教師資訊素養

資訊與網路安全

講者: 丁德榮

彰化師範大學 資訊工程系 教授

E-mail: deron@ms45.hinet.net or deron@cc.ncue.edu.tw

TEL: 04-7232105-7047

講者簡歷

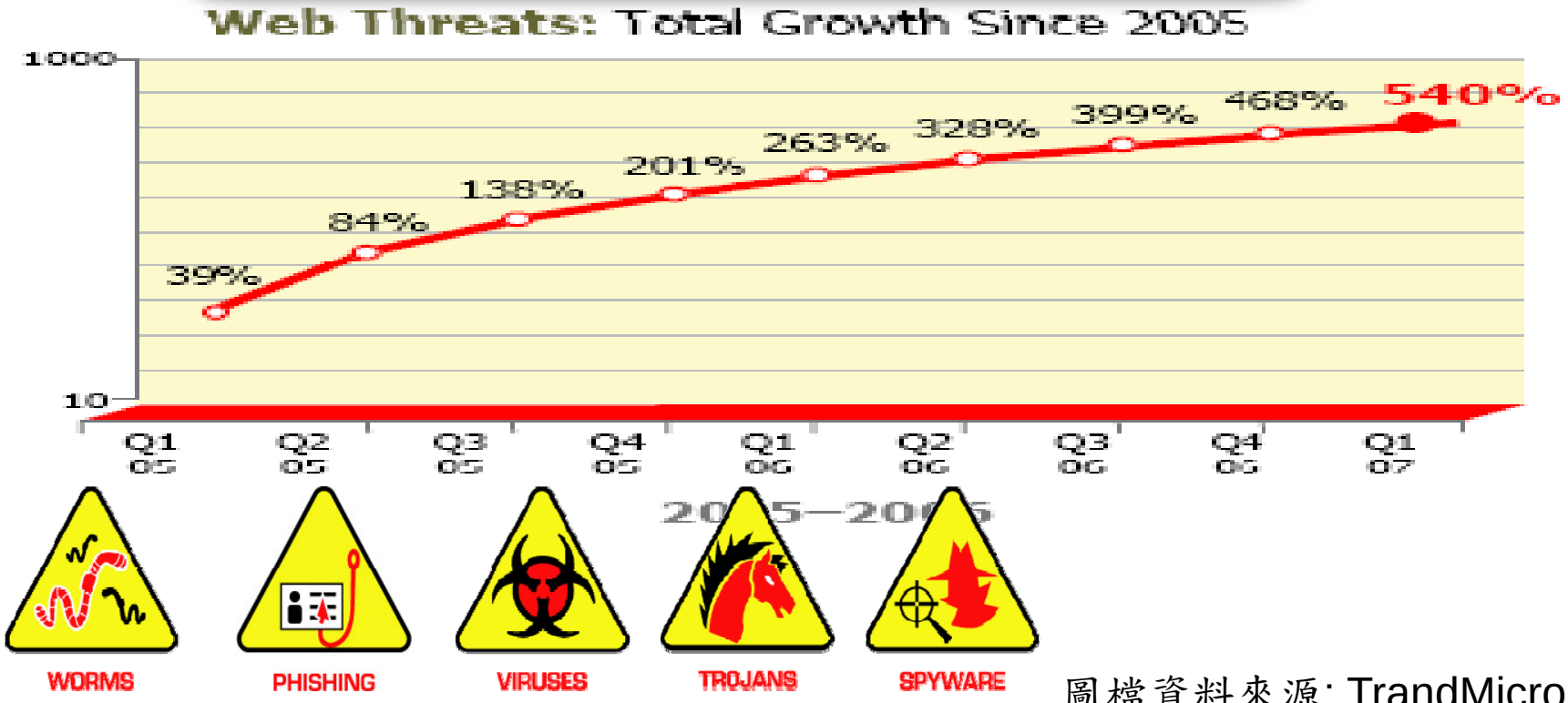
- 新竹師專 74級畢業
- 國小教師 6年(萬里、五常)
- 國中教師 4年(順天、北勢)
- 高職教師 4.5年(新力、嶺東、沙鹿)
- 弘光科大 2年
- 彰化師範大學 資訊工程系 6年
- 現職 彰化師範大學 資訊工程系 教授

專長

- 演算法設計
- 網路規劃研發
- 資訊數學
- 校務行政系統規劃

網路安全的問題?

過去一年內，被植入惡意程式的國內網站達383個，
純粹遭入侵的網站則高達1,483個



圖檔資料來源: TrandMicro

個資外洩事件

- **2006年的個資外洩事件**
  - 包括波音、美國退伍軍人事務部、惠普公司（HP）、McAfee、加州大學，誠品網路書局、東森購物等。
  - PayEasy受「駭」5400會員個資外洩
  - 博客來個資外洩事件
  - 大考中心
  - 網路選課

大綱

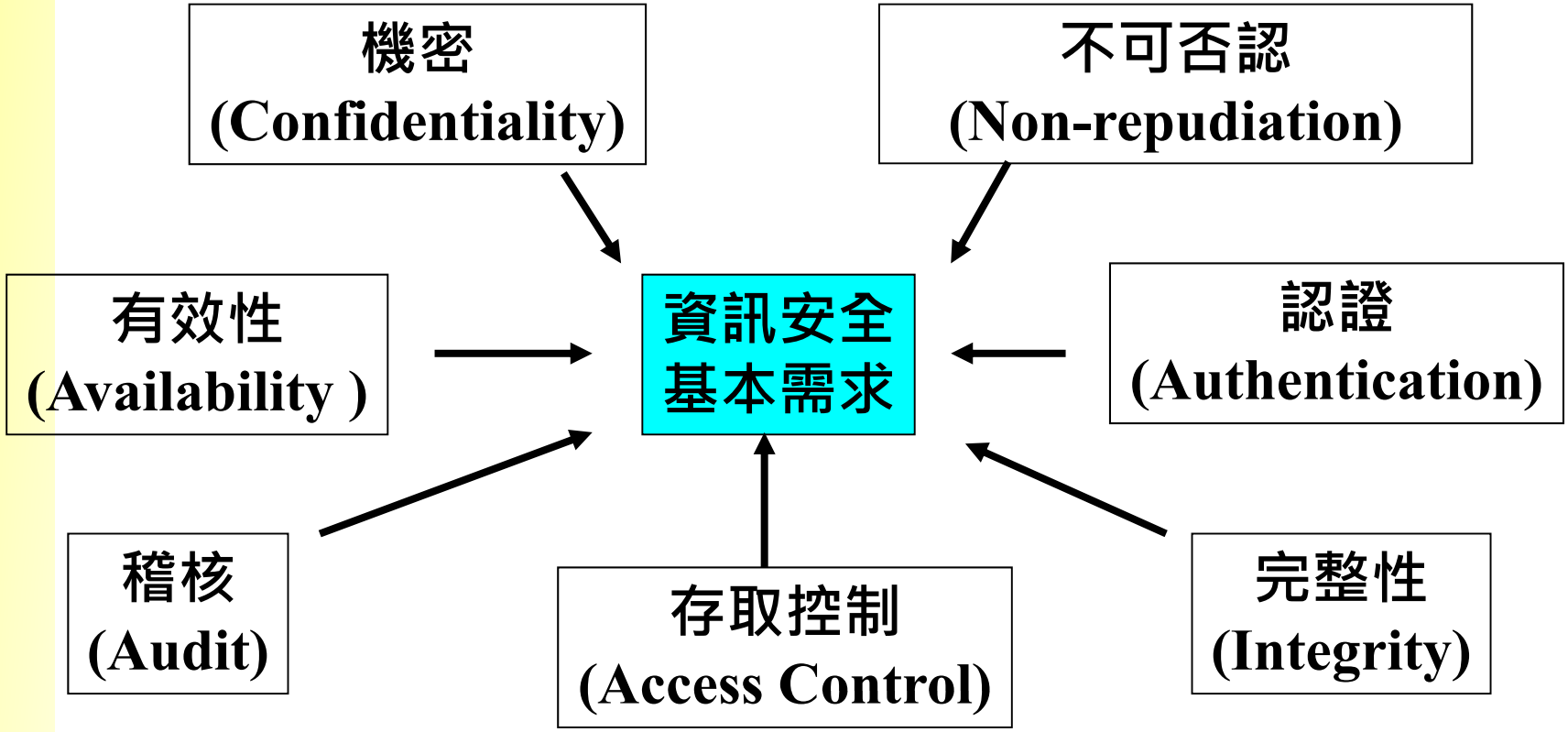
- 資訊安全與網路安全簡介
- 密碼學簡介
- 網路安全應用
- 電腦病毒簡介與防護

資訊安全與網路安全簡介

資訊安全是什麼?

- 資訊安全為:
  - 保護資料安全
  - 保護資料與網路傳送的安全

資訊安全基本需求


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

資訊安全的重點

- **機密性 Confidentiality**
  - 未經授權之人無法存取資料
  - 避免故意或無心而未經授權竊取及洩漏資料內容
- **完整性或真確性 Integrity**
  - 確保資產之正確性與完整性之性質
  - 未經授權之人員或程序無法竄改資料
  - 經授權之人員或程序無法執行未獲授權之修改
  - 資料之內外一致
- **可用性 Availability**
  - 確保有需要時，系統能上線或執行
  - 未經授權之人無法阻撓合法用戶使用系統資源
  - 經授權人員可及時可靠地存取資料或電腦資源

資訊安全的重點

- 不可否認性
  - 來源端不可否認性
  - 接收端不可否認性
- 認證(authentication)與數位簽章(digital signature)
  - 辨別傳送訊息者之身分
- 存取控制
- 稽核

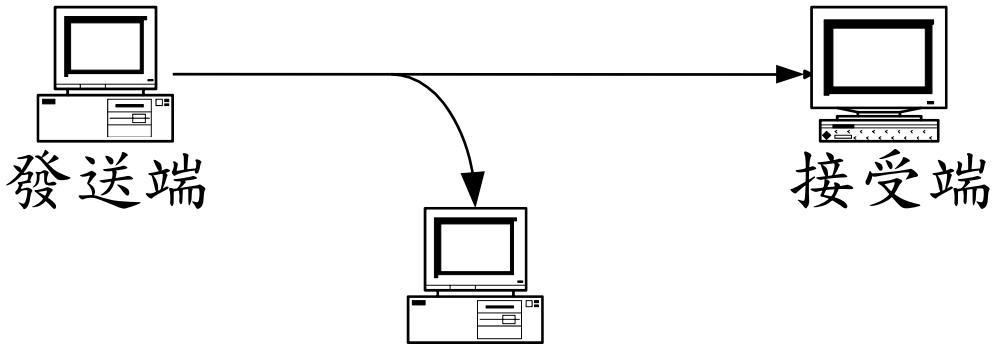
資訊安全的威脅

- 天然或人為
  - 天然災害
  - 管理人員的疏失
- 蓄意或無意
  - 企圖破解系統安全
  - 系統管理不良
- 主動或被動
  - 不會更改電腦系統資料
  - 電腦系統上資料會被篡改

經由網路的攻擊

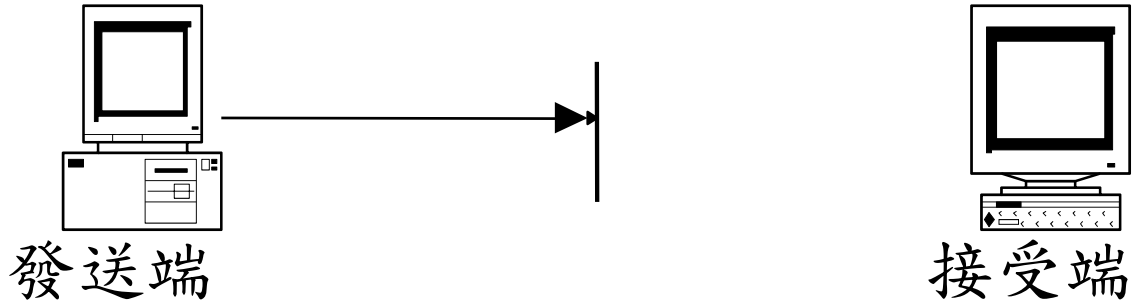
中途竊聽(Interception)

未經授權之團體或個人竊聽不該知道之機密資料。基本上這類威脅不會破壞整個系統，但會將機密資料洩露出去。



經由網路的攻擊

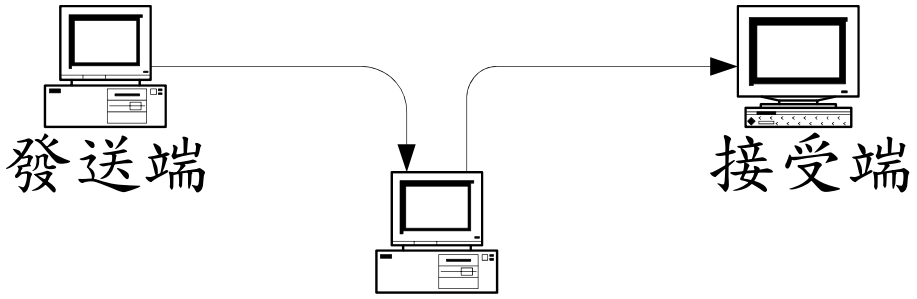
- 中斷、攔截(Interruption)



經由網路的攻擊

竄改(Modification)

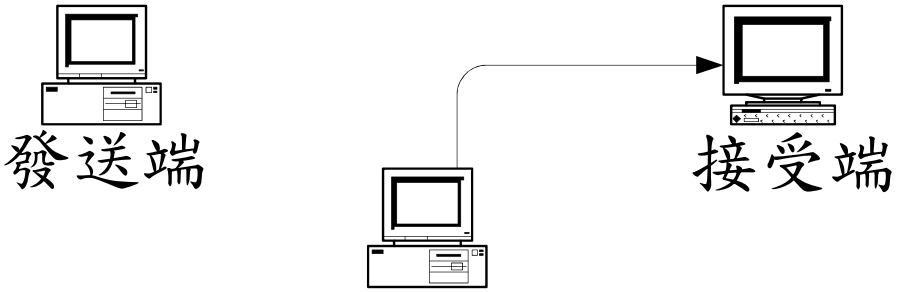
不法之徒未經許可篡改資料。這類威脅有時比洩露機密資料造成更大損失。



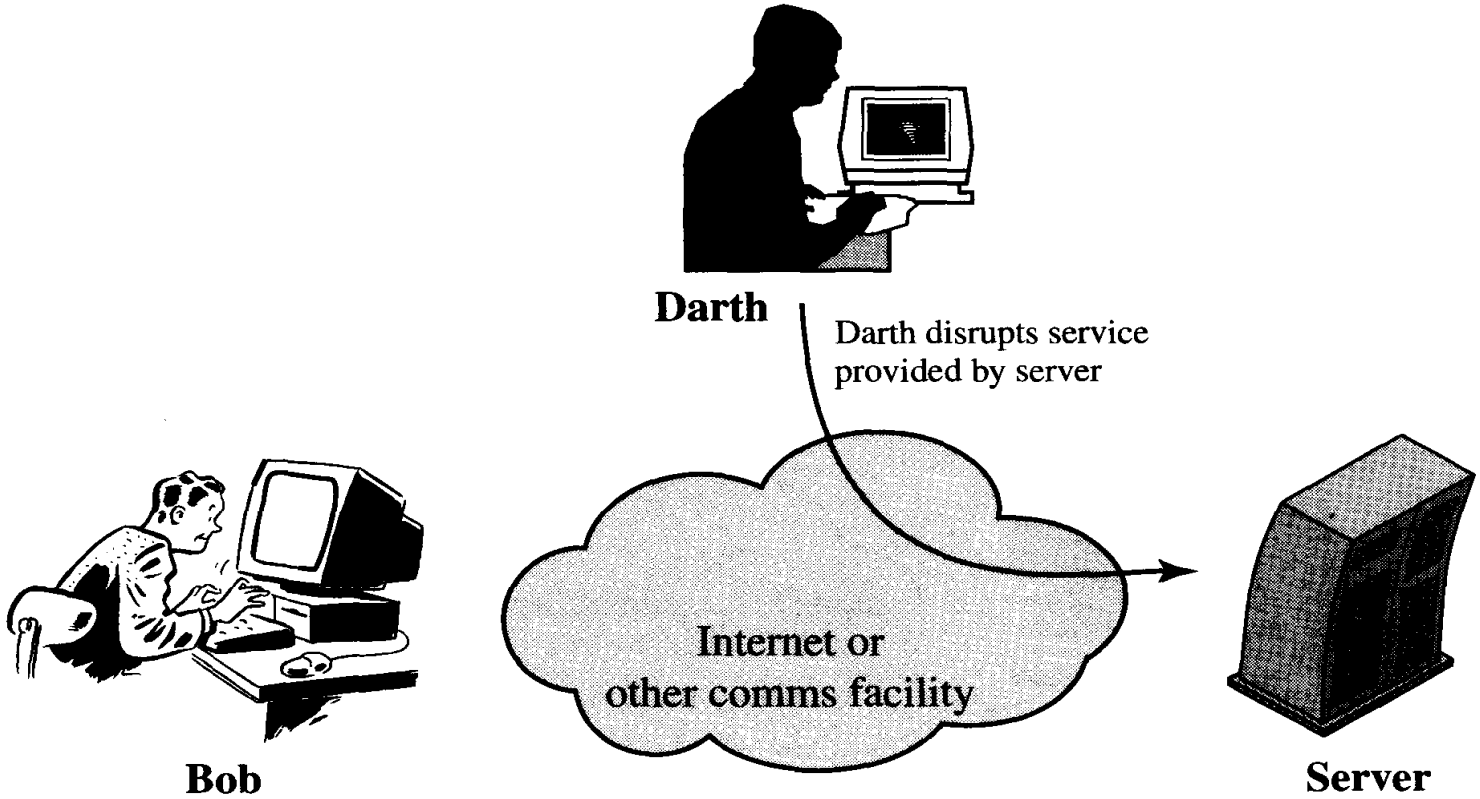
經由網路的攻擊

偽造(Fabrication)

