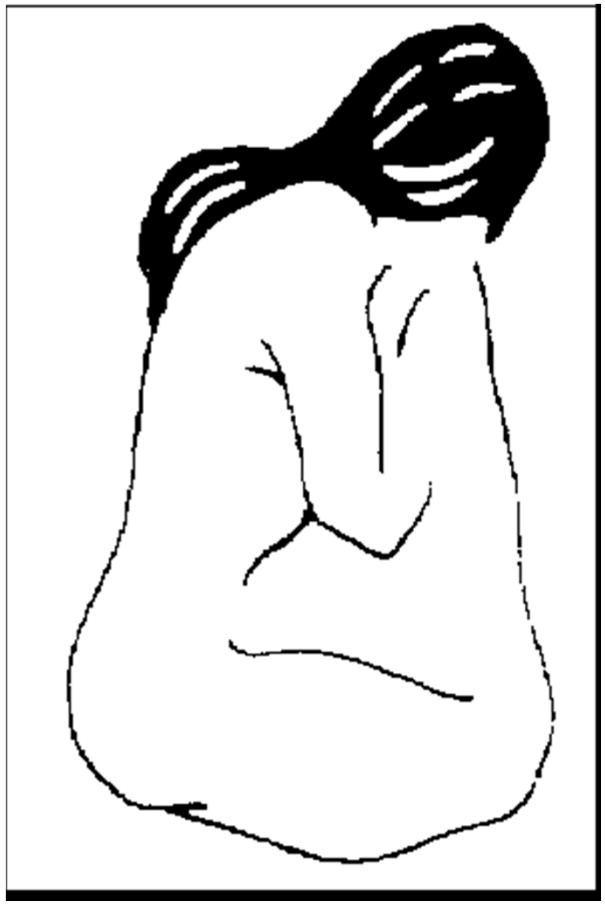
控管即時通訊軟體的功能

- 使用者的管理
- 哪些使用者在什麼時間什麼地方做什麼
- 檢查記錄進出的所有訊息內容和動作
- 對傳輸中的檔案做病毒掃描並控管
- 查看正在使用即時通訊軟體的使用者（ICQ, MSN, Yahoo Messenger, QQ）並察看交談內容

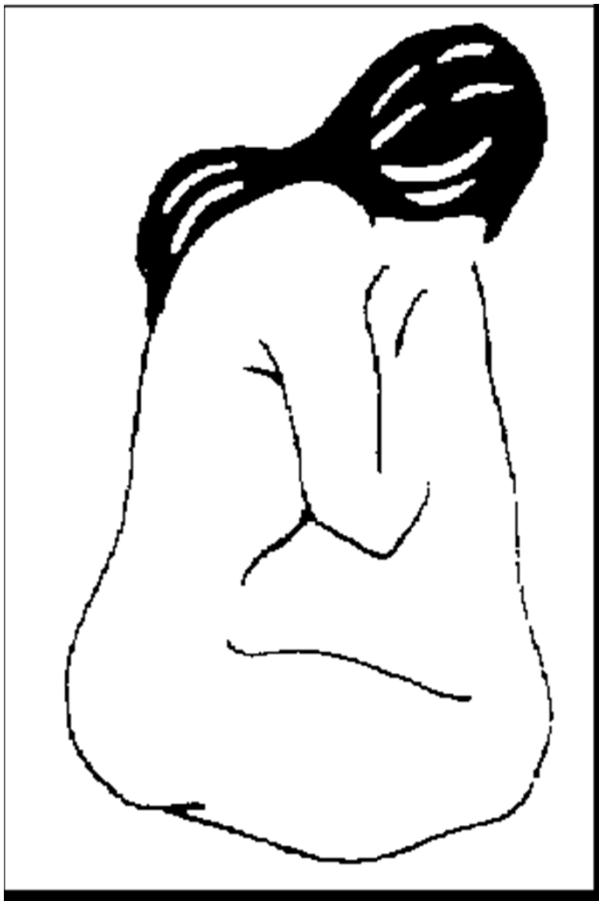


男人的臉?

