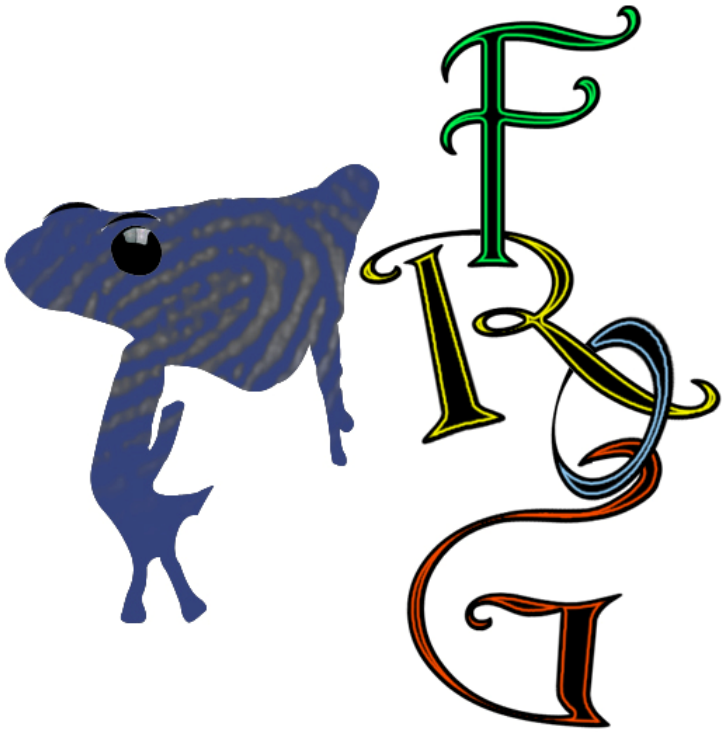
資訊/網路/鑑識安全

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

ICCL-FROG



Forensic Research & develOpment

task force Group

MY FROG and the FROG with you

Cyber Crime

- 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.

犯罪六何要件分析

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。

資訊安全與電腦犯罪

1. 資訊安全-PKI與自然人憑證
2. 軟體安全-常見軟體攻擊方式
3. 網路詐騙介紹

1.資訊安全

- 1-1、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

1-1、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

1-1、PKI 公開金鑰基礎建設(續)

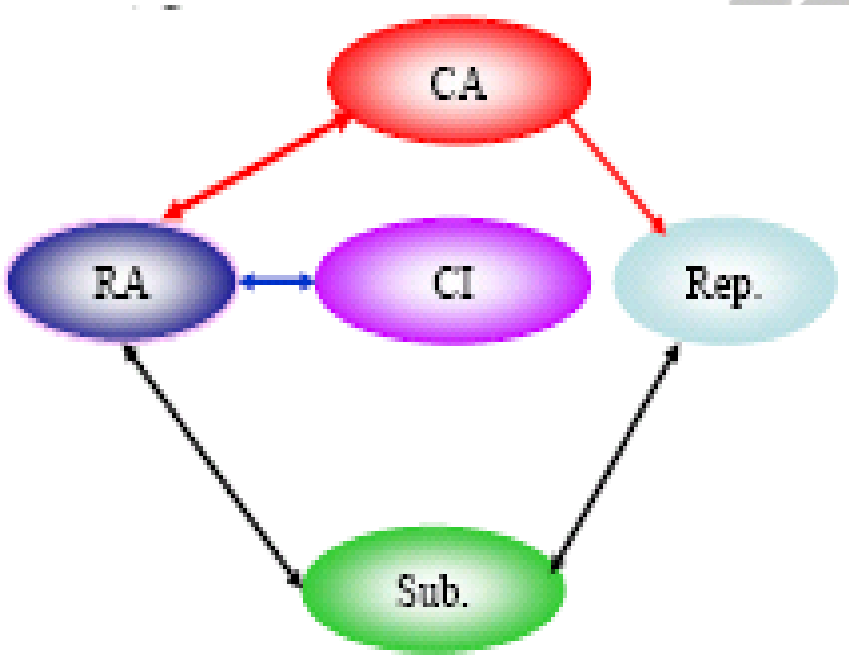
- 什麼是PKI？(1/2)
  - 雖然有數學理論或是長久的實務驗證說明公開金鑰密碼技術的各種演算法已達一定的安全性，然而如果無法確保“通訊雙方能夠正確地取得對方公開金鑰”，則縱使有完美的密碼演算法是沒有用的
  - 在實務上還需要建置一些管理機制、設施、或服務等，以確保可以達到“通訊雙方能夠正確地取得對方公開金鑰”重要前提
  - 所謂“公開金鑰基礎建設”（**Public Key Infrastructure，PKI**）是一種支持公開金鑰密碼技術正常運作的基礎建設，而所謂**Infrastructure**包含設備、設施、服務、人員、法律、政策、規範等