與篡改威脅之不同點在於篡改之資料為已經存在之資料，偽造假資料則是無中生有。



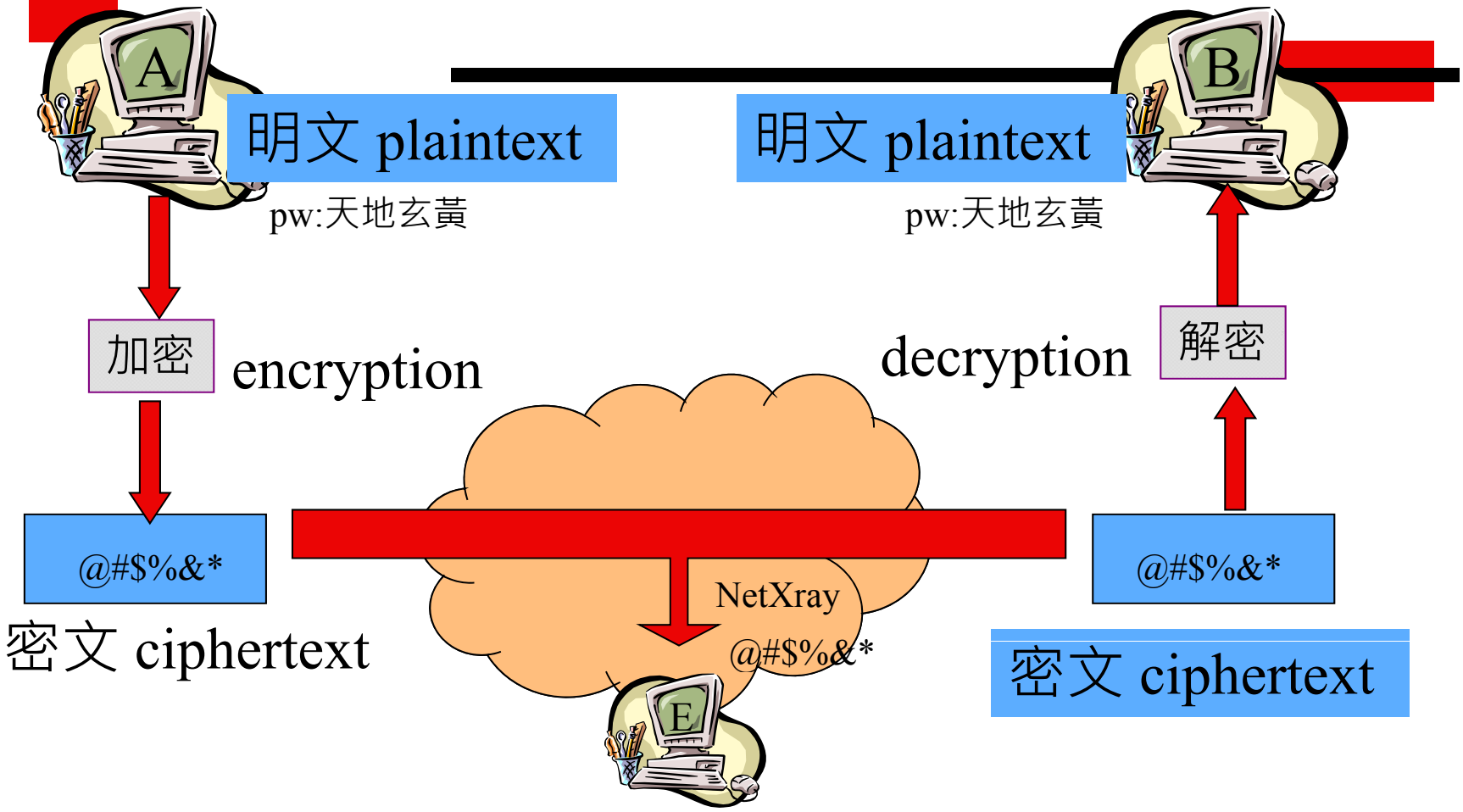
阻斷服務 Denial of Service (DOS)



(d) Denial of service

密碼學簡介

加密系統架構


A
明文 plaintext
pw:天地玄黃
加密
encryption
@#$%&*
密文 ciphertext
NetXray
@#$%&*
E
Eavesdropper (竊聽)
B
明文 plaintext
pw:天地玄黃
解密
decryption
@#$%&*
密文 ciphertext

密碼學的概念

- 加密 (Encryption)
  - 運用技術將要傳遞的訊息隱藏
- 中文範例?
  - 清末大儒紀曉嵐贈送的對聯
    鳳遊禾蔭鳥飛去
    馬走蘆邊草不生
  - 解密(謎)
    - 禾下加鳳去掉鳥字得禿字
      馬置蘆邊去掉草頭得驢字

中國古代密碼學

- **兵符**
  - 是中國古代調兵或傳達命令所用的憑證，用銅、玉、木或石製成。形狀似虎，也稱作**虎符**。兵符製成兩半，一半留給君主，另一半交給下屬，須兩半符合後命令才能生效。
- 驛馬、烽火、狼煙、金、旌、炮、馬、令箭、暗號、
- **素書(密信)**
  - **不成字**:是對文字進行拆解再重新加以排列組合，
  - **無形文**:是指以化學藥劑所書寫的文書，
  - **非紙簡**:是在書寫工具與資訊載體上動手腳。
- 〈六韜．龍韜．陰符〉　〈六韜．龍韜．陰書〉
- 磬書:明磬寫的書。
- 武則天時期　“青鵝”=> 此青字者，十二月。鵝字者，我自與也。”

古代的密文

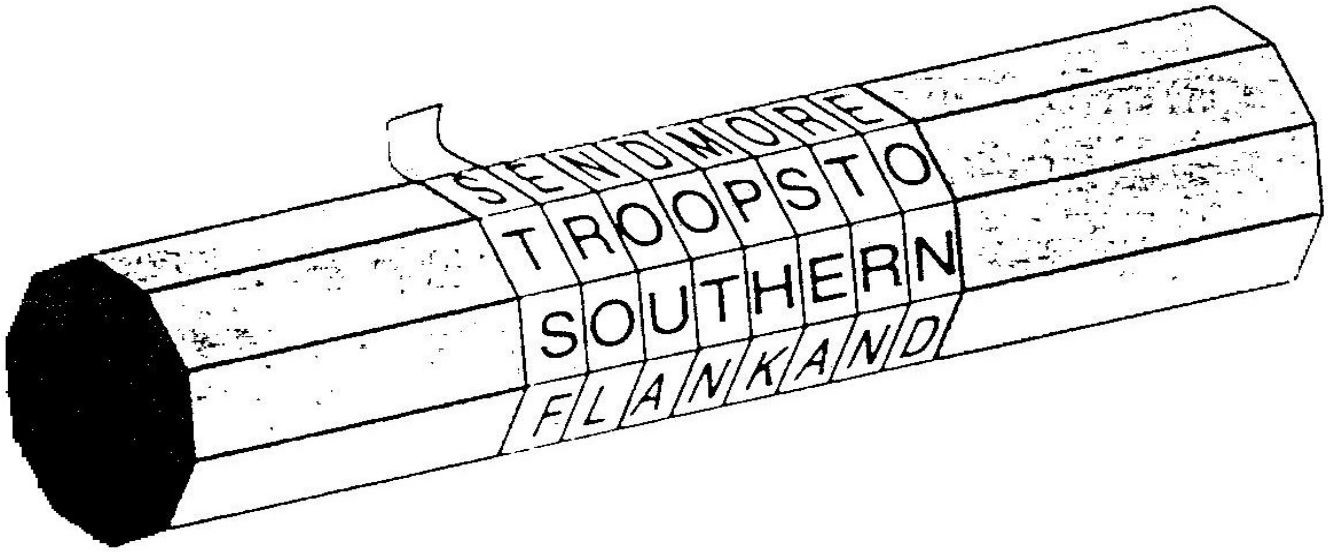


圖　：從發信人的密碼棒解下來時，這皮帶上的字母猶如隨意胡寫的；S、T、S、F……。唯有把這皮帶纏繞在一根直徑正確的密碼棒上，訊息才會重現。

Substitution Ciphers(取代)

原始文字與加密文字對照表

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

- 那麼**apple**這個字就會變成bqqmf了
- I love you 變成　j mpwf zpv
- 加密時向右移一位, 解密時向左移一位
- 加解密的 金鑰 (Key) 相同

凱薩密碼 Caesar Cipher

- 記載於羅馬凱撒大帝所著《高盧戰記》Gallic Wars中及蘇東尼烏斯寫於西元二世紀的《十二帝王傳》Lives of Caesars

0	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
										0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

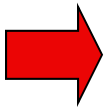
範例 I LOVE YOU => L ORYH BRX
Key =3

傳統密碼學

- 傳統密碼學的基本原理
  - 取代加密法 (Substitution Cipher)
  - 換位加密法 (Transposition Cipher)
- 換位加密法
  - 加密：利用一個特定排列規則，將明文中的字元重新排列過，來產生另一個無規律的密文。
  - 解密：使用同樣的規則，將密文倒回原來明文。

換位加密(Transposition Cipher)

一個人。這數字是公百六十六。都能夠出獸的數字，因為這數字代表能買賣。這裡需要有智慧。凡是聰明人代表名字的數字．沒有這印記的，就不額上打印記。這印記就是那獸的名字或富貴，奴隸或自由人，在他們的右手和這獸又強迫所有的人，無論大小，貧窮



這富額代能都一獸貴上表買能個又，
打名賣夠人強奴印字。算。迫隸記的
這出這所或。數裡獸數有自這字需的
字的由印；要數是人人記沒有字六，，
就有智，百無在是這慧因六論他那印。
為十
大們獸記凡這六小的的的是數。，右
右，聰字貧手字就明代窮和或不人表

Columnar Transposition Cipher

Plaintext: COMPUTER GRAPHICS MAY BE SLOW BUT AT LEAST IT'S EXPENSIVE.

```
COMPUTERGR
APHICSMAYB
ESLOWBUTAT
LEASTITSEX
PENSIVE
```

Ciphertext: CAELP OPSEE MHLAN PIOSS UCWTI TSBIV EMUTE RATSG YAERB TX

換位加密法

- **鑰匙排列法 (key =3412567)**
  - 明文：I SIT BY MY WINDOW WAITING FOR YOU
  - 鑰匙排列：
  - 密文：IIIRTNTYSWAOIYWFBDIOYONUMWGE

鑰匙：	3	4	1	2	5	6	7
明文：	I	S	I	T	B	Y	M
	Y	W	I	N	D	O	W
	W	A	I	T	I	N	G
	F	O	R	Y	O	U	E

Permutation Ciphers

- Example:

