『資訊保安和防止資料洩漏』公開研討會

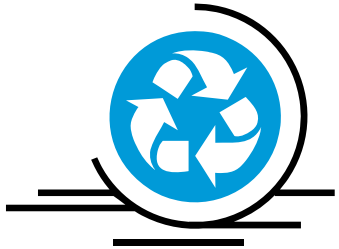
無線網絡保安

by

Professional Information Security Association (PISA)
專業資訊保安協會

楊和生
ws.young@pisa.org.hk

28-May-2010



關於 PISA

關於 PISA

- 非牟利組織
- 由一班資訊保安人員成立
- 宗旨
  - 提高大眾的資訊保安意識
  - 資訊保安技術交流
  - 關注資訊保安在香港和世界的發展
- 網址
  - http://www.pisa.org.hk
- 入會資料
  - http://www.pisa.org.hk/membership/member.htm

開　始

最近新聞

Google惹起軒然大波

2010-05-17

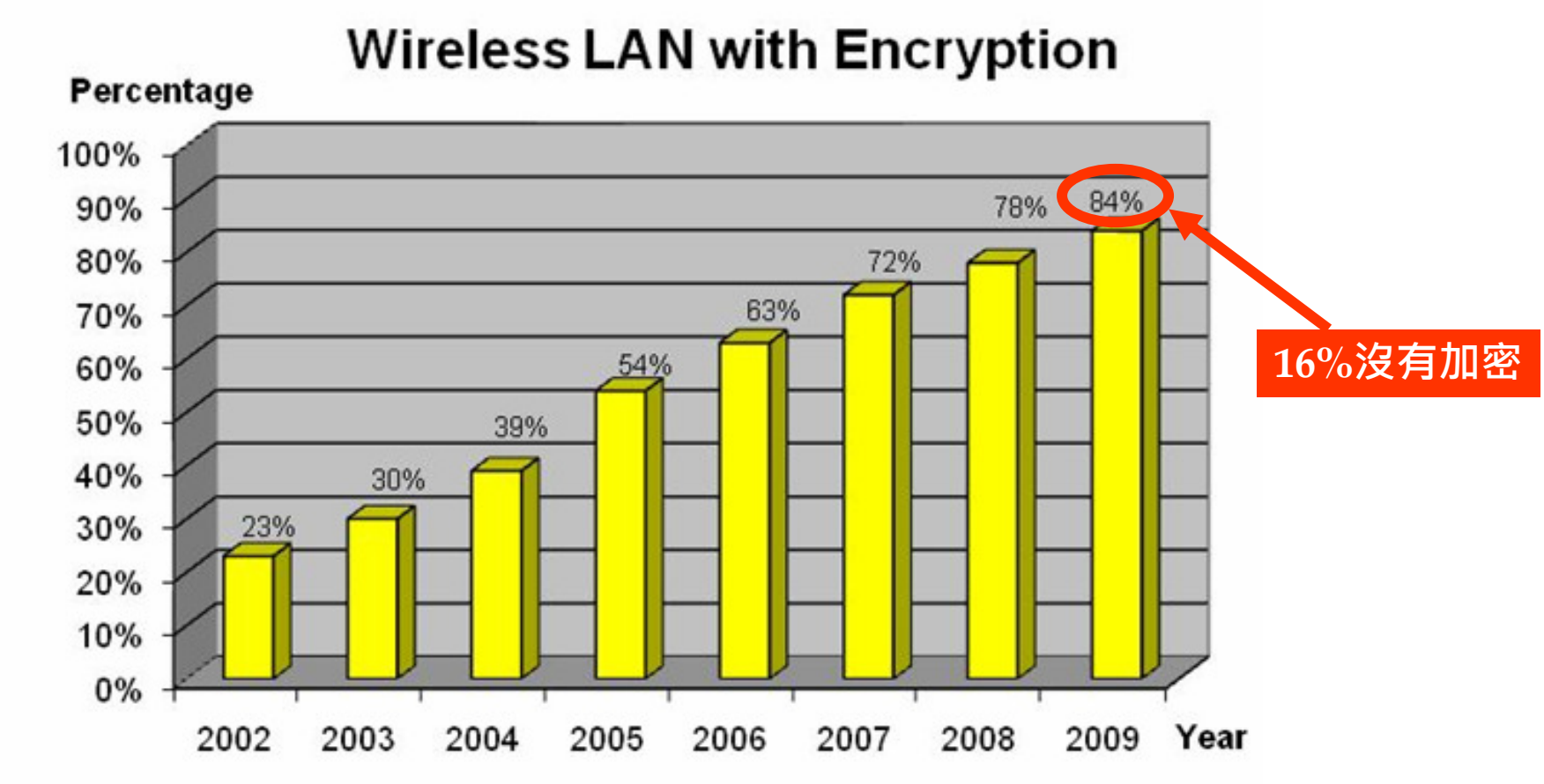
頭條日報 曾聲稱不滿黑客入侵，侵犯電郵用戶私隱而撤出內地市場的互聯網搜尋器Google，日前被揭發過去四年來在全球三十多個國家及地區，包括在香港進行地圖街景資料收集時，誤取Wi-Fi用戶資料，有網民憂心資料被人不法使用，日後會多加留意。