1-1、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

1-1、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.**

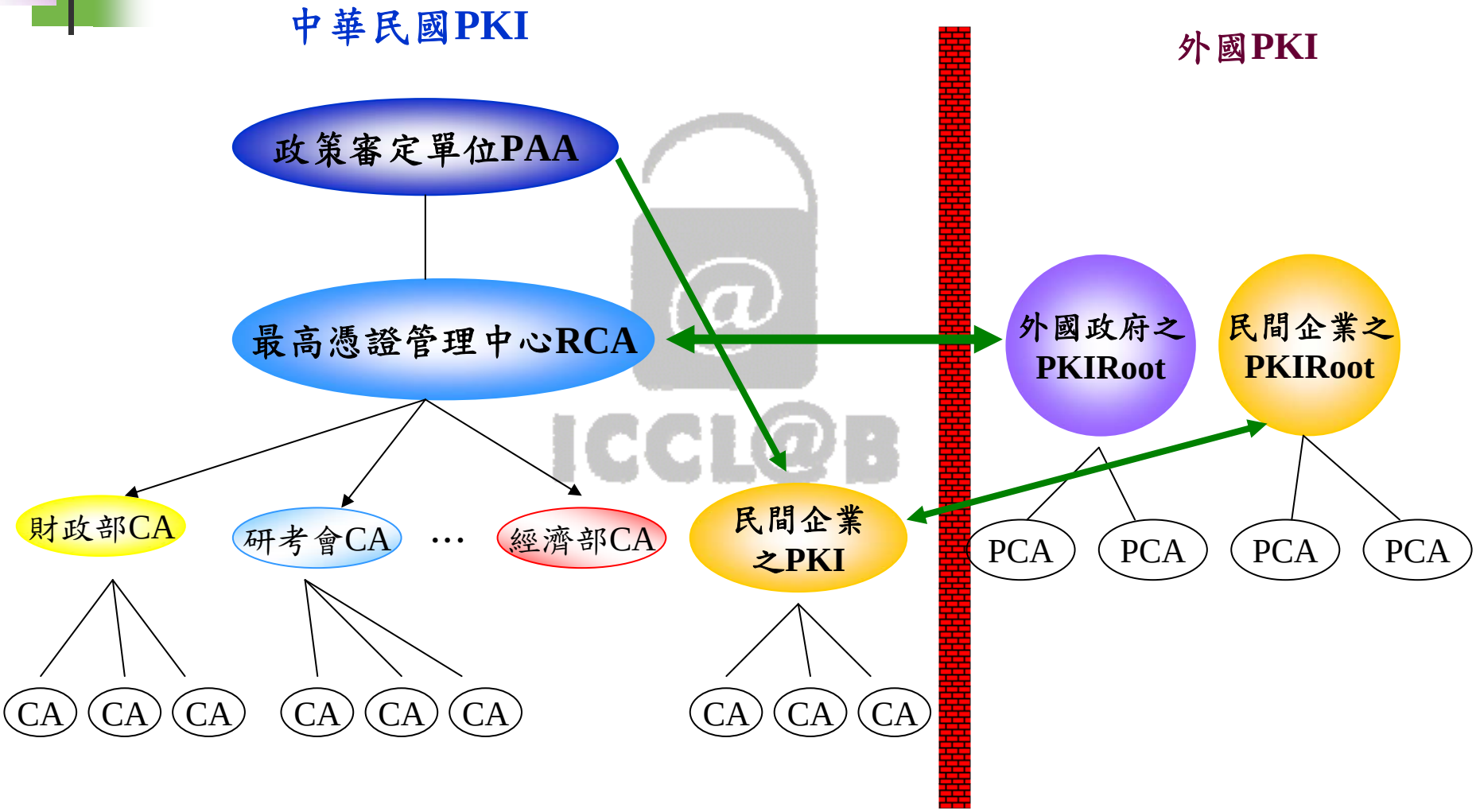


CA：憑證中心
RA：註冊中心
CI：憑證發給單位
Sub.：用戶
Rep.：儲存庫

1-2、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

1-2、我國政府公開金鑰基礎建設之架構



1-2、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

1-2、自然人憑證應用服務

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

2、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。
- 毀滅階段：
  - 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。

2-1、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。
- 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)。

2-1、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。

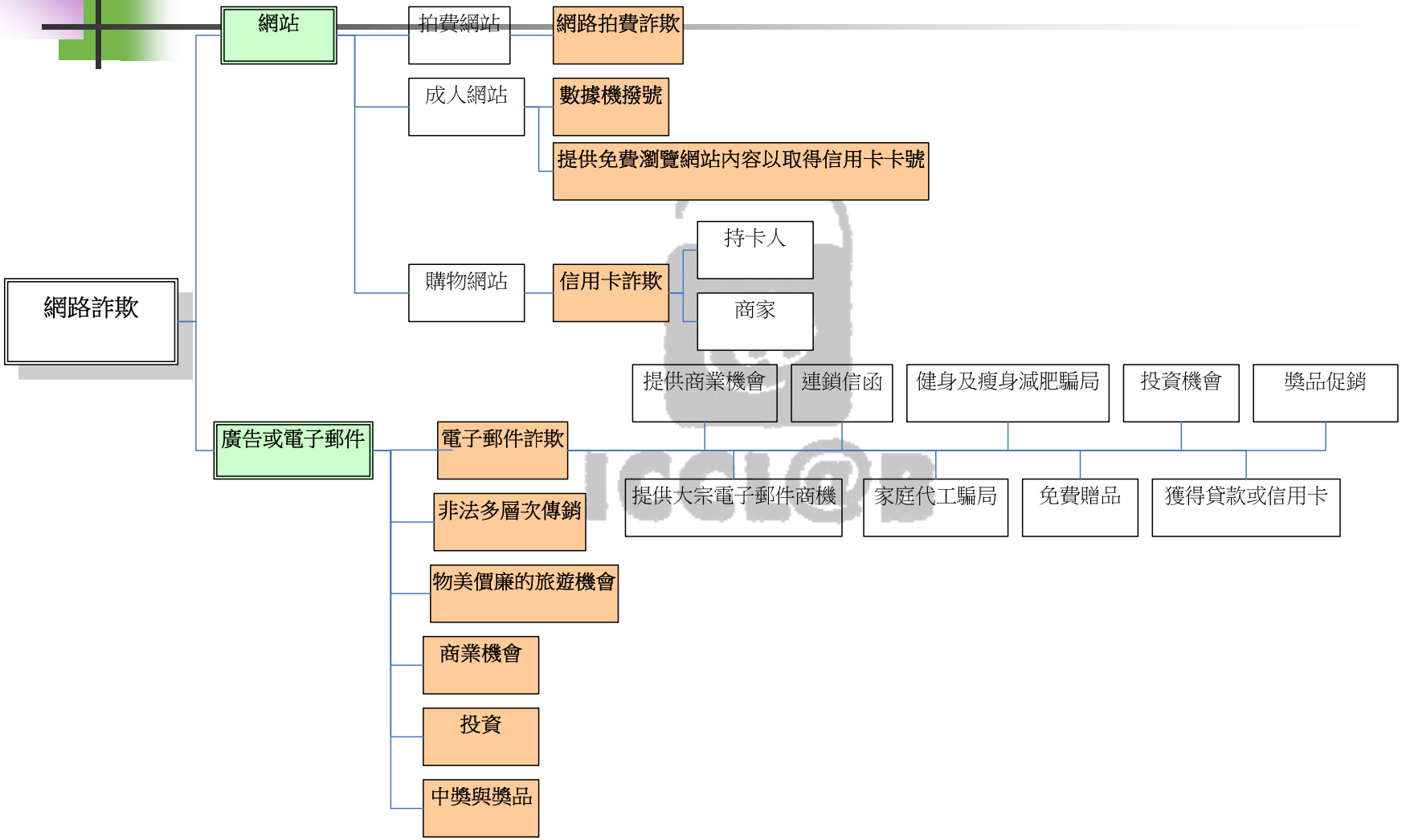
2-1、軟體安全-常見軟體攻擊方式

- 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。

3、網路詐騙

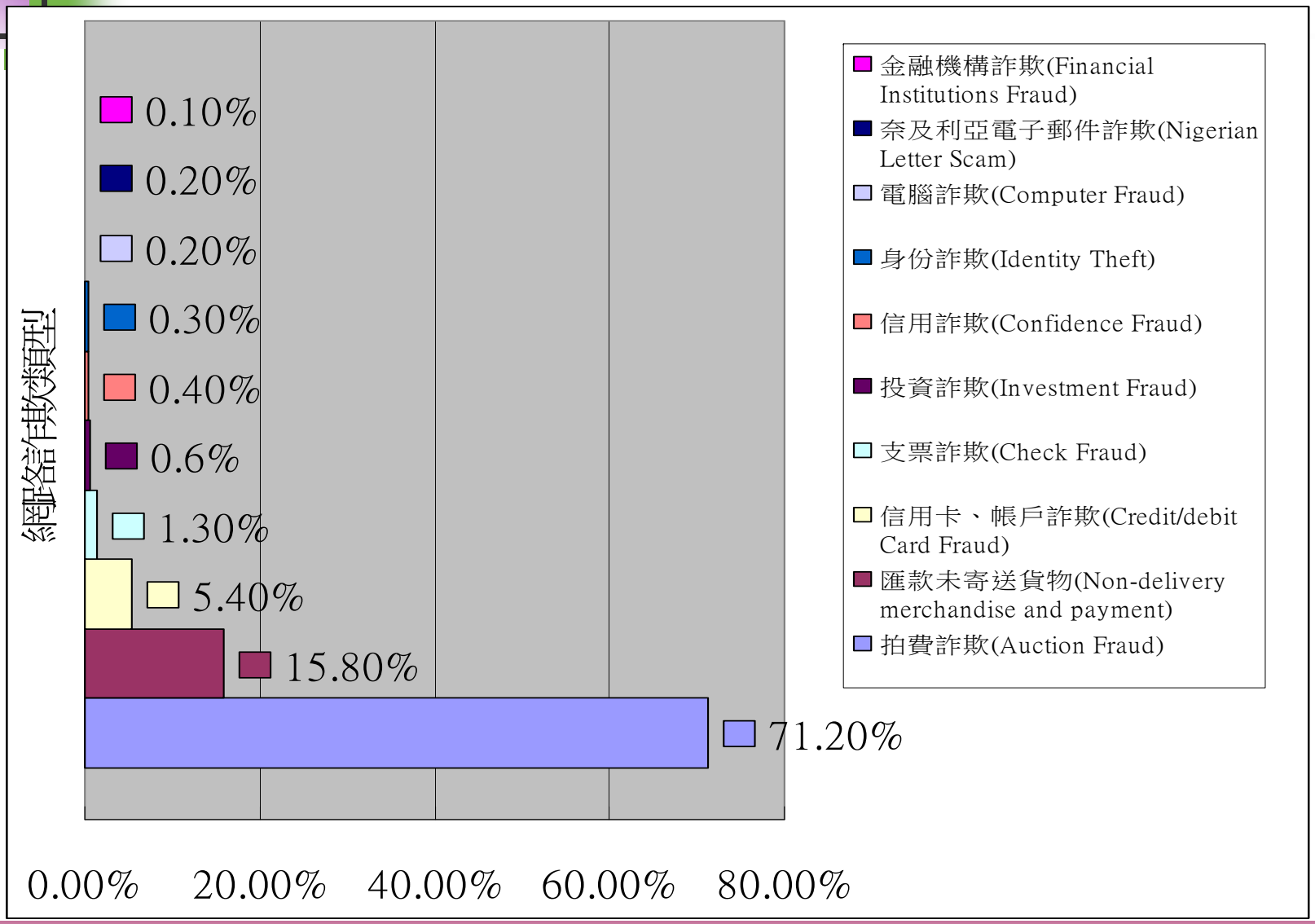
- 台灣網路詐欺的歷史發展
  - 中華民國內政部警政署刑事警察局統計：網路犯罪成長比率明顯超越其他刑事案件，其中網路性交易、網路詐欺、網路誹謗分別暫居前3位