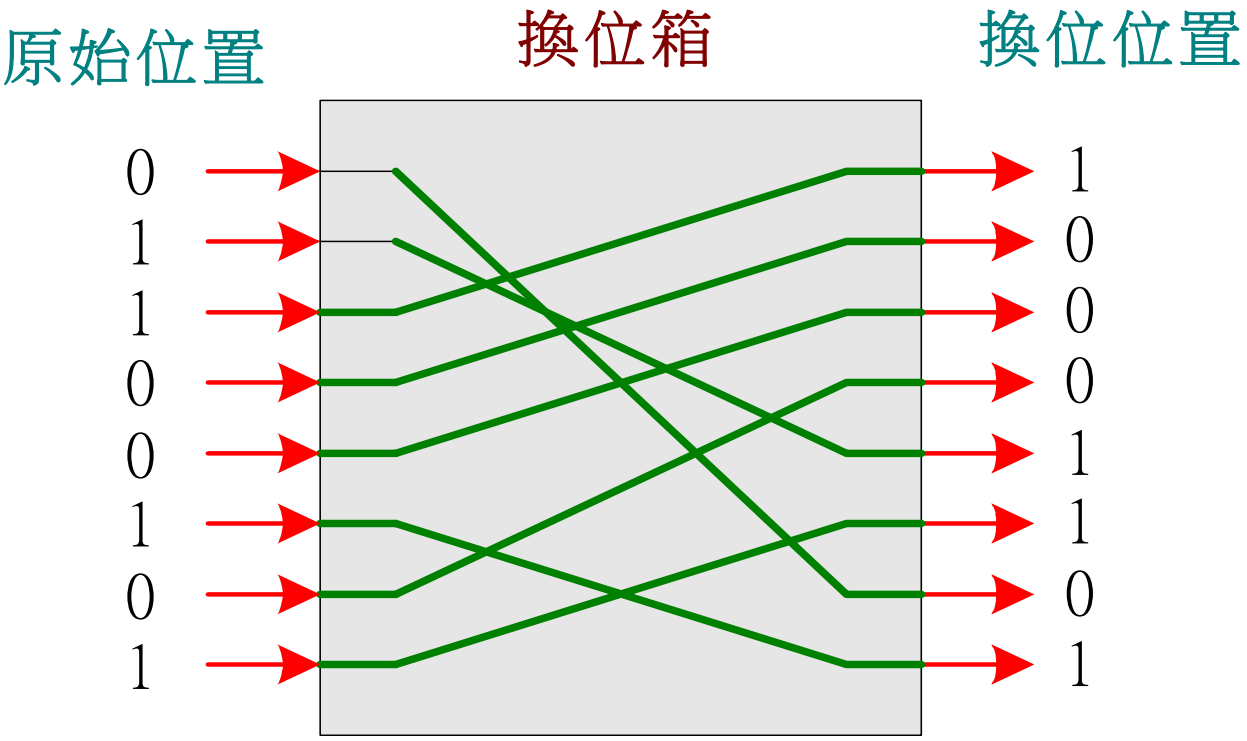
好 孩 子 密 碼 學

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 1 & 4 & 5 \end{pmatrix}$$

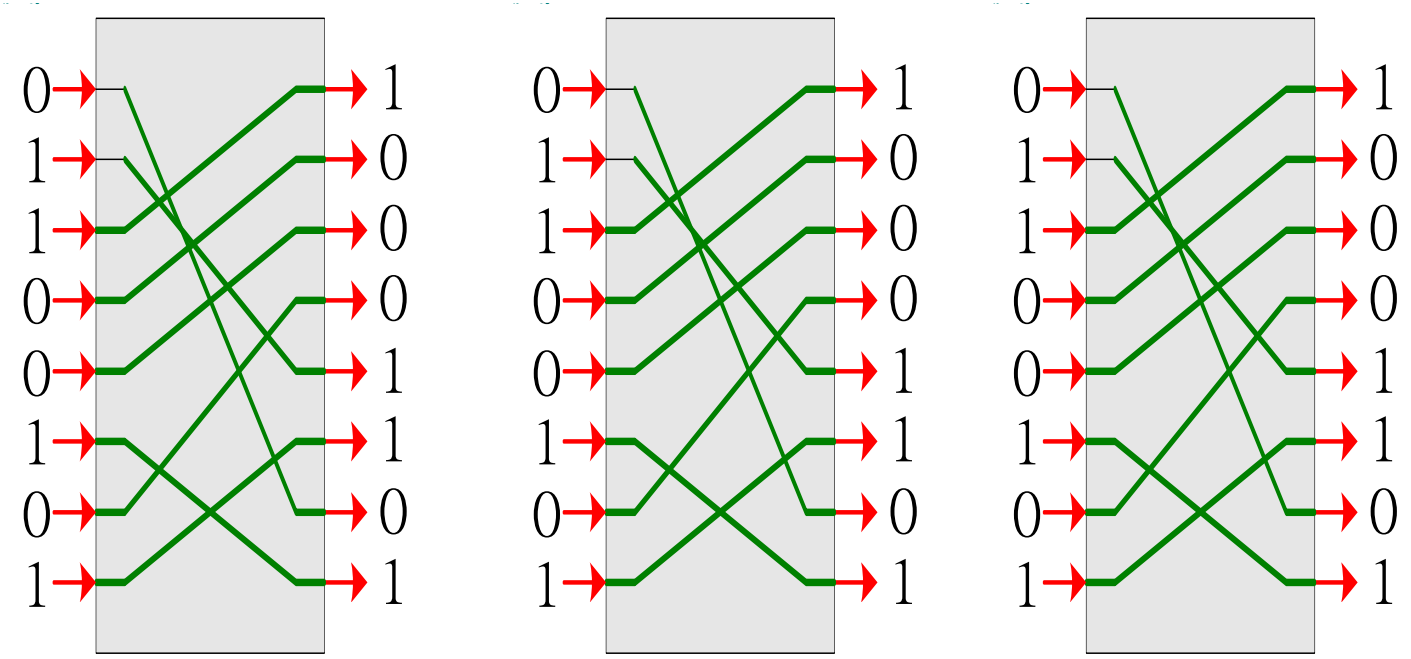
孩 子 學 好 密 碼

換位加密法

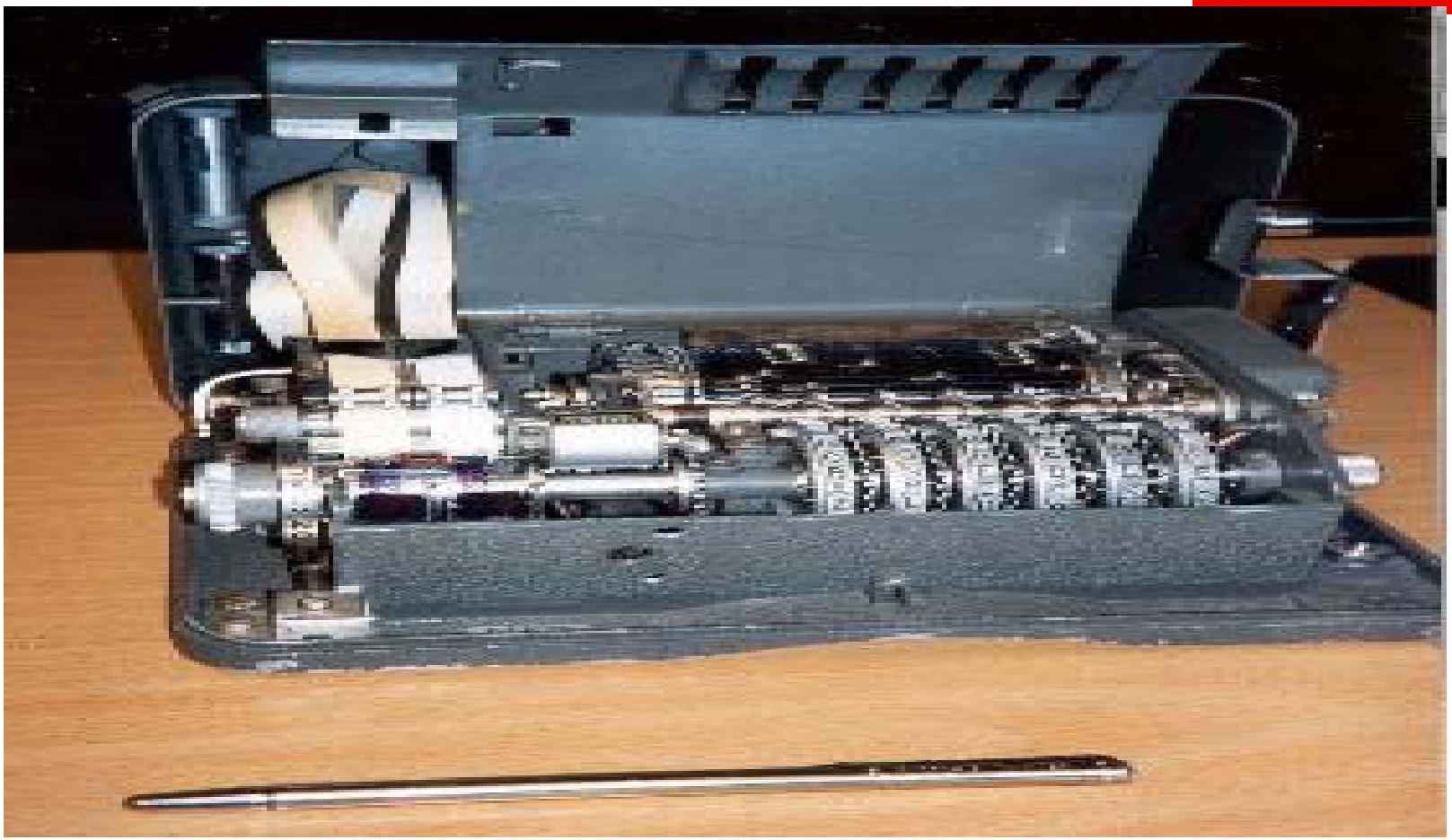
- 位元變換箱



多重變換箱



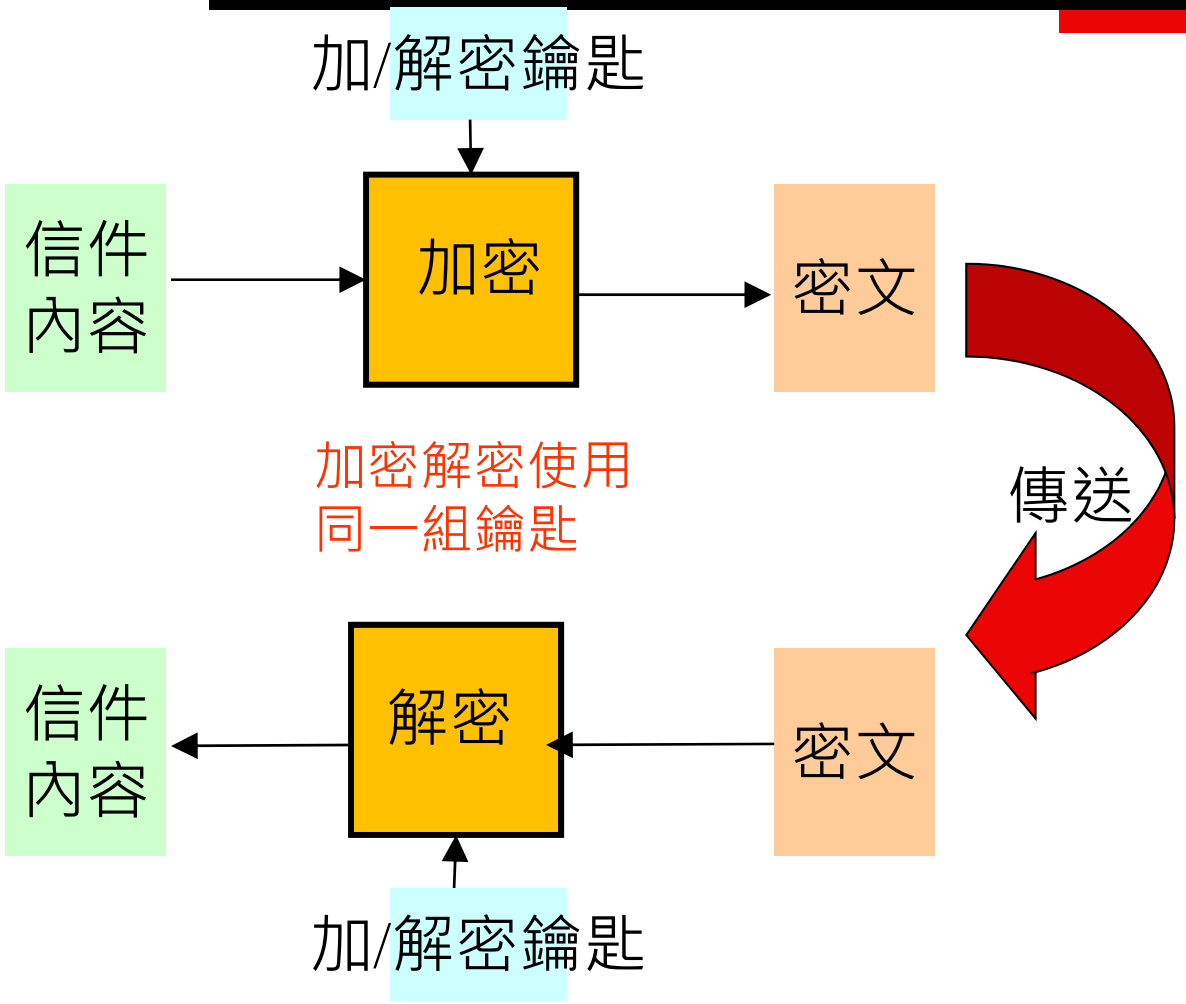
Rotor Machine



Cipher Machine

The German Lorenz cipher machine, used in World War II for encryption of very high-level general staff messages

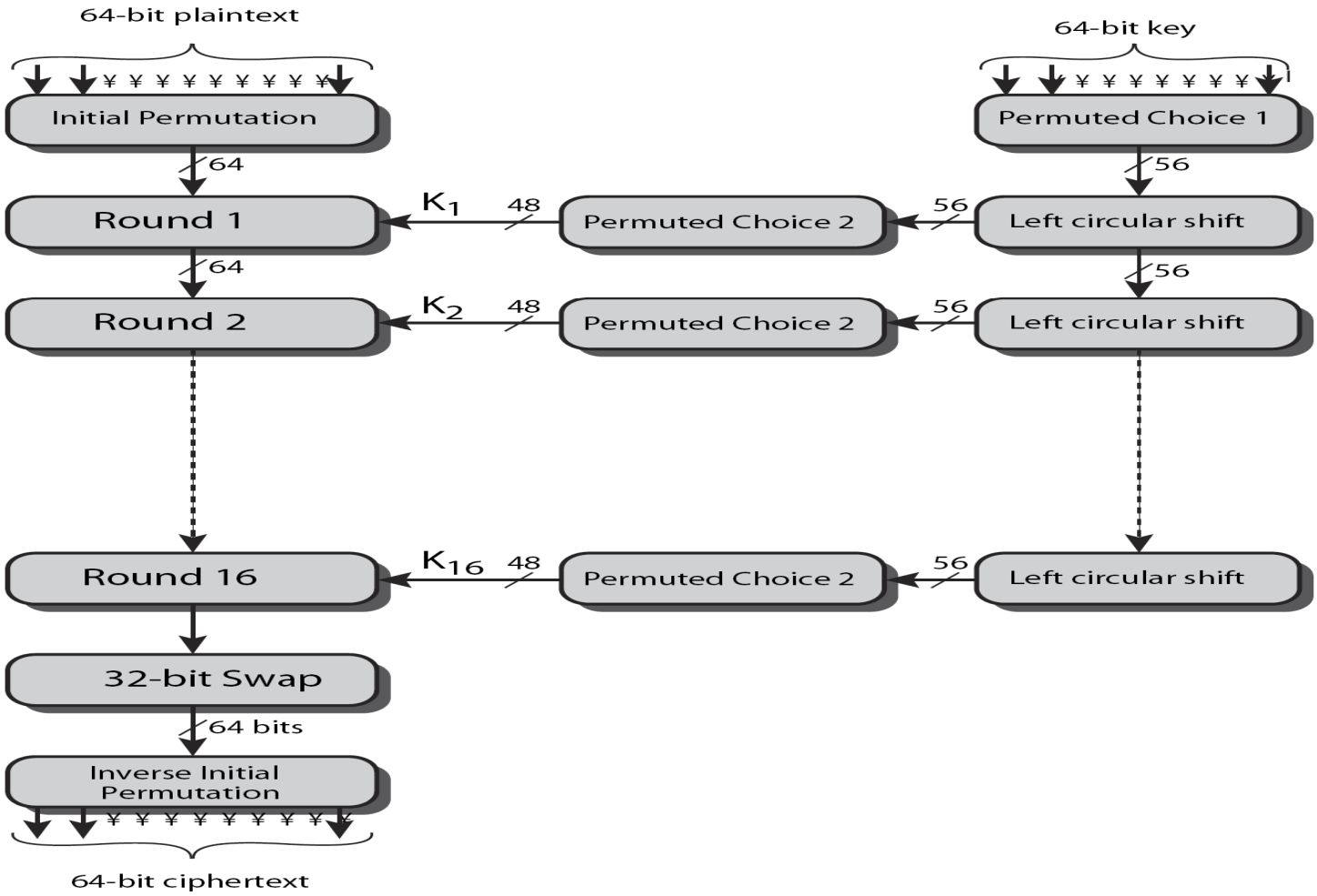
傳統加解密的系統



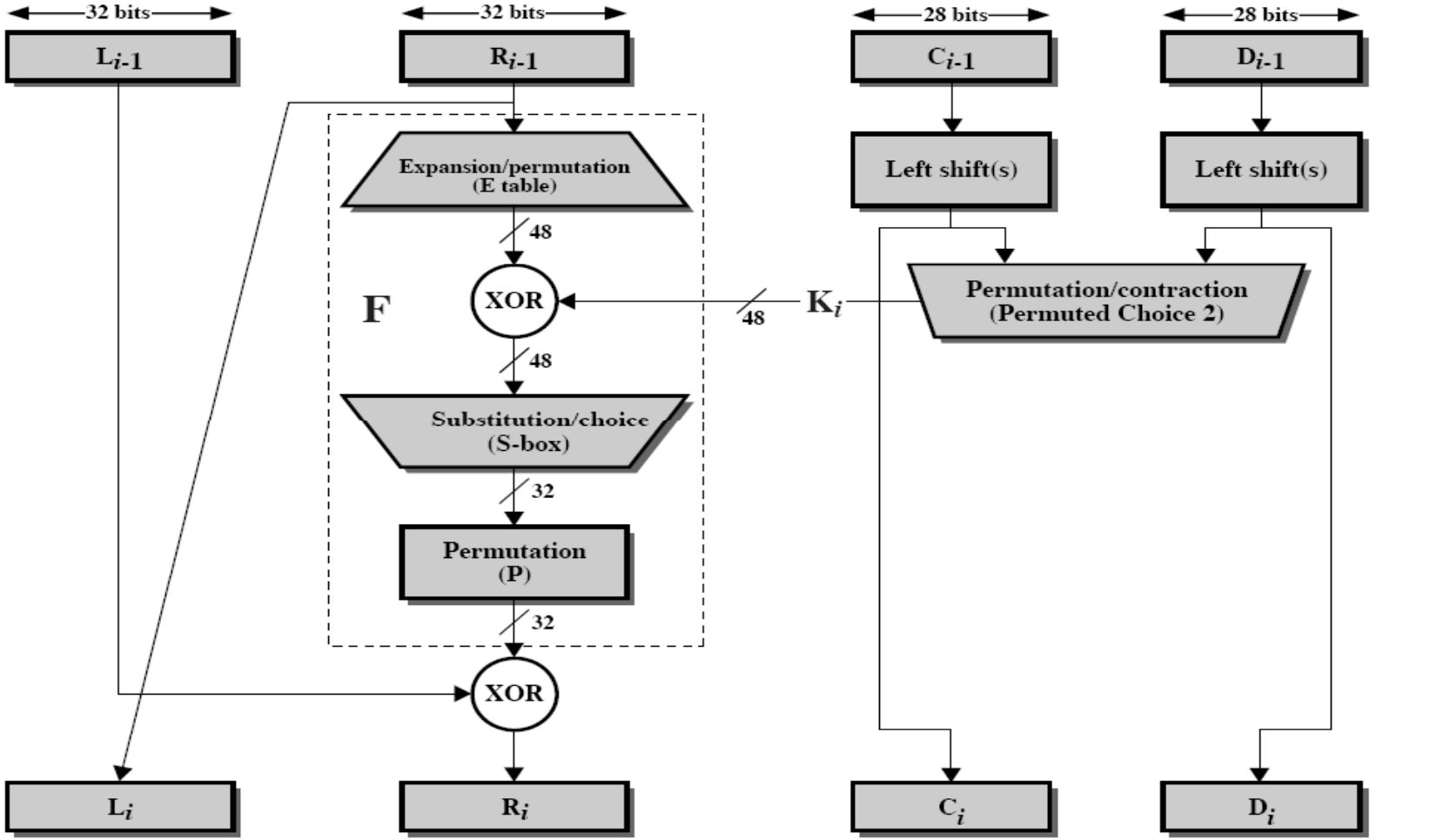
重要的加解密系統

- 資料加密標準 **Data Encryption Standard** (DES), 56 bits key, 1973
- **3-DES**, 112, 168 bits key
- 進階加密標準 **Advanced Encryption Standard** (AES), 2001, 192 bits key
- 公開金鑰加密**RSA**, 1978, MIT, 很大的質數 2^{200}~2^{1024}

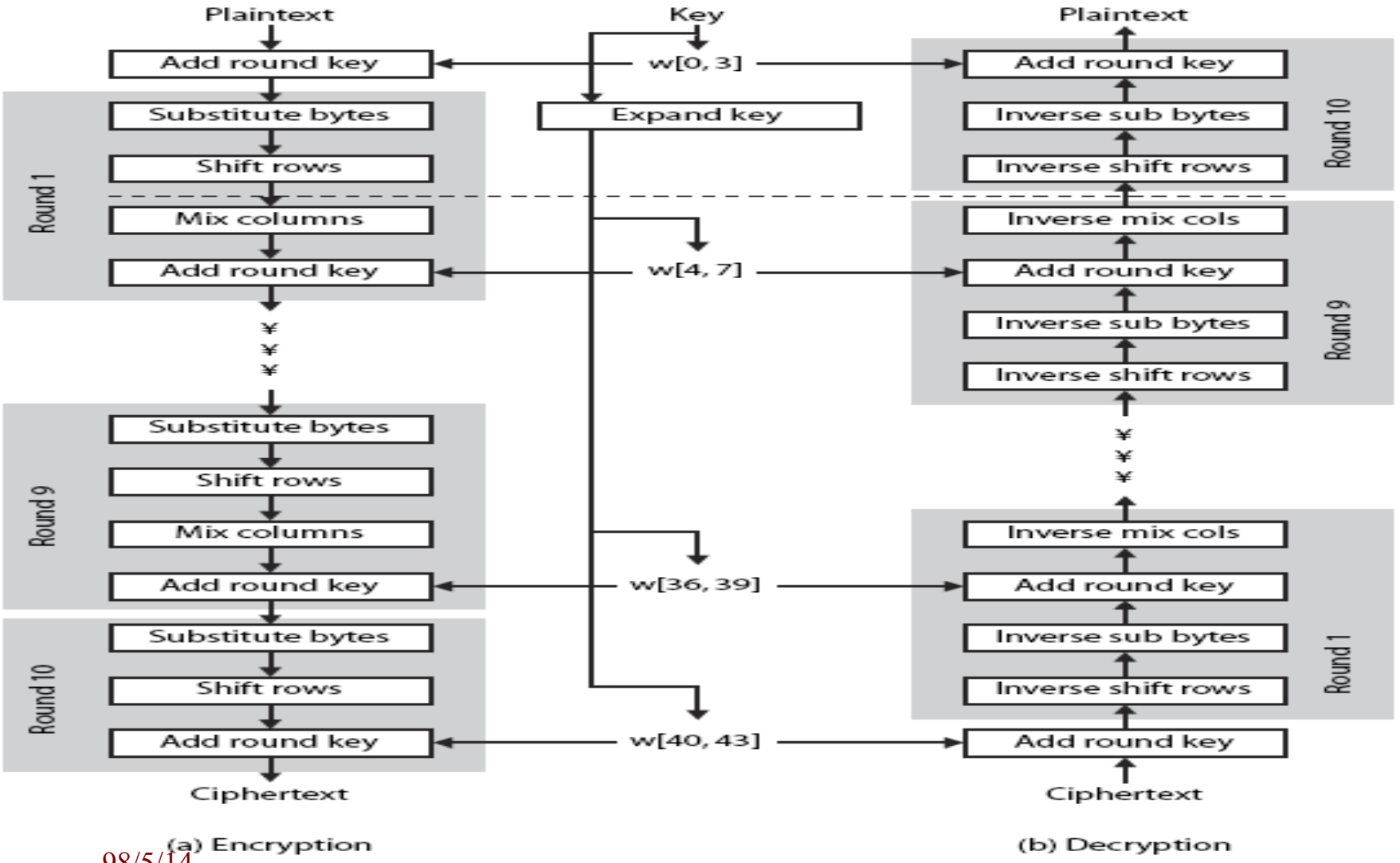
DES Overview



A RUN of DES


32 bits
32 bits
28 bits
28 bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Expansion/permutation (E table)
Left shift(s)
Left shift(s)
48
F
XOR
48
K_i
Permutation/contraction (Permuted Choice 2)
48
Substitution/choice (S-box)
32
Permutation (P)
32
XOR
L_i
R_i
C_i
D_i

