資通保密與國家安全

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

資通保密與國家安全

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

網路恐怖主義

以資訊和資訊技術為基礎的網路世界,在給人們帶來方便、快捷生活的同時，也為恐怖分子提供了可乘之機，網際網路已成為恐怖分子最具威力的武器之一。

反恐專家警告說，恐怖活動已經蔓延到網際網路上，網路恐怖主義已成為資訊時代恐怖主義手段和方式發展的新領域，成為非傳統安全領域挑戰國家安全的新的全球性問題。如何應對網路恐怖主義，已成為世界各國面臨的一個共同課題。

網路恐怖主義

網路的分散性使調查人員很難追蹤和阻止恐怖分子在網上發佈資訊；網路的隱蔽性又可以使恐怖分子透過不斷更換網域名稱隱蔽身分，而執法單位難以應對。

網路環境的複雜性、多變性，以及資訊系統的脆弱性，決定了網路安全威脅的客觀存在。也正是網路本身的特性及網路安全的脆弱性為恐怖主義提供了更大的活動空間和更隱蔽有效的攻擊手段。

網路恐怖主義

當網路延伸到世界每一角落，網路已成為國家安全「無形的疆域」。這種無形的「資訊領域」安全對一個國家來說，和傳統的領土、領海和領空安全地位同等重要。可以說「資訊領域」的安全，攸關到民族、國家在資訊時代的興亡。當前，網路恐怖主義正成為國家安全、國際政治與國際關係中一個新興問題，要求人們不僅要高度重視「資訊領域」的安全，更應從政治與國家安全的戰略層面予以密切關注。

網路恐怖主義

國際學者推測，在國際政治鬥爭和經濟競爭日趨複雜化、多樣化的背景下，隨著資訊網路技術的不斷發展，未來網路恐怖主義攻擊的可能性會大大增加，其主要目標可能是目前運行最繁忙、資訊最頻繁且最脆弱的全球金融證券交易網路系統，以及關係到國計民生的資訊通訊、電力與交通等網路系統。

911 事件

現實空間的恐怖襲擊正與網路空間的恐怖襲擊更緊密地結合在一起，成為人類社會面臨的新的恐怖威脅。

2001-9-11

英國 泰晤士報

英國泰晤士報 2001/10/06 報導：

美國聯邦調查局官員認為，賓拉丹領導的「開打」恐怖組織全球分部成員很可能是利用**數位加密技術**隱藏其電子郵件內容，並把恐怖行動用的地圖及相關指令藏在運動網路聊天室、色情網站及網路郵寄的照片裡。

《USA Today》

2001年2月5日的《USA Today》有一篇文章，報導外國和美國的官員曾說：「在1998年兩座東非美國大使館的炸彈攻擊事件中，賓拉登和其他人在休閒聊天室、色情佈告欄和其他網站藏入恐怖攻擊目標的地圖和照片，並且下達恐怖活動的指示」。

資訊隱藏技術

情報當局認為開打組織很可能曾利用電子資訊隱藏技術及其分布在全球各地的成員聯絡，色情網站則是最佳的選擇，因為色情網站數量龐大，也是伊斯蘭基本教義派教徒最不可能點選的網站。

Steganography

據信開打組織是利用一種名為Steganography的資訊隱藏技術，把秘密資訊隱藏在其他訊息如數位影像、MP3及一般文字檔案內，如不仔細觀察，這些檔案根本和一般檔案無異，而資訊隱藏技術的相關軟體早就可以輕易在網路上下載或市面上買到。

Secret message inside this letter

Dear George,
Greetings to all at Oxford. Many thanks for your Letter and for the summer examination package. All Entry Forms and Fees Forms should be ready for final dispatch to the syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16 + proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Hint

「your ...」

Got it?