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

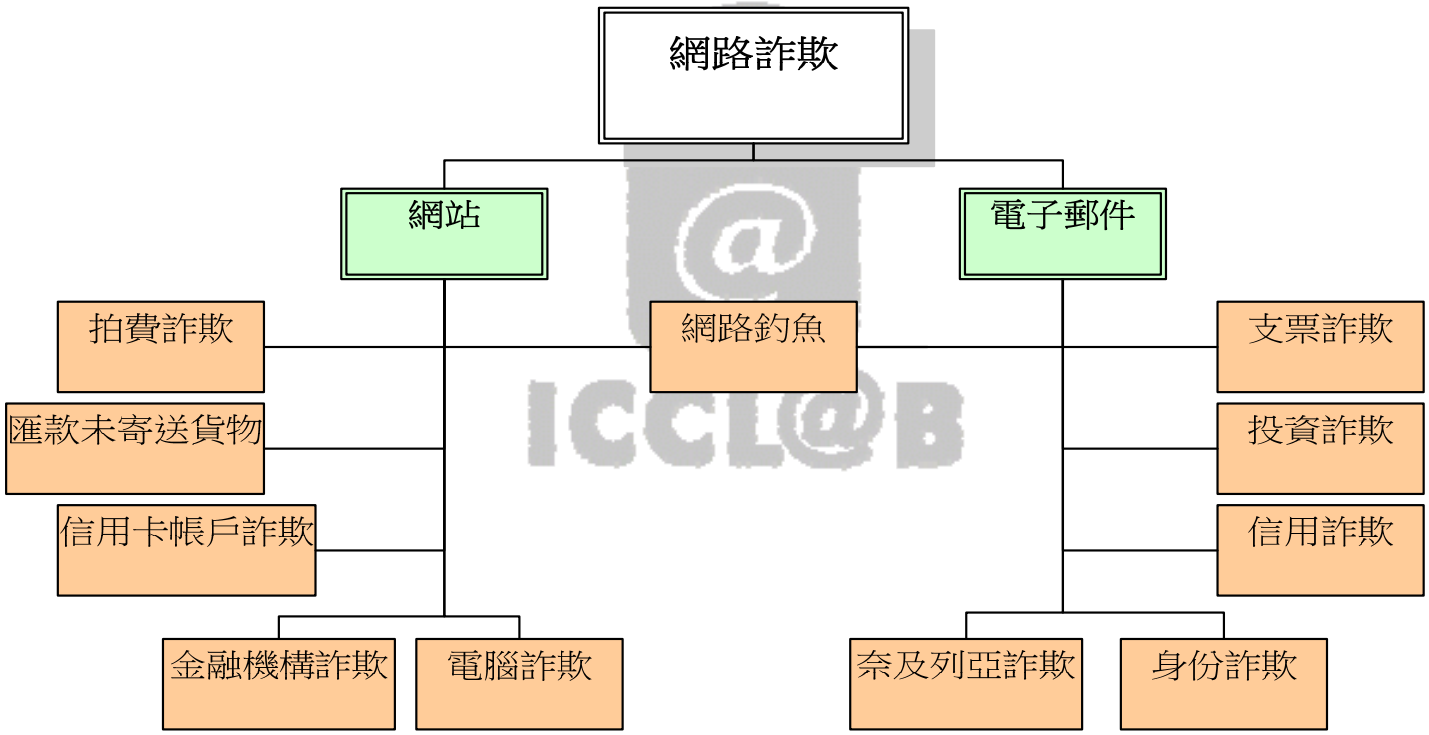
Internet Crime Complaint Center, IC3



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。

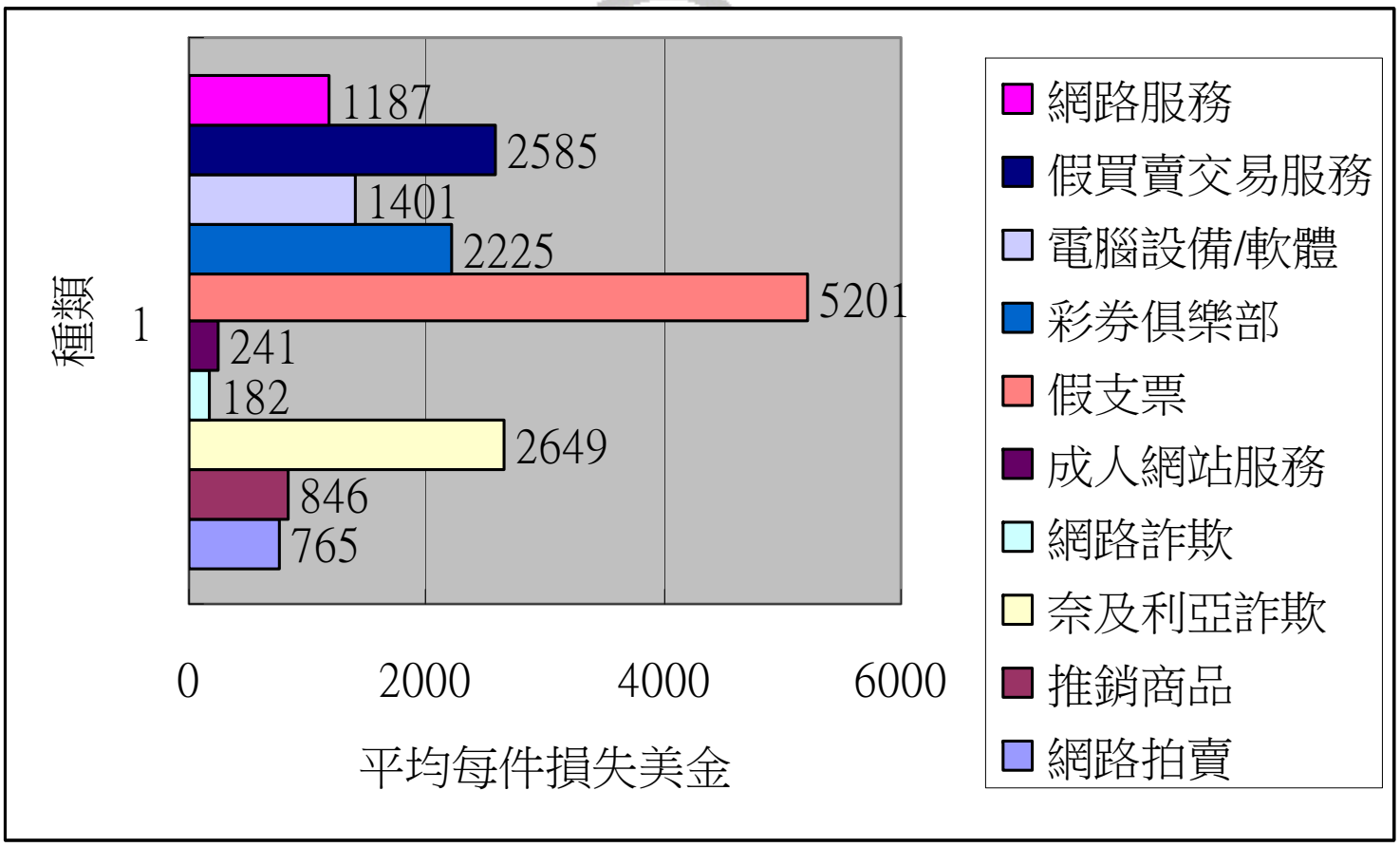
IC3十大網路詐欺分類



網路詐欺發展

- 透過電子郵件詐欺
  - 奈及利亞詐欺、網路釣魚、彩券俱樂部及假支票。
- 詐欺被害人主要支付款項的方法
  - 信用卡、直接付款、銀行借貸、信用卡借貸、支票。
- 接觸網路詐欺訊息管道
  - 依序是網站、電子郵件、網路新聞區

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。

網路詐欺工具分析-phishing

工具	功能說明	相關案例
網路釣魚 郵件偽造	是一種犯罪手法，他使用社交工程技術，特性是以欺騙方式來取得敏感的資訊如密碼和信用卡詳細的資料，利用偽裝成可信賴的公司、政府機關或相關人事之電子郵件和即時通訊，誘騙受害人回覆電子郵局與連結錯誤網址填寫資料，目的是使用者的金融資訊和密碼，再進行盜領 。	1. PayPal 網路釣魚 例如：偽裝成網路銀行。 2. SouthTrust Bank 例如：針對銀行顧客發送電子郵件，郵件嵌入使用圖片來避免反釣魚軟體(Anti-Phishing)的掃描，再誘騙使用者連結至假網站。

網路詐欺工具分析-pharming

工具	功能說明	相關案例