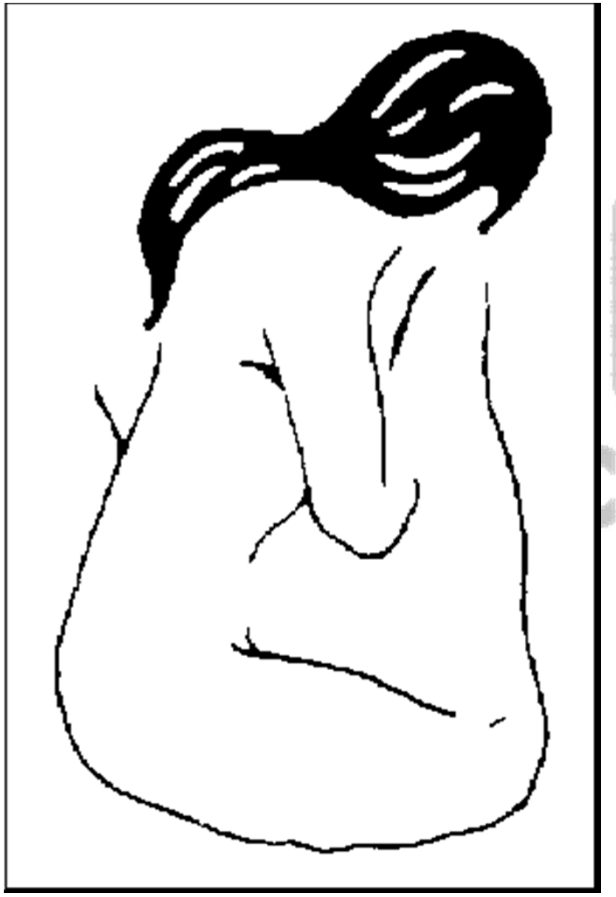


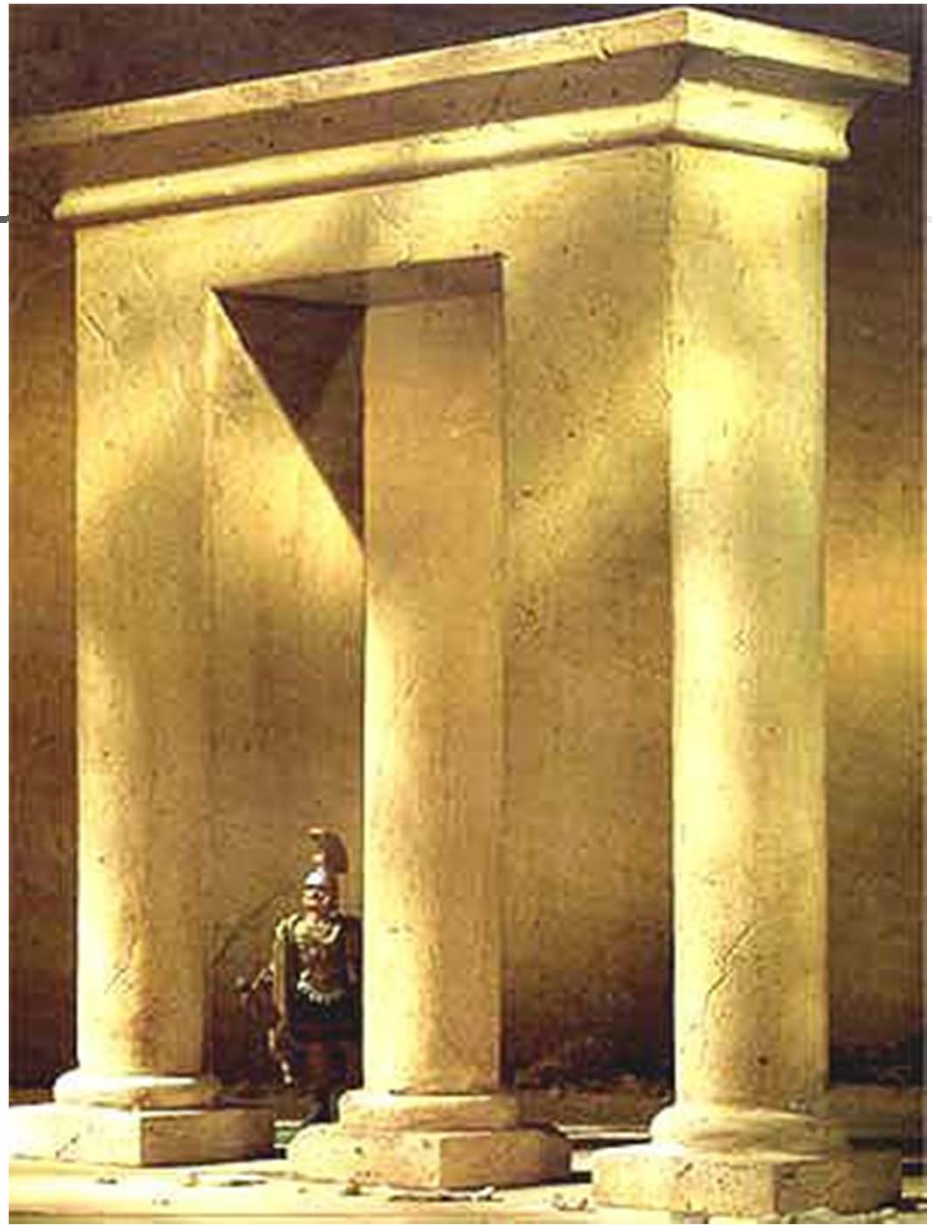


捲曲的女人?



擺在一起看看

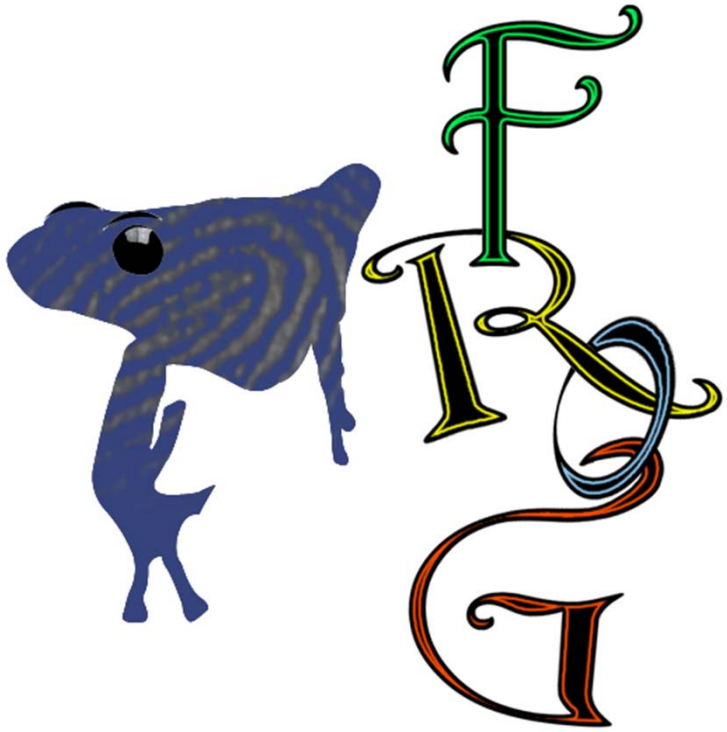




鑑識與鑑定

- HAKUNA MATATA
- C'est La Via
- Information/Network Security
- Authentication and Forensics
- Computer/Network Forensics
- Science Literature: http://hera.im.cpu.edu.tw/sjw_2006/nain.htm
  or http://hera.im.cpu.edu.tw/sjw_2006/trace.htm

ICCL-FROG



Forensic Research & develOpment

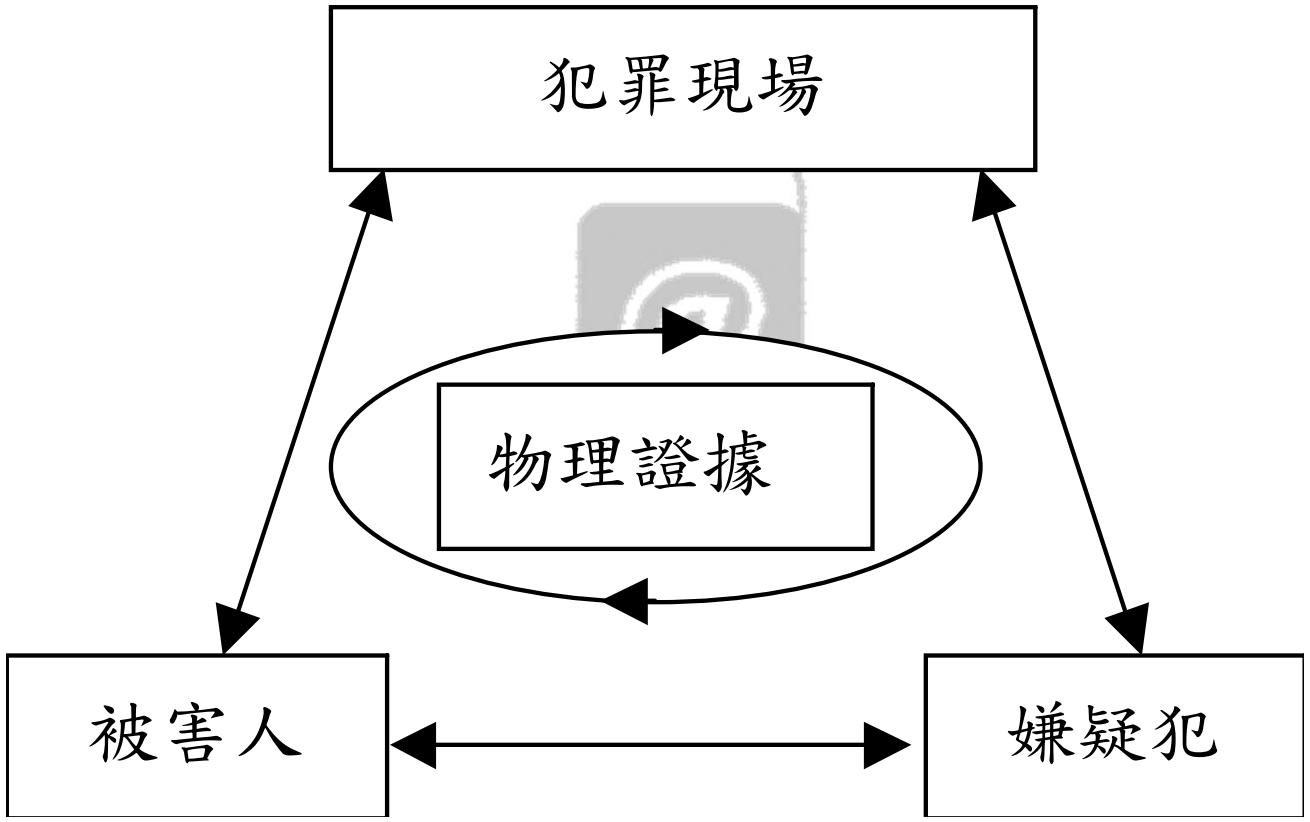
task force Group

MY FROG and the FROG with you

Clues

- Suspect, evidence, scene, victim

Clues and Relationships



PKI

- PKI 公開金鑰基礎建設
  - PKI：Public Key Infrastructure，公開金鑰基礎建設
  - PKI是一種基礎建設內含對稱及非對稱性密碼學、軟體和網路服務的整合技術，主要是用來提供保障網路通訊和企業電子交易的安全性
  - PKI為一種支援憑證的軟體、標準和協定的安全性整合服務。
  - 公開金鑰密碼技術安全地運行之根基

