



Wi-Fi 無線網路安全與防護新知

中華電信資訊技術分公司

2024/05

大綱

1. 為什麼要用無線網路?
2. 無線網路簡介
3. 無線網路的弱點
4. 如何加強無線網路安全
5. 結語



1. 為什麼要用無線網路?

有線網路麻煩之處

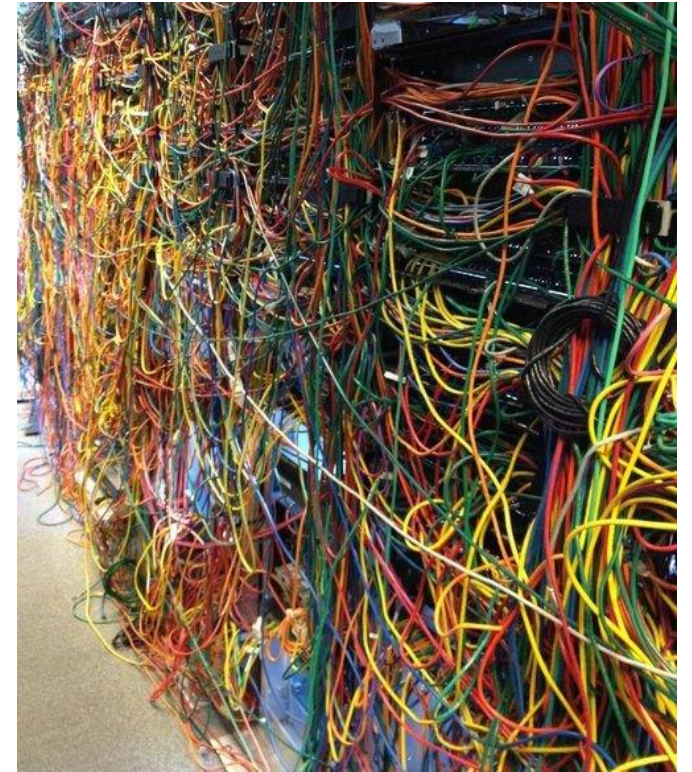
- 無法隨時隨地存取、移動受限、整線麻煩
- 所以人類發明無線網路技術
 - 區網: Wi-Fi
 - 行動: 2.5G、3G、3.5G、4G (LTE)、5G



資料來源: Business Insider



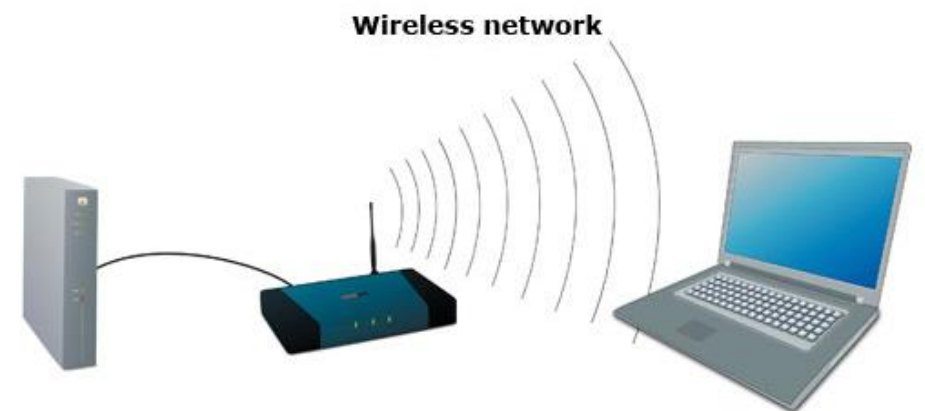
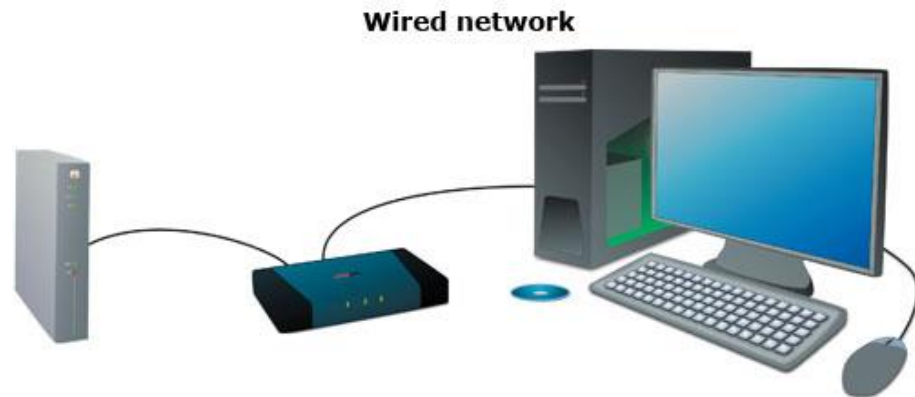
資料來源: Network World



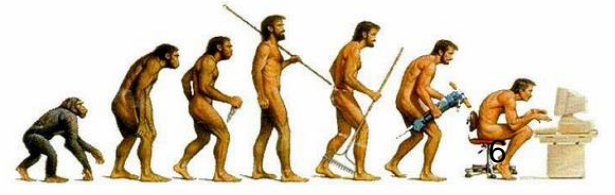
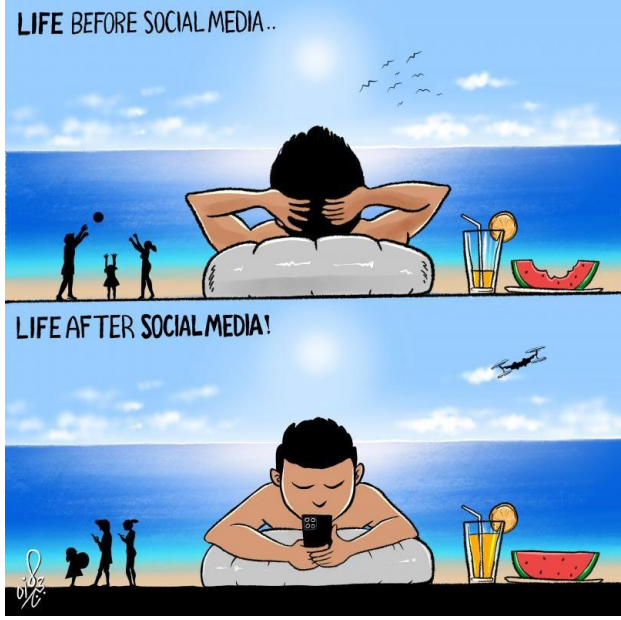
資料來源: @Fibrestore

有線網路 VS. 無線網路

議題	有線網路	無線網路
自由移動	定點，需要網路線連接網路埠	在收訊範圍內可自由移動、存取
網路線	需要足夠的網路線與網路埠	採無線傳輸，終端裝置不需接線
連接速度	較快	較慢 (較新技術已接近有線的速度)
安全性	較好，需要接線才能竊聽	較差，在無線電波範圍內就可竊聽 (有加密功能可補強)
可靠性	較好	較差，易受干擾
架設成本與難度	都需要花費成本與人力建置	都需要花費成本與人力建置

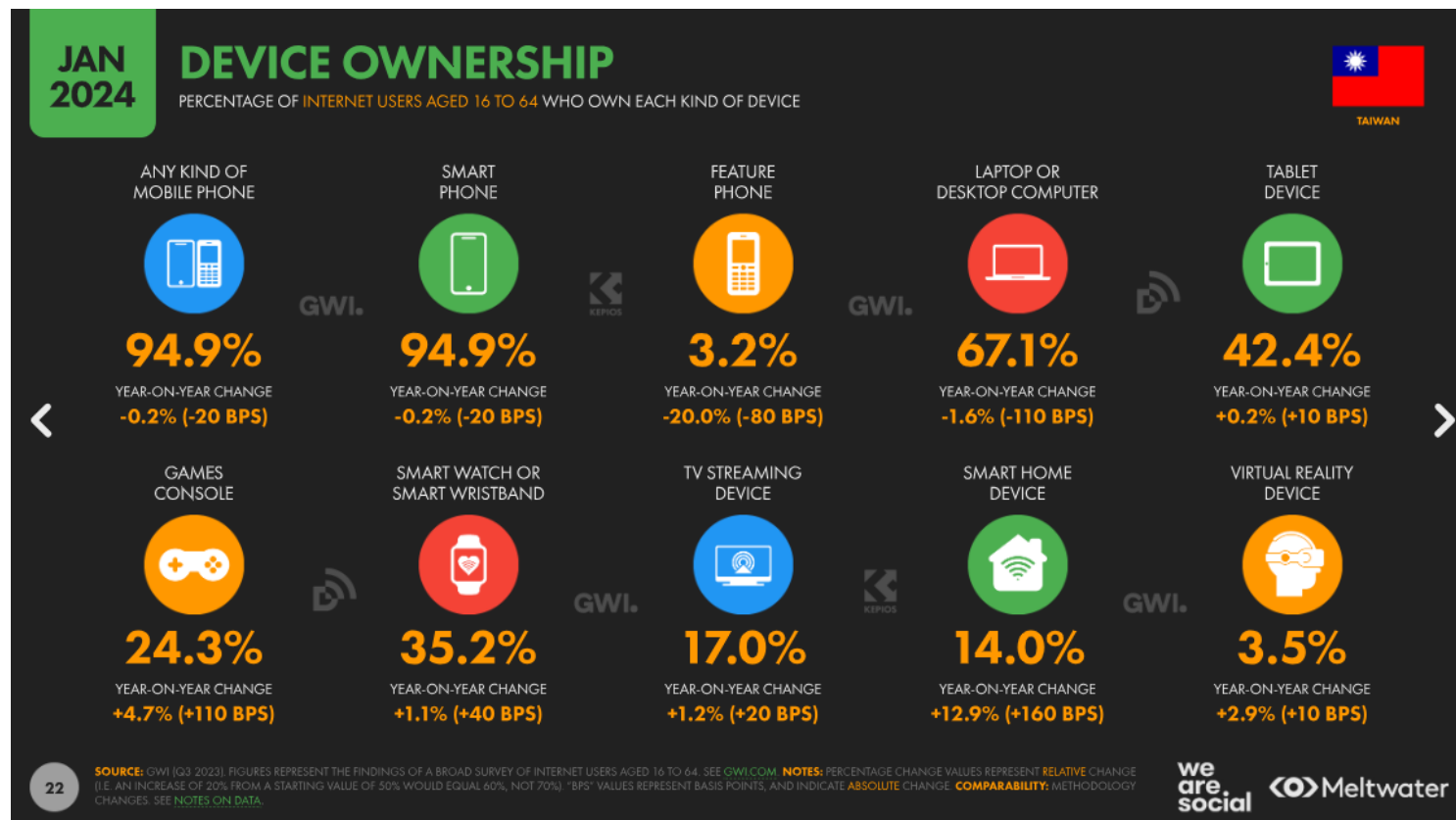


人類已離不開網路與智慧裝置



台灣數位使用概況

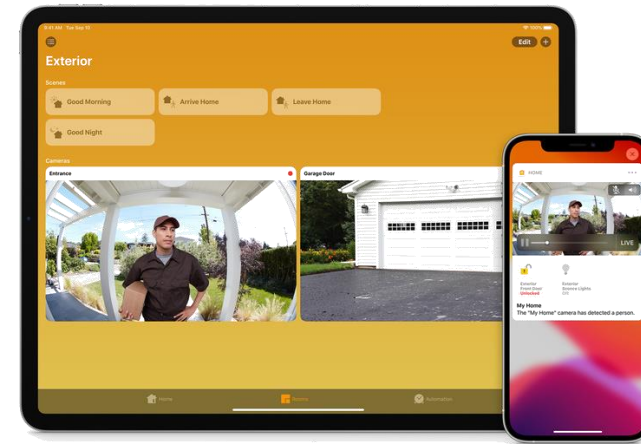
- 台灣上網人口有2171萬
占整體人口比例**90.7%**
- 16至64歲人口
 - **94.9%** 有智慧型手機
 - 67.1% 有筆記型電腦
 - 42.4% 有平板電腦
 - 35.2% 有智慧手錶或手環
 - 17% 有電視串流裝置
 - 14% 有智慧家庭裝置
 - 平均每日花**7小時13分**上網
- 行動上網平均下行網速為**73.31 Mbps**，較前年度增加**7.7%**