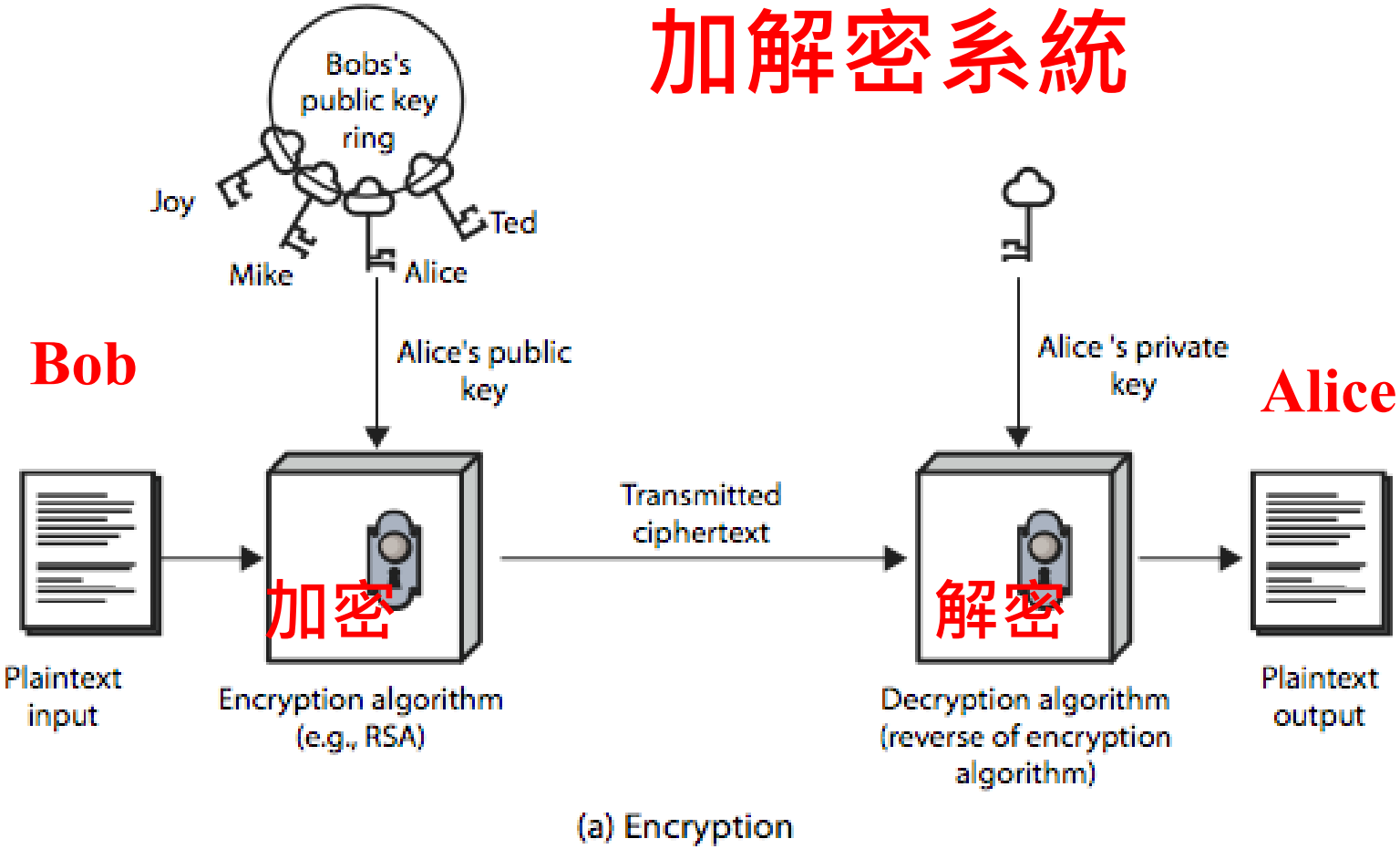
AES Encryption &Decryption



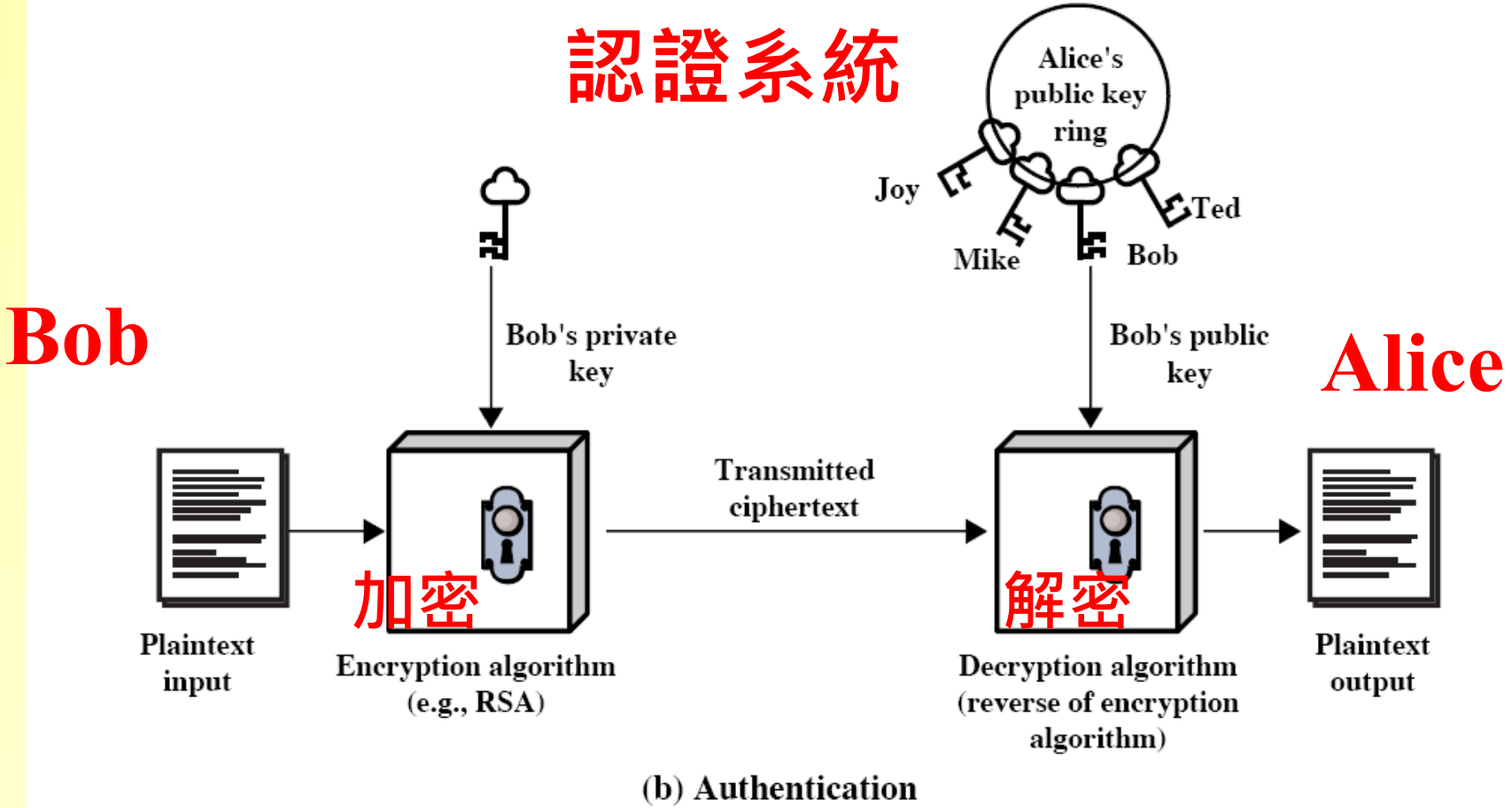
RSA Example - Key Setup

1. 選擇質數: p=17 & q=11
2. 計算 n = pq =17 x 11=187
3. 計算$\phi(n)=(p-1)(q-1)=16 \times 10=160$
4. 選擇e: gcd(e,160)=1;選擇e=7
5. 決定 d: $de=1 \bmod 160$ and $d < 160$ Value of d =23 since 23x7=161= 10x160+1
6. 公開金鑰(public key) PU={7,187}
7. 私鑰 (private key) PR={23,187}
8. 加密 a=2, $a^e \bmod n=2^7 \bmod 187=128$
9. 解密 c=128, $c^d \bmod n=128^{23} \bmod 187=2$

公開金鑰(public key) 系統



公開金鑰(public key) 系統



(b) Authentication

安全性的假設

- 攻擊者可以利用各種方法收集明文與密文的關係
- 攻擊者可能知道加密的方法
- 所有加密解密的方法都須經過許多密碼學的許多專家的分析與攻擊，確保安全性
- 所有的安全性完全由金鑰的長度來決定，亦即，攻擊者需要花費多少時間或成本來破解金鑰。
  - 破解成本大於破解後所獲的利益
  - 破解的時間超過所需要保密的時間

key長度與破解難度之關係

Key Size (bits)	Key 的可能種類	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs= 6.4×10^{12} years	6.4×10^6 years

數位簽章(digital signature)與認證 (authentication)

- 運用非對稱式加密法技術(如RSA)
- 數位簽章
  - 產生以私密鑰匙加密的數位簽章
  - 由於私密鑰匙並不公開, 因此加密簽章無法由其他人仿冒。收到加密數位簽章的人, 利用原簽章主人發送的公開鑰匙解密, 驗證簽章內容。
- 認證
  - 確認所收到的資料未被變動。

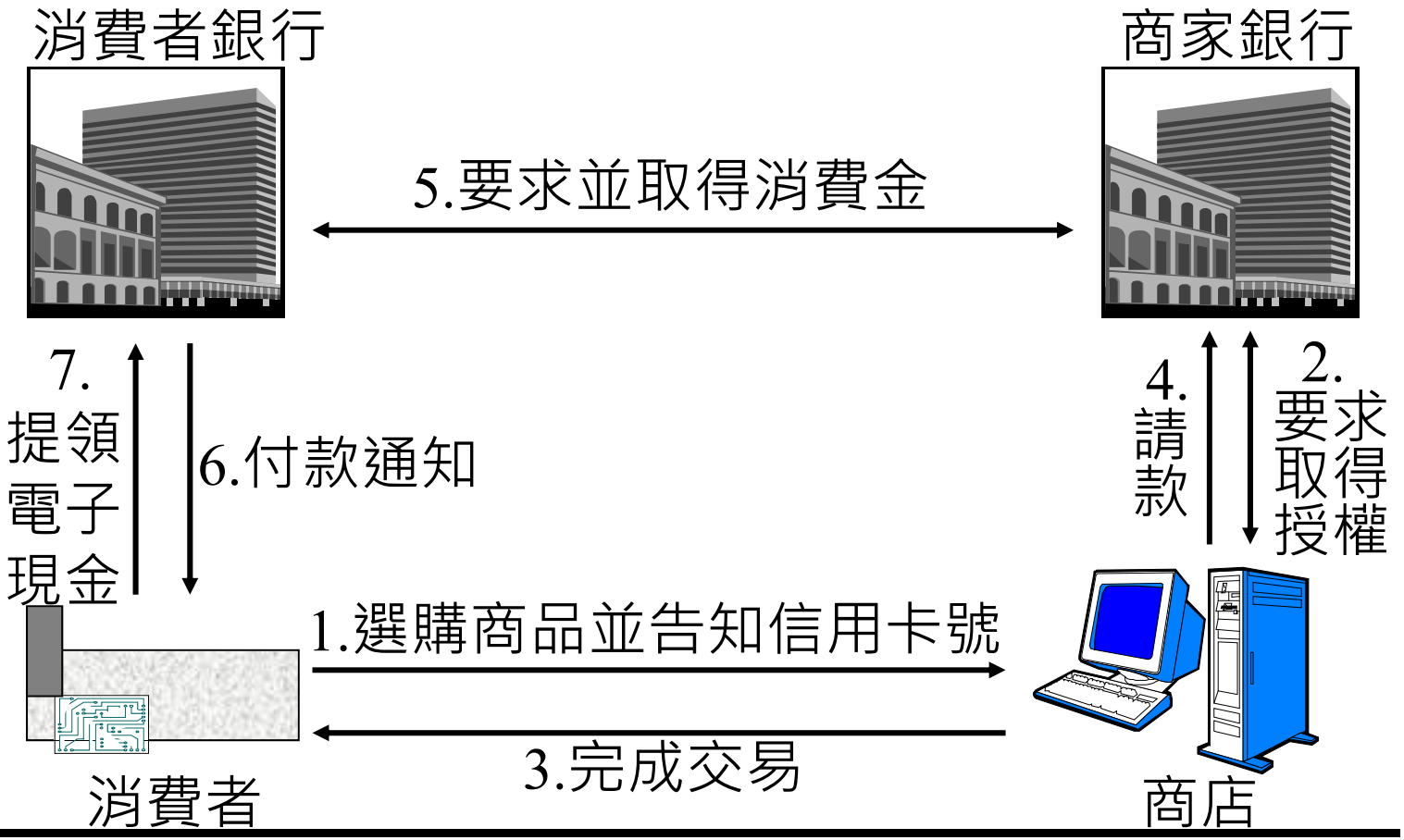
網路安全應用

網路安全的應用

- 電子信用卡交易 (SET 機制)
- 網路安全傳輸協定 (SSL 機制)
- 線上刷卡的安全驗證
- 網路金融卡
- 自然人憑證

電子信用卡交易

電子信用卡交易系統


消費者銀行
商家銀行
5.要求並取得消費金
7.
提領
電子
現金
6.付款通知
4.
請
款
2.
要求
取得
授權
1.選購商品並告知信用卡號
3.完成交易
消費者
商店

安全的電子交易(SET)的介紹

- SET全名**Secure Electronic Transcation**
- 用來保護消費者在開放網路(如Internet)持卡付款交易安全的標準
- 1996年由VISA、MasterCard、IBM、Microsoft、Netscape、GTE、VeriSign、SAIC、Terisa等公司聯合制訂
- 運用**RSA**資料安全的公開鑰匙加密技術
- SET的架構是由幾個元件所共同組合起來的。分別是電子錢包（Electronic Wallet），電子證書 (Digital Certificate)，付款轉接站（Payment Gateway），和 認證中心（Certification Authority）。而運用這四個元件，即可構成於Internet 上符合SET標準的信用卡授權交易。

SET的目的

- 確保輸入資料的私密性
- 確認訂單及付款資料在傳輸過程中的完整性
- 確認商店及持卡人雙方的身份的正確性(即認證)
- 確認銀行和商店的系統都可以處理線上交易的訊息(共同操作)

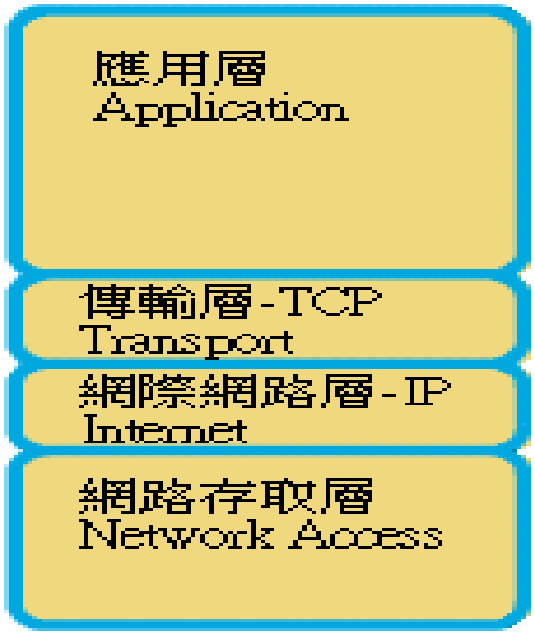
網路安全傳輸機制

網路安全傳輸機制

- SSL(Secure Sockets Layer)
- 此一網路資料安全協定是由Netscape首先發表。
- SSL利用公開金鑰的加密技術(RSA)來做為用戶端與主機端在傳送機密資料時的加密通訊協定。
- 已被大部份的Web Server及Browser廣泛使用。

SSL架構

在網際網路所使用的TCP/IP協定的應用層與傳輸層中間增加一SSL層，可以與原有網路設備及軟體相容又達到資料安全的目的。



TCP/IP

TCP/IP + SSL

如何辨識SSL

1. 通訊協定是採用https://而非http://

2.出現上鎖的金鎖頭，表示支援SSL安全協定，按此可以開啟安全性報表並檢核憑證資訊

NCUE webmail SSL

網路信用卡認證

網路信用卡使用的問題

- 不肖廠商或程式設計師惡意記錄使用者卡號，安全號，姓名與個人資料偽造刷卡。
- 不肖程式人員架設釣魚網站竊取個資。
- 旅遊仲介人員離職前偽造業績盜刷。
- **半數使用Wi-Fi無線網路的零售店家沒有採取足夠的防護措施，使信用卡帳號等機密資料，可透過無線網路訊號輕易竊得。（美國 彭博資訊）**

什麼是〔Visa驗證〕與〔MasterCard驗證〕？

- 為兩種線上刷卡的安全付款機制。
- 商家結帳頁面看到的圖示，而且當您使用VISA或MasterCard信用卡時，將會和VISA/MasterCard組織以及您的發卡銀行連線。

3D驗證密碼服務

- 以持卡人事先所設定的密碼來保護信用卡網路交易
- 只要持卡人完成註冊並設定好密碼之後，當每次至提供驗證服務的網路商店進行交易時，系統即會自動要求輸入密碼，並拒絕密碼錯誤的交易
- 降低卡片在網路上被偽冒的風險。

台灣目前提供「3D 認證」服務發卡銀行如下：

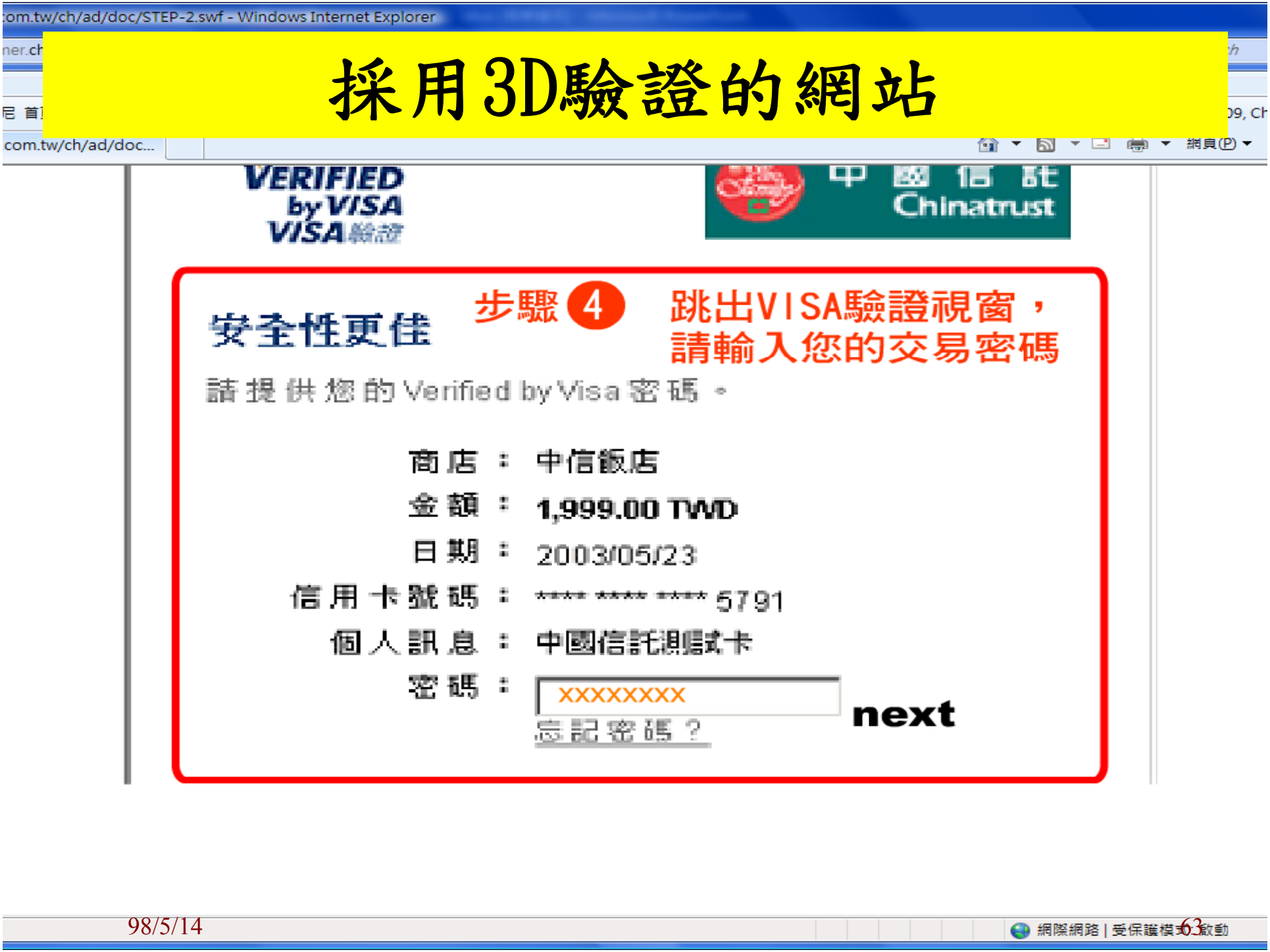
- 中國信託商業銀行、台新國際商業銀行、
- 台灣中小企業銀行、土地銀行、
- 日盛銀行、合作金庫銀行、
- 永豐(安信)信用卡公司、
- 第一銀行、國泰世華銀行、
- 新光銀行、彰化銀行 、聯邦銀行。

未採用3D驗證的網站

步驟 3
進入結帳櫃台填寫個人資料
和已註冊VISA驗證服務的中國信託信用卡卡號
卡號
填寫信用卡資料
使用「公務人員-國民旅遊卡」請打勾
*卡別：
VISA
*信用卡號：
4563191234567890
※請只輸入數字部份，勿包含 - , / 或空白
*到期日：
01
月
04
年
確認送出資料
完成
網際網路 | 受保護模式: 啟動
100%