Miracles with you

- (944) mod 9, (9445) mod 9, (94455) mod 9, (9445555449) mod 9
- 13^2 mod 3, 13^6 mod 7, 13^{22} mod 23
- g^a, g^b, g^{ab}, g^{ba} , …

  public key, g^a, g^b

  secret key, a, b

  X: a, g^a

  Y: b, g^b

  common key: g^{ab} *Related to* g^{ba}

- A, B, C, … X,Y, Z, check out

  –A,B,C,D,E,M,T,U,V,W,Y-

  - C, …,

PKI 公開金鑰基礎建設

- 為什麼需要PKI?
  - 傳統的對稱式密碼系統雖然提供高度通訊“私密性”的保護，但無法提供“不可否認性”或“數位簽章”的功能，而且產生金鑰管理與分配的問題
  - 電子化政府和電子商務交易需要更多層面和高度安全性的交易機制(譬如需要“私密性”、“身分鑑別”與“不可否認性”的安全功能)，所以必須仰賴對稱及非對稱式密碼系統的支援
  - 公開金鑰密碼技術是最具代表性的非對稱式密碼系統

PKI 公開金鑰基礎建設(續)

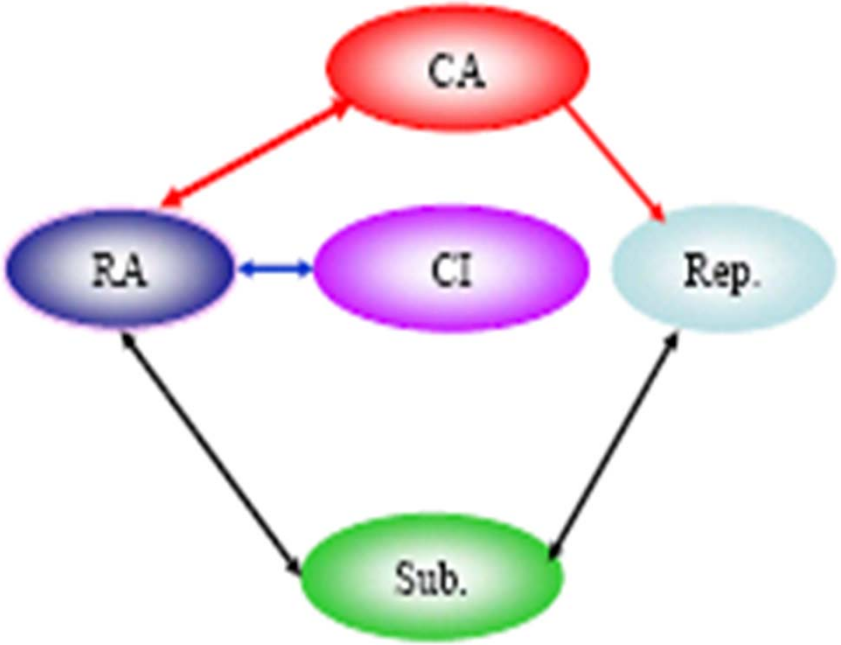
- 什麼是PKI？(1/2)
  - 雖然有數學理論或是長久的實務驗證說明公開金鑰密碼技術的各種演算法已達一定的安全性，然而如果無法確保“通訊雙方能夠正確地取得對方公開金鑰”，則縱使有完美的密碼演算法是沒有用的
  - 在實務上還需要建置一些管理機制、設施、或服務等，以確保可以達到“通訊雙方能夠正確地取得對方公開金鑰”重要前提
  - 所謂“公開金鑰基礎建設”（**Public Key Infrastructure，PKI**）是一種支持公開金鑰密碼技術正常運作的基礎建設，而所謂**Infrastructure**包含設備、設施、服務、人員、法律、政策、規範等

PKI 公開金鑰基礎建設(續)

- 什麼是PKI？(2/2)
  - CA是公開金鑰基礎建設之核心，但僅為其中很重要的一部份非其全部。
  - 狹義的公開金鑰基礎建設是指建置憑證機構提供憑證管理服務。
  - 廣義的公開金鑰基礎建設則涵蓋任何有助於公開金鑰密碼技術運作的機制或設施，甚至於相關管理措施或法規制度都可以算是公開金鑰基礎建設的一環
  - 除了憑證機構提供的憑證管理服務之外，常見的其他PKI服務有憑證路徑建構服務（Certification Path Construction Service）、憑證路徑驗證服務（Certification Path Validation Service）、數位時戳服務（Digital Timestamp Service ）、資料驗證服務（Data Validation and Certification Service）等

PKI 公開金鑰基礎建設(續)