越來越多裝置透過 Wi-Fi 互相連接



物聯網透過 Wi-Fi 的智慧家庭中樞服務

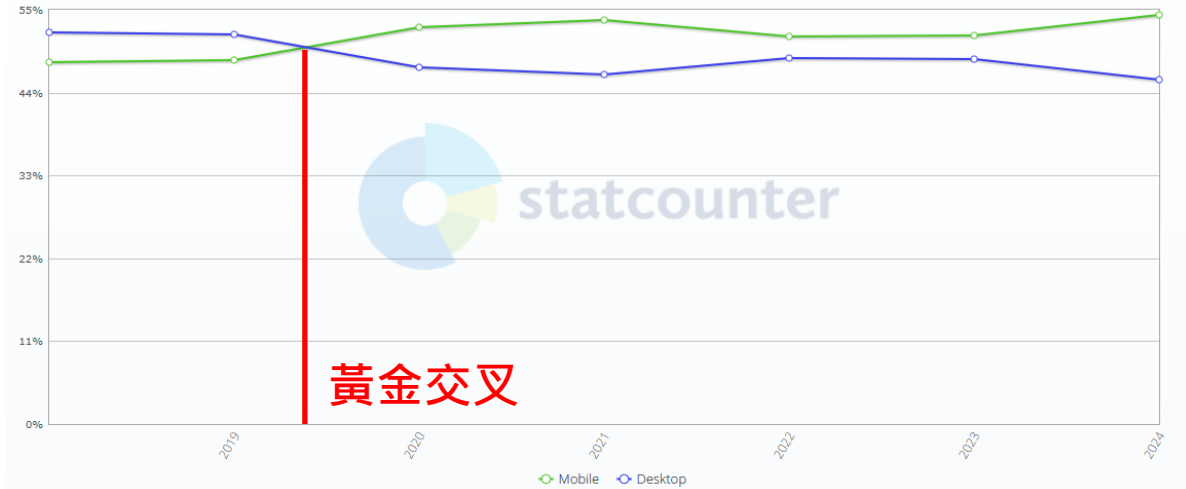


企業為何又要使用無線網路？

- 企業以往認為無線網路乃是**洪水猛獸**，難以管理，因此放棄使用，那為何現在又提出這個觀點？
 - **行動智慧裝置趨勢**
- 根據 StatCounter 針對網路使用流量統計報告指出，使用行動上網首度超越桌機用戶
- 作業系統 Android + iOS 54.75% 大於 Windows 32.69%+ OS X 8.26%
- 為了要使行動裝置，如手機、平板可以使用**企業網路**，具有管理、安全的**無線網路環境**是必須的

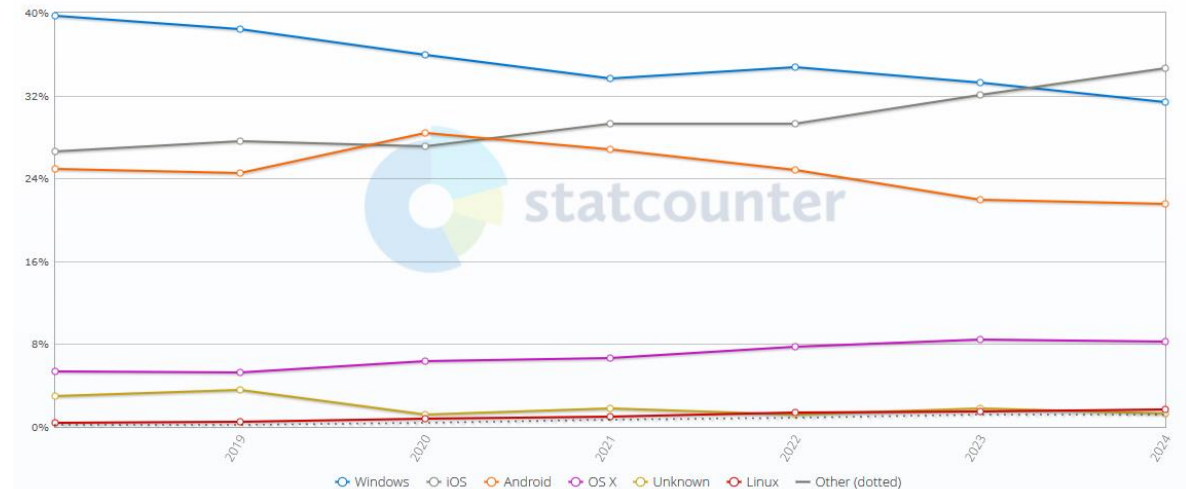
Desktop vs Mobile Market Share Taiwan
2018 - 2024

Edit Chart Data



Operating System Market Share Taiwan
2018 - 2024

Edit Chart Data





2. 無線網路簡介

無線網路歷史

自第二次世界大戰開始

- 無線通訊因在軍事上應用的成果而受到重視，無線通訊一直發展，但缺乏廣泛的通訊標準

IEEE 802.11

- IEEE在1997年為無線區域網制定了第一個版本標準——**IEEE 802.11**。其中定義了媒體存取控制層（MAC層）和物理層

展頻/調頻與紅外線

- 物理層定義了工作在2.4GHz的ISM頻段上的兩種展頻作調頻方式和一種紅外傳輸的方式，總數據傳輸速率設計為2M bit/s。兩個設備之間的通信可以設備到設備（ad hoc）的方式進行，也可以在基站（Base Station, BS）或者存取點（Access Point, AP）的協調下進行

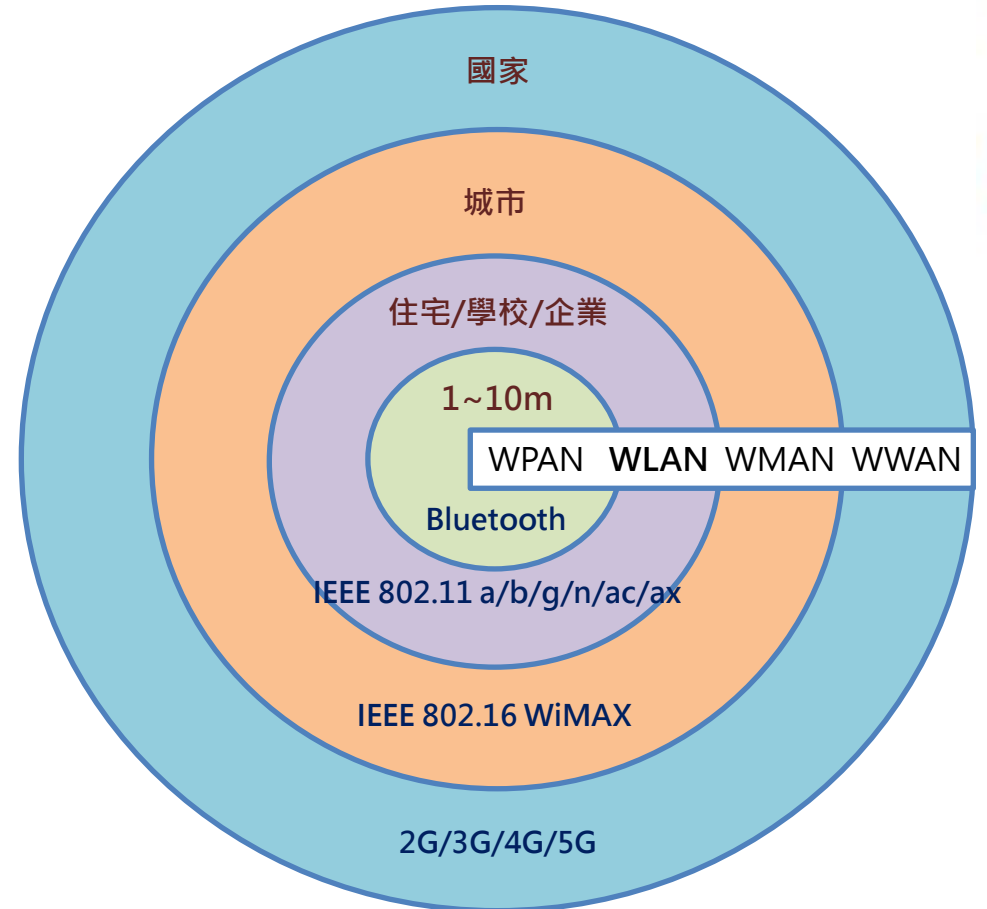
CSMA/CA

- 為了在不同的通訊環境下取得良好的通訊品質，採用CSMA/CA（Carrier Sense Multi Access/Collision Avoidance）硬體溝通方式

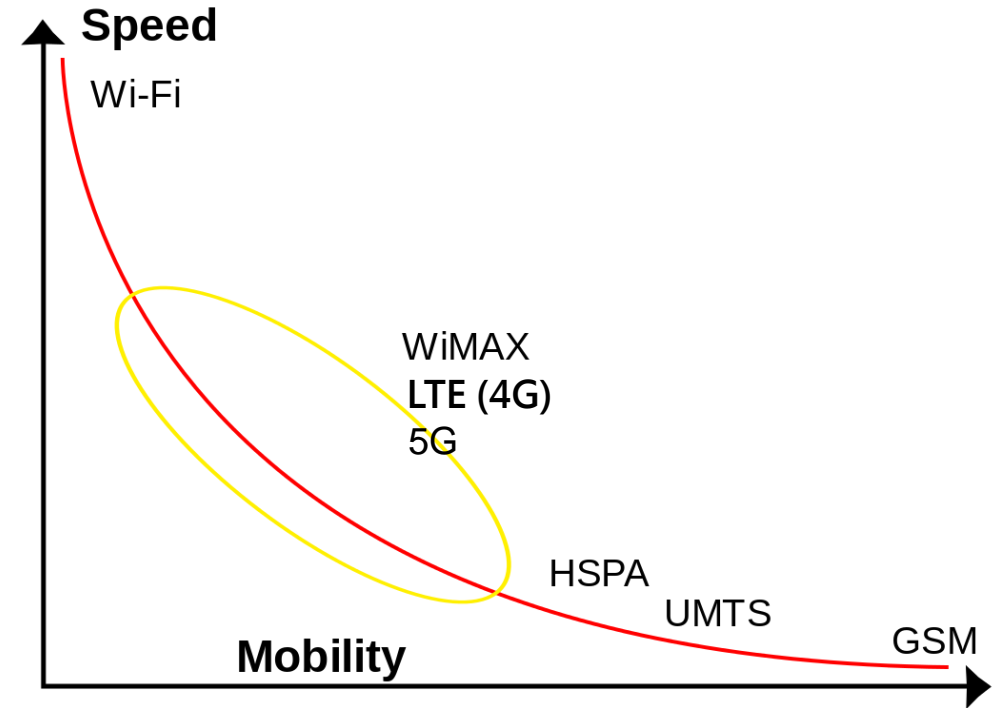
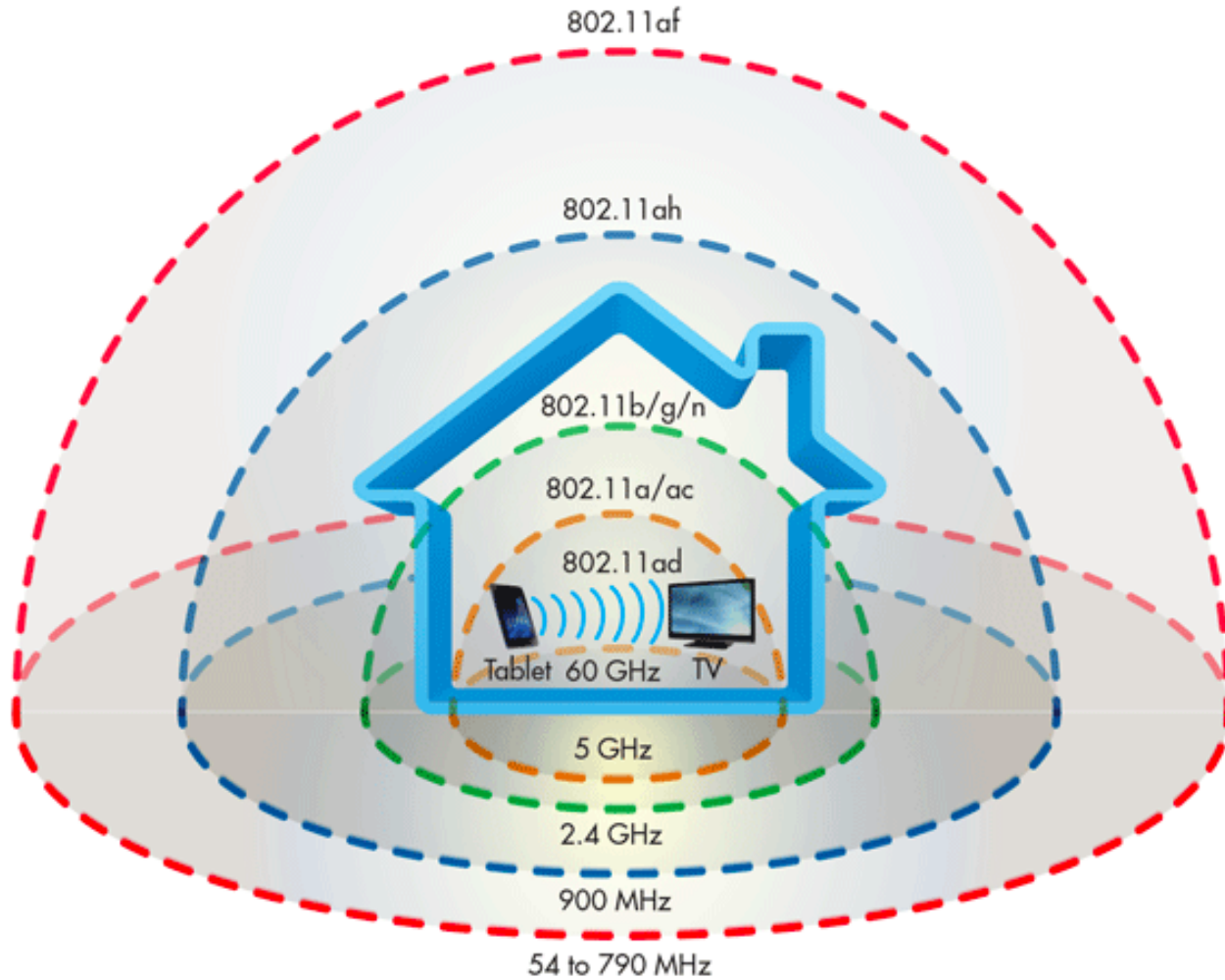