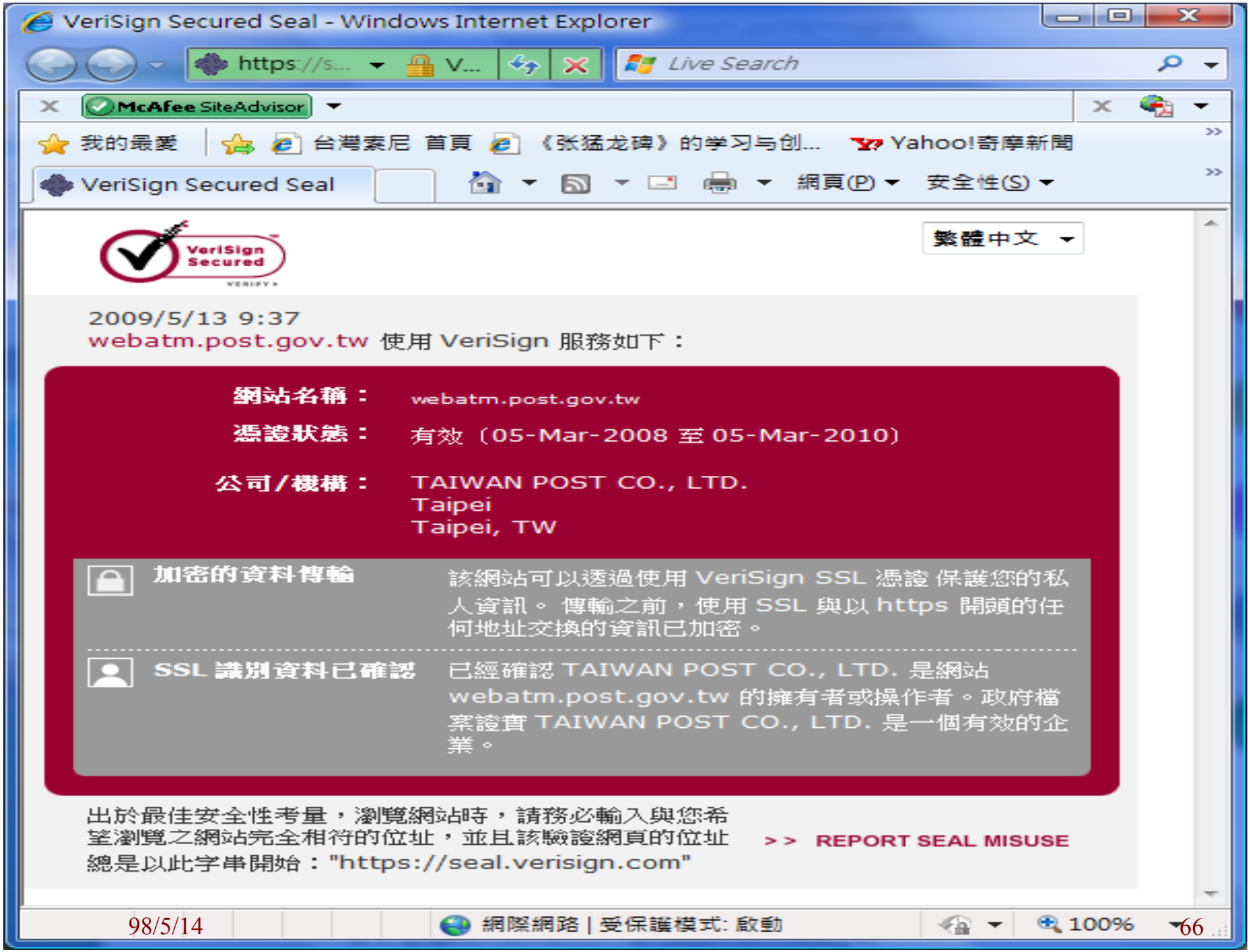
Enter Card Information - Windows Internet Explorer
https://acs.taishinbank.com.tw/ACS_CH/enrollments
Live Search
信用卡註冊
台新銀行
台新銀行 | 財富管理銀行 | 個人金融 | 中小企業金融
台新銀行信用卡網路交易驗證服務ACS
我要註冊 | 我要變更註冊資料 | 我忘記了密碼
MasterCard SecureCode
■請遵照畫面指示及說明登入您的資料，以便確認您的身分，有“*”的注記表示必須輸入。
請輸入您信用卡之英文姓名:
*(空隔請輸入空白鍵,如:KUO CHIH FENG)
請輸入您信用卡之卡號:
*
請輸入您信用卡之有效時間(月/年):
* (如0803表示2003年8月)
身分證號碼:
*
出生日期:
* (如1975/01/10)
檢核碼(CVV2):
* (請您參照信用卡背面之簽名欄位上之數字後3碼)
電子郵件:
*
送出
重填
完成
網際網路 | 受保護模式: 啟動
100%

採用3D驗證的網站


com.tw/ch/ad/doc/STEP-2.swf - Windows Internet Explorer
com.tw/ch/ad/doc...
網頁(P)
VERIFIED by VISA
VISA驗證
中國信託
Chinatrust
安全性更佳
步驟 4
跳出VISA驗證視窗，
請輸入您的交易密碼
請提供您的Verified by Visa密碼。
商店：中信飯店
金額：1,999.00 TWD
日期：2003/05/23
信用卡號碼：**** **** **** 5791
個人訊息：中國信託測試卡
密碼：
XXXXXXXX
忘記密碼？
next

網路金融卡

網路金融卡 –郵局網路ATM


VeriSign Secured Seal - Windows Internet Explorer
https://s...
V...
Live Search
McAfee SiteAdvisor
我的最愛
台灣索尼 首頁
《张猛龙碑》的学习与创...
Yahoo!奇摩新聞
VeriSign Secured Seal
網頁(P)
安全性(S)
VeriSign Secured
繁體中文
2009/5/13 9:37
webatm.post.gov.tw 使用 VeriSign 服務如下：
網站名稱：
webatm.post.gov.tw
憑證狀態：
有效（05-Mar-2008 至 05-Mar-2010）
公司/機構：
TAIWAN POST CO., LTD.
Taipei
Taipei, TW
加密的資料傳輸
該網站可以透過使用 VeriSign SSL 憑證 保護您的私人資訊。 傳輸之前，使用 SSL 與以 https 開頭的任何地址交換的資訊已加密。
SSL 識別資料已確認
已經確認 TAIWAN POST CO., LTD. 是網站 webatm.post.gov.tw 的擁有者或操作者。政府檔案證實 TAIWAN POST CO., LTD. 是一個有效的企業。
出於最佳安全性考量，瀏覽網站時，請務必輸入與您希望瀏覽之網站完全相符的位址，並且該驗證網頁的位址總是以此字串開始："https://seal.verisign.com"
>> REPORT SEAL MISUSE
網際網路 | 受保護模式: 啟動
100%

郵局ATM 妨駭功能

- **動態鍵盤**
  - 避免鍵盤側錄程式竊取密碼
- **圖形密碼**
  - 避免程式惡意入侵與攻擊網站
- **抽拔卡機制**
  - 確認轉帳繳費者確實擁有金融卡

郵局ATM 主畫面

中華郵政WebATM - Microsoft Internet Explorer
中華郵政股份有限公司
Chunghwa Post Co., Ltd.
WebATM
網際網路自動櫃員機系統
餘額查詢
BALANCE INQUIRY
交易明細查詢
TRANSACTION INQUIRY
轉帳交易
INTER BANK TRANSFER
密碼變更
CHANGE PASSWORD
繳費
BILL PAYMENT
保險單借款
INSURANCE-POLICY LOAN
繳稅
TAX PAYMENT
保險單還款
INSURANCE-POLICY LOAN REPAYMENT
登出
Logout
我們的服務
Our Services
網站連結
Websites Binding
服務信箱
Serve the Mailbox
https://webatm.post.gov.tw/postatm/portal#

郵局ATM 動態鍵盤

中華郵政WebATM - Microsoft Internet Explorer
中華郵政股份有限公司
Chunghwa Post Co., Ltd.
WebATM
登出
Logout
我們的服務
Our Services
網站連結
Websites Binding
服務信箱
Serve the Mailbox
請輸入6-12位晶片卡密碼:
晶片卡密碼請使用畫面上鍵盤輸入!!
1 0 6
8 4 9
2 5 3
7 確認 清除
版本建議MS IE5.0以上 最佳解析度1024 x 768 客服專線：0800-700-365

圖形密碼與動態鍵盤

中華郵政WebATM - Microsoft Internet Explorer
中華郵政股份有限公司
Chunghwa Post Co., Ltd.
WebATM
登出
Logout
我們的服務
Our Services
網站連結
Websites Binding
服務信箱
Serve the Mailbox
回主選單
Main Menu
請確認以下交易資料
轉出帳號
Transferor
轉入帳號
Transferee
交易金額
Transfer Amount
1.交易驗證碼：
Please Enter Verify No.
224359
依所顯示數字輸入，以確保交易更安全
2.請輸入6-12位晶片卡密碼：
Enter Pins (6 To 12 Digits)
8
3
1
7
4
2
9
0
6
5
確認
清除
版本建議MS IE5.0以上 最佳解析度1024 x 768 客服專線：0800-700-365

郵局ATM 交易明細表

- 建議列印或轉成pdf檔存檔

自然人憑證

自然人憑證

- 自然人憑證就是網路身分證，也是推動電子化政府的基礎建設，其主要功能如下：
  - 確認身分
  - 保障資料傳輸安全
  - 確保交易之完整性與不可否認性
  - 保護隱私性

法源依據

- **90年10月電子簽章法**立法通過。
- 行政院國家資訊通信發展推動小組於90年11月15日召開「推動我國電子簽章法之配套措施及因應作為工作座談會」及90年12月31日召開之「國家資通安全會報第一次工作小組會議」等決議。
- 行政院於91年10月14日核定自然人憑證發證計畫。

相關系統

- 內政部：
  - 戶政網路申辦服務系統、地政網路申辦服務系統、建築物公共安全檢查、個人有無限制出國查詢
- 交通部：
  - 電子公路監理網
- 經濟部：
  - 公司線上申辦系統、標準檢驗線上申辦管理系統、智慧財產權申請人/代理人登錄管理 系統

相關系統

- 財政部：
  - **網路申報繳稅系統**、稅務資料查詢、空運網際網路報關系統
- 行政院環境保護署：
  - 事業廢棄物管制系統
- 行政院國家科學委員會：
  - 研究人才個人網登錄、博士生/博士後個人網登錄
- 勞工保險局：
  - 勞保局網路申辦系統

申請方式

- 臨櫃申辦—民眾親臨戶所申請
- 機動櫃台申辦—配合臨時設置
- 集體申辦—提供公務機關（構）申辦

臨櫃申辦

1.上網註冊—取得預約密碼

2.上網預約—選取申辦時間及地點

3.臨櫃填表及製取卡—本人攜帶國民身分證至預約戶所辦理（填申請資料/審驗/製卡/寫入憑證/開卡）

*預約名額：每日每所30名

憑證廢止

- 狀況：
  - 本人懷疑或證實私密金鑰遭到破解
  - 憑證所記載之資訊重大改變，足以影響其信賴度（例如：用戶姓名變更)
  - 憑證永久不再需要使用
- 申辦方式：
  - 用戶本人持身分證正本至戶政事務所自然人憑證櫃檯辦理（不限戶籍所在地均可辦理）

憑證停用

- 狀況：
  - 憑證IC卡遺失或懷疑遭盜用
  - 自行認定必須暫時停用
- 申辦方式：下列二擇一
  - 臨櫃辦理—用戶本人持身分證正本至戶政事務所自然人憑證櫃檯辦理。
  - 線上申辦：用戶可連線至自然人憑證專屬網站，選擇【憑證作業】/【憑證停用】功能，進行線上憑證停用程序。此作業須輸入「用戶代碼」以做為身份驗證之依據

憑證復用

- **狀況**：憑證已停用，但尚在有效期限內
- **申辦方式**：下列二擇一
  - 臨櫃辦理—用戶本人持身分證正本至戶政事務所自然人憑證櫃檯辦理
  - 線上申辦—用戶可連線至自然人憑證專屬網站，選擇【憑證作業】/【憑證復用】功能，進行線上憑證復用程序。此作業須輸入「用戶代碼」做為身份驗證之依據

電腦病毒簡介與防護

電腦病毒

- 電腦病毒是一組具有傳染能力、會自我複製的程式碼，而且是對使用者有害而無用、使用者卻常渾然不知程式碼。
- 當電腦感染上病毒時，電腦將受到不同程度的損害，例如系統當機、資料毀損、異常

電腦病毒

- 可藏身在記憶體、硬碟之分割區(partition table),開機啟動區(boot sector),檔案,e-mail的附加檔或本文、分成數段存在於檔案之間的空隙（如CIH），藉由時間的設定或寄居程式中藉由系統的啟動發動病毒，再靠複製病毒與磁片的傳染來預防絕種。
- 可對軟碟或硬碟啟動區、檔案配置表或其他程式、硬體造成破壞
- 與一般程式不同處在於：具有傳染能力，會不斷複製程式碼至其他檔案或電腦內部。

病毒破壞力

- 侵入partition table、boot sector ，造成電腦無法開機或感染磁片繼續散播病毒。
- 破壞CMOS存放資料，造成BIOS階段執行失敗……CIH
- 侵入目錄區、檔案配置區混淆存取檔案的功能。
- 侵入中斷服務程式，使人誤判為硬體障礙。
- 格式化硬碟，毀掉全部資料檔案。
- 冒名重複不斷傳送有毒郵件感染，癱瘓郵件伺服器。
- 攻擊特定對象伺服器，造成網路癱瘓的後果。
- 植入木馬程式，監控你的電腦，盜取帳號、密碼、機密資料等行為。
- 自動透過網路上芳鄰尋找不當設定之共享目錄繼續散播病毒
- 攻擊防毒軟體或安全性軟體植入自建帳號以利再攻擊。

電腦病毒的種類

- 開機型病毒
- 檔案型病毒
- 巨集病毒
- 蠕蟲（Worms）
- 暗門程式（Trapdoor）
- 特洛依木馬（Trojan Horse）
- 邏輯炸彈（Logical Bomb）
- 視窗炸彈
- 隨身碟病毒

開機型病毒

- 透過開機而傳染的病毒，它會感染磁碟的啟動磁區(Boot Sector)或是硬碟分割表(Partition Table)。
- 例如:
  - Stone 石頭病毒
  - Blooy 血腥六四病毒
  - BURNING FIRE 燃燒之火病毒

檔案型病毒

- 依附在程式的可執行檔(.COM 或.EXE)
- 原本出現於DOS，目前已在Windows肆虐；依附的檔案種 類也增加了**.SCR或.PIF或.BAT**…
- 判斷是否中毒：檔案長度改變(變大變小)
- 病毒實例:
  - Friday_13 13號星期五病毒
  - Mummy 木乃伊病毒
  - REDX 紅色十字病毒
- 絕大多數的電腦病毒皆屬檔案型

蠕蟲（Worms）

- 屬於電腦病毒的一種，此型的病毒不會攻擊其他程式，它只會不停的複製自己。
- 經常透過區域網路、網際網路或是E-mail 來散播到其他伺服器，最後所有的伺服器將忙著複製、傳播病毒，沒空服務其他合法的使用者。

蠕蟲型病毒

- 蠕蟲型病毒植入電腦的行為
  - 僅植入惡意程式碼於記憶體，進行阻斷式(DOS)攻擊
    - 如2003年1月的SQL Slammer蠕蟲
  - 植入惡意程式碼於記憶體及檔案，進行阻斷式(DOS)攻擊並留下後門(root.exe)
    - 如2001年8月的CodeRed蠕蟲
  - 植入惡意程式碼於記憶體及檔案，進行阻斷式(DOS)攻擊、大量發信、利用CodeRed蠕蟲留下之後門(root.exe)、植入後門(tftp.exe)、開放完整權限共享目錄(其它類型病毒均可植入)
    - 如2001年9月的NIMDA蠕蟲

暗門程式（Trapdoor）

- 程式或伺服器中未公開的秘密通口，利用暗門程式可以自由進出系統，而不被別人發現。
- 最早的暗門程式是程式設計師預留做為追蹤、監控、除錯甚至修復系統。但後來演變成駭客入侵後，為了方便未來可以直接進入系統而保留的通口。
- 若電腦系統的管理者發現了漏洞，將漏洞補好了，駭客仍可利用早就安插好的暗門程式，繼續入侵此系統。

特洛依木馬（Trojan Horse）

- 特洛依木馬指的是類似電腦病毒的指令組合，暗藏在普通程式中，藉著普通程式的執行，偷偷的作自己的事。
- 特洛依木馬程式會記錄使用者做了哪些動作，**當然包括使用者所按下的密碼**。
- 特洛伊木馬程式本身既不會感染其他檔案也不會主動傳播自己到網路上的其他電腦所以如何將這些特洛伊程式『植入』到使用者電腦中便是駭客入侵成功與否的關鍵。
- 木馬程式會透過E-mail或將自己偽裝成一些特殊工具來吸引使用者下載並執行，或是電腦駭客直接入侵電腦主機將惡性程式植入對方系統以**竊取重要資料或進行大規模的『阻斷服務』（Denial of service）攻擊**。

邏輯炸彈（Logical Bomb）

- 屬於特洛依木馬的一種，它需隱藏在其他的程式中，當某個被預先設定的條件吻合時，它便會啟動。
- 例如被公司開除的員工因心中不滿，離職前便在公司電腦裡擺置了一個邏輯炸彈，若干時日以後，炸彈啟動，自動將電腦中的資料全數銷毀。

視窗炸彈

- 會不斷的在被害者電腦上開啟視窗，造成系統資源(memory)或CPU耗盡，最後導致當機或必須重開機才能正常使用。
- 設計原理
  - 使用Java Script 或VB Script寫一段永不結束的程式片段放在HTML檔(*.htm)或郵件內部送出即可。
  - 當不慎瀏覽到網頁或點選郵件附加檔執行即不斷的出　現視窗在桌面上。