- PKI的組成單位
  - **CA是公開金鑰基礎建設之核心，但PKI≠CA，而是PKI ⊃CA.**

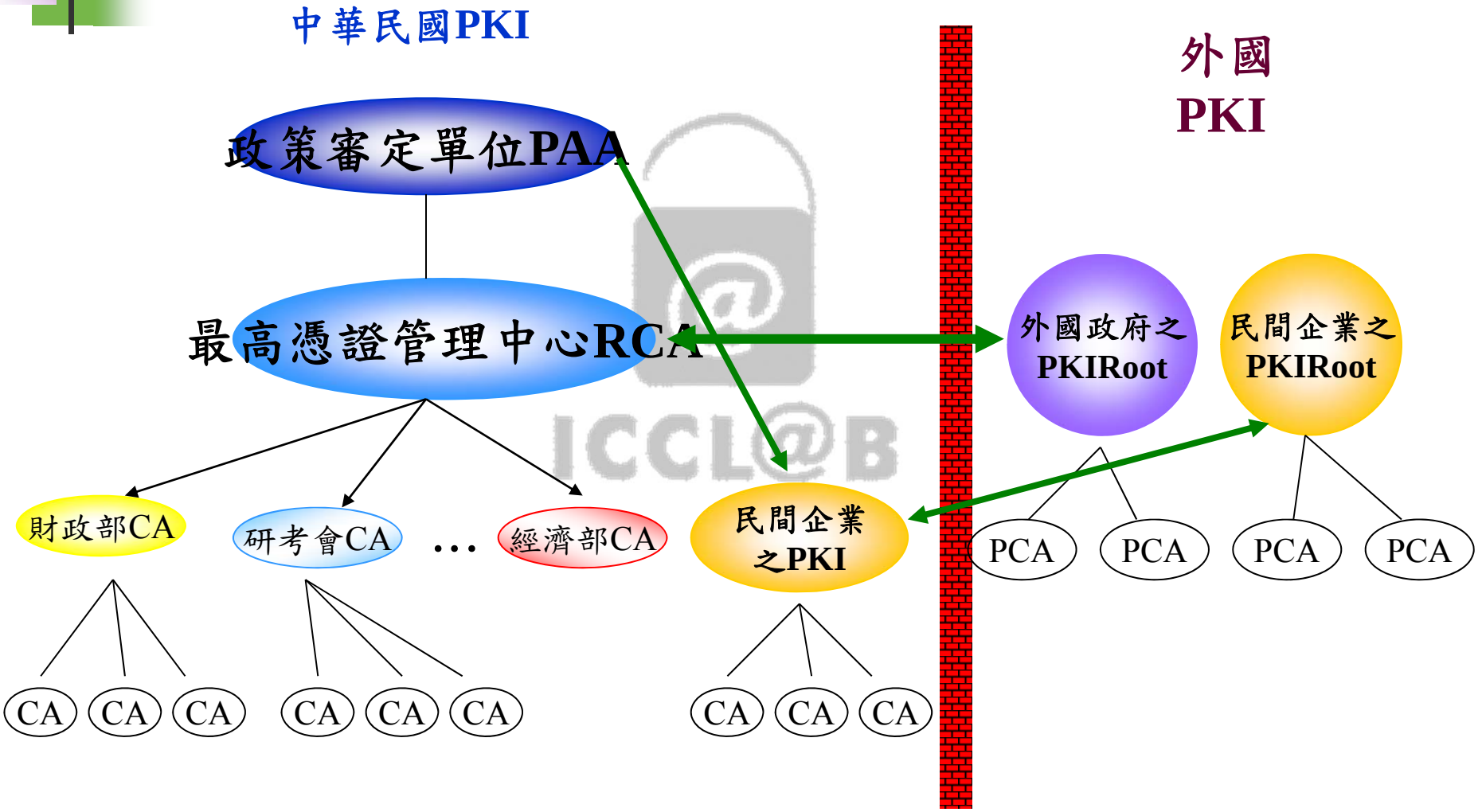


CA：憑證中心
RA：註冊中心
CI：憑證發給單位
Sub.：用戶
Rep.：儲存庫

自然人憑證簡介

- 自然人憑證是內政部憑證管理中心(MOICA)對我國滿18歲以上國民所核發的公開公鑰數位憑證，是我國電子化政府資訊安全基礎建設計劃之一，以提供電子化政府應用服務網路通訊的安全基礎
- 內政部憑證管理中心是電子化政府資訊安全基礎建設計劃之一，是一個我國電子簽章法所謂的“憑證機構”
- 自然人憑證提供其他自然人之電子化政府應用服務網路通訊的安全基礎

我國政府公開金鑰基礎建設之架構



自然人憑證的運作機制

自然人在合法申請後均會獲得一組公開/私密金鑰對，這一組金鑰對在經憑證管理中心認證過後，便會核發此公開金鑰的電子憑證，憑證內容包含：(1)用戶名稱(2)用戶公開金鑰(3)憑證有效期限(4)憑證序號及(5)憑證管理中心的數位簽章等

自然人憑證可做為網路上身份驗證之使用

自然人憑證應用服務

http://moica.nat.gov.tw/html/link_1.htm

軟體安全-常見軟體攻擊方式

- 一般攻擊方式
- 準備階段：
  - 主要是在獲取目標主機上各種資訊之行為，對於主機一般還未造成任何損害。
- 攻擊及攻佔後之階段：
  - 主要是在設法取得、提升、利用目標主機之存取權，這個部份對目標主機所造成之損害需視駭客取得之權限大小而定。
- 癱瘓階段：
  - 主要是阻絕服務，讓合法使用者不能使用目標主機之服務。這種行為可能是駭客無法完成在上一階段之攻擊時所作。

軟體安全-常見軟體攻擊方式(續)

- WHOIS、NSLOOKUP查詢工具：可藉此類工具調查入侵或攻擊目標的基本網路資料及相關公司資訊。
  - http://www.kloth.net/services/nslookup.php
  - http://www.whois.twnic.net.tw/
- IPSPOOFING：藉此手段來偽造來源端，以擾亂司法人員調查的方向並隱藏自己的真實位址。
- IP/PORT SCANNING：藉由IP或通訊埠掃瞄的工具來提供的服務及DMZ區各種的安全機制(如防火牆POLICY、弱點掃瞄及應用系統伺服器等資訊)。

軟體安全-常見軟體攻擊方式(續)

- 網路監聽：如Ethereal 、Sniffer等封包監聽工具常被利用來做為駭客工具最重要的資訊蒐集工具，可以透過封包的擷取，建立企業網路的各項交易封包複本，做為後續各種分析及破解的資訊來源。
- 漏洞調查：結合已知開放的服務、系統版本及監聽到封包可以分析到攻擊目標可能存在的系統或軟體漏洞，最常見的是緩衝區溢位問題。
- 密碼破解：如Stake公司的LC4/LC5系列軟體，常被用來做為破解工具。