無線網路種類與範圍

- 無線個人網路WPAN
(Wireless Personal Area Network)
- **無線區域網路WLAN**
(Wireless Local Area Network)
- 無線都會網路WMAN
(Wireless Metropolitan Area Network)
- 無線廣域廣路WWAN
(Wireless Wide Area Network)



無線網路種類與範圍



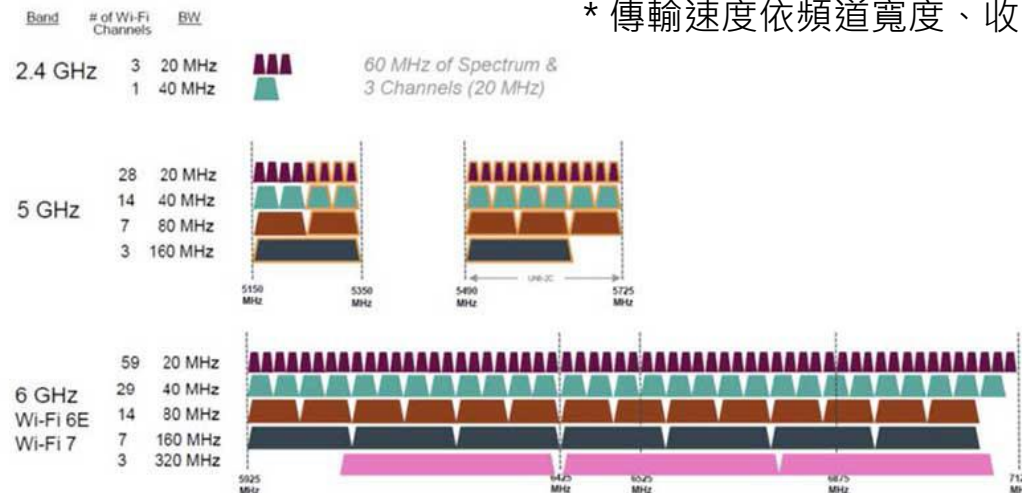
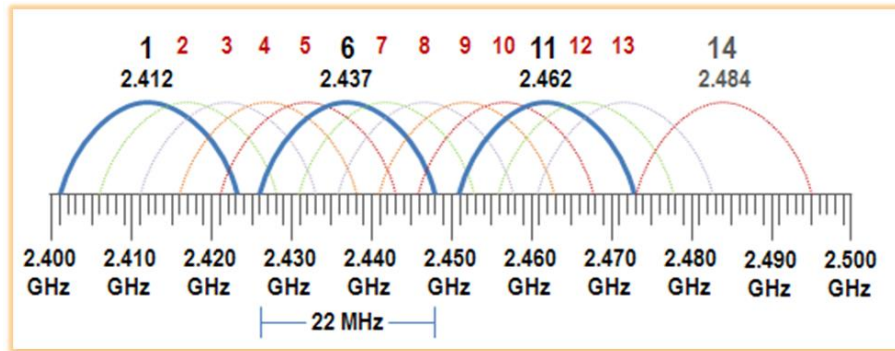
★ 無線網路標準 802.11 系列

- 802.11 : 1997年，原始標準(2 Mbps @ 2.4 GHz)
- 802.11a : 1999年，實體層補充(54 Mbps @ 5 GHz)
- 802.11b : 1999年，實體層補充(11 Mbps @ 2.4 GHz)
- 802.11c : 符合802.1D的媒體接入控制層(MAC)橋接(MAC Layer Bridging)
- 802.11d : 根據各國無線電規定做的調整
- 802.11e : 對服務品質(Quality of Service, QoS)的支援
- 802.11f : 基地站的互連性(Interoperability)
- 802.11g : 實體層補充(54 Mbps @ 2.4 GHz)
- 802.11h : 無線覆蓋半徑的調整，室內(indoor)和室外(outdoor)頻道(5 GHz頻段)
- 802.11i : 安全和認證(Authentication)方面的補充
- 802.11n (Wi-Fi 4) : 提供更高傳輸速率，基礎速率提升到72.2 Mbps，可以使用雙倍頻寬40 MHz，此時速率提升到150 Mbps。支持多輸入多輸出技術(Multi-Input Multi-Output, MIMO)
- 802.11ac (Wi-Fi 5) : 802.11n的繼承者，提供更高傳輸速率，當使用多基站時將無線速率提高到至少1 Gbps，將單頻道速率提高到至少500 Mbps
- 802.11ax (Wi-Fi 6) : 支援從1 GHz至5 GHz的所有ISM頻段，包括目前已使用的2.4 GHz和5 GHz (5.8 GHz) 頻段，向下相容 IEEE 802.11a/b/g/n/ac。目標是支援室內室外場景、提高頻譜效率。其相比802.11ac，密集使用者環境下實際吞吐量提升4倍，標稱傳輸速率提升37%，延遲下降75%
- 802.11ax (Wi-Fi 6E) : E表示延伸，與Wi-Fi 6一樣使用802.11ax連接，不同之處在於增加6 GHz的可用頻段，最多有額外7個160 MHz的頻道，該頻段較不易受到干擾，可帶來更好的連線效能



無線網路標準 – 實際應用

協定	發布年份	頻率	頻道寬度	理論最大傳輸率	範圍 (室內)	範圍 (室外)
Legacy	1997	2.4 GHz	20 MHz	2 Mbps	約20m	約100m
802.11a	1999	5 GHz	20 MHz	54 Mbps	約35m	約120m
802.11b	1999	2.4 GHz	20 MHz	11 Mbps	約35m	約120m
802.11g	2003	2.4 GHz	20 MHz	54 Mbps	約38m	約140m
802.11n (Wi-Fi 4)	2008	2.4 / 5 GHz	20、40 MHz	72 – 600 Mbps *	約70m	約250m
802.11ac (Wi-Fi 5)	2014	5 GHz	20、40、80、160 MHz	433 – 6933 Mbps *	約70m	約250m
802.11ax (Wi-Fi 6)	2019	2.4 / 5 GHz	20、40、80、160 MHz	574 – 9608 Mbps *	約70m	約250m
802.11ax (Wi-Fi 6E)	2020	2.4 / 5 / 6 GHz	20、40、80、160 MHz	574 – 9608 Mbps *	約70m	約250m



* 傳輸速度依頻道寬度、收發天線數量而有所不同

Wi-Fi同盟認證

- Wi-Fi同盟 (Wi-Fi Alliance)
 - 負責Wi-Fi標準的制定及測試來自製造商的無線設備，提供產品認證、商標授權等
 - 總部位於美國德州奧斯丁
 - 目前全球有918個會員(2022資料)
 - 共有12個實驗室負責認證工作
 - 會員比例：美洲30%、亞太中東51%，歐洲及非洲19%
 - 臺灣知名廠商如華碩、宏碁、宏達電、仁寶、友訊、台達電、鴻海等都是Wi-Fi聯盟成員
 - 不是每樣符合IEEE 802.11的產品都會申請Wi-Fi聯盟認證，相對地缺少Wi-Fi認證的產品並不一定意味著不相容Wi-Fi裝置



看到這個標誌，代表通過了Wi-Fi同盟(Alliance)的相容性測試

802.11ac的規格標示

- 買路由器經常看到規格標示ACxxxx，其意義如下

無線傳輸速率快選

- └G54Mbps
- └N150Mbps
- └N300Mbps
- └N450 Mbps
- └N600 Mbps
- └N900 Mbps
- └AC600Mbps
- └AC750Mbps
- └AC1100Mbps
- └AC1200Mbps
- └AC1300Mbps
- └AC1750 Mbps
- └AC1900 Mbps**
- └AC2400 Mbps
- └AC2600 Mbps
- └AC3200 Mbps
- └AC3900 Mbps
- └AC5300 Mbps

商家的規格標籤	2.4 GHz最高理論速度 (Mb/s)	5 GHz最高理論速度 (Mb/s)
N150	150 (n)	N/A
N300	300 (n)	N/A
N450	450 (n)	N/A
N600	300 (n) 600 (n)	300 (n) N/A
AC1200	300 (n)	867 (ac)
AC1300	450 (n)	867 (ac)
AC1750	450 (n)	1300 (ac)
AC1900	600 (n)	1300 (ac)
AC2200	450 (n)	1733 (ac)
AC3200	600 (n)	1300 (ac band1) + 1300 (ac band 2)
AC5300	600 (n)	2167 (1024-QAM band1) + 2167 (1024-QAM band 2)

如果只用802.11ac (5GHz) 頻道
兩者無差別

單一端點最高1300 Mb/s

802.11ax的規格標示

- Wi-Fi 6 路由器，按速度分為 AX1500、AX3000、AX6000 與 AX11000 四款規格
- 與 AX11000 及 AX6000 型號相比，AX3000 的無線部分由「Tx：4、Rx：4」改為「Tx：2、Rx：2」，在 2.4GHz 頻譜提供 600Mbps 連線速度，於 5GHz 頻譜配合 160MHz 頻率及 OFDMA 等技術下，提供 2,402Mbps 最高連線速度
- 最入門的 AX1500，則在 5GHz 頻譜降至 80MHz 頻率，故只提供 1,201Mbps 連線速度，於 2.4GHz 則為 300Mbps

各 Wi-Fi 6 (802.11ax) 規格比較

無線規格	使用頻譜	支援 MIMO 規格	頻寬	2.4GHz 連線速度	5GHz 連線速度
AX11000	三頻	Tx：4、Rx：4	160MHz	1,148Mbps	4,804Mbps + 4,804Mbps
AX6000	雙頻	Tx：4、Rx：4	160MHz	1,148Mbps	4,804Mbps
AX6000	雙頻	Tx：8、Rx：8	80MHz	1,148Mbps	4,804Mbps
AX3000	雙頻	Tx：2、Rx：2	160MHz	600Mbps	2,402Mbps
AX1500	雙頻	Tx：2、Rx：2	80MHz	300Mbps	1,201Mbps

802.11ax/Wi-Fi 6功能與優點對應表

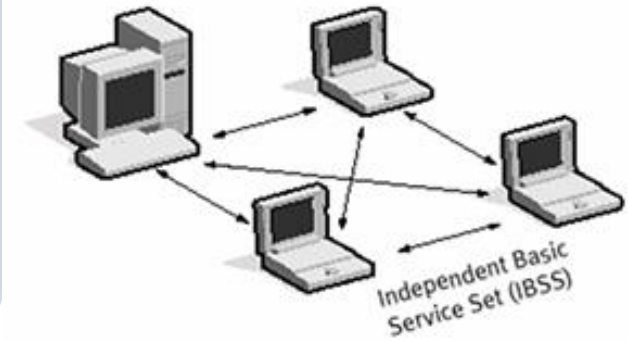
功能	優點					
	降低負擔開銷	高密度網路效率	增加傳輸量降低延遲	網路邊緣效能	戶外網路體驗	裝置能源效率
上傳OFDMA	○	○	○	○	○	
下載OFDMA	○	○			○	
上傳MU-MIMO	○	○	○		○	
1023QAM、符元持續時間、保護區間等	○	○	○	○	○	
Target Wake Time	○					○
Operating Mode Indication						