網址嫁接 DNS Cache poisoning DNS下毒	是針對所發現的DNS伺服器軟體弱點來攻擊，使得允許駭客來取得網站的網址名稱並改寫它，舉例來說，網頁的連結是透過 DNS 伺服器自動化回應網頁名稱所轉變的實際的IP位址，即為網路的指標，而改寫後即使用戶跳過連結，直接輸入正確網址仍然會被導入到假網站中。	相關報導指稱美國ISP業者之域名伺服器曾遭駭客入侵，並改寫網域名稱所連結的IP位址，將網址連結路徑改寫連結至假網面。

網路詐欺工具分析-Malicious code

工具	功能說明	相關案例
鍵盤動作側錄間諜程式	是一種木馬程式，一旦電腦被植入鍵盤側錄木馬，只要由這個鍵盤打出的任何按鍵，都回被傳回植入者的手中，藉由這種方法來盜取帳號等資料。	相關報導指稱犯罪者易擅常設立假網站，利用被害者瀏覽假網站時，安裝後門程式(Key-logger)於被害者的電腦，以獲取相關私密資訊。

何謂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。

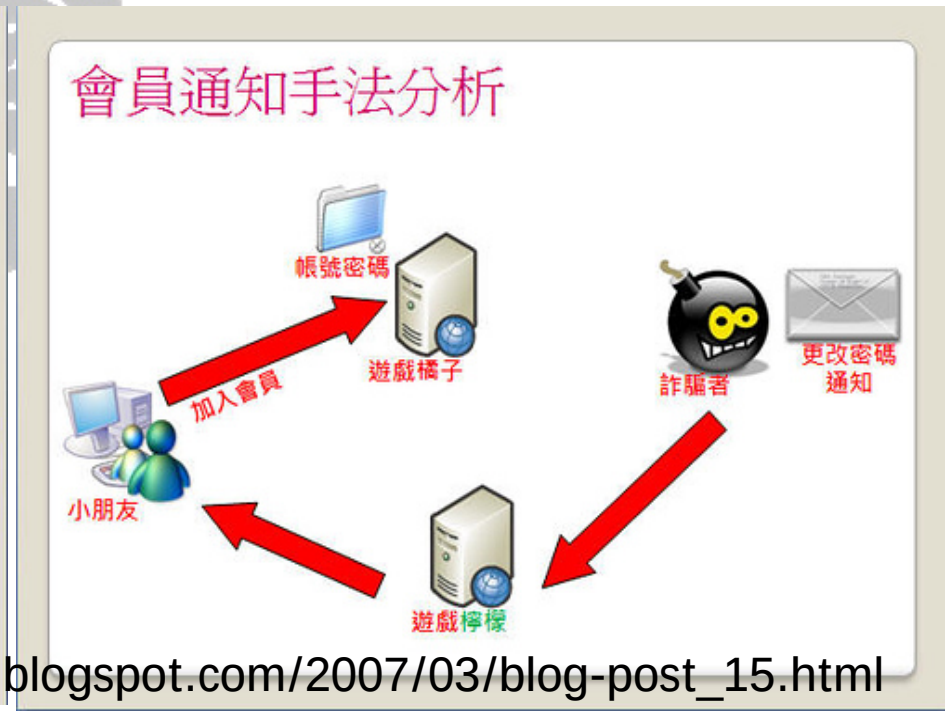
Outlook and Outlook Express 安全設定

- Outlook Express屬於Microsoft Windows作業系統附贈的軟體，功能比較簡單。
- Microsoft Outlook是屬於Office系列軟體，功能較Outlook Express多，而且也比較強，比較適合辦公室的人使用這套軟體。

功能	Outlook Express	MicroSoft Outlook
收發電子郵件	✓	✓
個人通訊錄	✓	✓
行事曆		✓
工作管理		✓
郵件規則	簡單	完整
安全性要求*	低	高

網路釣魚的方式(1)

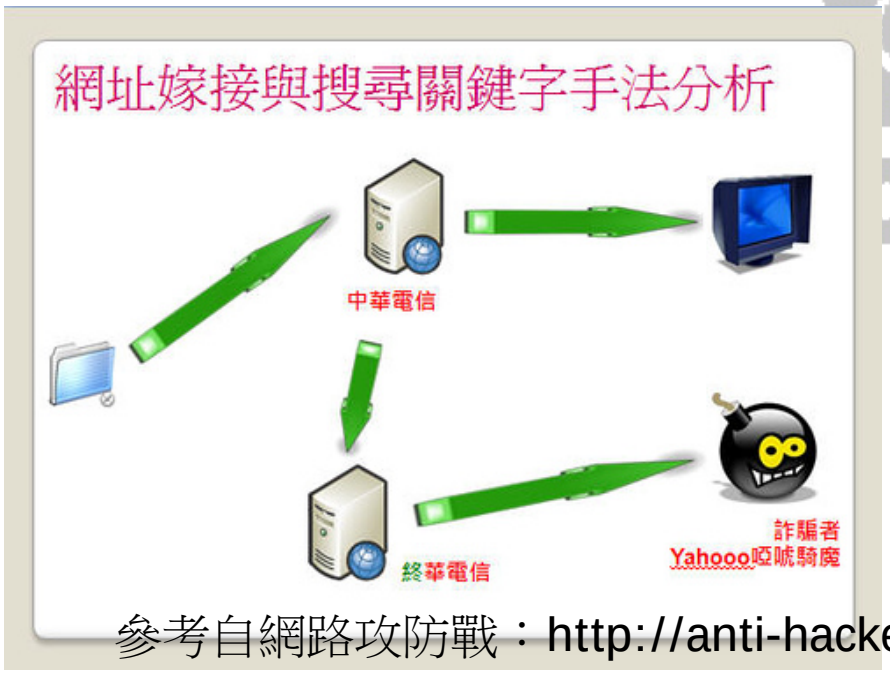
- 郵件(Yahoo拍賣及會員通知)
- 垃圾郵件
- 郵件內及網站上的錯誤連結