軟體安全-常見軟體攻擊方式

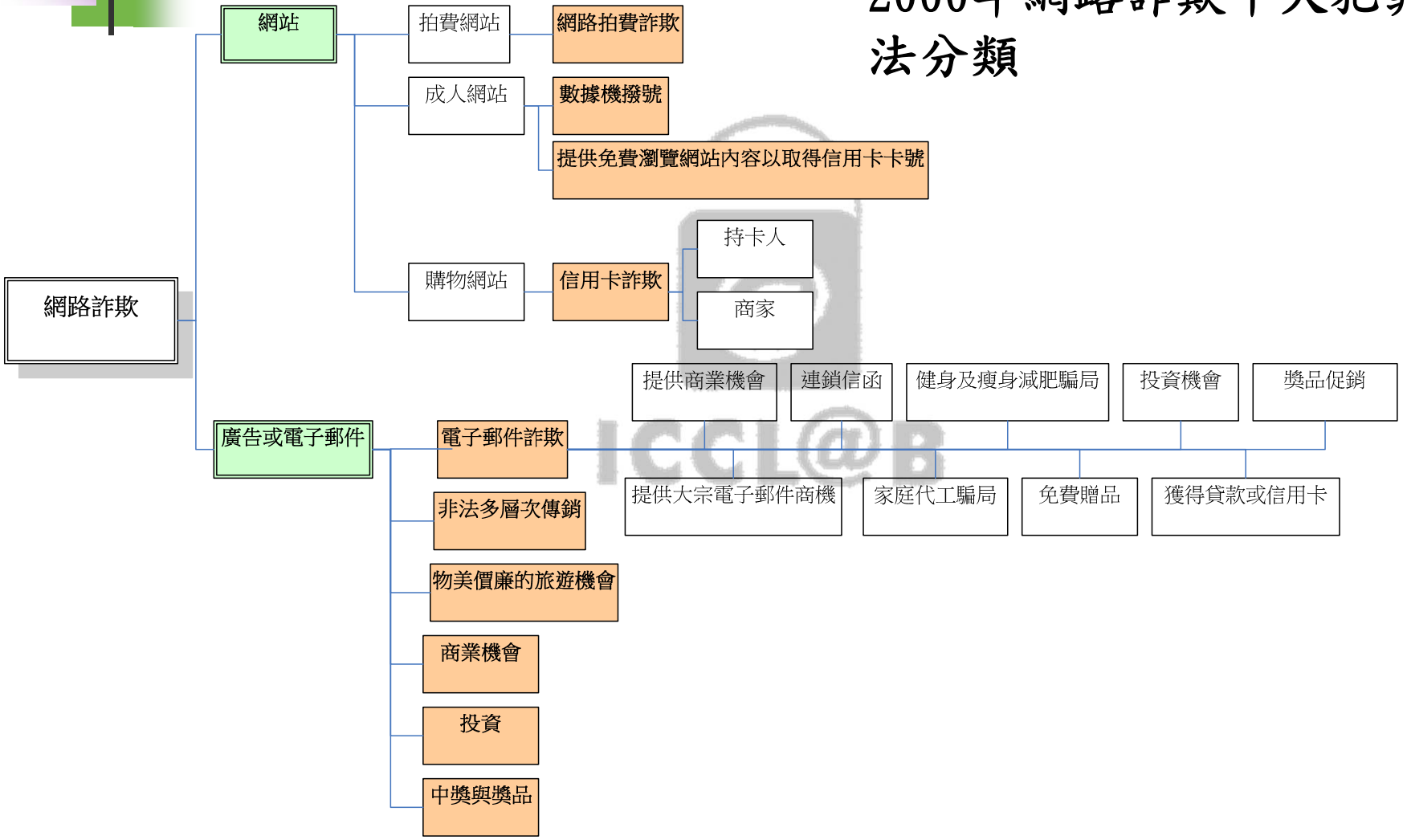
- 木馬程式(Trojan)：被入侵的主機被建立一個開放遠端控制的後門，進法不法的破壞。
- 間諜程式(Spyware)或p2p程式：被植入的主機會將資訊開放分享，提供植入者或不特定者使用。至於p2p則是在商業公司管理下的程式，當被惡意使用者，亦能扇為入侵的工具。
- 傀儡程式(Bot-Net)：利用傀儡程式來替代傳統的IPSPOOFING工具，使攻擊者的身份更加隱匿，達到更高的匿名性，及調查的難度。
- 開放伺服器(Open Proxy Server)：利用公/民機關較封閉的網管政策，在開放網路架設不同服務(如P2P、MSN、網路遊戲)的代理伺服器，吸引無知使用者在連線過程中留下機密資料。