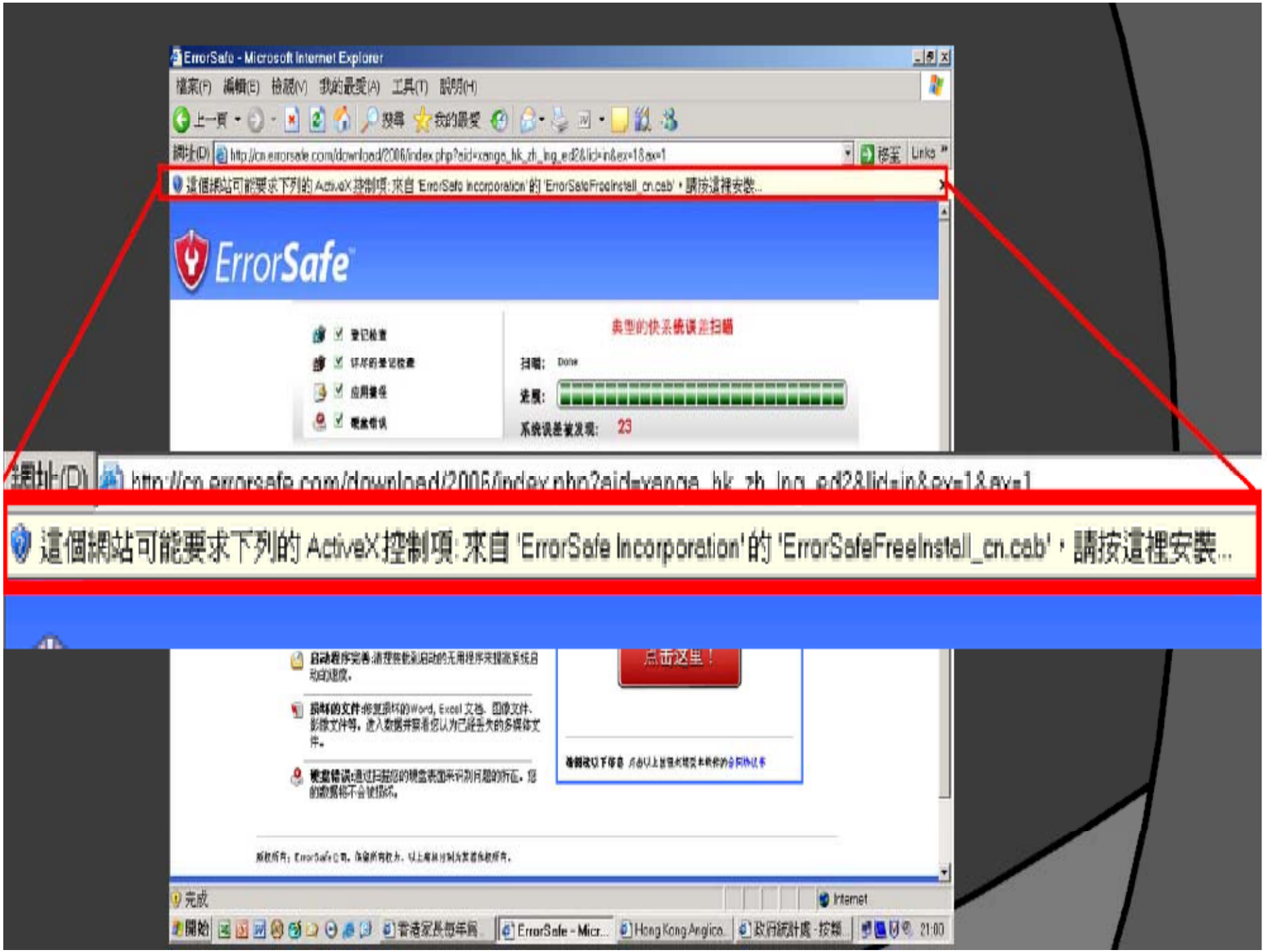
電腦病毒的傳播途徑

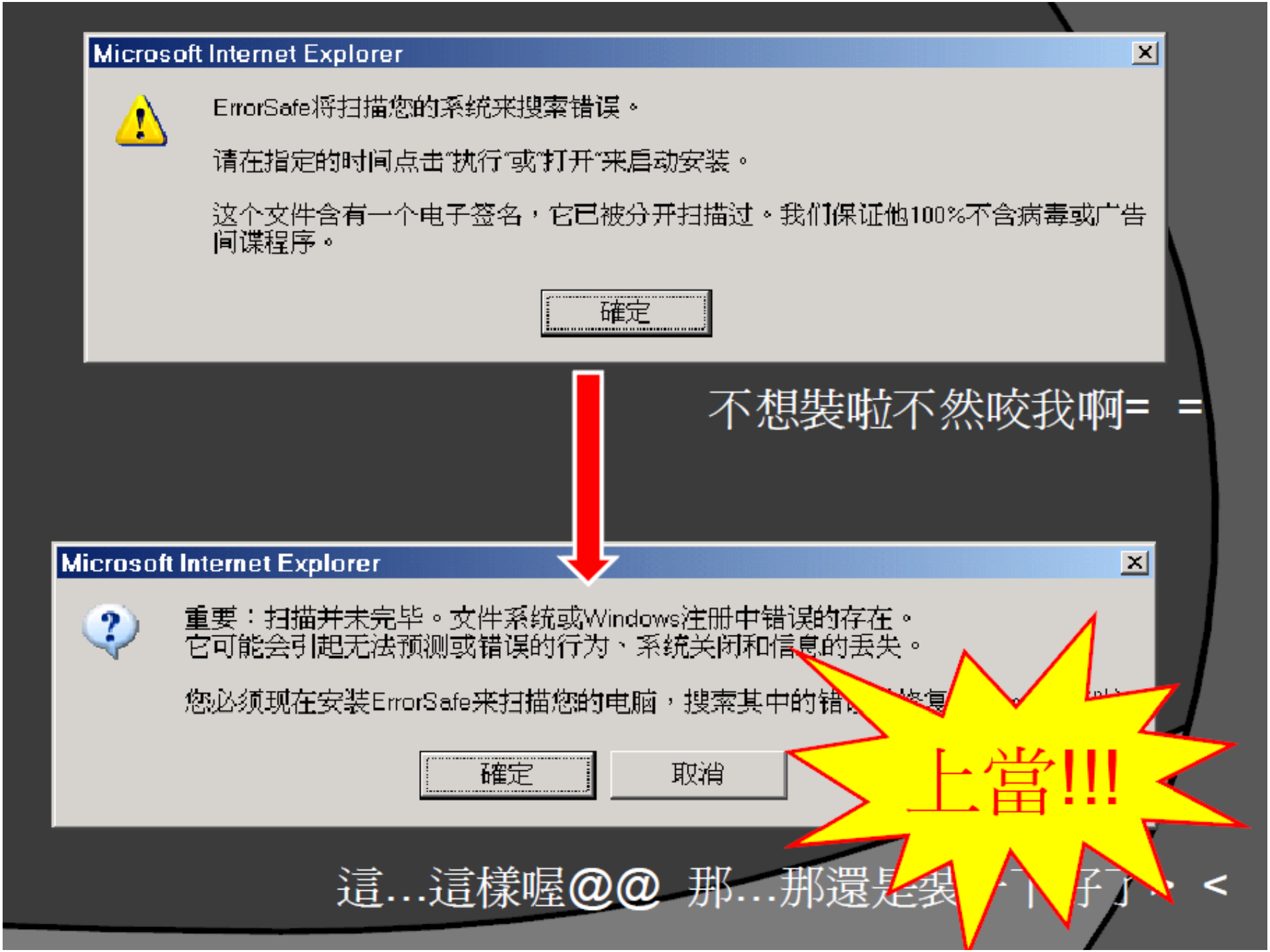
- **製造病毒**—病毒的製作人將病毒播灑在磁片、電子郵件或網際網路中，讓人無意間去執行它。
- **接觸感染**—當含有病毒的磁片或檔案載入個人電腦，則病毒即可潛入電腦系統而隱身於電腦記憶體或系統軟體中。
- **病毒傳播**—使用已帶菌的個人電腦來執行健康的應用程式時，病毒即可藉機侵入這些應用軟體。
- **病毒蔓延**—由於有些受病毒感染的個人電腦不會立即出現病狀，因此在不知不覺中透過帶菌檔案而感染的個人電腦愈來愈多。

惡意軟體 (Malicious Code)

惡意軟體 (Malicious Code)

- 惡意軟體又稱流氓軟體或間諜程式，跟木馬程式很像，藉由一些管道，偷偷安裝到使用者的電腦上且無法停止移除。
- 潛伏在電腦中，從事資訊蒐集（比如記錄你的鍵盤操作獲得密碼，或擷取你的螢幕畫面）方便駭客遠端連結登入（幫你開關機，增刪你的檔案，或讓你在自己的電腦控制遠端機器下達操作指令）。


ErrorSafe - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
這個網站可能要求下列的 ActiveX 控制項: 來自 'ErrorSafe Incorporation' 的 'ErrorSafeFreeInstall_cn.cab'，請按這裡安裝...
ErrorSafe
典型的快系统误差扫描
扫描: Done
进展:
系统误差被发现: 23
http://cn.errorsafe.com/download/2006/index.php?aid=xango_hk_zh_lng_ed2&lid=in&ex=1&ex=1
這個網站可能要求下列的 ActiveX 控制項: 來自 'ErrorSafe Incorporation' 的 'ErrorSafeFreeInstall_cn.cab'，請按這裡安裝...
点击这里！
完成
Internet
開始
ErrorSafe - Micr...
Hong Kong Anglico...
21:00

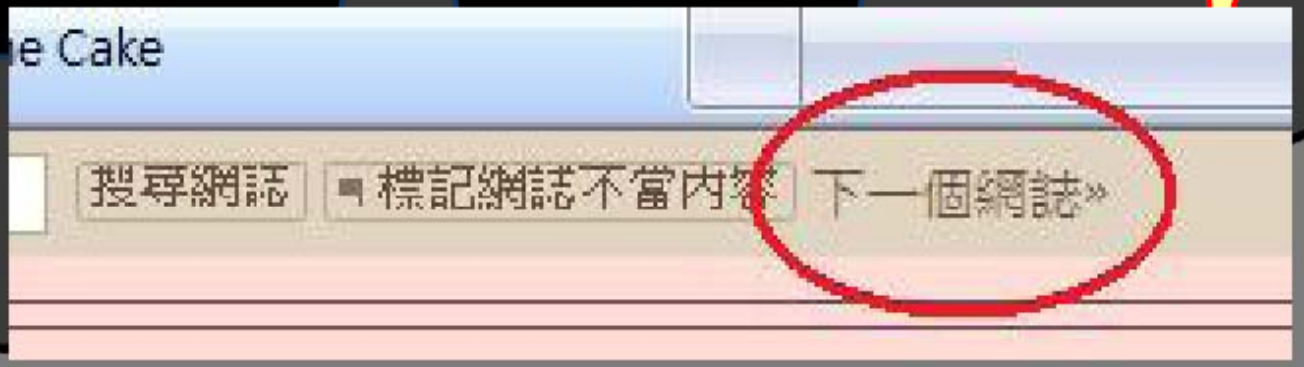

Microsoft Internet Explorer
ErrorSafe将扫描您的系统来搜索错误。
请在指定的时间点击"执行"或"打开"来启动安装。
这个文件含有一个电子签名，它已被分开扫描过。我们保证他100%不含病毒或广告间谍程序。
確定
不想裝啦不然咬我啊= =
Microsoft Internet Explorer
重要：扫描并未完毕。文件系统或Windows注册中错误的存在。
它可能会引起无法预测或错误的行为、系统关闭和信息的丢失。
您必须现在安装ErrorSafe来扫描您的电脑，搜索其中的错
確定
取消
上當!!!
這...這樣喔@@ 那...那還是裝一下子了...<

間諜軟體滲入BLOG

有心人在免費提供給BLOG作者拿來強化網站功能的JavaScript程式藏入間諜軟體

不知情的作者下載並在自己的BLOG上使用這些工具

BLOG成爲間諜軟體傳播的平台!!!



駭客利用陳冠希私密照片攻擊手法

1

有180個網站內有惡意連結，其中60個網站還具有攻擊性

2

這60個惡意連結，分析最終都連到下列5個網址下載Downloader惡意程式，企業應該立即封鎖這5個惡意連結。

ccc.969222.com/bak.css

dd.749571.com/bb/014.exe

user1.1a2b3c0.net/bak.css

user1.1a2b3c1.net/bak.css

mm.sqmnoopt.com/mm/mm.exe

3

這些Downloader最終都會連到 kv8.info網域，下載惡意程式，種類多達40種

資料來源：阿碼科技，2008年2月

如何防範惡意軟體

- 儘量不要安裝來路不明的軟體，尤其是遊戲外掛及來自中國的工具軟體(如雅虎上網助手、百度超級搜霸、eBay工具條..等)。
- 所以防範惡意軟體只能靠自己!!

釣魚網站與信件

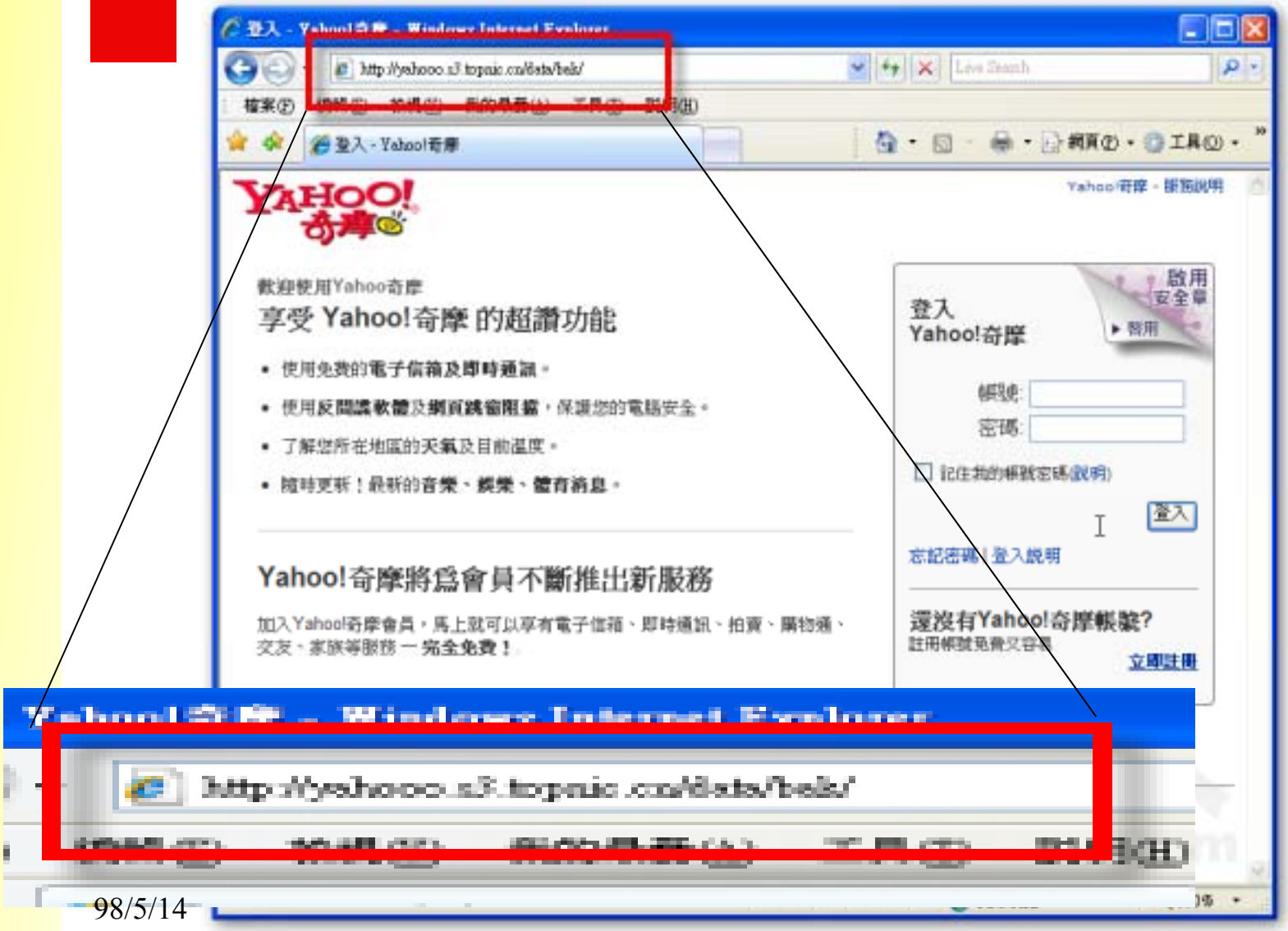
何謂釣魚網站

- **釣魚網站(Phishing)**是模仿真實網站，通常會唯妙唯肖地模仿合法的網站，藉以誤導使用者輸入帳號密碼或個人資料，達到騙取個人資訊的目的。
- 釣魚網站的網址通常會申請與受害網站非常相似的網域名稱，例如遊戲橘子的官方網站 如**gamania.com** ，日前發現，位於大陸的詐騙者，申請了 **gamannia.com**的網址，多了一個 “n”。

釣魚網站

CANON EP 70-200mm f2.8 L鏡Yahoo!奇摩拍賣 - Windows Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
CANON EP 70-200mm f2.8 L鏡Yahoo!奇摩拍賣
釣魚網站連結
請用滑鼠點擊下邊(前往我的拍賣賣
Yahoo!奇摩拍賣6周年慶
滿1,000送100再回饋2%現金
點擊這黃色
場~還有很
屋~保證買
http://yahooo.x3.lognic.cn/data/bak/
網際網路
100%

釣魚網站


YAHOO! 奇摩
歡迎使用Yahoo奇摩
享受 Yahoo!奇摩 的超讚功能
使用免費的電子信箱及即時通訊。
使用反間諜軟體及網頁跳窗阻擋，保護您的電腦安全。
了解您所在地區的天氣及目前溫度。
隨時更新！最新的音樂、娛樂、體育消息。
Yahoo!奇摩將爲會員不斷推出新服務
加入Yahoo!奇摩會員，馬上就可以享有電子信箱、即時通訊、拍賣、購物商、交友、家族等服務 一 完全免費！
登入 Yahoo!奇摩
帳號:
密碼:
登入
忘記密碼 | 登入說明
還沒有Yahoo!奇摩帳號?
立即註冊

如何防範釣魚網站

- 注意網址是否正確
- 自己輸入網址或使用書籤，而不要點選網站或E-Mail中的連結
- 注意網站是否與平常不同
- 網站是否要求過多的個人資料

何謂釣魚信件

- 釣魚信件是由駭客以知名公司的名義發出假的E-mail，
  - 標題多半為「系統更新，請檢查帳號」、
  - 「請變更密碼」、
  - 「帳號將被關閉，請上網重新啟動」等字眼
- 然後提供一個假的超連結，誘騙使用者登入假網站輸入帳號密碼及個人資料，或誘騙使用回覆帳號密碼至某個信箱，達到騙取個人資訊的目的。

釣魚信件

寄件者: eBay <ebay@ebay.com> 收件者: deron@ms45.hinet.net <deron@ms45.hinet.net>
主旨: [X-Spam]Security alert

eBay sent this message to deron@ms45.hinet.net.
Your registered e-mail is included to show this message originated from eBay.

eBay confirmation form

Dear eBay user,

We would like to inform you that we have released a new version of eBay Confirmation form. This form is required to be completed by all eBay users.

Please follow these steps:
1.Open the form at http://cgi.ebay.com/ws/eBayISAPIdll?cfom=14568289644303767291198799257484739113414047715120 7.
2.Follow given instructions.

Thank you,
eBay

This eBay notice was sent to deron@ms45.hinet.net from eBay. Your account is registered on www.ebay.com. As outlined in our User Agreement, eBay will send you required notifications abou format, change your notification preferences.

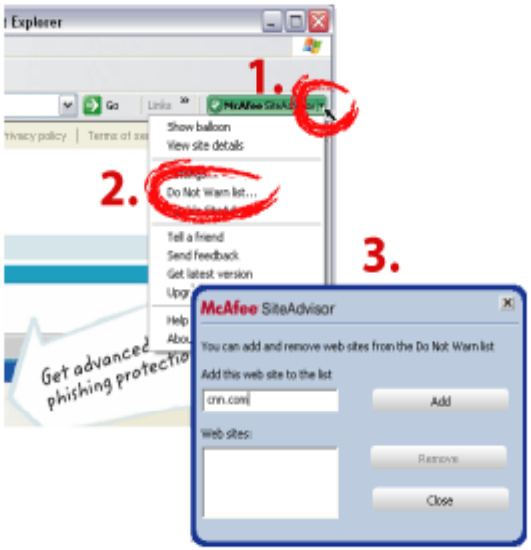
See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.
Privacy Policy: http://pages.ebay.com/help/policies/privacy-policy.html
User Agreement: http://pages.ebay.com/help/policies/user-agreement.html

Copyright © 2006-2009 eBay, Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
eBay and the eBay logo are registered trademarks or trademarks of eBay, Inc.
eBay is located at 2145 Hamilton Avenue, San Jose, CA 95125.

msfddre.com可能會嘗試竊取您的資訊。

為何會將您重新導向至這個網頁？我們相信這個網站可能會嘗試詐騙您，讓您輸入您的財務或個人資訊。這是一個嚴重的安全性威脅，可能會導致身份遭竊、財務遺失或散佈其他個人資訊。

- 更多關於「網路釣魚」攻擊的資訊
- 返回到上一頁
- 如何覆寫這個警告



如何覆寫這個網站的此項網路釣魚警告：

如果您非常確定仍想要造訪這個網站，則請遵循下列作法：

1. 按一下 SiteAdvisor 下拉式功能表箭號 (按一下 SiteAdvisor 安全按鈕右邊的黑色箭號)

   附註：如果您所使用的是處於「保護模式」的 SiteAdvisor Plus，則可按一下 SiteAdvisor 的下拉式功能表並選擇 [停用保護模式]。出現提示時，輸入您的「保護模式」密碼，然後...