1. OFDMA：提高網路效率並降低延遲
2. MU-MIMO：提高資料同時傳輸量並使每台裝置的網路速度增加
3. 1024-QAM：比起 Wi-Fi 5，輸送量有25%的提升，理論速率提升39%
4. BSS Coloring：讓基地台可以辨認要存取的資料，提高效率
5. TWT：讓 Wi-Fi 設備 (如物聯網 IoT 設備) 的電池壽命增加

無線網路的基本架構

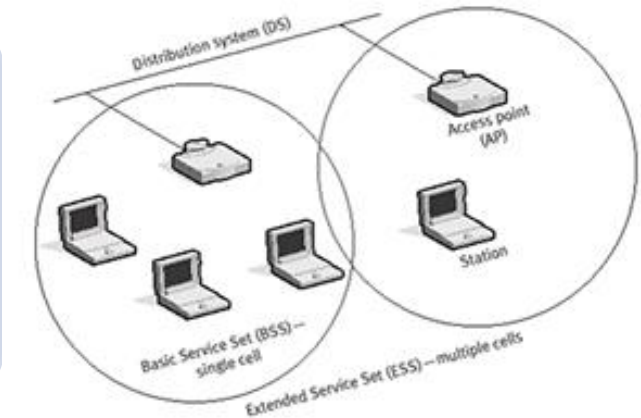
Ad Hoc模式

- 如果是兩台PC間以點對點方式互相傳遞資料，只需無線網路卡即可，不需透過AP來轉送，比較屬於個人使用環境



Infrastructure 模式

- 如果要能連上網際網路或區域網路，必需要增加AP設備，與無線網路卡形成基本網路環境，常見於企業與學校等無線網路



無線網路基本設備

- 基地台 (Access Point)

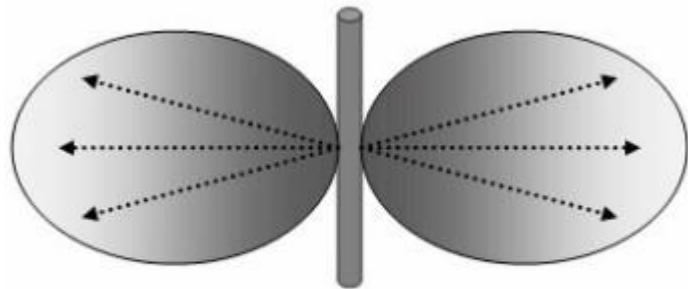


- 無線網路卡

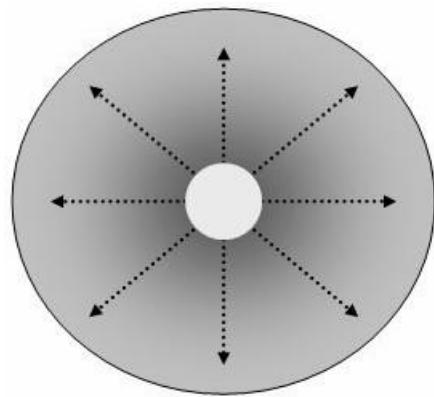


無線網路的天線種類

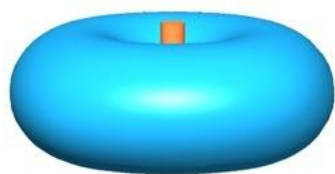
- 全向性天線



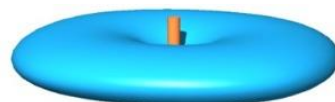
高增益全向式天線側視



全向式天線波束俯視圖

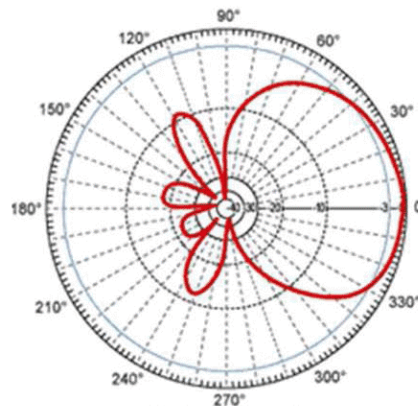


低功率

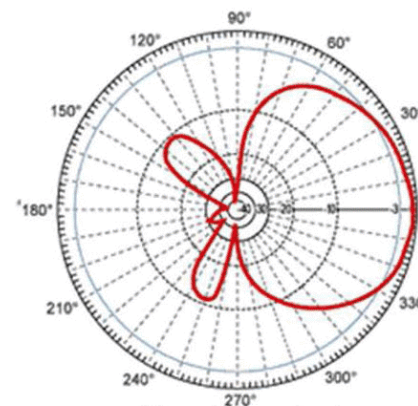


高功率

- 指向性天線



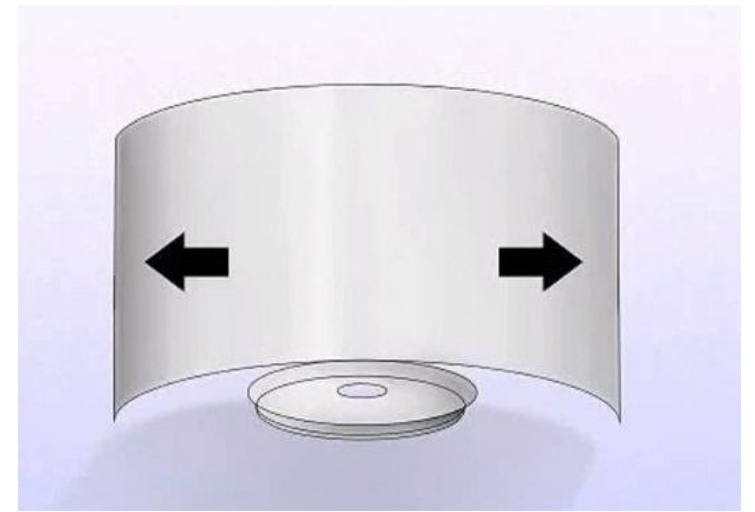
Vertical



Horizontal

一個汽水罐就可以增加Wi-Fi訊號

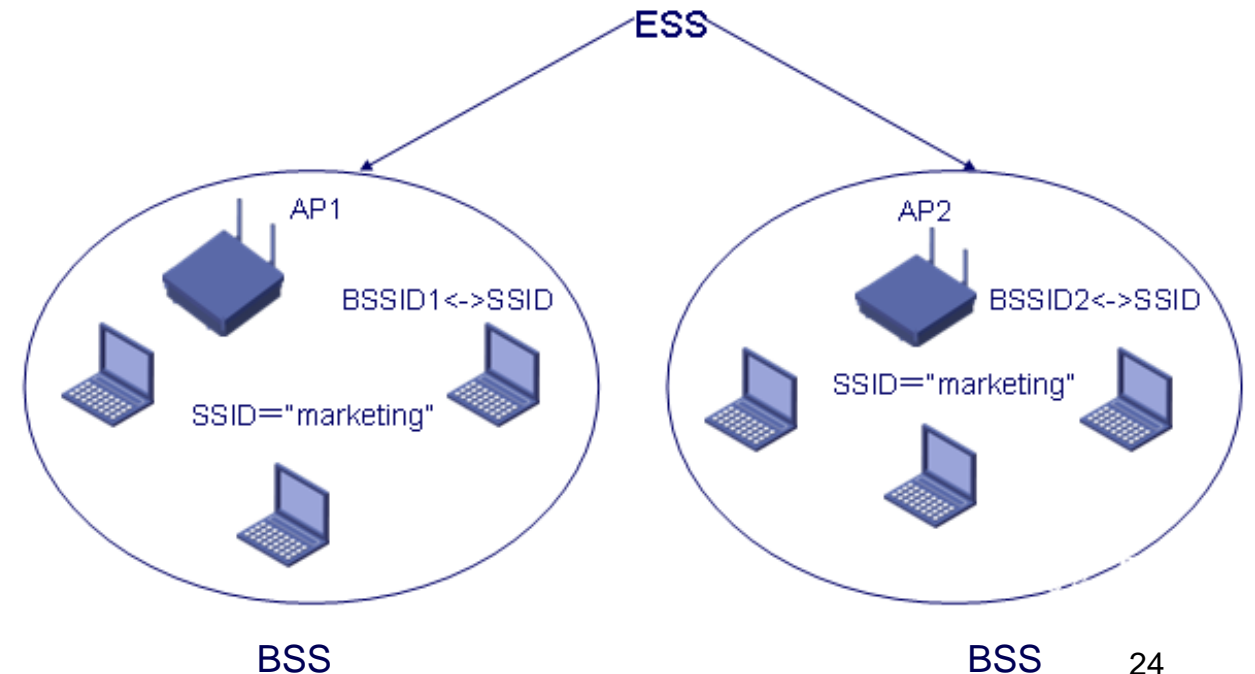
- 大部分人家中都用 Wi-Fi 上網，不過無線網路有時始終比傳統插線遜色。最明顯的缺點就是會受訊號強弱影響網路速度，而訊號本身會受很多因素影響
- 如果想加強家中路由器的訊號強度，除了使用更強的路由器，也可以自製一個「訊號加強裝置」，而且只需一個汽水鋁罐



SSID和BSSID (1/2)

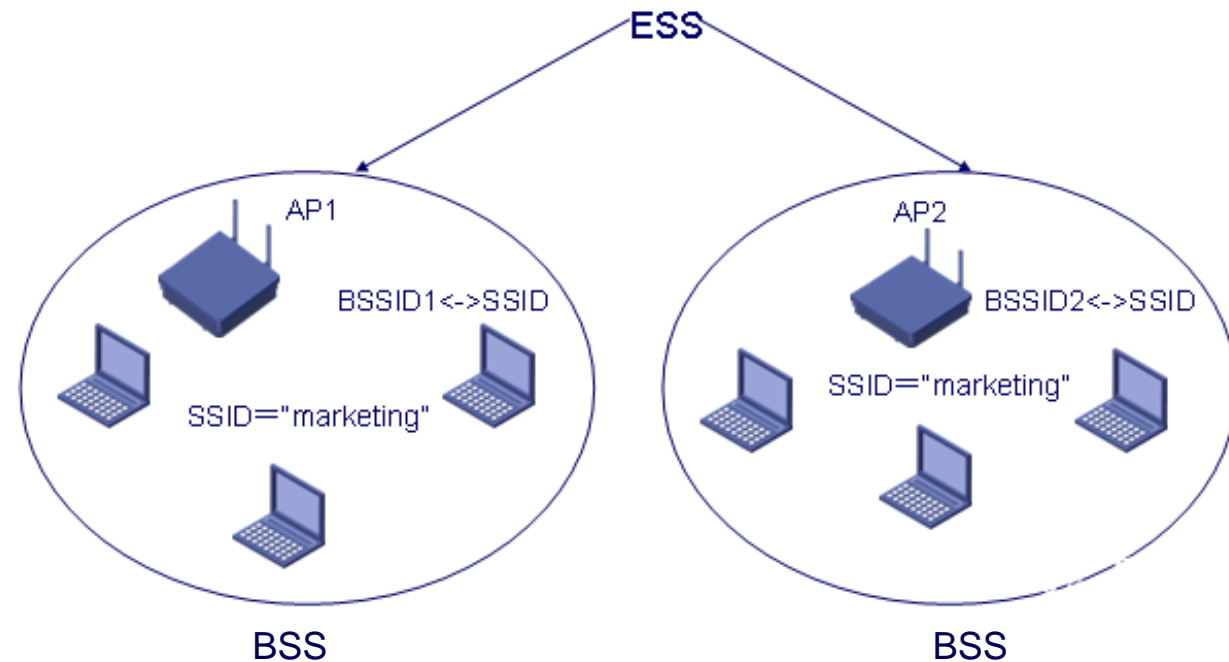
- 服務設定 (Service Set)
 - 無線網路構成單位
 - 使用**服務設定識別碼 (SSID)**作為識別
 - 有基本服務設定 (Basic Service Set, BSS) 及擴充功能服務設定 (Extended Service Set, ESS) 等幾類
- 基本服務設定 (BSS)
 - 無線網路基本構成單位
 - 由一組可互相連繫的無線裝置所組成
- 擴充功能服務設定 (ESS)
 - ESS由多個BSS所構成