網路詐騙

- 台灣網路詐欺的歷史發展
  - 中華民國內政部警政署刑事警察局統計：網路犯罪成長比率明顯超越其他刑事案件，其中網路性交易、網路詐欺、網路誹謗分別暫居前3位

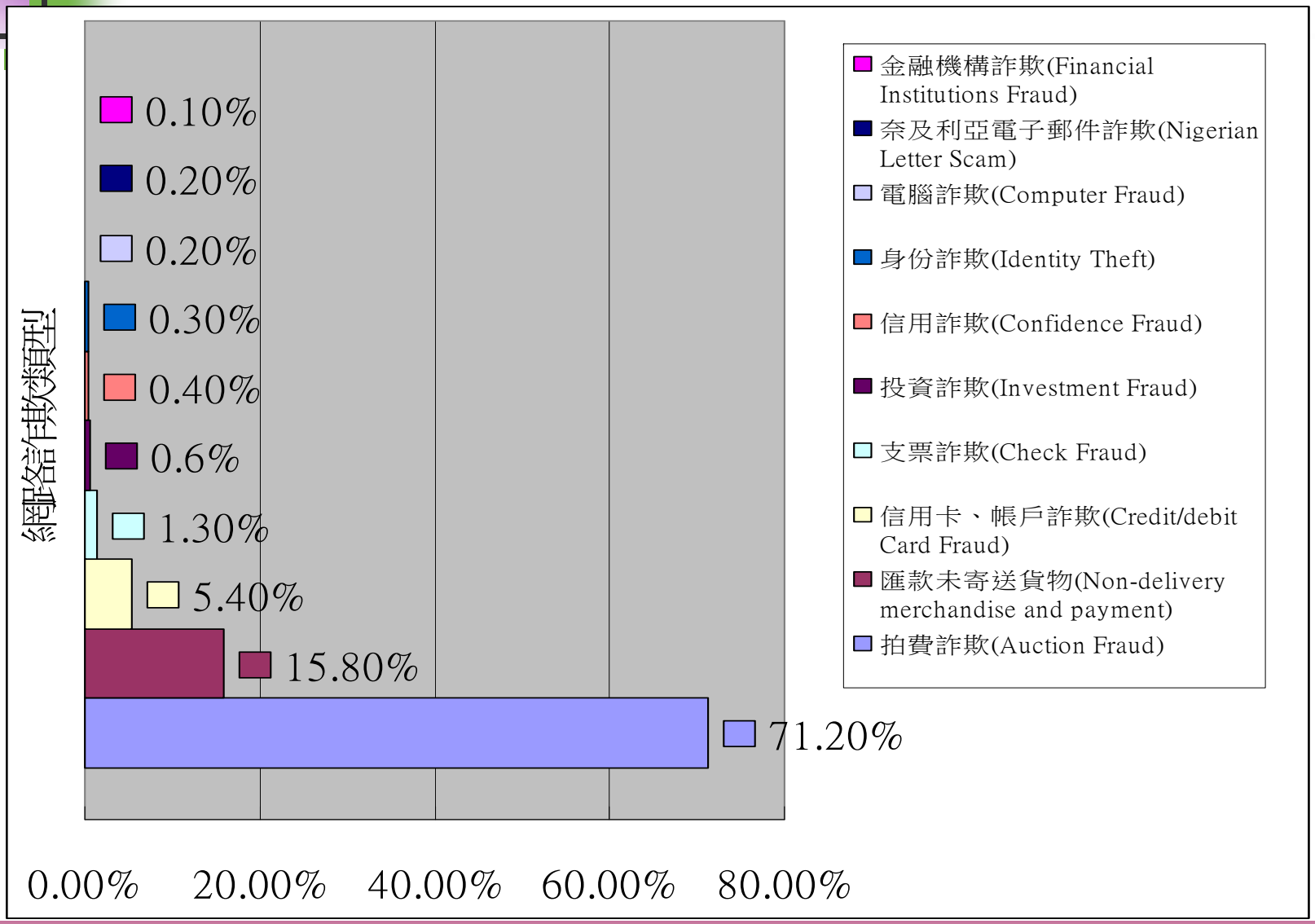
美國網路詐欺的歷史發展

2000年網路詐欺十大犯罪手法分類



Internet Crime Complaint Center, IC3

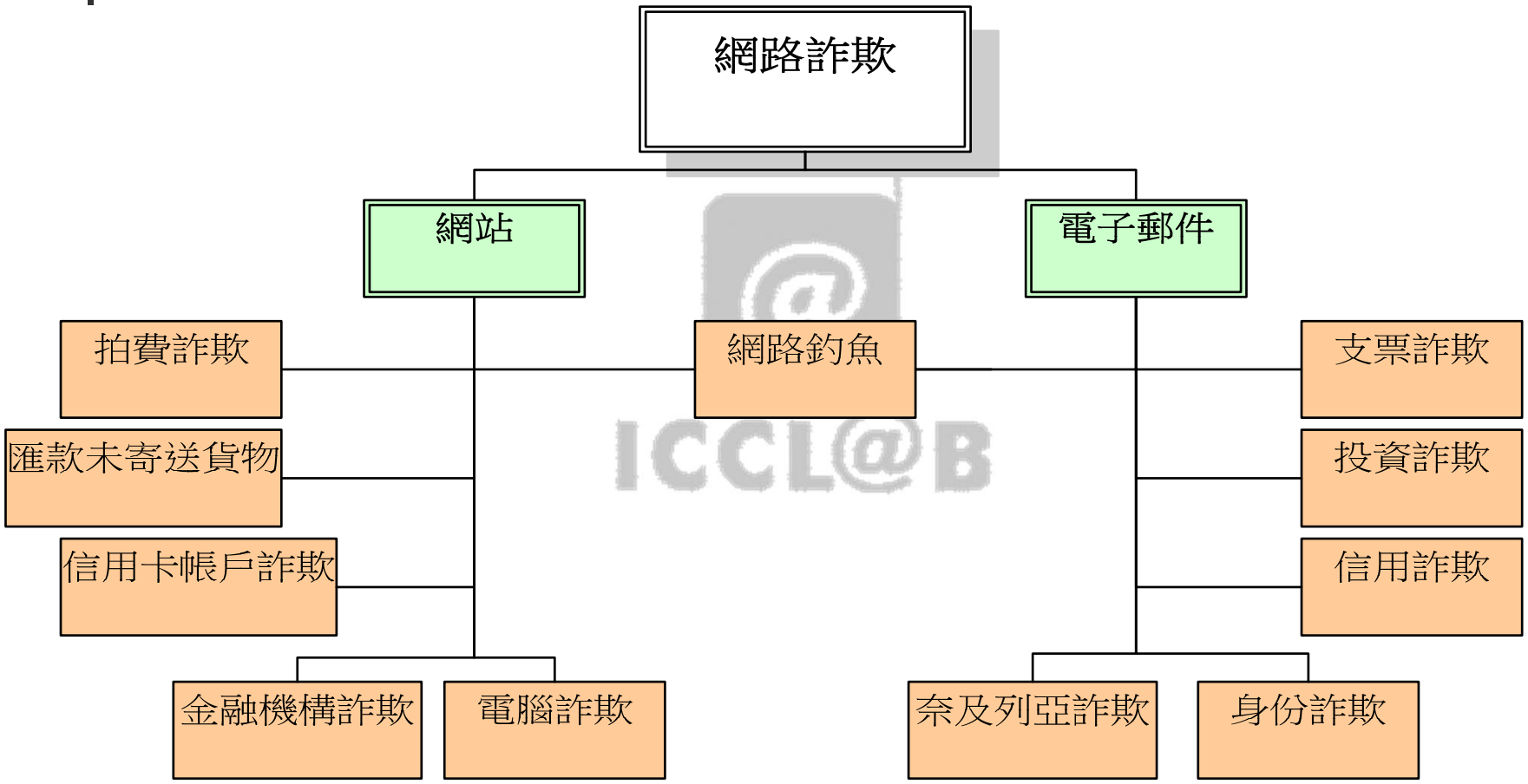
2004年十大IC3申訴網路詐



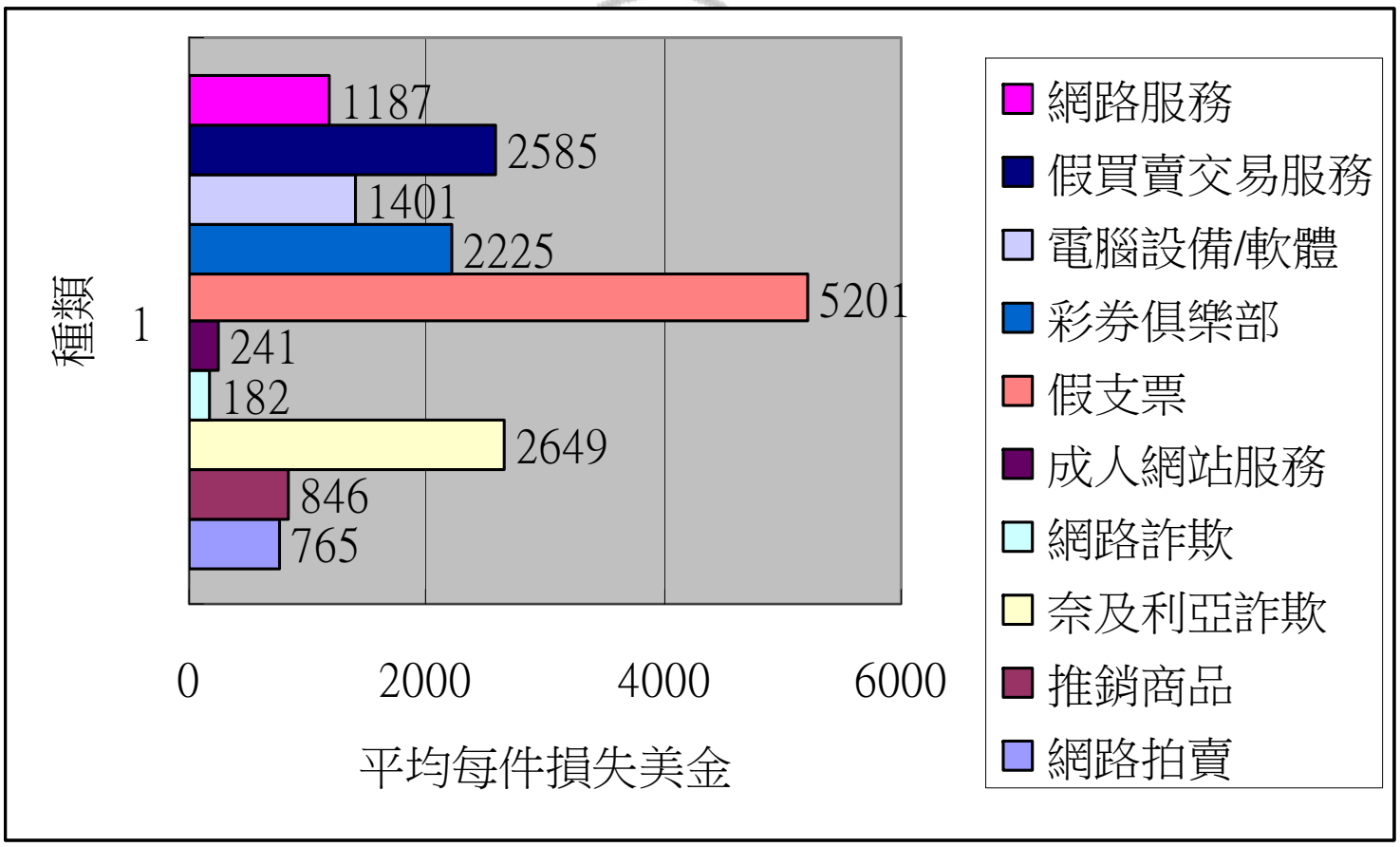
網路詐欺犯罪特性

- 網路拍賣詐欺約占了71.2%；
- 匯錢但賣方未寄送貨物約占了15.8%；
- 信用卡、帳戶詐欺約占了54%，
- 其他依序是支票、投資、信用詐欺、竊取身份、電腦詐欺、金融機構等詐欺總共約2.3%。
- 網路詐欺主要透過寄送電子郵件和網頁是兩種主要機制。