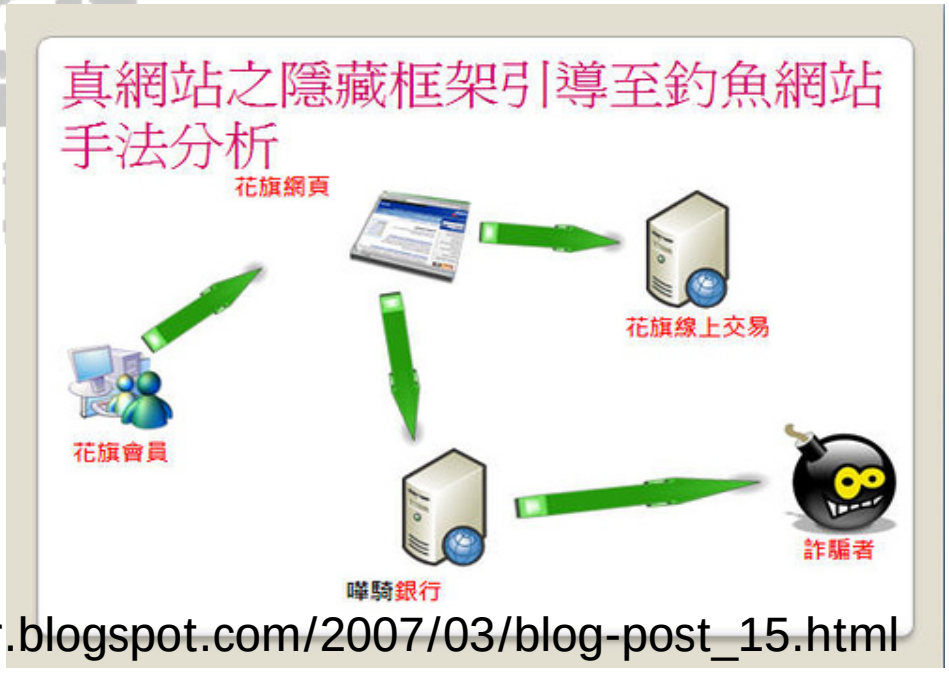


參考自網路攻防戰：http://anti-hacker.blogspot.com/2007/03/blog-post_15.html

網路釣魚的方式(2)

- 網址嫁接
- 冒牌網站(dns名稱類似、搜尋引擎清單問題)
- 遭植入木馬網站





參考自網路攻防戰：http://anti-hacker.blogspot.com/2007/03/blog-post_15.html

關閉傳送回條

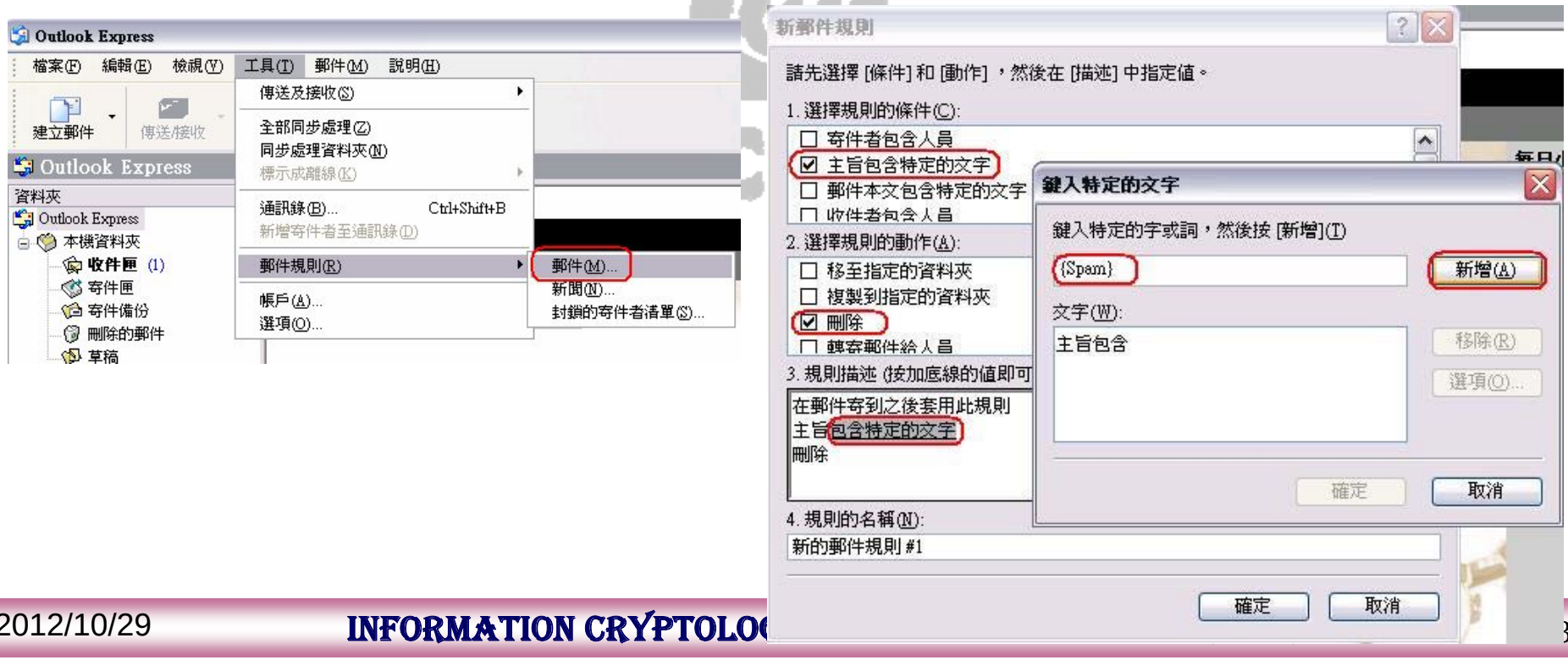
- 許多人都習慣使用「傳送回條」功能以確認對方是否有收到寄出的信，但是此功能很可能會被垃圾郵件發信者拿來確認是否有此帳號，所以建議將之關閉。
- 使用Outlook Express
  「工具」→「選項」→「回條」→點選「不要傳送回條」
- 使用MS Outlook
  「工具」→「選項」→「偏好」→「電子郵件選項」→「追蹤選項」
  點選「不要傳送回覆」

關閉預覽功能

- 許多郵件有包含網頁程式VB Script，可能在不知不覺間造成系統的危害，故建議關閉郵件預覽，以加強安全性
- 使用Outlook Express
  「檢視」→「版面配置」→取消打勾「顯示預覽窗格」
- 使用MS Outlook
  「檢視」→「讀取窗格」→「關」
- 注意附件檔案
  當收到附加檔案的副檔名為「.Com」、「.VBS」、「.Scr」、「.Exe」等，都要特別注意寄件人是否熟識，因為此類檔案都極有可能會造成系統重大危害。