SSID



SSID和BSSID (2/2)

- BSSID (Basic Service Set Identifier)
 - 用來標識AP所在的BSS
 - AP的MAC位址，獨一無二
 - 如: aa:bb:cc:dd:ee:ff
- SSID (Service Set Identifier)
 - 網路的名稱、ESS的網路標識 (ESSID)
 - 最長32位元組、區分大小寫的字串
 - 如: TP_Link_1201
- 同個AP內BSSID與SSID是一一對應
- 一個ESS內SSID是相同的，但ESS內的每個AP與之對應的BSSID是不相同的
 - 若一個AP可以同時支援多SSID的話，則AP會分配不同的BSSID來對應這些SSID



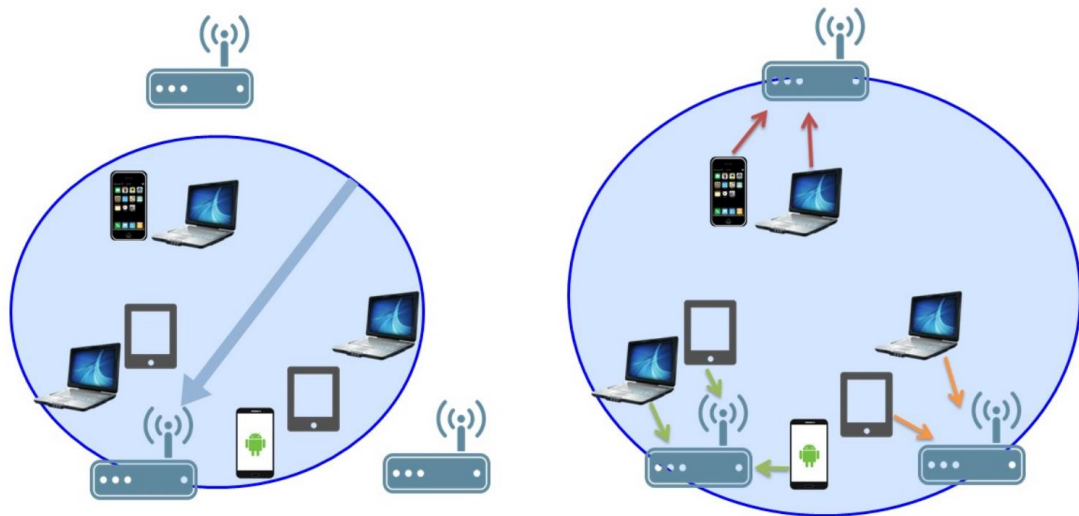
Wi-Fi Mesh



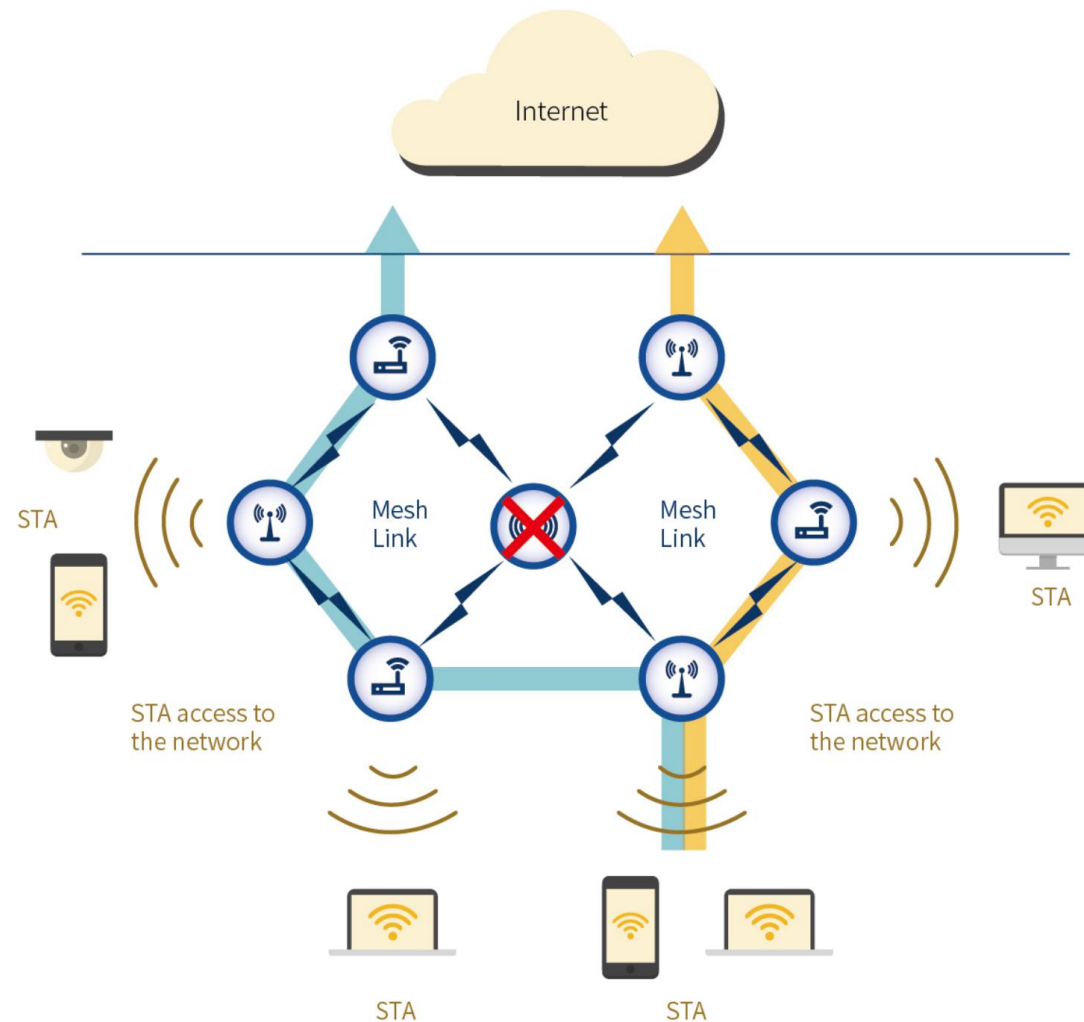
只架設一台機器無法滿足家庭需求

Without Client Steering

With Client Steering



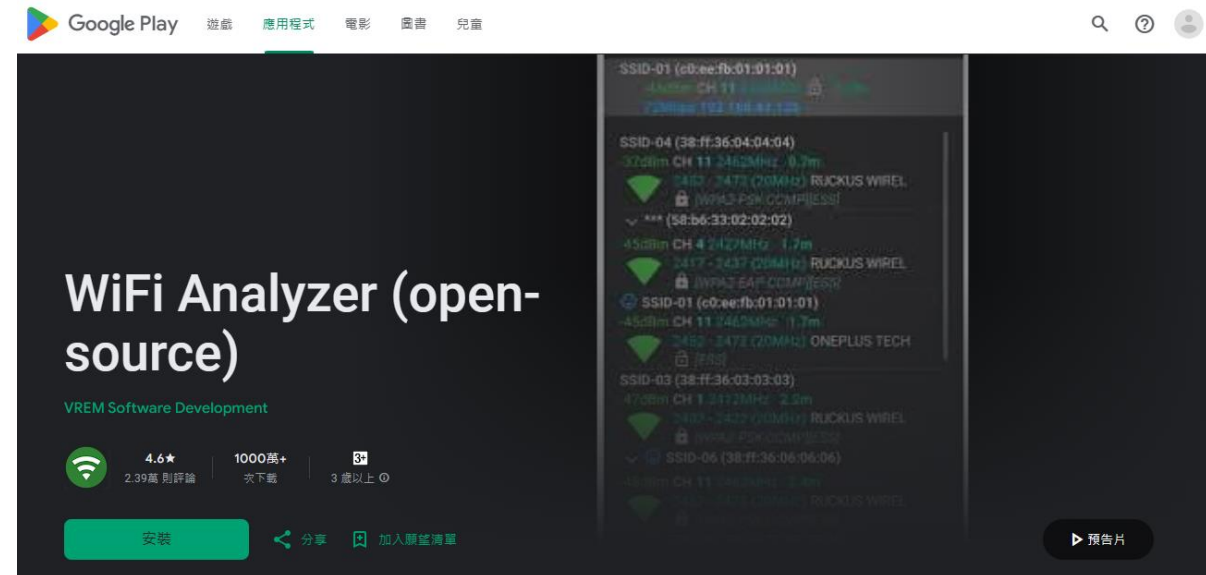
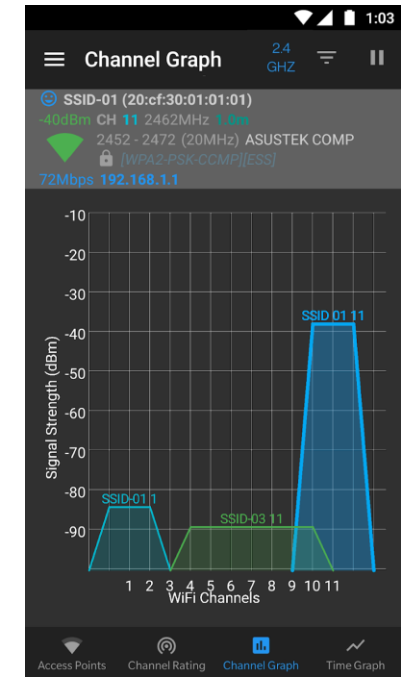
裝置引導



自我修復

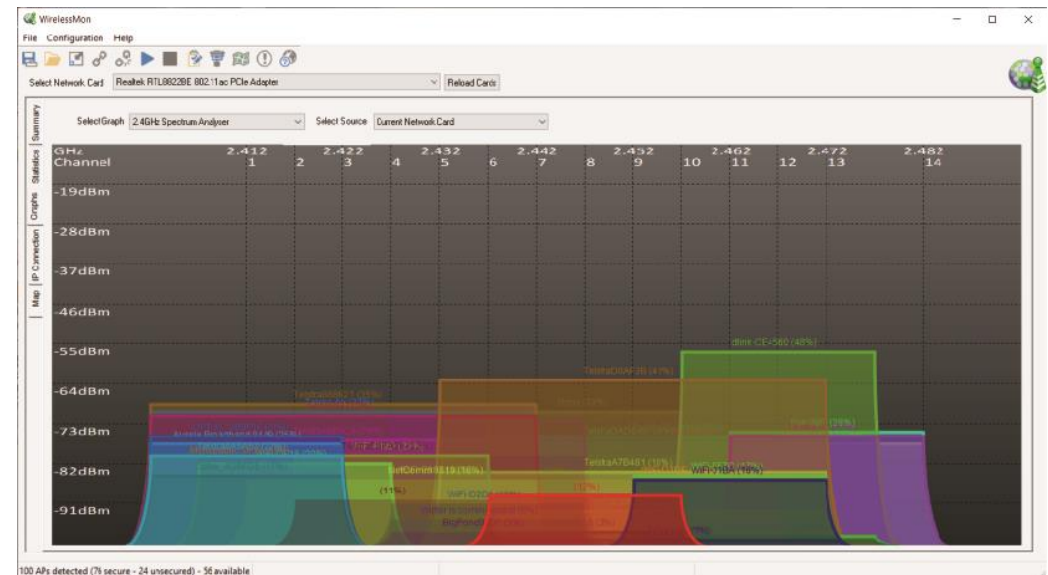
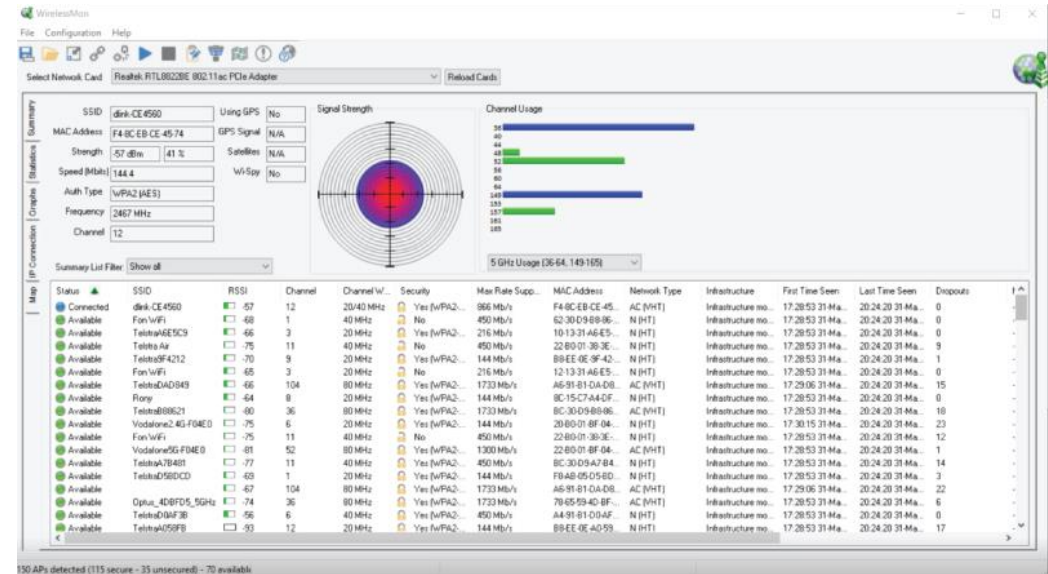
無線網路基地台網路規劃 (1/2)