IC3十大網路詐欺分類



十大網路詐欺損失金額


種類
1
1187
2585
1401
2225
5201
241
182
2649
846
765
0
2000
4000
6000
平均每件損失美金
網路服務
假買賣交易服務
電腦設備/軟體
彩券俱樂部
假支票
成人網站服務
網路詐欺
奈及利亞詐欺
推銷商品
網路拍賣

網路釣魚案件六何要件分析

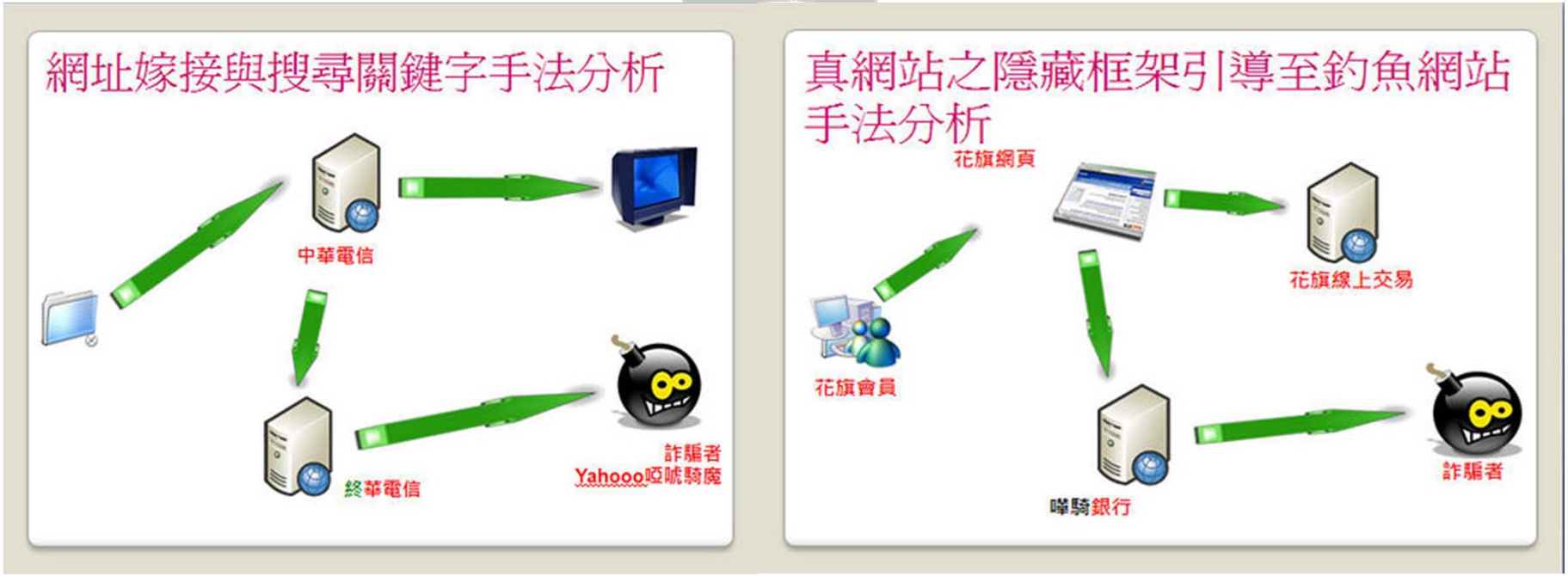
六何(5W1H)要件	概要	內容
如何 How	犯罪手段	電子郵件、假網站、惡意程式。
	獲利方式	網路銀行、信用卡。
	操作方式	社交工程、駭客工具、系統漏洞等。
何人 Who	犯罪主體 嫌疑人	Phisher(個人/組織)
	被害人	被害者(持卡人，帳號使用者)
	關係人	銀行、網站所有人(個人/組織)、ISP、安全組織(CERT/公司)政府機關
何事What	犯罪類型	詐欺罪、竊盜罪、防害電腦使用罪、電腦處理個人資料保護法、洗錢防制法等。
何時When	犯罪時間	檔案的「建立日期」、「存取日期」、「修改日期」
	出入時間	帳號登入網站之「起訖時間」及「使用時間」
何地Where	犯罪地點	連線詐騙網站IP 位址 電子郵件 相關入侵工具軟體
為何 Why	犯罪動機與目的	信用資料的疑義與金融需求的必要。

社交工程與網路釣魚

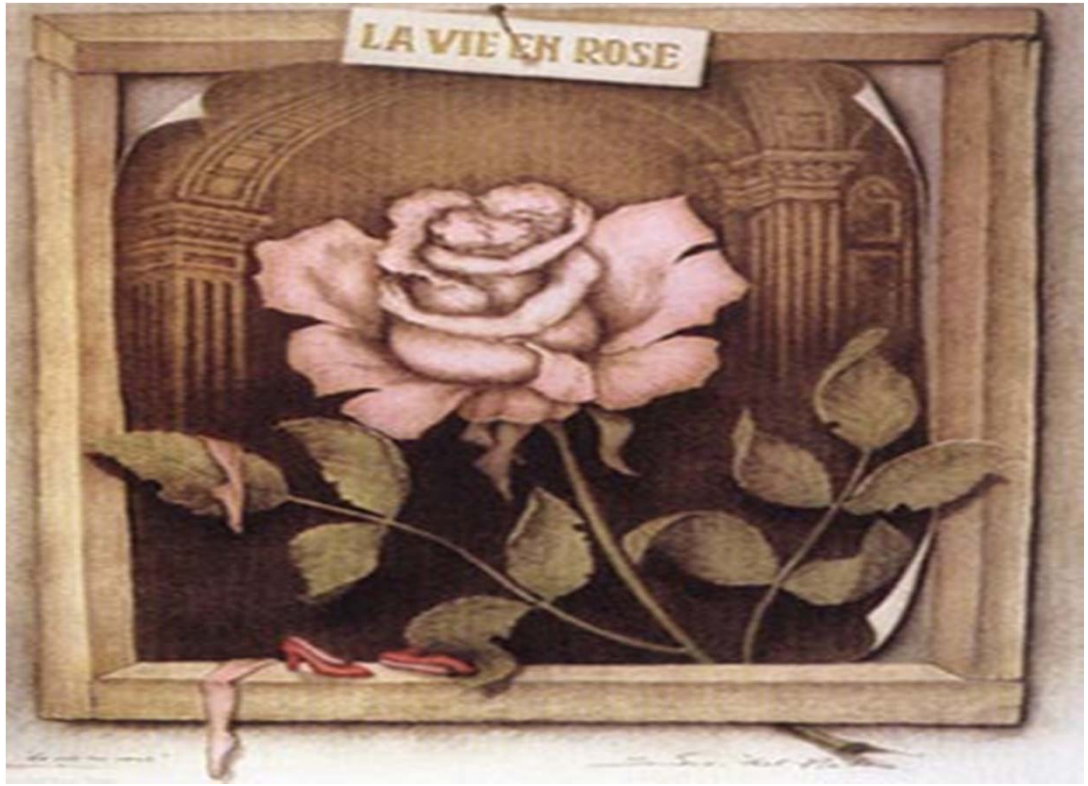
- 社交工程：透過人性認知的弱點及錯誤來達到竊取機密資訊的目的。
- 網路釣魚：將社交工程的概念應用到網際網路資訊交換的過程(如電子郵件、網頁資訊登錄)中，在網頁及電子郵件中設下不同的陷阱，以竊取所要個人資料及相關的資訊。