2. 在功能表中選擇 [核准的網站...]。
3. 將「msfddre.com」加入清單。

   將「msfddre.com」重新輸入您的 Web 瀏覽器。

如何防範釣魚信件

- 不要開啟來路不明信件的附檔或連結。
- 不要將個人資料(如密碼、信用卡卡號)告訴任何人。
- 使用電子郵件應有的警覺性觀念：
  - 我為何會收到這封郵件？
  - 我是不是應該收到這封郵件？
  - 我是不是有必要開啟附件或點選連結？

更進一步預防釣魚信件

- 做好信箱管理
- 很多網站會員或抽獎活動都要填寫個人E-Mail，現在人應該不只一個E-Mail信箱，可以填寫其中一個不常用的信箱來收垃圾信，這樣可以保護其他重要的信箱不受垃圾信或釣魚信的騷擾。

辯識正確網址

- 比較看看那裡不一樣:

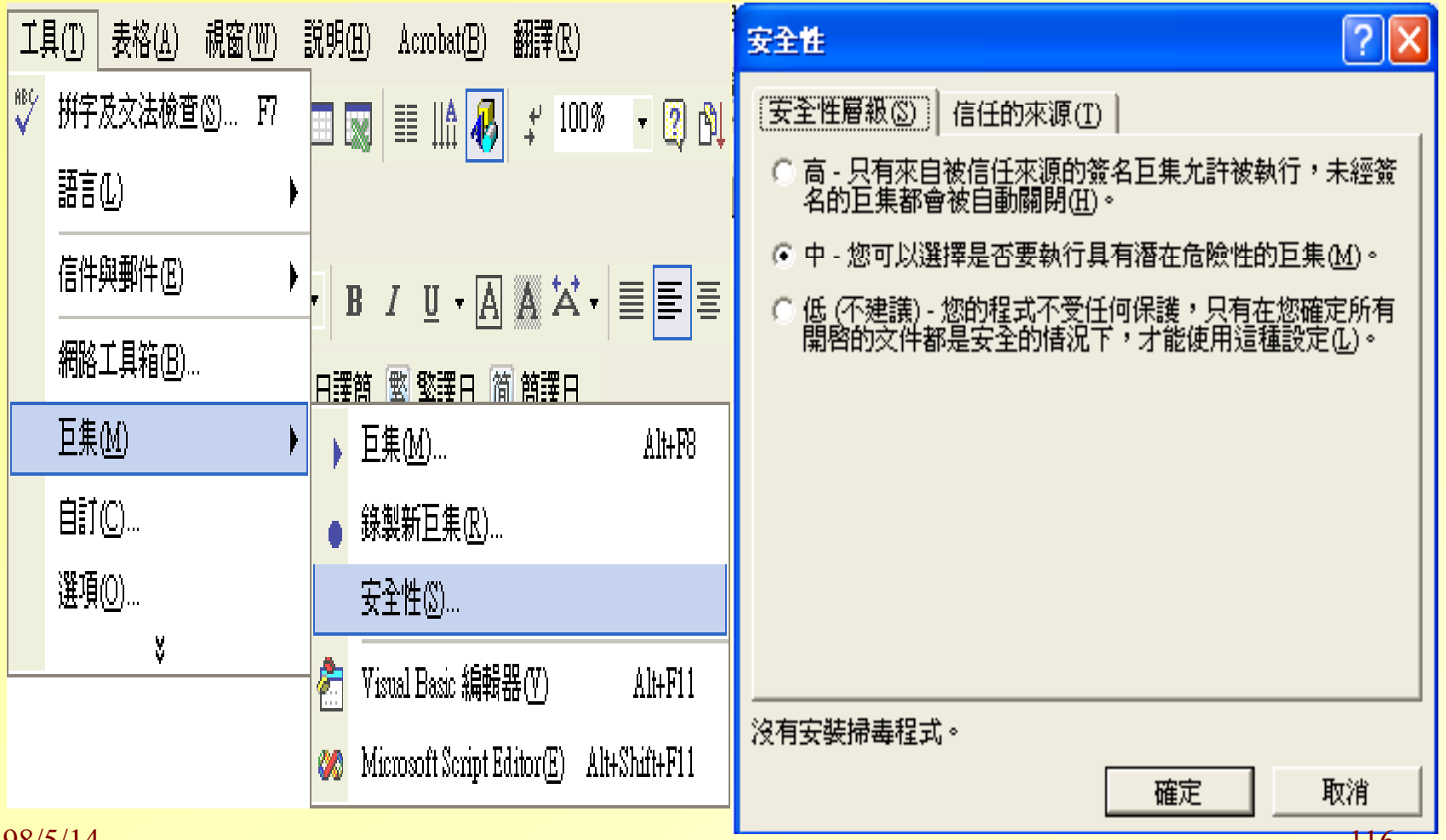
webmail.tku.edu.tw	webmail.tku.eud.tw	淡江大學webmail
www.chinatrnst.com.tw	www.chinatrust.com.tw	中國信託
www.ntx.gov.tw	www.ntx.com.tw	財政部北區國稅局
TW.BID.YAHOO.COM	TW.BID.YAHO0.COM	雅虎拍賣
http://www.vvretch.cc/	http://www.wretch.cc/	無名小站
http://www.pchome.com.tw	http://www.pchorne.com.tw	PCHome
service@1andbank.com.tw	service@landbank.com.tw	土地銀行

巨集病毒

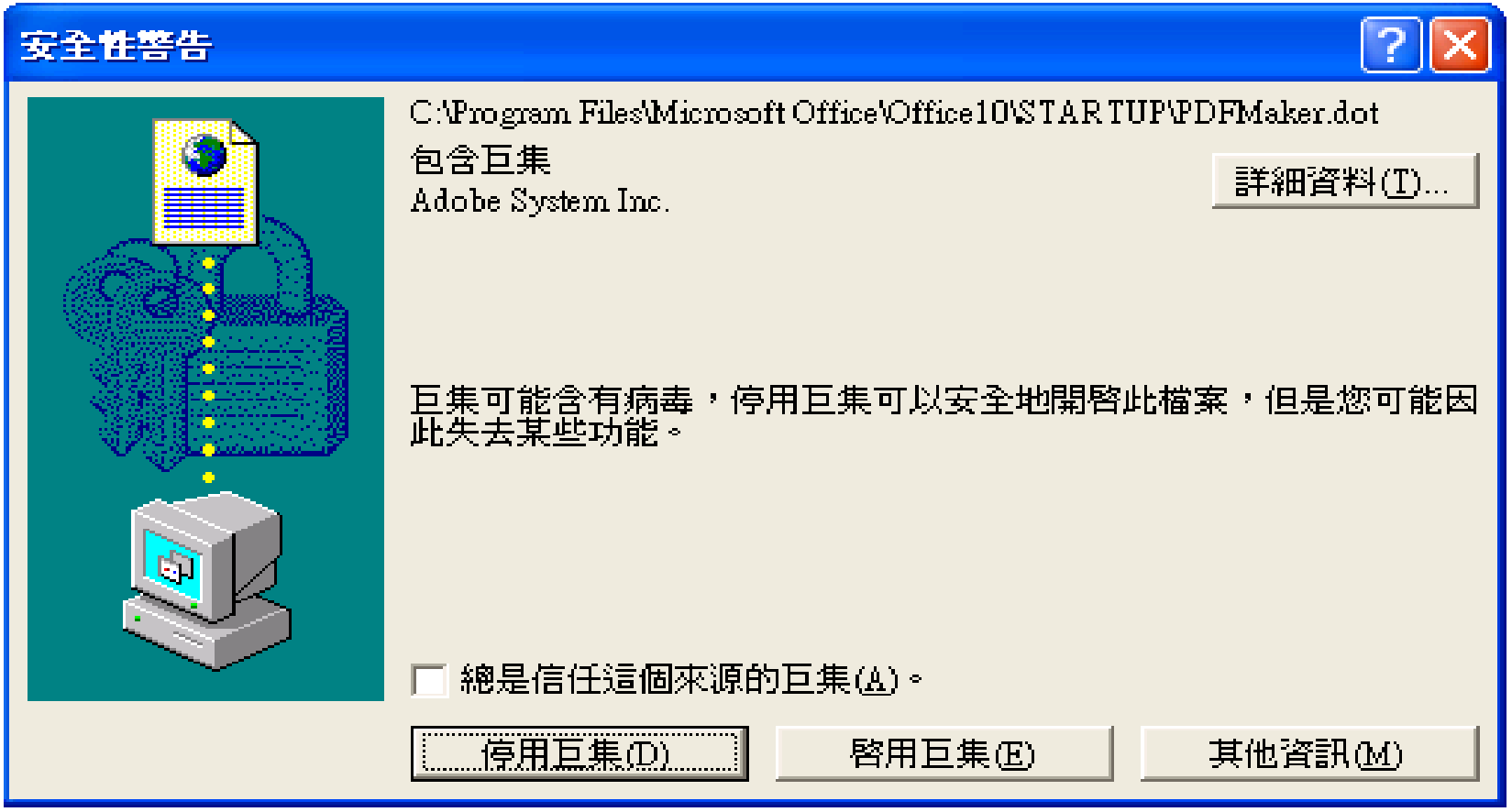
巨集病毒

- 它專門感染經由 WORD 所編輯過的文件，而這一類型的病毒又是一隻跨平台的病毒
- 此類型的病毒其感染方式為，一旦我們開啟有巨集病毒的文件之後，以後我們所開啟的舊檔或者是開啟新檔案等等都難逃 WORD 巨集病毒的惡夢。
- 早期以『臺灣 No.1 』巨集病毒流傳率最高。
- 目前以梅莉莎病毒較有名

防止巨集病毒


工具(T)
表格(A)
視窗(W)
說明(H)
Acrobat(B)
翻譯(R)
拼字及文法檢查(S)... F7
語言(L)
信件與郵件(E)
網路工具箱(B)...
巨集(M)
自訂(C)...
選項(O)...
100%
巨集(M)... Alt+F8
錄製新巨集(R)...
安全性(S)...
Visual Basic 編輯器(V) Alt+F11
Microsoft Script Editor(E) Alt+Shift+F11
安全性
安全性層級(S)
信任的來源(T)
高 - 只有來自被信任來源的簽名巨集允許被執行，未經簽名的巨集都會被自動關閉(H)。
中 - 您可以選擇是否要執行具有潛在危險性的巨集(M)。
低 (不建議) - 您的程式不受任何保護，只有在您確定所有開啓的文件都是安全的情況下，才能使用這種設定(L)。
沒有安裝掃毒程式。
確定
取消

防止巨集病毒



自行決定是否開啟此巨集功能

如果中了巨集病毒怎麼辦

- 檔案巨集病毒通常會放在C:\windows\Application Data\Microsoft\Templates\normal.dot
- 然後感染Program File\Microsoft Office\Templates\normal.dot
- 因此必須移除上述兩個檔案
- 複製一份新的normal.dot(使用者範本)
- 關閉巨集功能
- 開啟帶病毒檔與另開新檔
- 複製內容再貼到新檔
- 新檔存檔
- 刪除原帶病毒檔
- 完成

圖片與e-mail病毒

瀏覽圖片也有可能會中毒？

- 瀏覽圖片也有可能會中毒？
- 不管你是從Email所收的圖片，或是上網路相簿瀏覽的圖片，或是根本只是用ACDSee秀圖軟體觀看在你電腦中的圖片，都有可能會中毒！
- 這是在今年9月由微軟所公佈的一個名叫「**JPEG處理程序(GDI+)處理緩衝區溢出**」的安全性漏洞，只要是JPEG格式的圖片，經過特殊的處理後，都有可能引發這個漏洞，導致駭客趁虛而入，引發你的系統中毒。

瀏覽圖片也有可能會中毒？

- 主要的原因並不在於圖片檔，而在於**微軟作業系統中一個「GDIPlus.dll」的動態連結檔案；**
- 當我們要瀏覽JPEG圖片或是對JPEG檔案作影像處理時，多半都要用到這個檔案裡頭的程式指令，而漏洞就存在這個檔案裡頭。

病毒圖片製造機

- 2004年的10月份，在網路上就出現一只叫做「**JPGDownloader**」的軟體，又被暱稱為「**病毒圖片製造機**」，
- 這個程式可以讓任何人隨便用一個JPEG圖檔，製作出JPEG圖片病毒；不過這個程式攻擊的目標，僅針對英文版的作業系統，所以國內目前尚未聽到有人成為受害者。

可能病毒程式

- **延伸副檔名為.PIF**
  - 對於附件檔案是pif 的電子郵件，千萬不要打開pif 附件檔以免中毒，既使收到病毒信件，只要不打開.pif檔就不會中毒。這一隻病毒危害的系統相當廣泛。
  - 包括Windows 95, 98, ME, NT, 2000 和XP系統都是目標。
- **延伸副檔名為.SCR**
  - 螢幕保護程式

可能病毒程式

- 兩種病毒(Beagle worm & NetSky worm)的變種肆虐。這些病毒都是透過**email**傳播，
- **凡是附件為.pif以及.zip都請不要隨意開啟**。 由於這些病毒會假造寄件者，所以即使看到認識的寄件者寄來有問題的附加檔也不要輕易開啟。
- **W32.Beagle.C@mm偽裝成ZIP壓縮檔**，此變種病毒還會停止防毒軟體更新病毒碼的機制，造成防毒軟體無法偵測新病毒。

E-mail型病毒

- 大部份存在於附加檔案，少數存在於郵件的本文內部之Html程式片斷
- 如果**IE本身有漏洞未修補會自動執行病毒附加檔**
- 如果IE本身安全性設定較弱也會自動執行本文內部之Html 程式片斷
- E-Mail病毒附加檔案類型如下：

  .com， .exe， .bat， .pif， .scr 雙副檔名

『非病毒信件』：

  - Spam:垃圾郵件（廣告信）
  - Hoaxes :惡作劇郵件

判斷E-mail信件有病毒入侵

- 內含附加檔為雙副檔名之E-mail信件幾乎可確定含有病毒
- 多數新型E-mail病毒均為冒名傳送，需由信件內容方可判斷出入侵來源
- 若游標移至E-mail信件時有提示開啟或另存新檔(附加檔)之對話方塊時，可判斷出信件八成含有病毒(操作請小心謹慎)

選取含毒信件後出現對話方塊

IE 6.X版自動封鎖附加檔

USB隨身碟病毒

關於USB的防護

- USB病毒主要是利用autorun.inf將病毒植入電腦主機，或反向從遭感染的主機把病毒散播到各種USB介面的儲存裝置中。就是因為具有這種雙向傳遞的方式，病毒才能在電腦及USB儲存裝置中不斷擴散，而autorun.inf就是最主要的媒介。
- **身邊的所有的USB儲存裝置，都要清查裡頭是否有兩個隱藏檔**

  Autorun.inf ntdelect.com
- **防護測試**
  1. Autorun.inf 的唯讀資料夾 ----- OK
  2. 機碼啟動隨身碟的唯讀功能 ---無效
  3. shift 鍵開啟隨身碟 ----------無效
  4. 隨身碟磁區上右鍵開啟檔案總管 ----------無效
  5. 機碼關掉自動啟動功能 ----------無效

McAfee SecurityCenter
說明
首頁
保護狀態
更新
鎖定防火牆
掃描
檢視最近的事件
管理網路
維護電腦
首頁
報告與記錄
設定
還原
工具
基本功能表
掃描結果
病毒及特洛伊程式
病毒及特洛伊程式
項目名稱
類型
狀態
G:\UTCN8C63.EXE
特洛伊病毒
已隔離
詳細資料
偵測類型: 特洛伊病毒
偵測名稱: PWS-OnlineGames.ei, PWS-OnlineGames.ei
狀態: 已隔離
檔案名稱: G:\UTCN8C63.EXE
我要...
使用 [還原] 來還原這個項目
上一步

注意事項與解決方法

- 不開啟來路不明的檔案、附件
- 儘速安裝防毒軟體、並更新病毒碼
- 開放源碼的隨身碟防毒軟體－
  Wow! 隨身碟防毒系列

檢查示範1

```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\teachernote23>f:

F:\>dir /a
 磁碟區 F 中的磁碟沒有標籤。
 磁碟區序號:  78E5-D69D

 F:\ 的目錄

2007/05/06  下午  12:08    <DIR>          常用軟體h
2007/08/20  下午  09:23    <DIR>          tsaikl
2007/09/22  上午  11:05    <DIR>          autorun.inf
               0 個檔案              0 位元組
               3 個目錄     611,188,736 位元組可用

F:\>
```

若找到沒有〈dir〉（資料夾）的autorun.inf檔或*.exe檔就要當心了

檢查步驟2

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\teachernote23>cd..
C:\Documents and Settings>cd..
C:\>dir c:\a
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號: 50CD-CE6D
c:\ 的目錄
2007/05/22 下午 03:05 <DIR> history10
2007/06/01 下午 03:44 38,244 debug.log
2007/09/22 上午 02:33 <DIR> autorun.inf
2007/08/16 下午 12:11 <DIR> 道教
2002/07/03 下午 03:10 6,191,421 tea250k.wmv
2007/09/03 下午 02:08 <DIR> 254CANON-b1-3
2007/08/29 下午 10:11 <DIR> 00taiwanhis
(2) 輸入cd..
(3) 輸入cd..
這是進入C槽的方法
(4) 輸入dir c:/a或\/a
若找到沒有〈dir〉(資料夾)的autorun.inf檔就要當心了

清除隨身碟autorun.inf等病毒檔

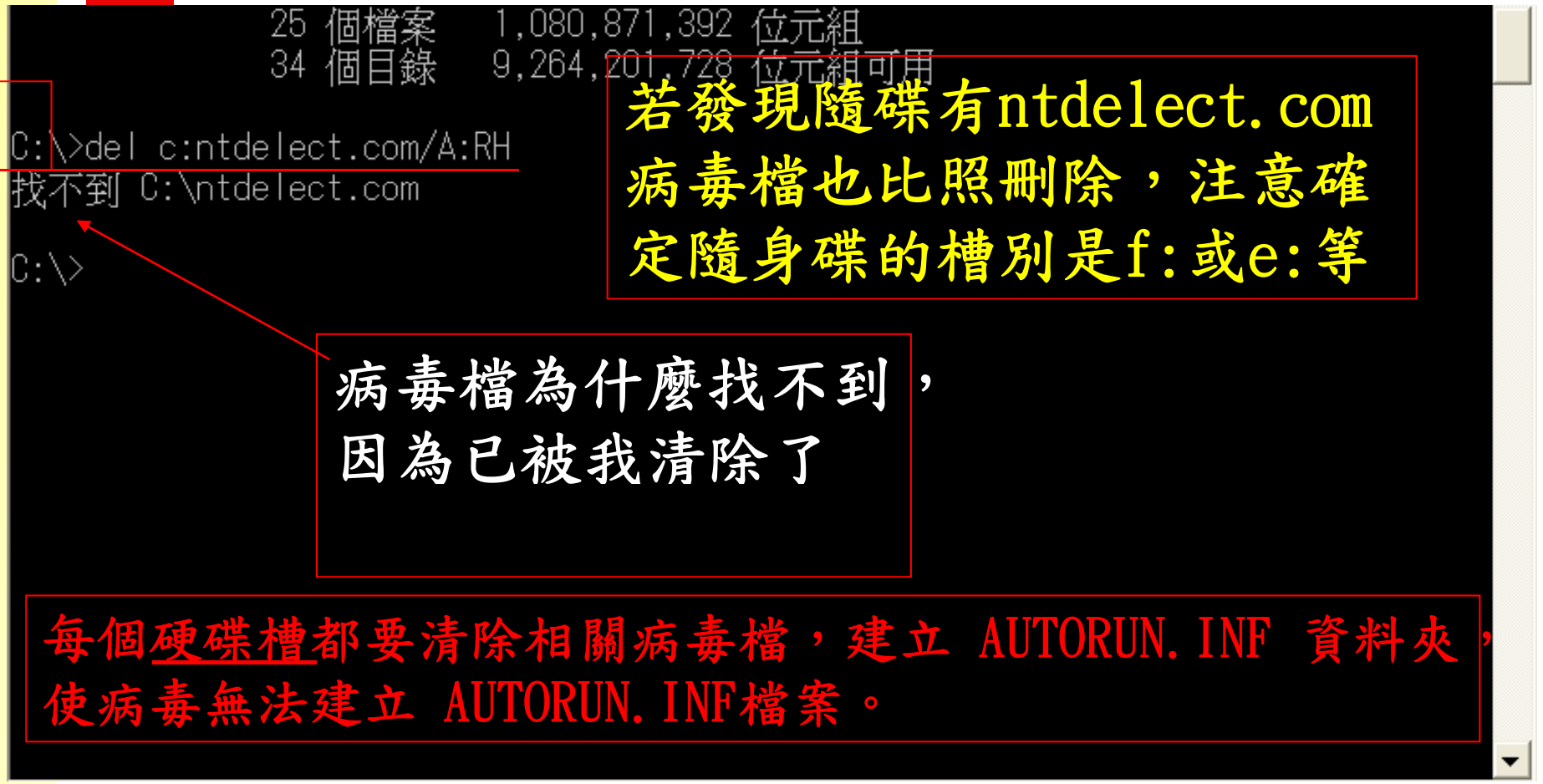
```
F:\>del autorun.inf/A:rh

F:\>md  autorun.inf

F:\>CD  autorun.inf

F:\autorun.inf>
```

autorun.inf是隱藏檔，所以要加A:RH才能清除。其他的*.exe檔也一樣。

在隨身碟建立 AUTORUN.INF 資料夾，使病毒無法建立 AUTORUN.INF 檔案。

恭喜！你已建立AUTORUN. INF 資料夾了

檢查


25 個檔案 1,080,871,392 位元組
34 個目錄 9,264,201,728 位元組可用
C:\>del c:ntdelect.com/A:RH
找不到 C:\ntdelect.com
C:\>
若發現隨碟有ntdelect.com病毒檔也比照刪除，注意確定隨身碟的槽別是f:或e:等
病毒檔為什麼找不到，因為已被我清除了
每個硬碟槽都要清除相關病毒檔，建立 AUTORUN.INF 資料夾，使病毒無法建立 AUTORUN.INF檔案。