Google官方網誌中表示，最近德國漢堡當局要求谷歌抽查拍攝「街景地圖」服務時，有否截取個人資料，揭發Google〇六年起利用車隊在全球國家及城市拍攝街景及蒐集街道資訊時，同時展開搜集Wi-Fi熱點基本資料的工作，過程中意外截取未經加密處理的個人資料，數據存量高達六百GB，但未有表明截取內容，強調只是零碎數據。外界估計包括電郵內容、圖片及網頁瀏覽歷史等。

事件引起軒然大波，Google隨即停止拍攝車收集Wi-Fi資訊，以及將數據隔離，禁止其他人接觸，以便日後安排第三方進行調查及確保資料被刪除。

香港無線網絡安全情況

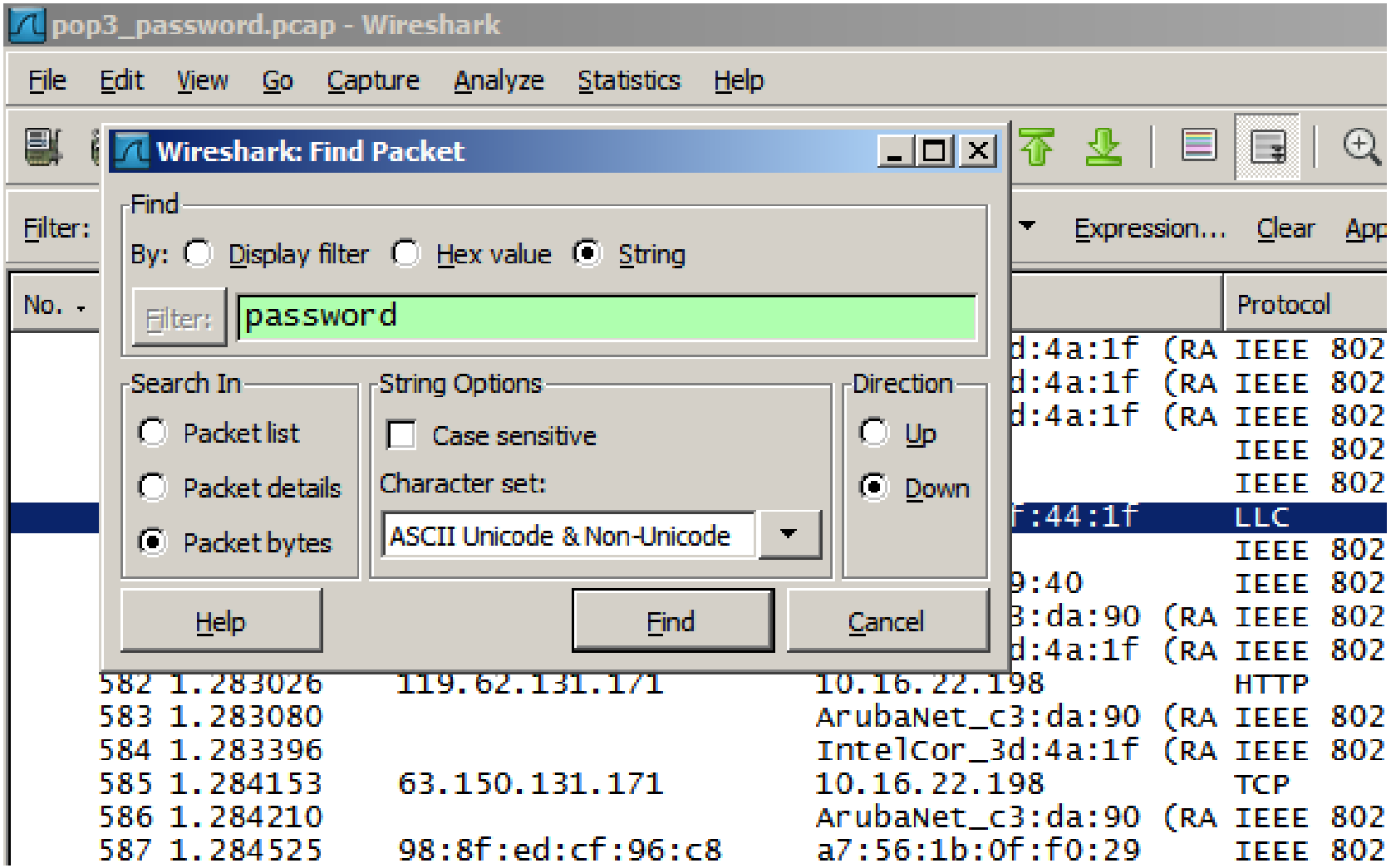
Wi-Fi Security Survey 2009 conducted PISA & WTIA, sponsored by OFTA