網路釣魚的方式

- 垃圾郵件
- 郵件內及網站上的錯誤連結
- 網址嫁接
- 冒牌網站(dns名稱類似、搜尋引擎清單問題)



參考自網路攻防戰：http://anti-hacker.blogspot.com/2007/03/


LA VIE EN ROSE

科技與人文管理結合

一 企業和員工都成為內容管理的受益者

- 內容管理不只是科技產品，更包含許多人文管理層次的問題
- 從資訊管理角度以及行政管理角度都保持溝通的誠意，達成提昇企業網路運用效率以及上班時間生產力的目標
- 預防勝於治療的概念，從報表有了資訊流內容的情報，進一步掌握資訊安全的先機。從內而外進行防禦，補足了傳統上僅注重外層防禦的不足

結論

- 人們仰賴科技的程度日深，資訊科技變成了企業競爭力的核心，而資訊安全也被提升到企業的核心。科技---安全---完美/信賴
  - 資訊安全環境整體的規劃可以分成程序、技術及人三大塊來看，簡單來說就是要有標準的程序、適當的工具及技術、人員的訓練等。
- 營造機關/企業的安全文化，了解資訊安全不是口號，也不只是把機器安裝上即可。
  - 資安必須從心理建設開始，將資安認知擺在最重要的位置，資訊安全才會受到重視。
- 世上「沒有100%安全」，任何政府機構或私人企業都可能發生資安事件。

References

- **王旭正,** 林祝興 and ICCL(資訊密碼暨資料建構實驗室), 數位科技安全與鑑識-高科技犯罪預防與數位證據偵蒐, 博碩文化出版社, ISBN: 978-986-201-196-6, Feb. 2009.
- **王旭正,** 柯永瀚,and ICCL(資訊密碼暨資料建構實驗室), 電腦鑑識與數位證據-資安技術、科技犯罪的預防、鑑定與現場重建, 博碩文化出版社, ISBN: 978-986-201-004-4, June, 2007.
- **王旭正,** 柯建萱,and ICCL(資訊密碼暨資料建構實驗室), 資訊媒體安全- 偽裝學與數位浮水印, 博碩文化出版社, ISBN: 978-957-527-980-6, July, 2007.
- **王旭正**, 高大宇, and ICCL-資訊密碼暨資料建構實驗室, 資訊安全與鑑識科學, 博碩文化出版社, Jan., 2007.
- **王旭正**, 柯宏叡, and ICCL-資訊密碼暨資料建構實驗室, 秘密通訊與與網路安全, 博碩文化出版社, March, 2006.
- **王旭正**（資訊密碼暨資料建構實驗室), "資訊安全鑑識程序建立與有效證據萃取作業(XXXIII) －直擊Unix/Linux系統入侵Using the Power of TCT鑑識," 網管人雜誌, http://www.netadmin.com.tw/, 城邦文化電腦雜誌系列, to appear in April, 2009.
- **王旭正**（資訊密碼暨資料建構實驗室), "資訊安全鑑識程序建立與有效證據萃取作業(XXXII) －即時通訊媚力vs.數位鑑識魁力," 網管人雜誌, http://www.netadmin.com.tw/, 城邦文化電腦雜誌系列, to appear in March, 2009.
- **王旭正**（資訊密碼暨資料建構實驗室), "資訊安全鑑識程序建立與有效證據萃取作業(XXXI) －新USB介面: U-Key於資安與鑑識應用," 網管人雜誌, http://www.netadmin.com.tw/, 城邦文化電腦雜誌系列, Feb., 2009.
- **王旭正**（資訊密碼暨資料建構實驗室), "資訊安全鑑識程序建立與有效證據萃取作業(XXX) －以小搏大: 遠端鑑識的閃靈工具-Helix 2.0," 網管人雜誌, http://www.netadmin.com.tw/, 城邦文化電腦雜誌系列, Jan, 2009.
- **王旭正**（資訊密碼暨資料建構實驗室), "資訊安全鑑識程序建立與有效證據萃取作業(IXXX) －數位證據縱橫談：抽絲剝繭之藕斷絲連," 網管人雜誌, http://www.netadmin.com.tw/, 城邦文化電腦雜誌系列, Dec., 2008.
- **S.J. Wang** and D.Y. Kao, "The IP Address and Time in Cyber-crime Investigation," Policing: An International Journal of Police Strategies & Management, accepted in Feb. 2009. (SCI).
- **S.J. Wang**, D.Y. Kao, and Frank F.Y. Huang, "Procedure Guidance on Internet Forensics Coping with Copyright Arguments of Client-Server-based P2P Models," International Journal Computer Standards & Interfaces, on-line, 2008. (SCI)
- **S.J. Wang**, "Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime," International Journal Computer Standards & Interfaces, Vol. 29, Jan. 2007. (SCI)
- **S.J. Wang** and D.Y. Kao, "Internet Forensics on the Basis of Evidence Gathering with Peep Attacks," International Journal Computer Standards & Interfaces, Vol. 29, pp. 423-429, 2007. (SCI)
- **S.J. Wang,** H.J. Ke, J.H. Huang, and C.L. Chan, "Hash Cracking and Aftereffect on Authentication Procedures in Cyberspace," IEEE Transactions on Aerospace and Electronic Systems, Jan. 2007. (SCI)

5W1H with researches and lives

- "*Think **why** you are here*".
- "*Find **where** you are interested in here*".
- "*Marry **whom** you look for here*".
- "*Get **what** you want to have here*".
- "*Honor here **when** you own something special with knowledge*".
- *HAKUNA MATATA – "**H**"*

- **Dr. Professor Shiuh-Jeng WANG**
- PhD. National Taiwan University, Taiwan, 1996
- Full Professor, Central Police University, Dept. of Information Management
- Director Information Crypto and Construction Lab
- Chair of ICCL-FROG (**F**orensic **R**esearch devel**O**pment task force **G**roup)
- Vice-President, Chinese Cryptography Information Security Association (**www.ccisa.org.tw**)

- Chairs of IEEE-CS/LNCS Proceedings, Internat'l confs.
  http://www.sersc.org/SH08/ http://www.ftrg.org/MPIS2009
  http://ncs2009.ntpu.edu.tw/CI/CI.htm http://www.ftrg.org/futuretech2010
  https://sites.google.com/site/uicuipm2012/ IEEE-sponsored,
  http://www.ftrai.org/music2012
- Editor-in-Chief AT JITAS (http://jitas.im.cpu.edu.tw)
- SCI-Journals, Guest-editors-,
  - IEEE J-SAC, http://www.comsoc.org/livepubs/sac/index.html
    http://hera.im.cpu.edu.tw/sjw_2006/meeting_report/IEEE-GUEST-EDITORIAL-0808-2011-.pdf
  - Journal of Internet Technology (JIT)
    http://jit.ndhu.edu.tw/callforpaper/April-2011-SI-JIT.pdf
  - The Computer Journal, http://comjnl.oxfordjournals.org/
  - Springer Telecommunication Systems
    http://www.springer.com/business/business+information+systems/journal/11235
  - The Journal of Supercomputing,
    http://www.springer.com/computer/swe/journal/11227 (Springer)
  - Peer-to-Peer Networking and Applications,
    http://www.editorialmanager.com/ppna/ (Springer)