Wow! USB Protector

- 中央研究院資訊科學所自由軟體鑄造場，於 2008年 2 月釋出 Wow! USB Protector 隨身碟病毒偵測軟體。採用開放原始碼 GPL3 授權，供個人或企業自由使用與研究。
- Wow! USB Protector 是一款自動偵測隨身碟是否含有惡意程式的自由軟體。可以偵測出常見的隨身碟病毒，提供即時捕捉隨身碟病毒或可疑程式的功能，是一款輔助防毒軟體的安全工 具。目前有繁體中文與英文介面，支援 Windows 2000/XP/2003/Vista 32bit/64bit 作業系統。使用 Ruby 程式語言撰寫、支援系統常駐、自動更新惡意程式病毒碼、合法程式白名單、可疑程式警訊等功能。

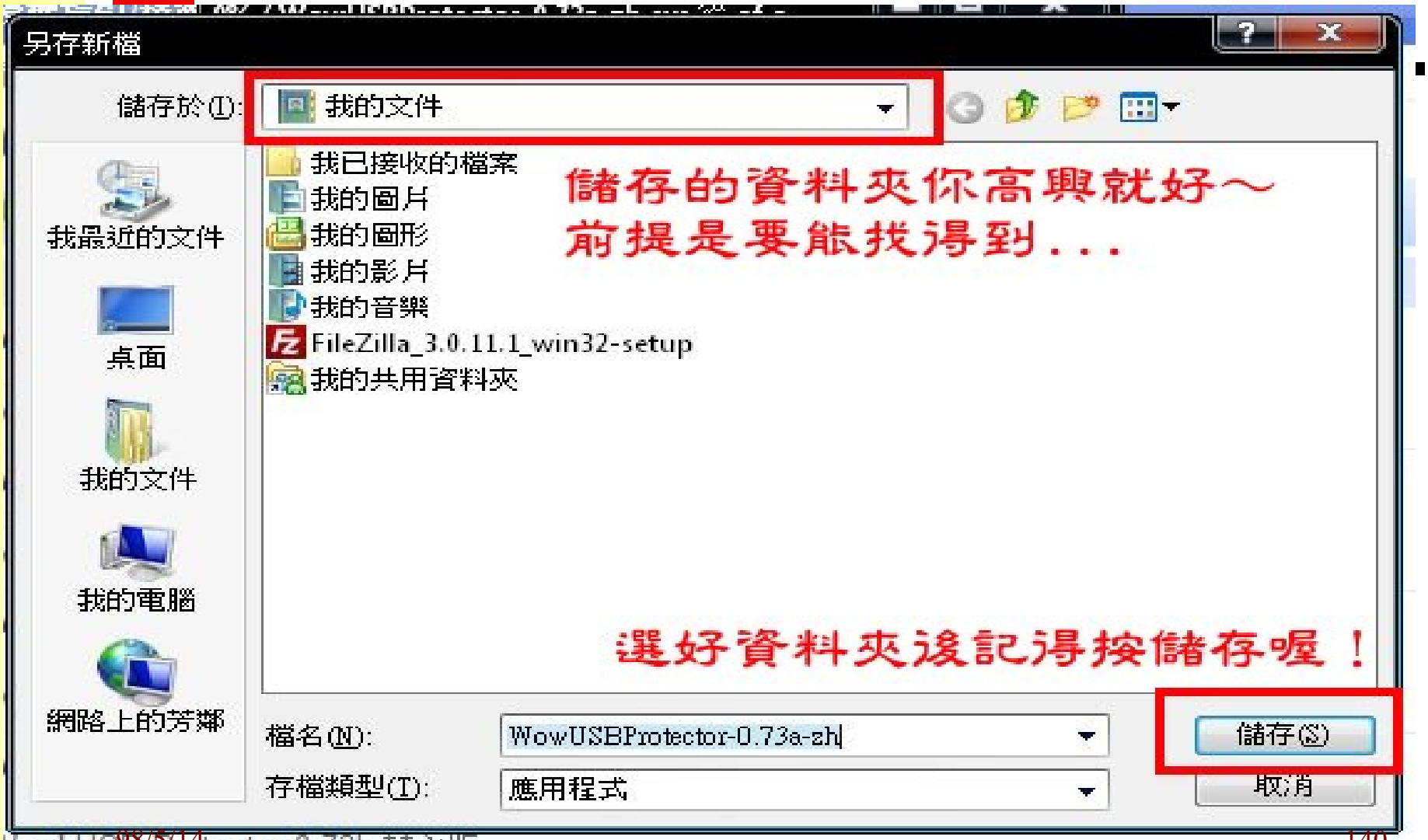
防毒軟體

程式	Wow! USB Protector	Wow! USB VirusKiller
適合對象	了解隨身碟病毒的使用者	電腦初學的新手
偵測出隨身碟病毒	多種選項供使用者選擇	自動刪除惡意程式
偵測出可疑程式	多種選項供使用者選擇	提出可疑程式檔案的警訊
專案網址	Wow! USB Protector	Wow! USB VirusKiller

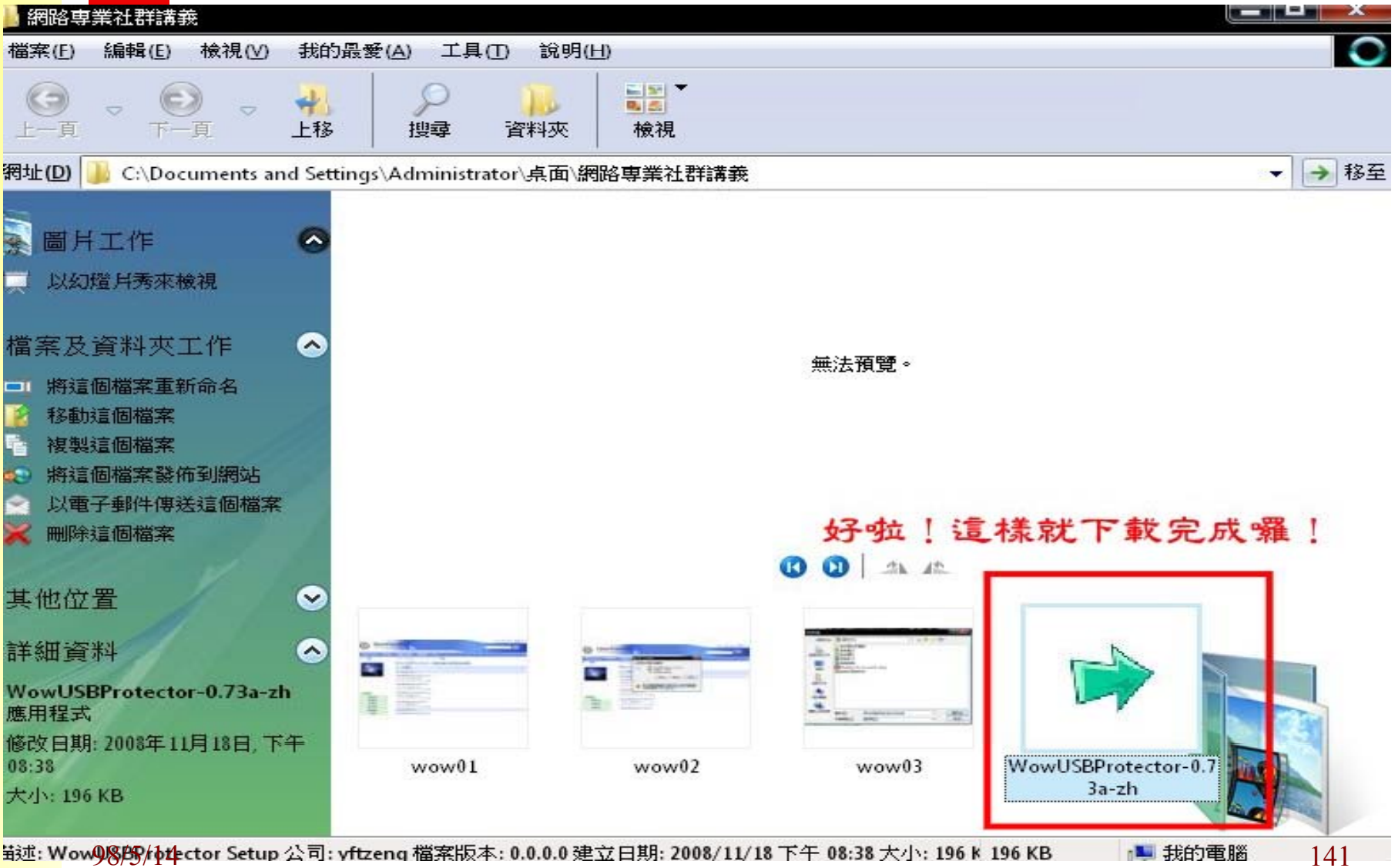
WowUSBProtector

WowUSBProtector

WowUSBProtector



WowUSBProtector

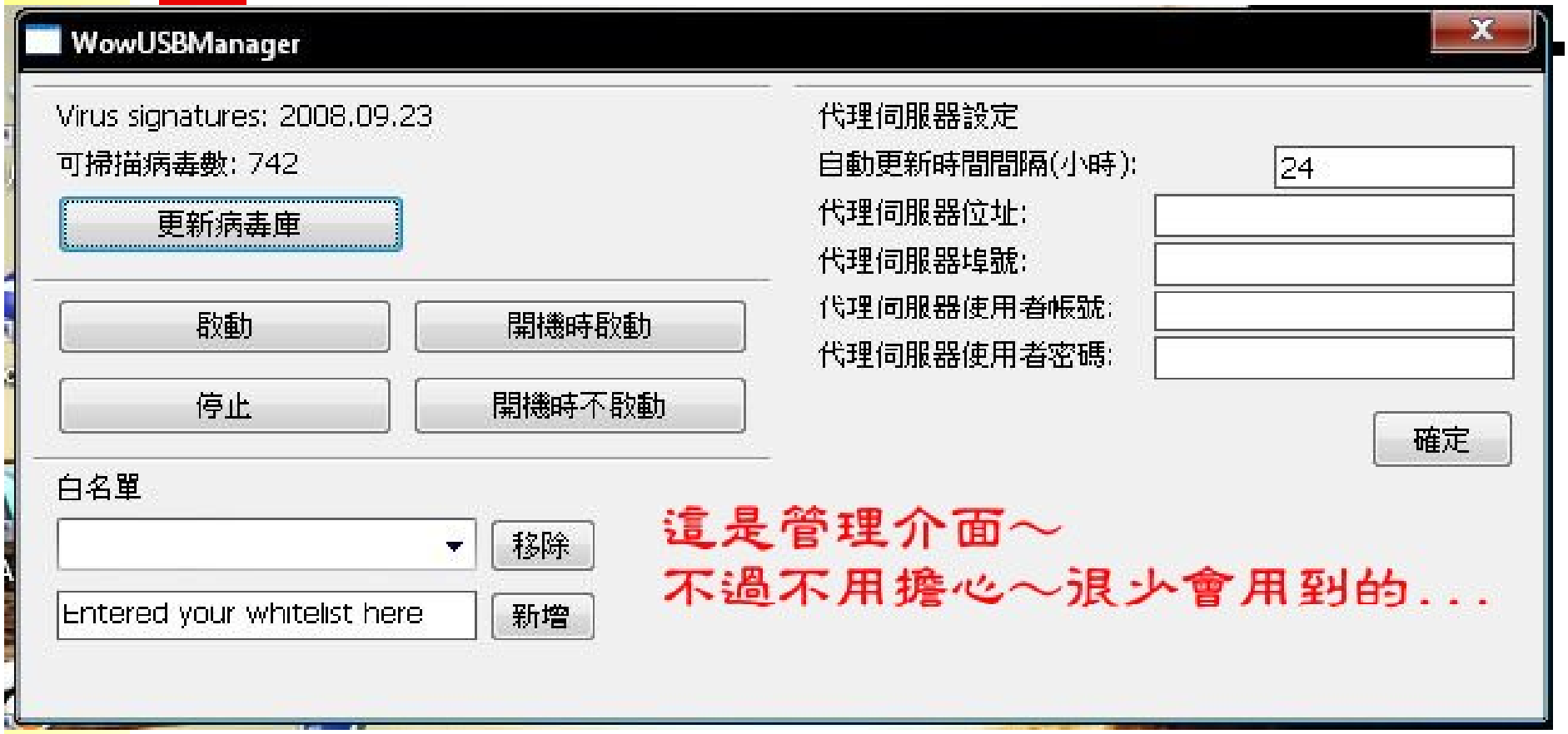


WowUSBProtector

WowUSBProtector

WowUSBProtector

WowUSBProtector



WowUSBProtector

- 以後使用可攜式儲存媒體，如：隨身碟、光碟片、行動硬碟等等，Wow都會自動進行偵測。並跳出如下視窗：

網路芳鄰

網路芳鄰漏洞

- 2005年在網路大流行的病毒，如myDoom、Netsky，除了以往的電子郵件之外，也出現變種透過網路芳鄰、P2P傳播等共享資料匣的服務來傳遞。此類傳染途徑結合「社交工程」（social engineering）使病毒散佈情況更為嚴重。
- 共享服務不是新傳染技術，不過卻因結合「社交工程」而使得病毒防堵難上加難。社交工程是一種利用人的互動行為來傳播的傳染方式。社交工程過去是真正產生人的互動，如向IT人員誘騙出總經理電腦的密碼，轉變電子郵件偽裝出特定主旨、附檔名稱，利用人性的弱點，使電腦使用者被騙而打開郵件或附檔。

不要用網路芳鄰共享資料夾。

- 病毒會利用網路芳鄰作散播的途徑，感染其他電腦共享資料夾中的檔案。
- Windows NT/2000/XP安裝完成後，預設會把電腦中全部資料夾分享於網路上，造成資料被竊取及破壞。
- 若要檢查電腦目前已分享了哪些資料夾，請在Windows的「開始」→「執行」→輸入“cmd”，再輸入“net share”即可。
- 關閉預設分享資料夾之方法

關閉預設分享資料夾之方法

- 注意：下列操作會更動 Windows 作業系統之重要檔案，若操作有誤，有可能會導致無法開機或作業系統損毀，請使用者自行評估風險。
- 於「開始」→「執行」→ 輸入「regedit」，打開下列路徑：
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
  增加一個 「REG_DWORD」 的類型，名稱為 AutoShareServer (大小寫需相符)，值設定為「0」，然後重開機即可生效。

如何關閉「網路芳鄰」？

- 「控制台」→「網路和網際網路連線」→「網路連線」→「區域連線」→「一般」→取消以下元件：
  - Client for Microsoft Networks
  - File and Printer Sharing for Microsoft Networks
- 「控制台」→「網路和網際網路連線」→「網路連線」→「區域連線」→「一般」→「Internet Protocol(TCP/IP)」→「內容」→「進階」→「WINS」→停用[NetBIOS over TCP/IP]

如何關閉「網路芳鄰」?

- 「控制台」→「效能及維護」→「系統管理工具」→「服務」→找到以下服務項目,將其更換為手動或停用
  - Messenger
  - TCP/IP NetBIOS Helper Services

病毒預防與治療

預防電腦病毒的方法

- 不要使用盜版軟體。目前沒有百分之百的防毒方式。
- **經常修補window漏洞，windows updated。**
- **選擇功能完善的防毒軟體，定期檢查電腦並定時更新病毒碼。**
- 盡量使用硬碟開機。因為磁片的流通性很大，所以很難確保它的啟動磁區是否無毒。
- **勤於更新密碼注意密碼取用原則以防止他人偷竊使用，並加以「惡作劇」。(假設你的所有資訊可能被有心人知道，密碼一定要不同)**
- 不抄襲或拷貝來歷不明的電腦軟體，以免感染。

預防電腦病毒的方法

- **定期將重要程式與資料檔案備份保存**，並定期更新資料內容。
- 如發現程式或資料已受病毒感染，**則該程式或資料必須立即隔離**，切忌再用，以免病菌蔓延，並應立即消毒，找出病源。
- 設定執行檔為唯讀(Read only)，以避免被寫入病毒程式。
- 不要隨意到別人的網路下載軟體回來使。
- **收到內含附加檔案的電子郵件時，可以先另存新檔，在經過測試之後才開啟它。**
- **製作還原光碟，以備不時之需。**
- 注意正確設定資源分享。

防毒及防駭網站

- CERT　http://www.cert.org/
- GSN-CERT/CC　http://gsn-cert.nat.gov.tw/
- 國家資通安全會報資通安全技術服務中心
  http://www.icst.org.tw/
- 趨勢科技個人電腦防毒網站
  http://www.trendmicro.com/tw/
- 賽門鐵克諾頓防毒網站
  http://www.symantec.com/region/tw/
- 金帥防毒網站　http://www.ggreat.com.tw/

防毒及防駭網站

- MCAfee http://www.mcafee.com/tw/default.asp
- 台灣電腦網路危機處理中心：http://www.cert.org.tw/
- 台灣微軟網站

  http://www.microsoft.com/taiwan/support/content/Security%20Patch%20index.htm

  http://www.microsoft.com/taiwan/security/bulletins/(最新資訊安全公告)

免費線上病毒掃瞄

- 防毒軟體名稱：Kaspersky
  - http://www.kaspersky.com/service?chapter=161739400
- 防毒軟體名稱：Norton
  - http://security.symantec.com/sscv6/home.asp?langid=ch&venid=sym&plfid=23&pkj=LNUVWYDMGJCDBXWVPGC
- 防毒軟體名稱：PC-cillin
  - http://housecall.antivirus.com/housecall/start_corp.asp

結語

- 具有正確的使用習慣
- 即時修補安全漏洞
- 正確設定資源共享
- 設定複雜的帳號密碼
- 即時防毒軟體更新