沒有加密的風險

- 網上活動可被偷看
  - 電郵內容
  - 使用密碼
  - 即時通訊(IM)對話
  - etc

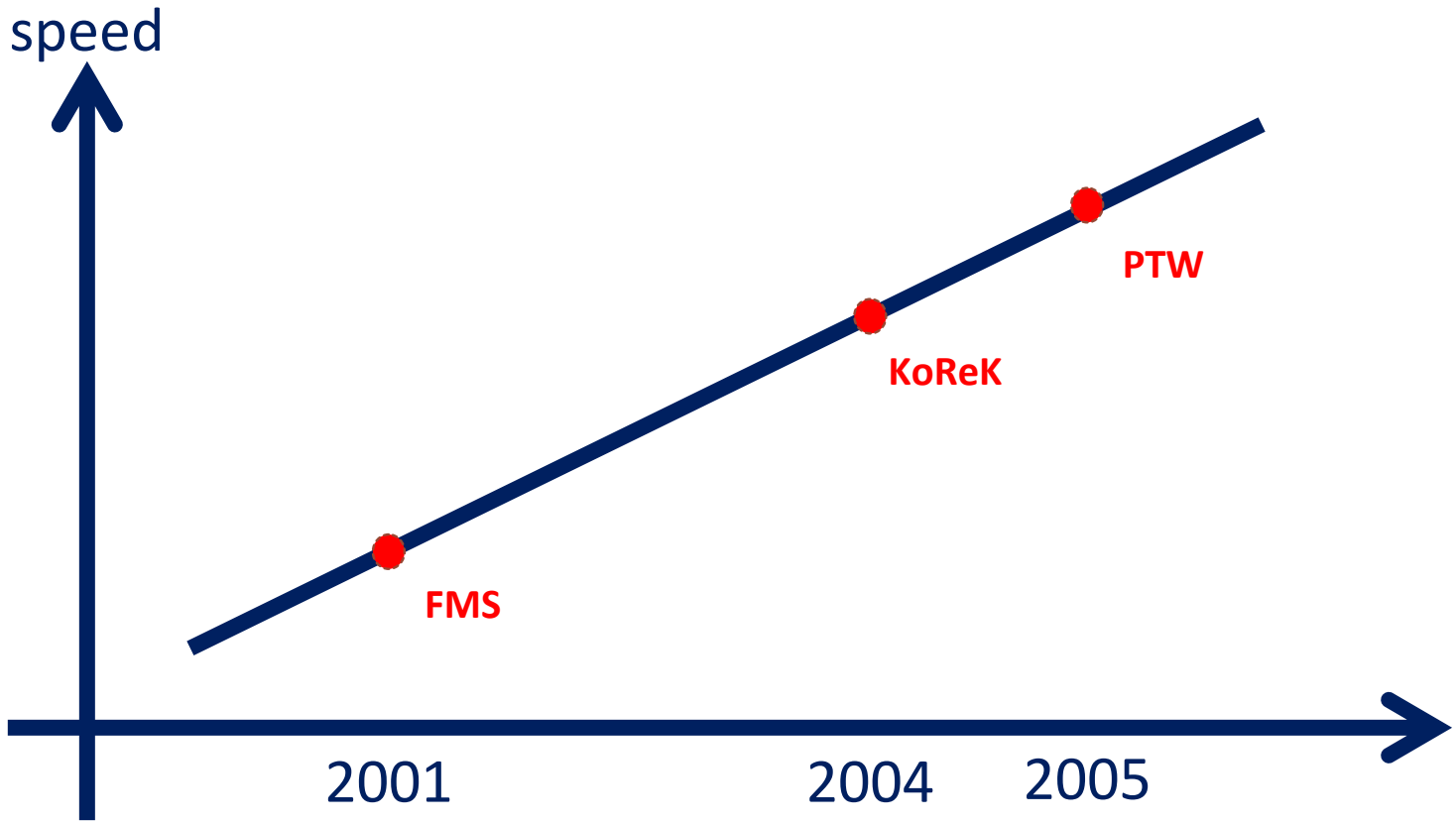
WiFi Sniffing Demo



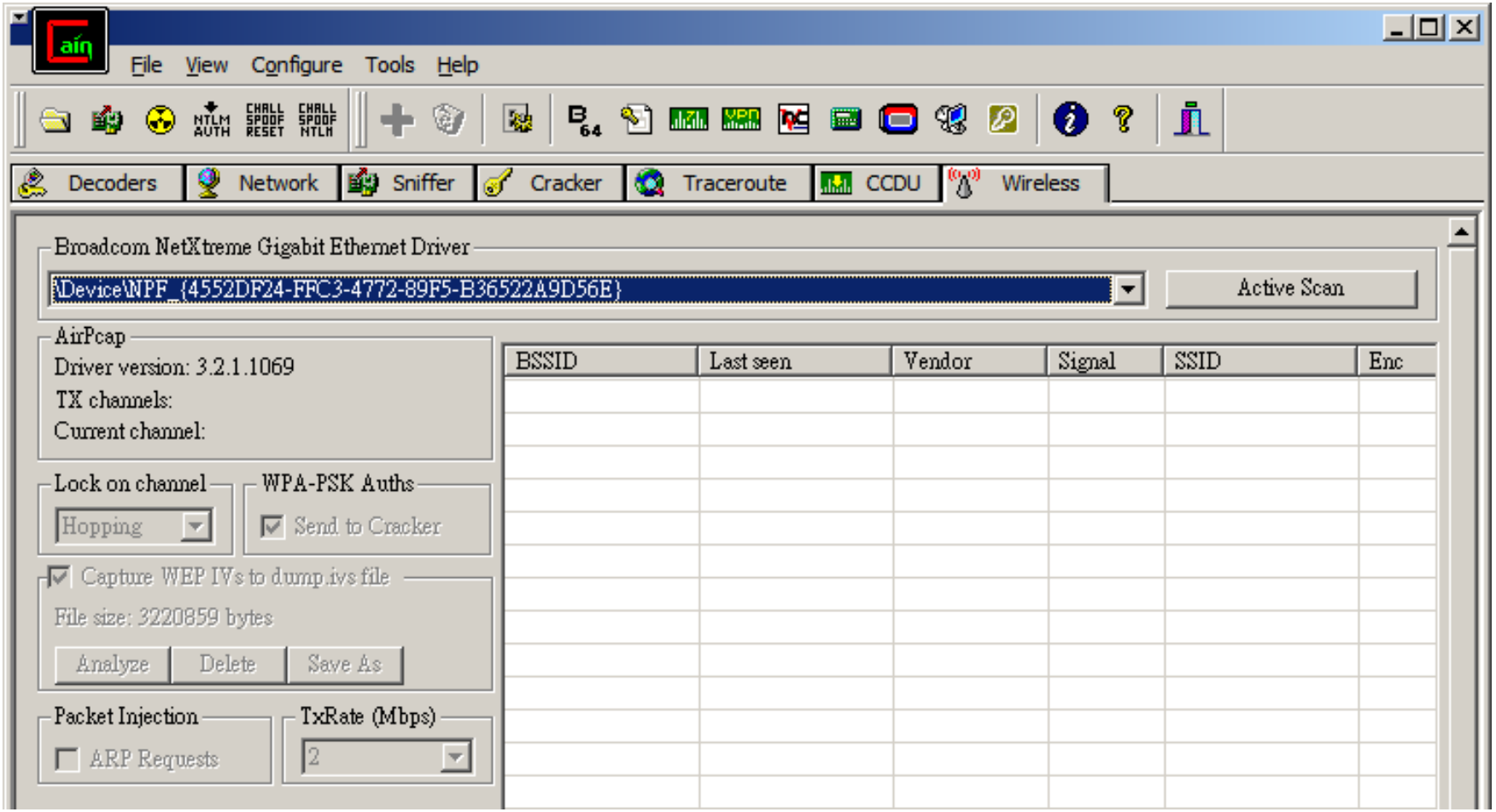
加密:不等於安全

- 無線網絡加密法
  - WEP → 2001年發現有漏洞
  - TKIP → 2008年發現有漏洞
  - AES

WEP破解歷史