- 工具: WiFi Analyzer (Open Source) (Android)
- 功能:
 - 顯示周圍的 Wi-Fi 頻道佔用情況
 - 幫助無線路由器選擇一個相對空閒的頻道以提高連線品質
- 下載位置:
 - <https://play.google.com/store/apps/details?id=com.vrem.wifianalyzer>



無線網路基地台網路規劃 (2/2)

- 工具: WirelessMon (PC)
- 功能:
 - 列出目前電腦附近所擁有的無線網路或基地台等相關資訊
 - 列出電腦與基地台間的訊號強度
 - 即時的監測無線網路的傳輸速度，以便了解網路的下載速度或其穩定性
- 下載位置:
 - <https://www.passmark.com/products/wirelessmonitor/> (30天免費試用)

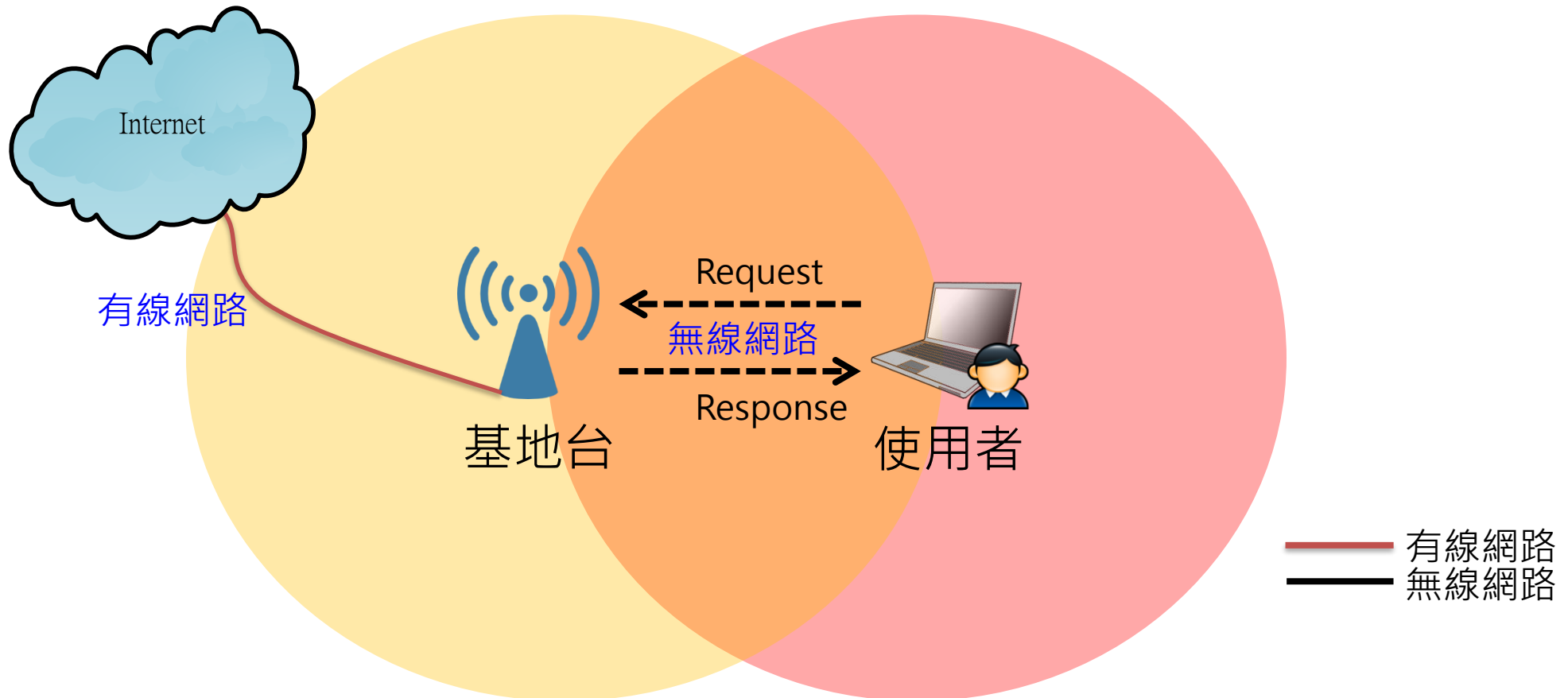




3. 無線網路的弱點

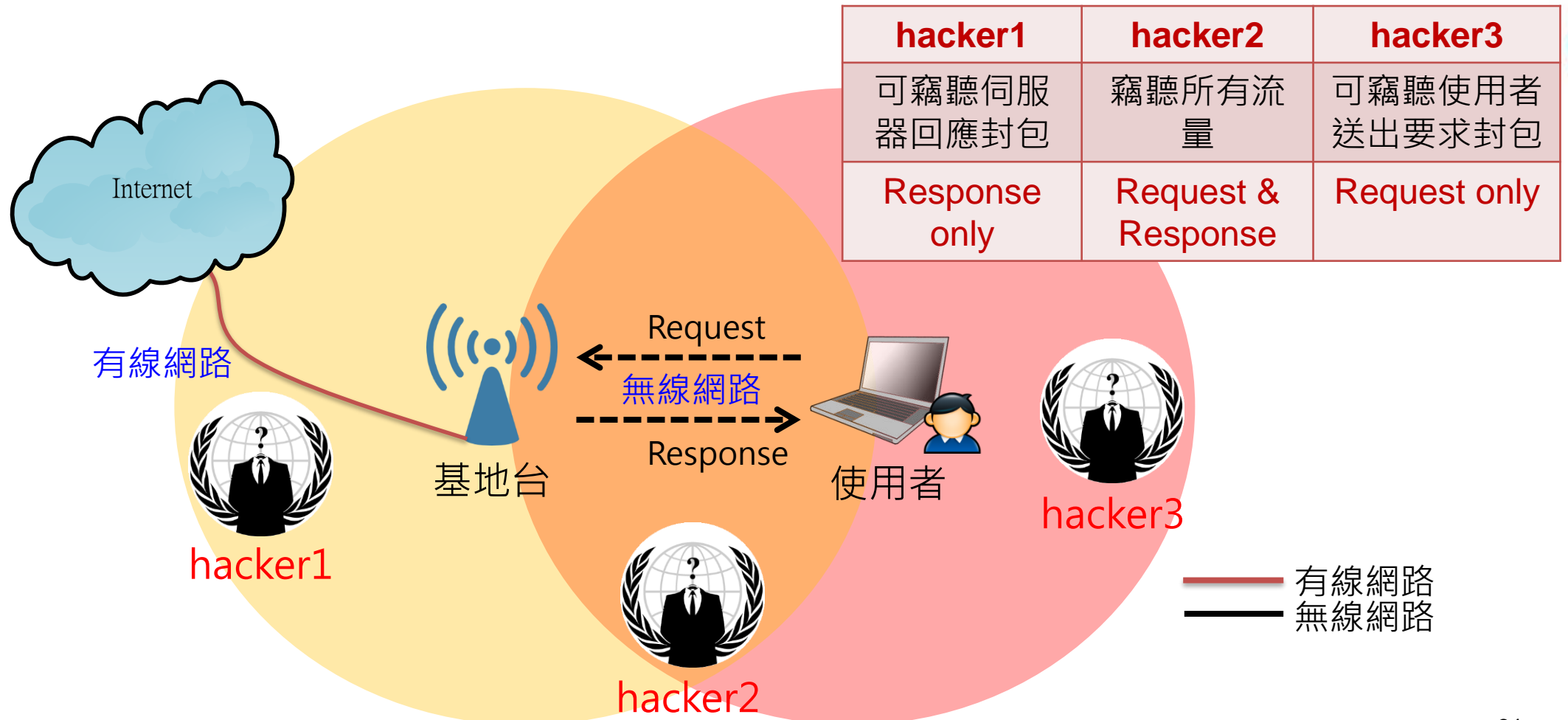
一般無線網路的使用狀況

- 使用者與基地台透過無線網路進行溝通，因無線網路屬於**廣播**形式，所以實際上狀況如下圖



當駭客存在時的無線網路狀況(1/2)

- 駭客可以透過可抓封包網卡竊聽廣播封包



當駭客存在時的無線網路狀況(2/2)