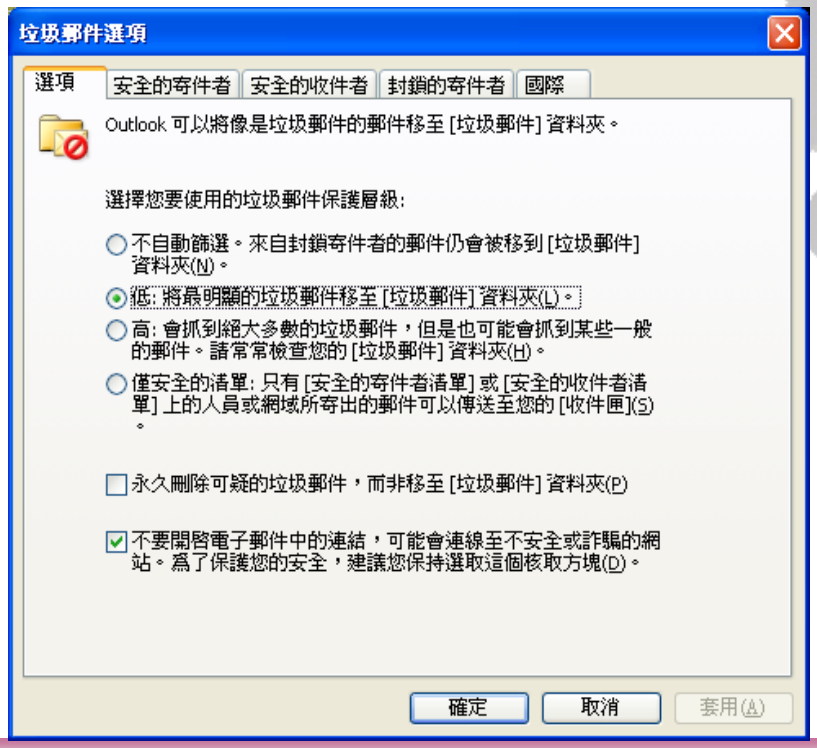
結合企業垃圾郵件管理服務—自訂「郵件規則」自動刪除垃圾信

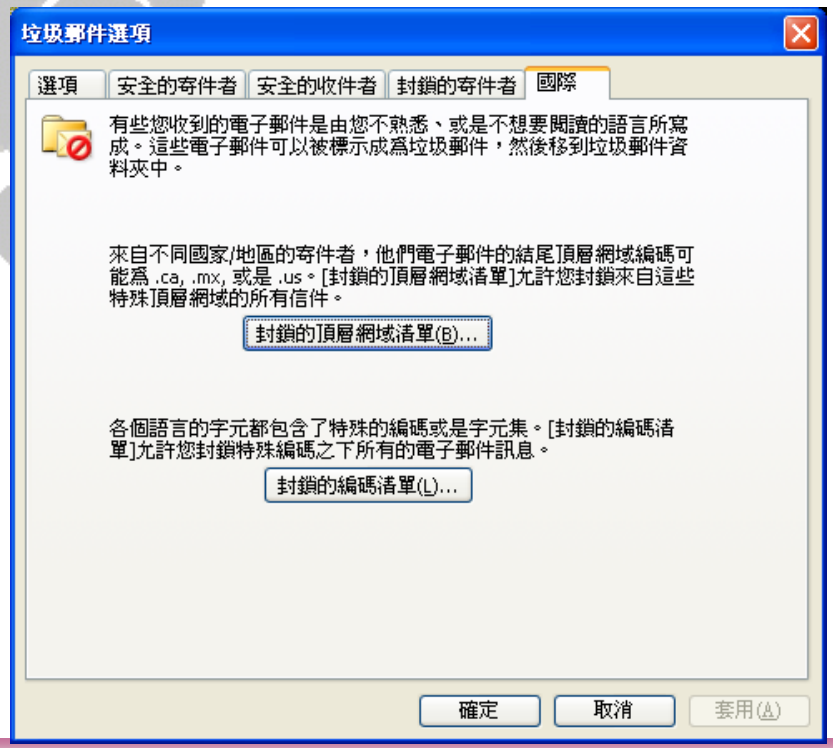
- 「工具」→「郵件規則」→「郵件」
- 勾選「主旨包含特定的文字」、「刪除」後，點選下面的「包含特定的文字」，輸入「{Spam}」再按「新增」，然後確定離開即可。



MS Outlook 垃圾郵件選項

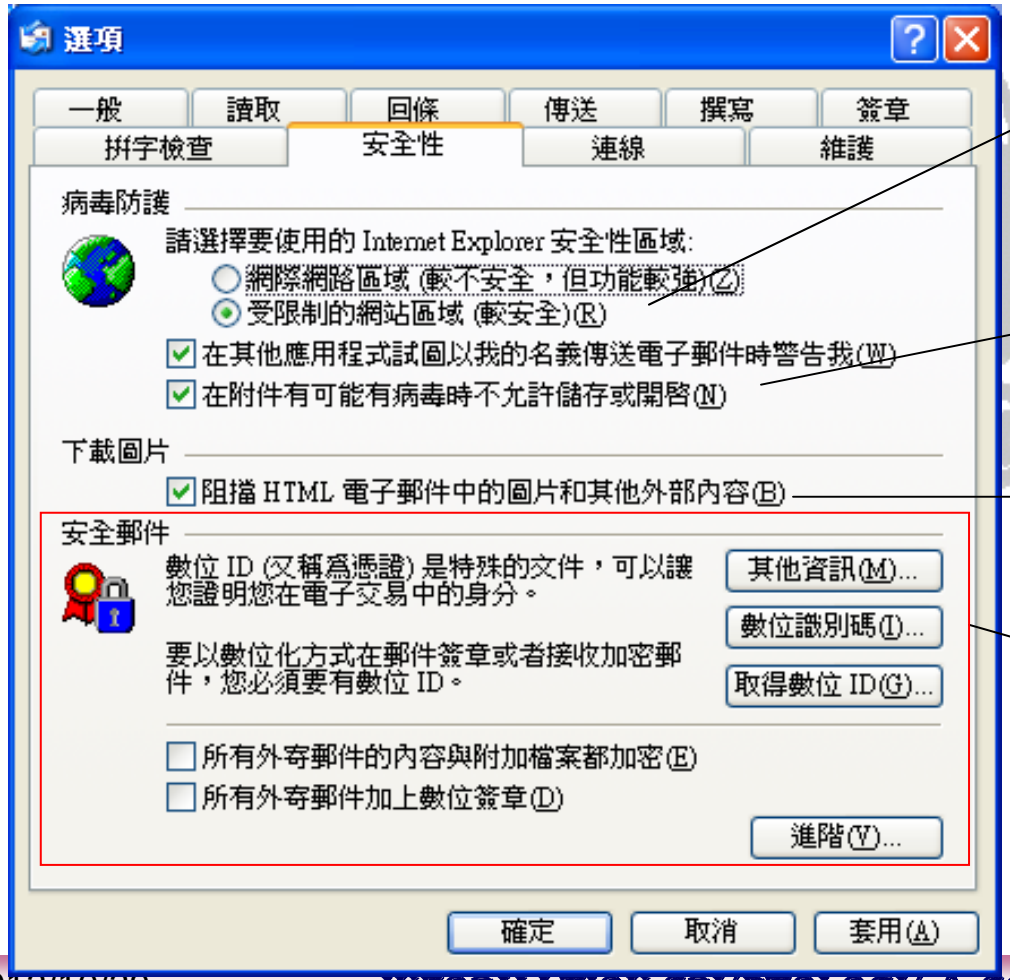
- 啟動Microsoft Outlook的[執行]→[垃圾郵件] →[垃圾郵件選項]確認各項設定：寄件、收件者來源、郵件編碼等。