WEP破解示範

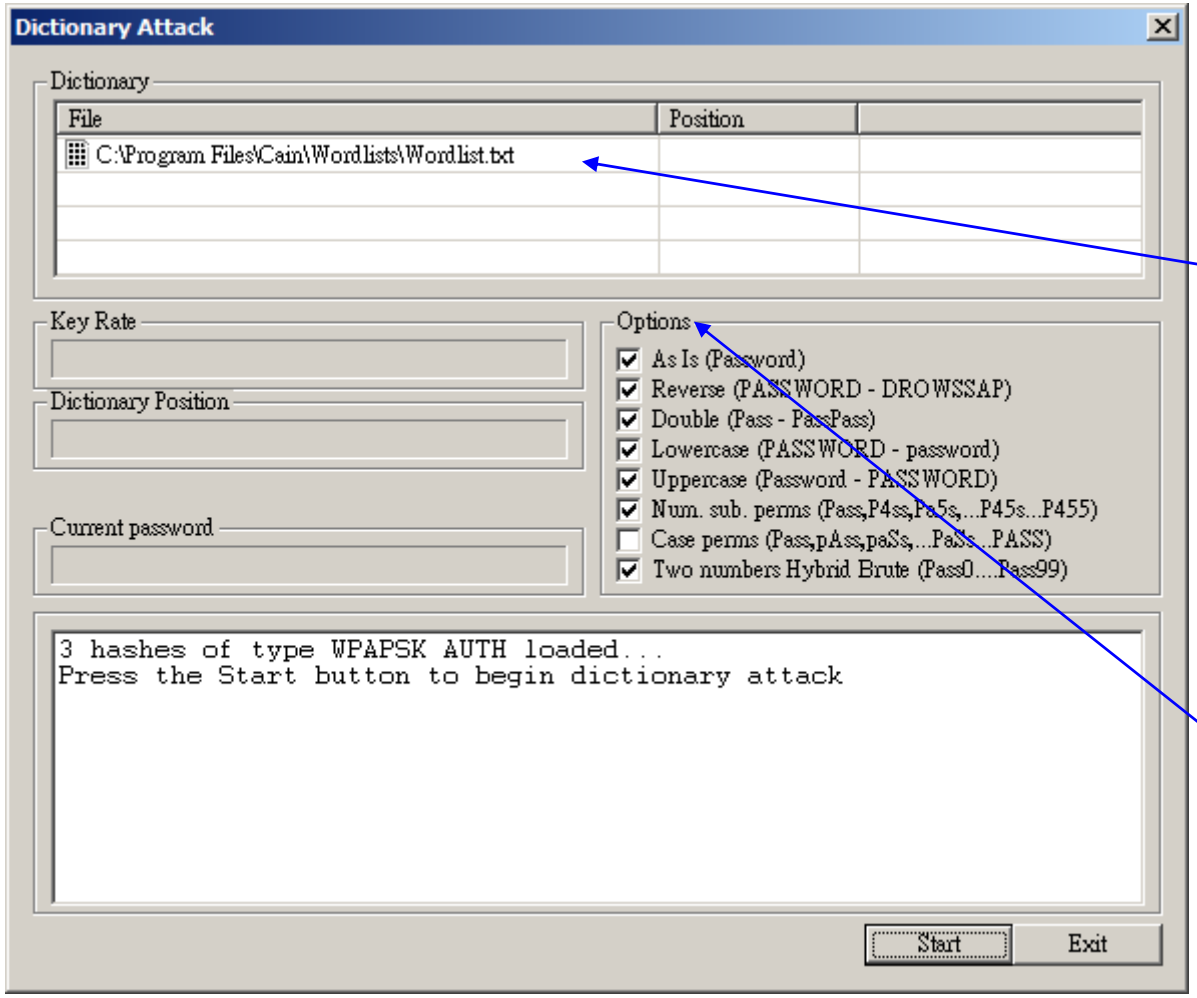

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless
Broadcom NetXtreme Gigabit Ethernet Driver
\Device\NPF_{4552DF24-FFC3-4772-89F5-B36522A9D56E}
Active Scan
AirPcap
Driver version: 3.2.1.1069
TX channels:
Current channel:
Lock on channel
Hopping
WPA-PSK Auths
Send to Cracker
Capture WEP IVs to dump.ivs file
File size: 3220859 bytes
Analyze
Delete
Save As
Packet Injection
ARP Requests
TxRate (Mbps)
2
BSSID
Last seen
Vendor
Signal
SSID
Enc