• Request

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: zh-TW
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Host: www.google.com.tw
Cookie: PREF=ID=2a777ac97db2eb6f:U=6cfda9b98e43c98e:FF=0:TM=1303715105:LM=1322623574:S=m75_OPNpvHAXUKhf;
NID=53=H1Ewv_4wWSRmtL_Q4a2ZeWf5ObXmMSa6OY2D--auUTzPOIqoVWoNnAZ2A3wBJNF7-OTbUBDJ388_yUJ9BhdZ12VoBcAaEyQh1xbyhBjC-
kv3xnHHx1N2x29THz3SA1VR;
SID=DQAAAHoAAADtZkeH9pAfe3jrGkRZRmondOknY3cLqEzJZW7-tnj08X1d47hwcISGDvxHzmrhVBUZ1K9KMKQuo3h3LhFHeWuWks5mRC9E3IfT
2q99h0fZ6Y07Ke5BCSuTD_oIvSeRA5WEQKR5nLHA_Eo2Evm1D7AOTaY2ytShq4s2yCKEaBYNQA; HSID=AK7EO9LcYHXUS_1U5
```

• Response

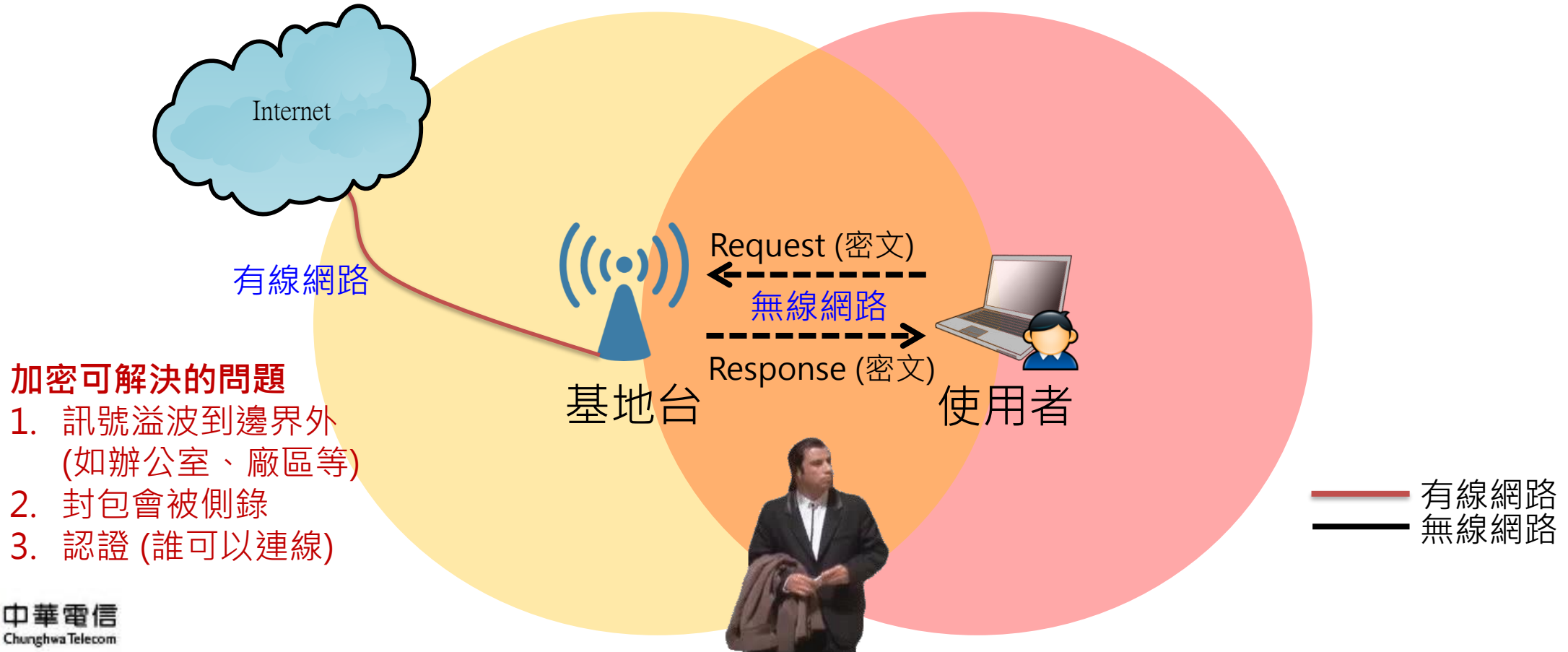
```
HTTP/1.1 302 Found
Location: https://www.google.com.tw/
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Date: Tue, 20 Mar 2012 02:05:51 GMT
Server: gws
Content-Length: 223
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="https://www.google.com.tw/">here</A>.
</BODY></HTML>
```

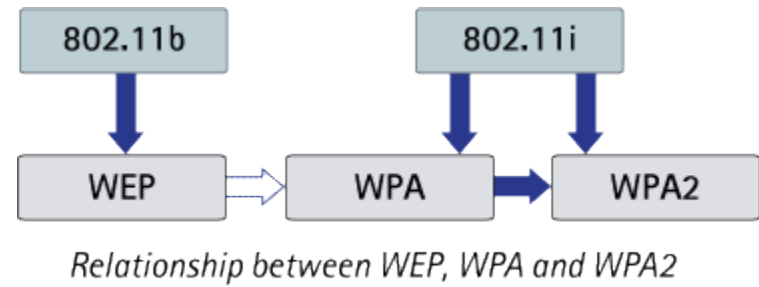
hacker1	hacker2	hacker3
可竊聽伺服器回應封包	竊聽所有流量	可竊聽使用者送出要求封包
Response only	Request & Response	Request only

★ 解決方案

- 透過**加密**方式使得廣播的封包就算被聽到也無法理解
- 目前廣泛使用的加密方式有**WEP**、**WPA**、**WPA2**、**WPA3**



★ 無線網路加密技術介紹



WEP(Wired Equivalent Privacy)



Wi-Fi Protected Access-WPA/WPA2/WPA3



Wi-Fi Protected Setup-WPS

無線加密協議WEP (Wired Equivalent Privacy)

- 1999/9 成為 802.11 標準的一部分
- 主要使用的加密法為RC4 (Rivest Cipher) , 驗證傳輸訊息的檢驗方式為CRC (Cyclic Redundancy Check)
- 2001年就已有研究者指出 , 只要收集到足夠的封包 , 就能反向算出RC4的金鑰
- WEP先天不足
 - 每一次封包的加密 , 都是透過24位元的IV (Initialization Vector)值與固定的40或104位元WEP金鑰去演算 , 形成一個64或128位元的RC4加密值 , 然後傳輸出去
 - WEP的金鑰是固定不變 , IV值則是一組僅有24位元的變動值 , 並且以明碼的方式傳輸
 - 24位元的變動IV值 , 僅有1,600萬種加密的可能性 , 在比較繁忙的網路上 , 這些可能性很快就會被用完 , 這使得有意破解的惡意使用者 , 只要收集到這數量的封包 , 就能透過反推算的方式 , 算出WEP的金鑰
 - 另外 , 傳輸訊息CRC驗證機制也存在問題 , 由於CRC資料與檢驗值為線性關係 , 只要同時變更封包與驗證WEP傳輸完整性的CRC檢驗值 , 就可以騙過接收方 , 將有問題的訊息視為正確導致混亂
- 在2003年由Wi-Fi聯盟推動的WPA取代
- 2004年802.11i標準通過後 , 更由全新架構的WPA2取代 , 幾乎完全被淘汰

WPA/WPA2 (Wi-Fi Protected Access)

- Wi-Fi Protected Access

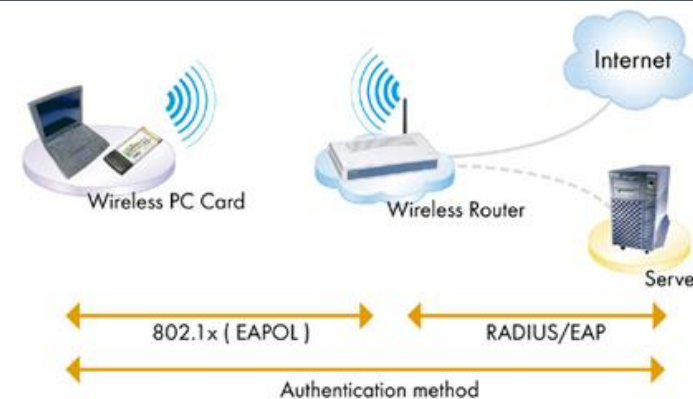
- WPA 全名為 **Wi-Fi Protected Access**，是一種保護無線電腦網路 (Wi-Fi) 安全的系統，它是因應研究者在前一代的系統有線等效加密 (WEP) 中找到的幾個嚴重的弱點而產生的

- WPA

- 在WPA的設計中要用到一個 [802.1X](#) 認證伺服器來散佈不同的鑰匙給各個用戶；不過它也可以用在較不保險的“**pre-shared key**” (PSK) 模式，讓每個用戶都用同一個密鑰
- WPA的資料是以一把128位元的鑰匙和一個48位元的初向量，使用RC4演算法進行加密
- Wi-Fi聯盟把這個使用pre-shared key的版本叫做WPA個人版或WPA2個人版，用802.1X認證的版本叫做WPA 企業版或WPA2 企業版
- 藉由增大鑰匙和初向量、減少和鑰匙相關的封包個數、再加上安全訊息驗證系統，WPA 使得侵入無線區域網路變得困難許多。WPA 網路每當偵測到一個企圖的攻擊行為時就會關閉 30 秒鐘

- WPA2

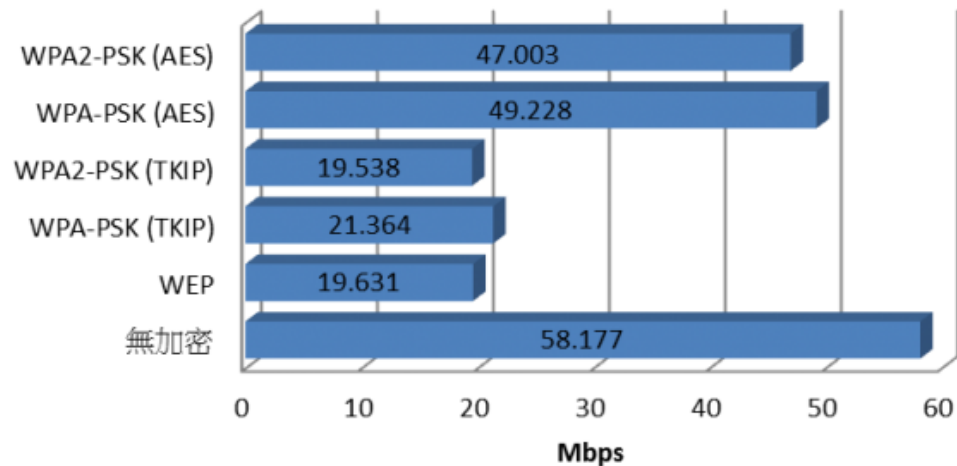
- WPA2 是經由 Wi-Fi 聯盟驗證過的 [IEEE 802.11i](#) 標準的認證形式。WPA2 實現了 802.11i 的強制性元素，特別是 Michael 演算法由公認徹底安全的 [CCMP](#) 訊息認證碼所取代、而 RC4 也被 [AES](#) 取代



WPA/WPA2速度比較

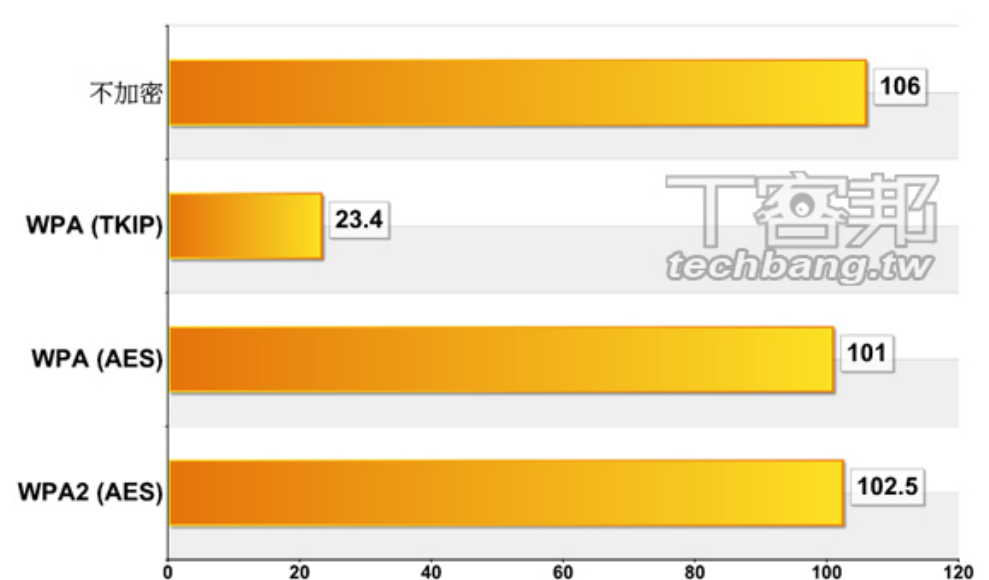
- 以華碩RT-N56U無線路由器測試，不加密的傳輸速度經測試約為106Mbps。WPA加密分為2種安全加密技術，分別為TKIP與AES，這也是目前無線路由器所會看到的2種選擇方案。其中AES比TKIP採用更高級的加密技術，而如果採用TKIP的話，網路的傳輸速度就會被限制在54 Mbps以下
- 使用WPA跟WPA2的AES加密方式，效能都蠻不錯的

TP-Link 300M

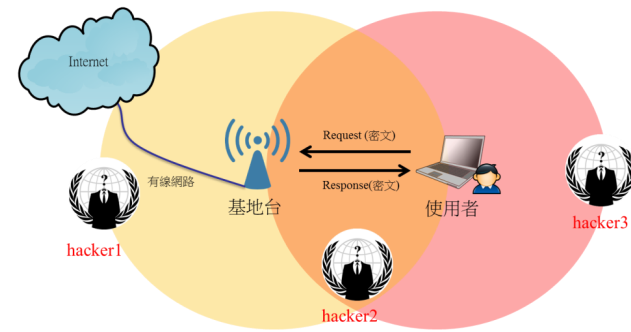


Asus RT-N56U連線速度 (無線)

單位: Mbps 越大越好→



WPA/WPA2的安全性



- 預共用密鑰模式下的安全性
 - 預共用密鑰模式 (Pre-Shared Key , PSK , 又稱為個人模式) 是設計給負擔不起 802.1X 驗證伺服器的成本和複雜度的**家庭**和**小型公司**網路用的
 - 每一個使用者必須輸入密鑰來取用網路，而密鑰可以是 **8 到 63 個 ASCII 字元**、或是 **64 個 16 進位數字 (256位元)**
- 駭客的攻擊方式
 - 攻擊者可利用spoonwpa等工具，搜尋到合法用戶的網卡地址，並偽裝該地址對路由器進行攻擊，迫使合法用戶斷線重新連接，在此過程中獲得一個有效的**握手封包**，並對握手封包暴力破解猜密碼（如果猜密的字典中有合法用戶的密碼）。經過實驗，此攻擊方式仍有下列限制:
 1. 此方式需要使用大量的時間進行運算，通常搭配**GPU**與多台電腦仍需花費**數星期至數月**之時間
 2. 駭客必須位於前面圖形中**hacker2**的位置方能發揮作用，使用範圍小很多

Wi-Fi管理上的困境

- 當連線無線網路時，通常必須先選擇**無線基地臺的SSID**，而且為了無線安全的疑慮，大多會建立WEP或WPA/WPA2加密方式，以避免連線時，遭駭客入侵竊取機密資料
- 其中在加密方式上，為了確保傳輸的高安全性，會利用特殊的數值，建立**加密金鑰**，在使用者取得加密金鑰並輸入到電腦的連線資料後，才能建立安全的無線網路連線
- 如果加密金鑰的**數值太複雜**，使用者很容易輸入錯誤，太簡單又怕被盜用破解，管理上就陷入兩難的局面