「your package ready Friday ...」

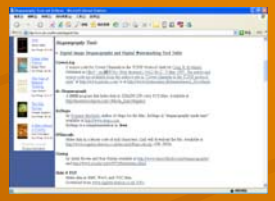
攻擊/防禦的指令

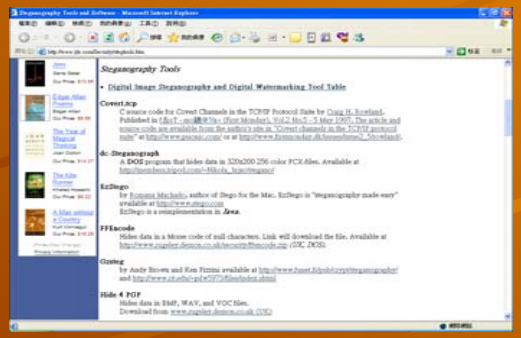
八 月 湖 水 平，涵 虛 混 太 清。
氣 蒸 雲 夢 澤，波 撼 岳 陽 城。
欲 濟 無 舟 楫，端 居 恥 聖 明。
坐 觀 垂 釣 者，徒 有 羨 魚 情。

Hint

將各種情報，例如：請糧料、請添兵、請固守、被賊圍、將士叛、將領病、賊退軍、賊進軍…等40項，隨機用40個字的一首詩來表示，這首詩的文字每個字都只出現過一次，並且把不含重複的40字詩與這些情報內容依序相對應，編上相應的數字代號，從1至40，此一數字與情報相對應的內容即為密碼本。

Steganography軟體下載





資訊隱藏技術

資訊嵌入技術的其中一種方式是「資訊隱藏」(Steganography 或稱為 Information Hiding)，或者翻譯成「隱匿法」，Steganography的緣起最早可追溯到古希臘時代，是由希臘字Steganos轉換而來，它的字面意義是「遮蔽所寫的字」。概括而言，幾千年來人類把訊息隱藏在圖畫、文字或物體之中的手法就稱為資訊隱藏。

資訊隱藏技術

資訊隱藏技術
(Steganography Tech.)

- LSB技術 (Least Significant Bit Tech.)
- 遮罩技術 (Masking Tech.)
- 頻率域轉換技術 (Frequency Transformation Tech.)
- 壓縮法技術 (Compression Manner Tech.)
- 展頻技術 (Spread-spectrumTech.)

資訊隱藏技術

資訊隱藏技術可以想成是一種固若金湯的加密方式。與加密技術不同的，是其隱藏訊息的方式會讓竊聽者不易察覺到有訊息的交換行為存在。簡而言之，資訊隱藏的基本原理是將欲隱藏之資料打散並且藏入數位媒體之中。

密碼學與資訊隱藏之差異

	密碼學	資訊隱藏
原理	打散原有資訊內容	隱藏資訊在數位媒體中
目的	保護資訊	隱藏通訊
注重	加密演算法	隱匿能力

隱藏分析技術

LSB嵌入技術主要的偽裝分析技術可以大致分為兩大主流，分別為：

- 視覺分析法 (Visual Analysis)
- 統計分析法 (Statistical Analysis)

ART and WAR

古往今來的偽裝技術多數運用在與文辭字意與視覺感官中上，創作者利用文字隱藏玄機或者圖像感官變化，讓人得費心思解出答案。然而，偽裝藝術的創作者本身需要具備相當水準的文學造詣或者繪畫天份，才有能力將主題隱藏在背景當中，讓當局者發揮想像/應用的空間。

結論-1

二十一世紀的網際網路世界裡，隱藏技術與偽裝分析兩門重要的技術絕對佔有一席之地。不僅如此，兩者之間的戰爭已經在網際網路上無聲無息的開戰。前者陣營企圖使用數位媒體當掩護，祕密傳送機密訊息；後者陣營則致力於偵測所有可疑的數位媒體，避免隱藏機密訊息的數位媒體成為漏網之魚，值得注意的是彼此技術的消長過程將深切影響著未來多媒體資訊安全的議題。

結論-2

縱使許多資訊隱藏軟體已經發展成熟，使用者在網路上可以輕易的取得以及操作使用，然而在專家學者前仆後繼的實驗測探下，亦能化解隱藏技術背後的玄機。相信在可以預見的日子裡，隱藏技術與偽裝分析雙方的拉鋸戰，將會是網路的科技世界眾所矚目的精采好戲。

Pleasure comes after pressure

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.

- **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)