使用PSK注意事項

- WPA-PSK
- WPA2-PSK

- **問題所在: 使用不安全密碼**

破解PSK密碼示範



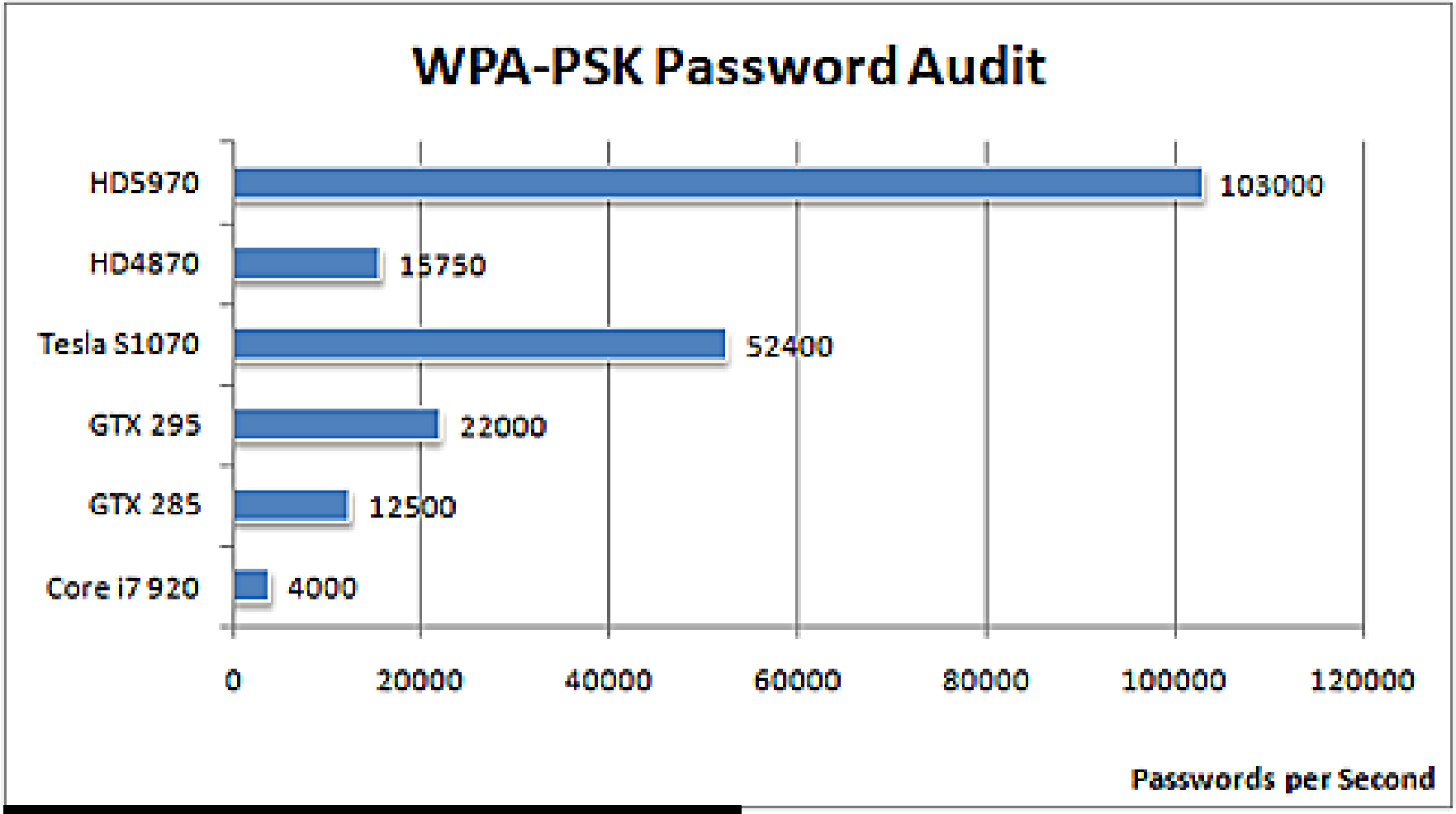
Dictionary file(s)

Modification Options

能否增加速度嗎?

- 新方法: General Purpose GPU Computing (GPGPU).
  - 利用顯示咭來加快運算
  - 例子: AMD/ATI 或 Nvidia

專用軟件



http://www.elcomsoft.com/ewsa.html

Rainbow Table 破解

- 預先計算一個對照表
  - 參照對照表比即時運算快
- 針對一些用戶使用
  - 常見的網名(SSID): default, linksys etc…
  - 使用不安全的密碼
- 現時可下載的Rainbow Table特點
  - 40G容量
  - 1000 SSIDs
  - ~1,000,000 密碼