安全性選項設定

由Outlook Express的[工具]→[選項]→[安全性]標籤設定



結合IE的[受限制的網站]設定

附件格式為.exe及其它可能隱含病毒的格式時不允許使用者開啟

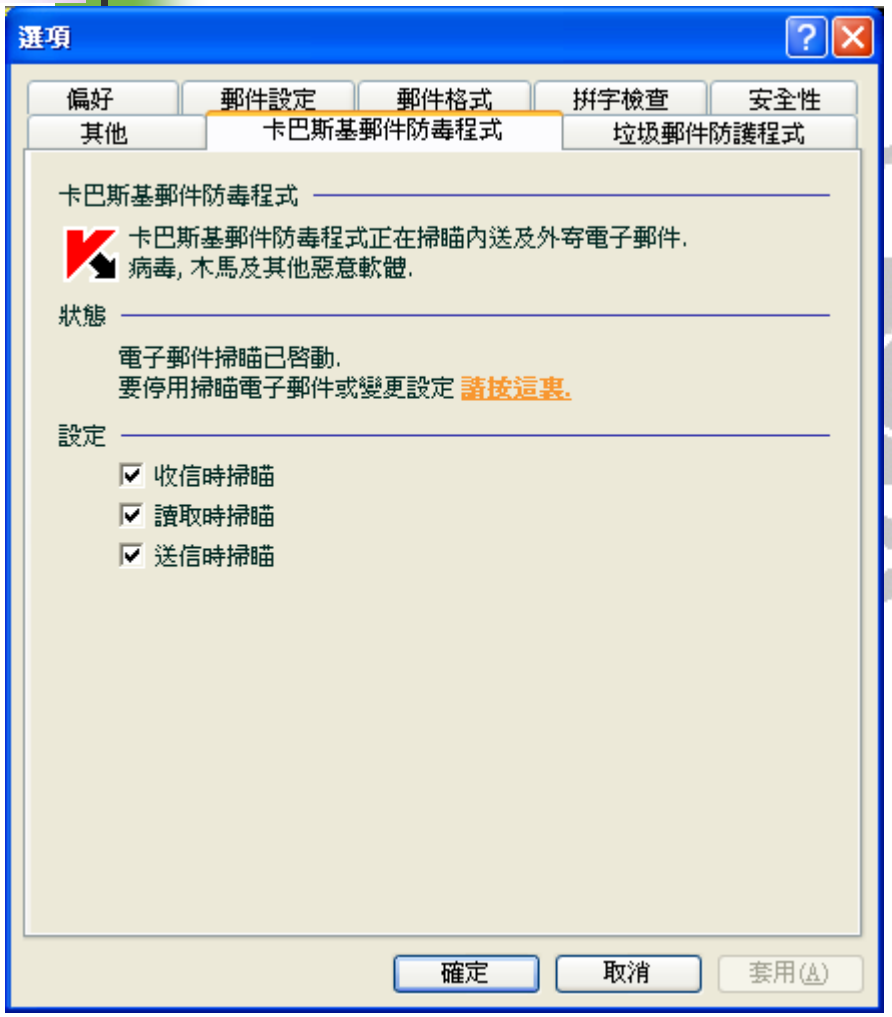
不允許郵件中直接顯示來自網際網路的超連結圖片

結合身份認證功能

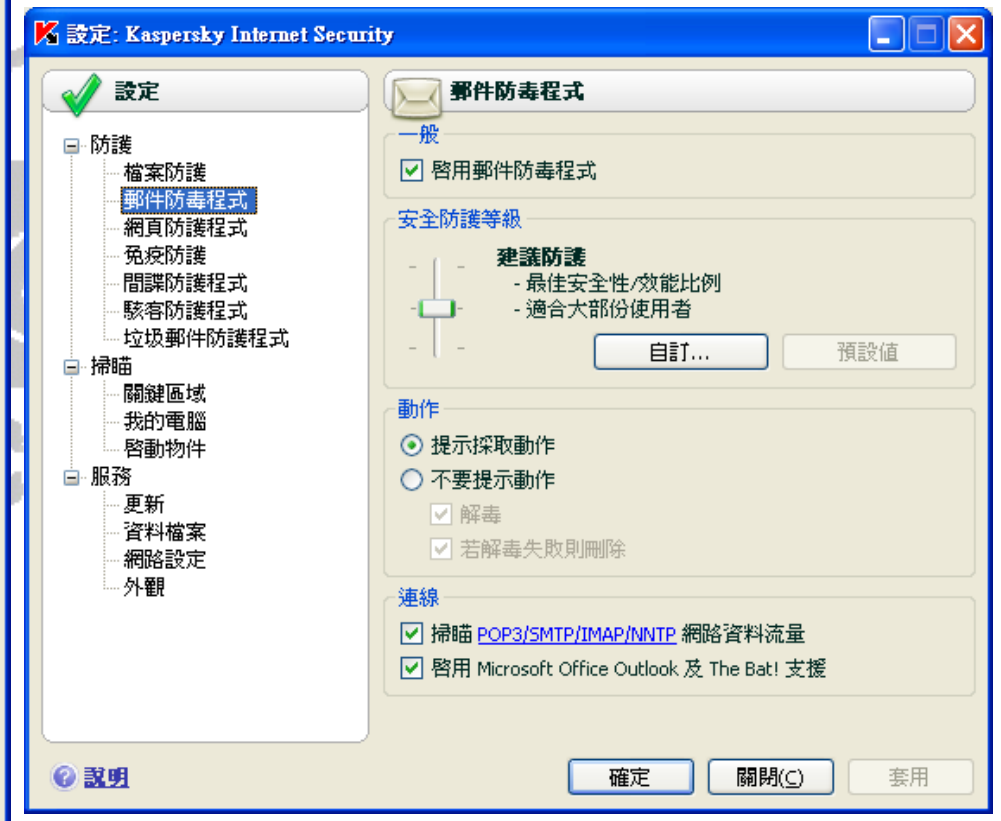
結合工具軟體

- 企業內部的郵件伺服器安裝防垃圾郵件及掃毒功能。
- 現代的單機防毒軟體除了檔案防護、防駭等功能外，多已結合郵件防毒及垃圾郵件功能。如Kaspersky Internet Security、NOD、Symantec等多家產品皆已多功能化。
- 另有如單一功能的軟體，Ad-Ware、Anti-Trojan等來達到防護的目的。