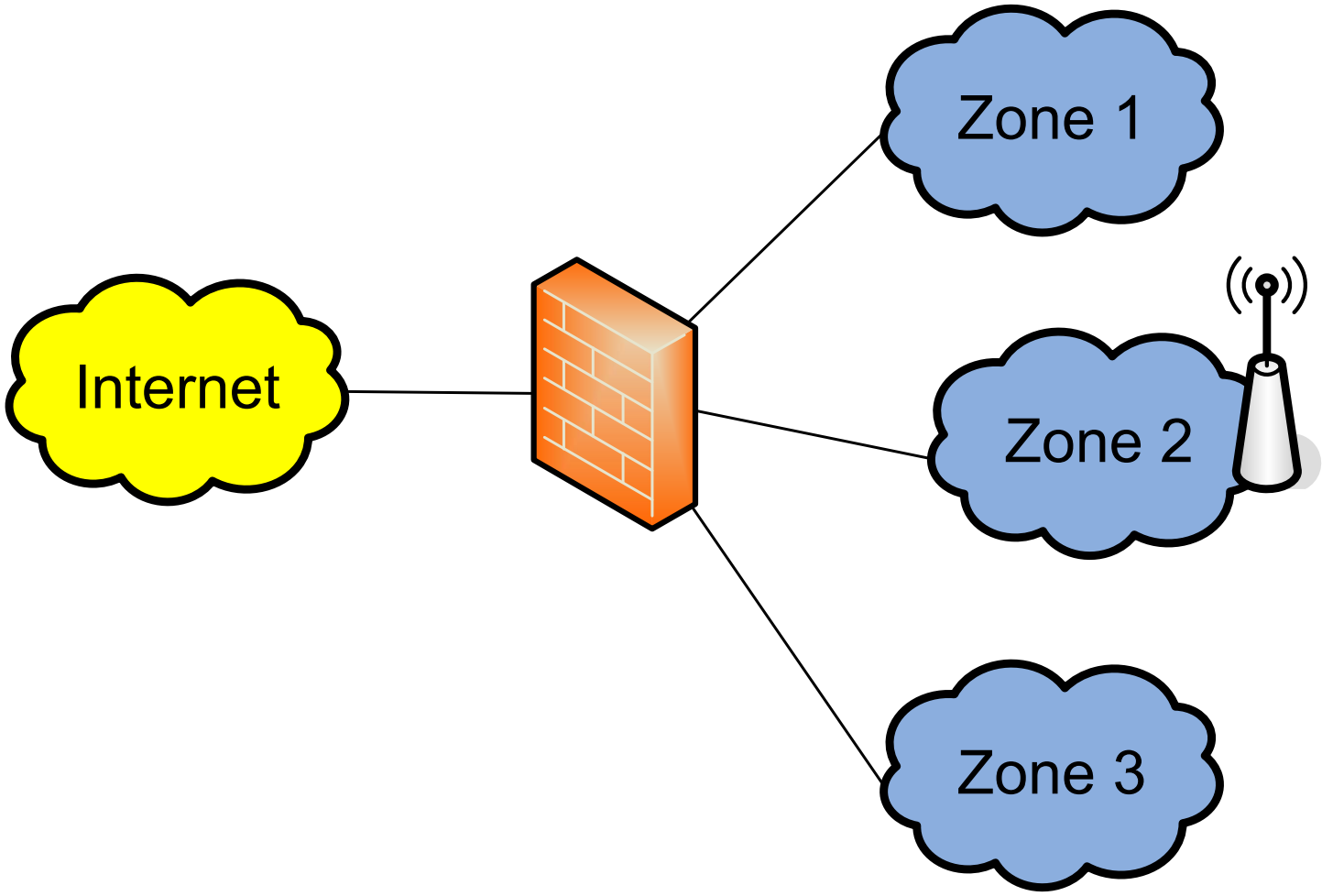
雲端服務

- 破解 WPA or WPA2 PSK
  - 400部電腦組成
  - 20 時間
  - 測試135,000,000 組合
  - 價錢: $34

架設無線網絡注意事項 (1)

- 使用最安全加密技術
  - WPA-PSK/AES
  - WPA/AES
- 網絡名稱(SSID)
  - 更改網絡名稱
  - 不要廣播網絡名稱 (Disable SSID Broadcast)
- 使用安全密碼
  - 管理員密碼
  - PSK的密碼

架設無線網絡注意事項 (2)



使用公共無網絡又如何?

公共熱點 (Hotspot)

- 公共熱點:提供無線上網的公共地方
  - 機場
  - 酒店
  - 咖啡室
  - 餐廳
  - 商場
  - 鐵路
  - 巴士

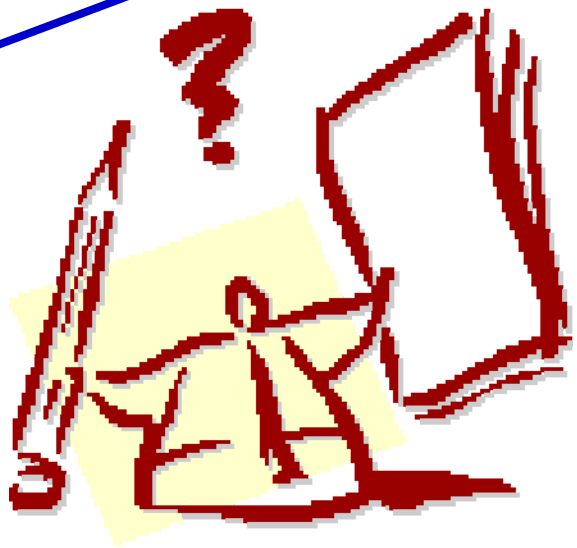
Hotspot Security Threats

- 大部份沒有加密
- 真?假? (Evil Twin)

Evil Twin


選擇一個無線網路
按下列清單中的一個項目來連線到範圍內的無線網路或取得其他資訊(W)
PCCW
自動
無安全性的無線網路
Y5ZONE
自動
無安全性的無線網路
Lo Family
啓用安全性的無線網路
TOPCON
啓用安全性的無線網路
freegovwifi
無安全性的無線網路

真? 假?



Evil Twin

Legitimate AP
Network Name = PCxW

Fake AP
Network Name = PCxW

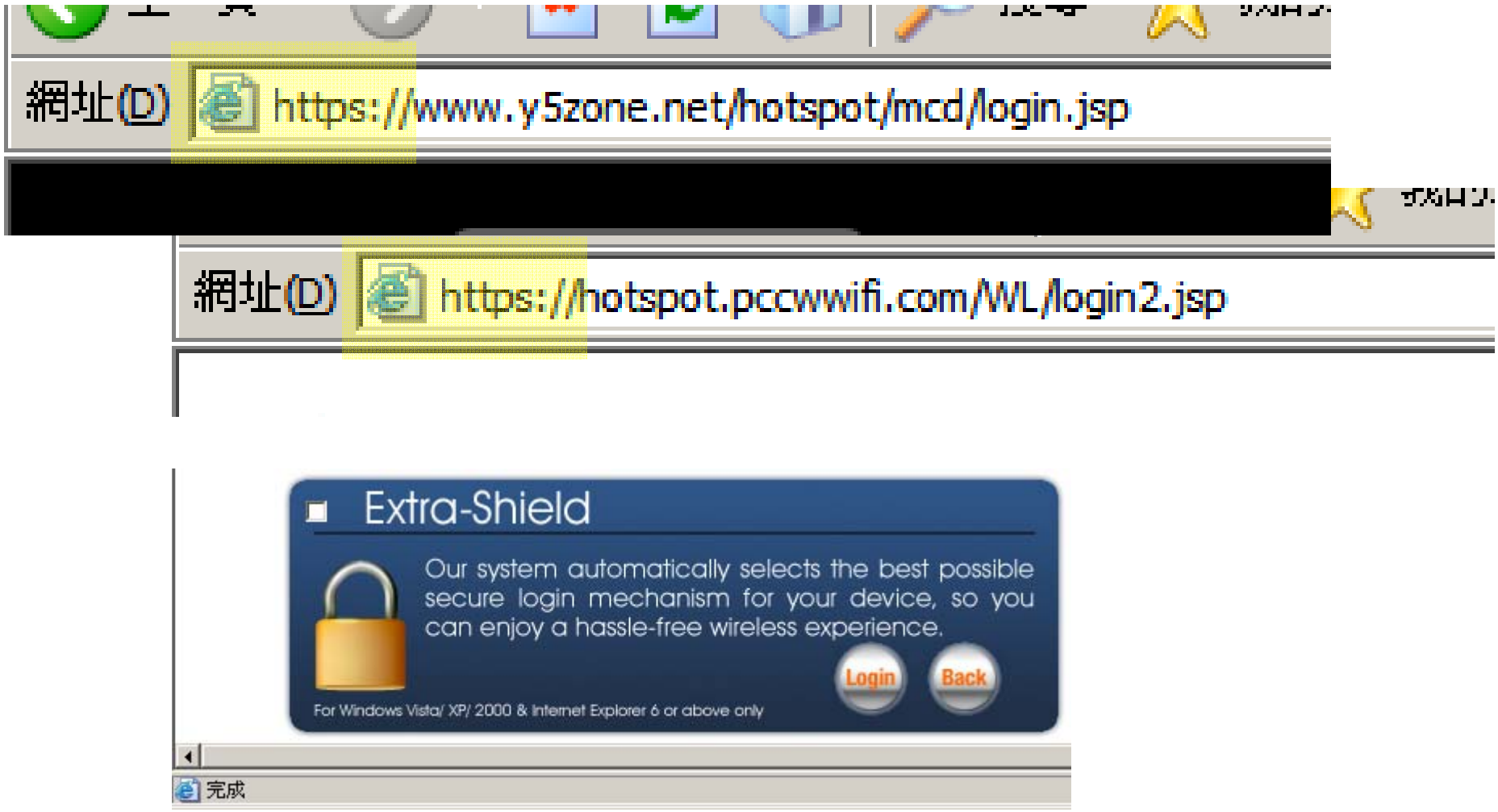
使用公共熱點小貼士

- 確保電腦已安裝最新的安全修補程式
- 確保電腦上的防毒軟件已經更新
- 電腦防火牆經已啟動
- 不共用所有資料夾
- 應理重要資料時要加密
- 當不用無線網絡時，把它關掉
- 要認清楚公共熱點首頁的特性
- 其他資料: http://www.safewifi.hk

加密的特徵


Gmail: Google 提供的電子郵件服務 - Windows Internet Explorer
https://www.google.com/acc
Learn more
Browser connection:
Always use https
Don't always use https
Learn more
Save Changes
www.google.com
Security Padlock
Internet

公共熱點供應商首頁的例子

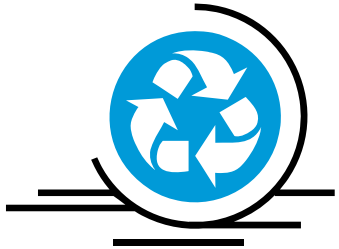


使用無線公共熱點(Public Hotspot)

使用安全的無線公共熱點

My Own Computer

Beware of
Shoulder Surfers



Q & A