範例：結合卡巴斯基防毒軟體

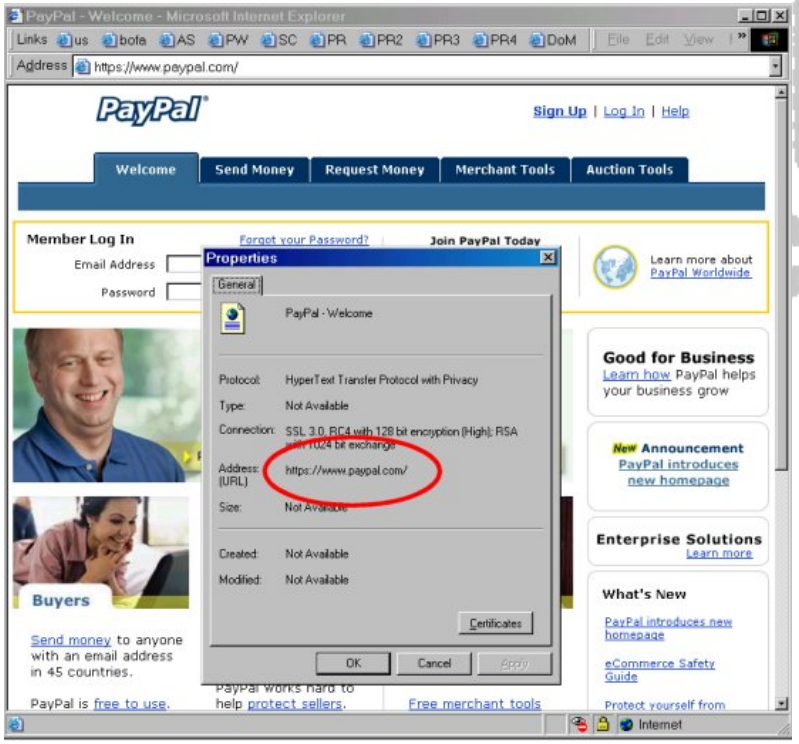


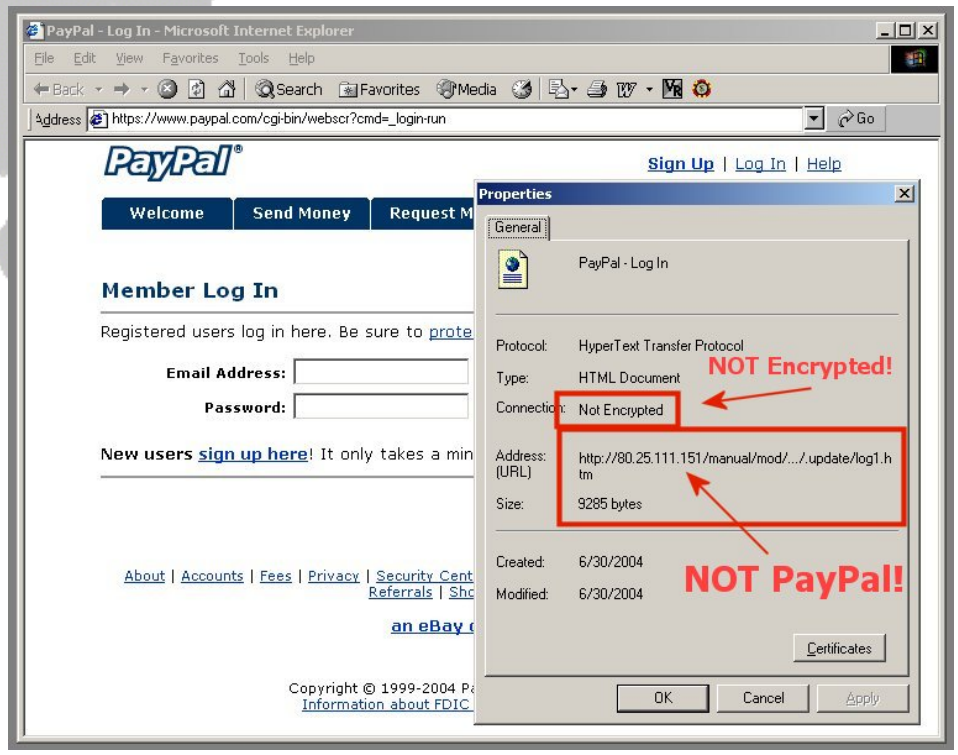
Microsoft Outlook



防禦網路釣魚終極手段

- 別在電子郵件按下任何超連結
- 確定上的是「正確的網站」





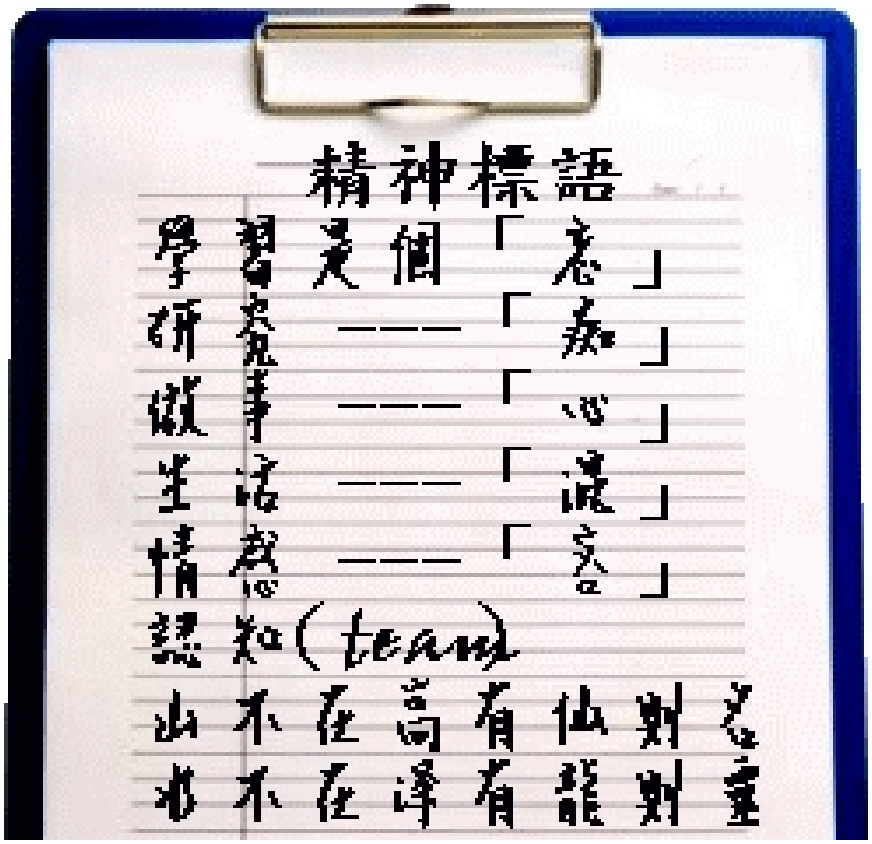
References

- **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: 978-957-527-980-6, May, 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, scheduled to publish, in May, 2007.
- **王旭正**（資訊密碼暨資料建構實驗室）,“資訊安全與密碼語言的世界（I）－中西密碼史,” 兒童月刊小學生巧連智中年級版, 編輯審定, Appear in June, 2007.
- **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（IX）－Cookies on the Internet Forensics,” 網管人雜誌, 城邦文化電腦雜誌系列, March, 2007.
- **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（VIII）－置信的武器-數位交叉鑑識,” 網管人雜誌, 城邦文化電腦雜誌系列, Feb., 2007.
- **王旭正**（資訊密碼暨資料建構實驗室),“網路時代多媒體資料的隱私性/隱蔽性/偽裝性的趨勢(XI) －有「緣」千里來相會: 論遺傳基因與視覺安全的血緣,” iThome, Vol. 23, PC home Publication Group, http://service.pchome.com.tw, Oct., 2006.
- **S.J. Wang**, “Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime,” International Journal Computer Standards & Interfaces, Vol. 29, Jan. 2007. (SCI)
- D.Y. Kao, **S.J. Wang**, and F.F.Y. Huang, “Forensic Assessment Model in Profiling P2P Copyright Infringement,” The 3th Asia-Pacific International Conference on Knowledge management (KMAP2006), Hong Kong, Dec. 2006.
- D.Y. Kao, **S.J. Wang**, and F.F.Y. Huang, “An Investigation to Verify the Reliability of Log-related Evidence upon Time-based Models,” The 3th Asia-Pacific International Conference on Knowledge management (KMAP2006), Hong Kong, Dec. 2006.
- **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.
- **S.J. Wang** and D.Y. Kao, "Internet Forensics on the Basis of Evidence Gathering with Peep Attacks," International Journal Computer Standards & Interfaces, accepted in June, 2006. (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**"*

ICCL tough team



- **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)