- 消費電子晶片製造商已經有辦法跳過使用者選出弱密碼的問題，而自動產生和傳播高強度金鑰
 - 做法是透過軟體或硬體介面以外方法把新的 Wi-Fi 介面卡或家電加入網路
 - 按鈕：[Broadcom SecureEasySetup](#) 和 [Buffalo AirStation One-Touch Secure Setup](#)
 - 透過軟體輸入一個短的挑戰語：[AtherosJumpStart](#)
 - 產生QR Code讓訪客掃描即可連線

製作QR Code讓使用者直接加入無線網路

- <https://www.mywifisign.com/zh-hant>
- <https://qifi.org/>

pure JS WiFi QR Code Generator

SSID

Encryption: WPA/WPA2/WPA3

Key

Hidden

Generate!

我的WiFi卡片

繁體中文

註冊

請在下方填入WiFi資訊

WiFi名稱: SpaceX WiFi

密碼: Mars2021

列印 下載

這是什麼?

這個網站可以讓你方便地建立一張A4大小的卡片，卡片中包含了WiFi的資訊和可提供手機掃描連接WiFi的行動條碼。你只需要在上方表格中填入WiFi資訊，就可以列印或者下載PDF了。

OK，這個行動條碼能幹嘛？

好問題！這個行動條碼能讓你使用手機或者平板的相機，一步到位的連接WiFi，省去了搜尋WiFi和輸入密碼等繁雜的手續。

用這個安全嗎？

安全！你的WiFi資訊會被安全的傳輸，只會用於創建卡片。這些資訊絕對不會被儲存或者分享給任何人。

這是誰做的？

三位利用業餘時間做出的：Cody Mikol, Kostas Nasis, 和張盈盈。繁體中文翻譯由賴建宏提供。



WPS (Wi-Fi Protected Setup)

- 由於無線網路的技術中，關於One Touch的概念開始發酵，Wi-Fi聯盟於2004年開始討論是否能建立具備安全且容易使用的無線網路連線標準
- **Wi-Fi Protected Setup (WPS)**目標是快速建立安全的無線網路連線設定，減少用戶操作上的錯誤，在許多無線設備都可看見它的身影，以下為一些支援WPS的AP



- WPS除了提供容易操作的步驟外，在無線安全方面支援WPA及WPA2等加密方式，它基於EAP的認證協定，SSID及加密金鑰都是在此協定上傳輸資料，所有的資料都是先經過加密再傳送到無線網路中，參與者收到資料後，再轉換成可接收的內容，安全性較佳
- 以PIN及PBC建立WPS連線
目前WPS支援2種連線模式：**PIN (Personal Information Number)**及**PBC (Push Button Configuration)**，這2種連線方式也都受到Wi-Fi聯盟認可
 - PIN就是輸入一組序號建立連線
 - PBC則是透過按鈕的方式 (它可以是軟體模擬的按鈕或設備上的硬體按鈕)

WPS一鍵加密安全漏洞

- 2011年底安全研究員Stefan Viehbock在其Blog上公佈了WPS存在著安全漏洞，而且涉及了多家廠商的大量的無線設備。Viehbock所發現的漏洞，將會使WPS變得較為容易被暴力窮舉PIN的方法所破解。利用該漏洞可以輕易地在2小時內破解WPS使用的PIN碼
- 下列要素導致透過PIN碼進行破解變為可行：
 1. 在WPS加密中PIN碼是設備間獲得**唯一要求**，不需要其他身份識別方式
 2. WPS PIN碼的第8位數是一個**checksum**，因此駭客只需算出前7位數即可。唯一的PIN碼的數量變成了10的7次方，也就是說有1000萬種變化

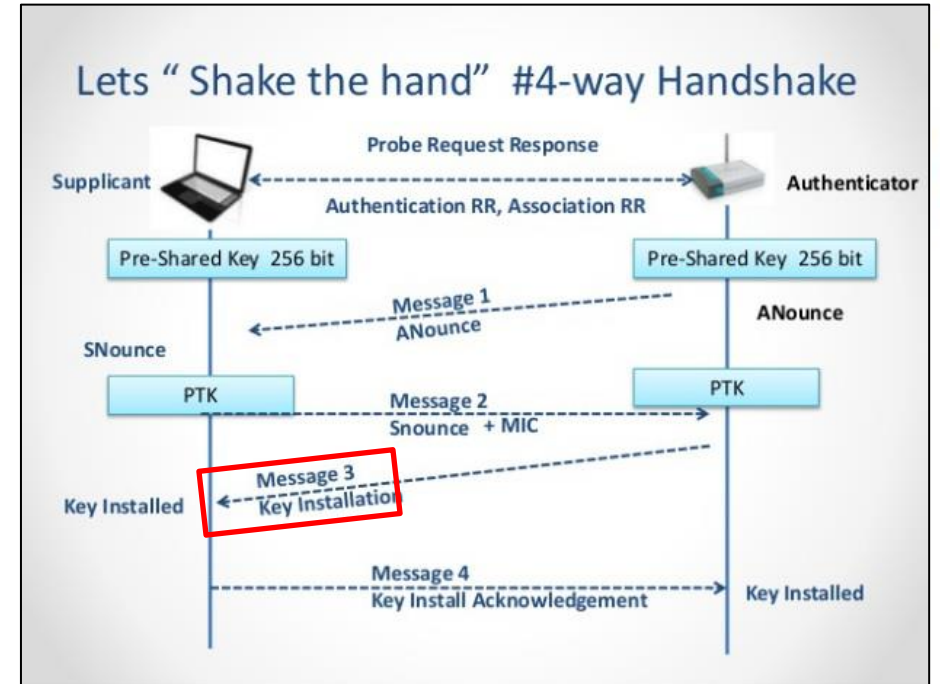
1	2	3	4	5	6	7	0
1 st half of PIN				checksum			
				2 nd half of PIN			



3. 在實施PIN的身份識別時，接取點(無線路由器)實際上是要找出這個PIN的**前半部分**(前4位)和**後半部分**(後3位)是否正確即可。Viehbock稱當第一次PIN認證連接失敗後，路由器會向客戶端發回一個EAP-NACK信息，而通過該回應，攻擊者將能夠確定的PIN前半部或後半部是否正確。駭客只需從7位數的PIN中找出一個4位數的PIN和一個3位數的PIN。這樣一來，級次又被降低，從1000萬種變化，減少到11000 (10的4次方+10的3次方) 種變化

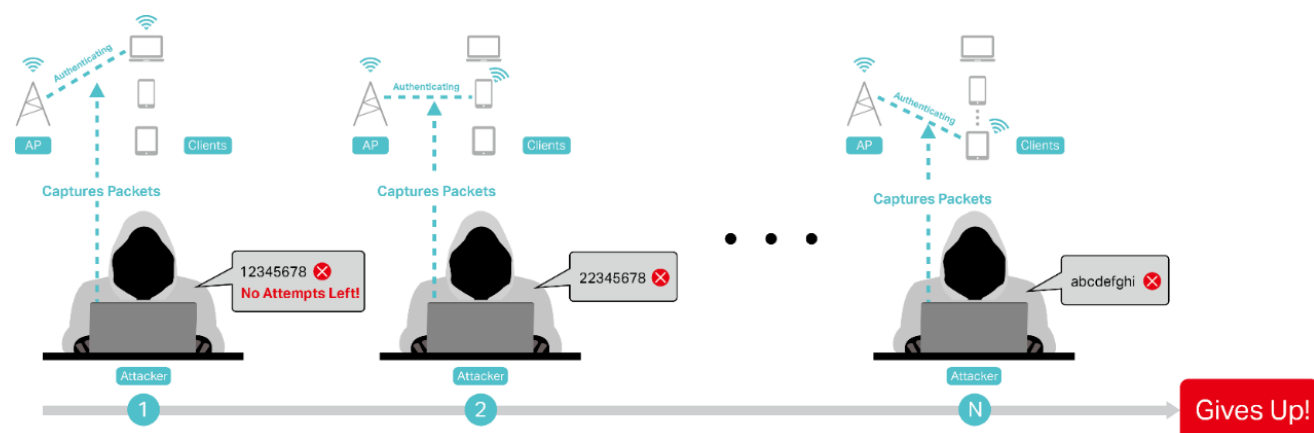
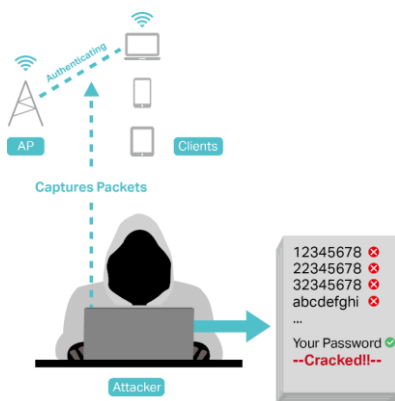
WPA2密鑰重裝攻擊KRACK

- KRACK全名為Key Reinstallation Attack
- 針對保護Wi-Fi連線的Wi-Fi Protected Access (WPA) 協定的攻擊手段，於2017年由比利時研究員Mathy Vanhoef和魯汶大學Frank Piessens發現，並於2017年10月公布了此攻擊有關細節
- 此攻擊針對WPA2協定中建立一個Nonce (一種共享金鑰) 的四次握手
 - WPA2的標準預期有偶爾發生的Wi-Fi斷開連線，並允許使用同樣的值重連第三次握手，以做到快速重連和連續性
 - 由於標準不要求在此種重連時使用不同金鑰，所以可能出現**重送攻擊**。攻擊者可以反覆**重發第三次握手**來重複操縱或重設WPA2的加密金鑰
 - 當裝置重複安裝相同的加密金鑰，就會使得Nonce被重置與封包序號計數器歸零，透過比對使得**傳輸封包的解密變為可能**



WPA3

- WPA3 (Wi-Fi Protected Access 3) 是一個由 Wi-Fi 聯盟提出的安全性驗證程序
- 分為WPA3-Personal (適合一般家庭使用) 和 WPA3-Enterprise (適合企業使用)
 - WPA3-Personal，藉由將 WPA2-Personal 的預共用金鑰 (PSK) 替換成對等實體同步驗證 (SAE) 來改善驗證的強度
 - WPA3-Enterprise，推出 192-bit 安全性功能提供政府、國防和工業應用更高的加密安全性
- 改用定義在RFC 7664 中的Dragonfly交握來取代四向交握預防KRACK攻擊
- 採用SAE：具前向保密，可確保入侵者即使金鑰被洩漏，也無法解密任何取得的資料



Before SAE: 駭客可以攔截封包離線猜測

After SAE: 駭客要持續攔截封包猜測(花費時間精力)

實際上，駭客是如何破解WEP與WPS？

- 事前準備
- 進行破解
- 側錄無線封包



事前準備 – 採購網卡

- 需要使用可以抓取封包的網卡，如：
 - 瑞昱 Realtek RTL8187
 - 雷凌 Ralink RT3070



RTL8187L+RTL8225+se2527 大功率無線網卡 駭客必備
附贈無線網路破解教學 40GB暴力破解密碼檔

定價 **\$400** / 已售出 26 件

數量

立即購買 加入購物車 即時通

付款方式 詳細內容

運費 郵寄掛號 — 單件運費\$40、滿999件或消費滿\$3000000免運費 合併運送

商品狀況 全新品

所在地區 新北市

商品編號 100123340922

Yahoo拍賣保障
放心買！我們給你五萬交易保障！



ARGtek ARG-1000

黑金剛

Enjoy Incredible Download Speed!

飆升【五倍】網路速度
超高功率 **1000mW**
802.11n 多重合併頻寬
唯一支援 BT4 RT3070

飆網五倍速率 實現不可思議的下載速度!!



贈送!! 獨家超強新 BT5(奶瓶)光碟

Beini

2011 最新學習程式 獨家新 BT5 一鍵神功
內附 WPA / WPA2 / WEP 獨家中文操作說明
內附獨家研發 USB 隨身碟 製作程式及說明
強力支援本賣場所有高功率無線網卡



事前準備 – 作業系統

- 安裝虛擬機器
 - VMWare Workstation
- 下載破解無線網路專用Live CD
 - Beini
 - XiaopanOS
 - **CDLinux**
 - BackTrack 5
 - **Kali Linux**
- 透過虛擬機器啟動Live CD，燒成開機光碟效能會更好

實戰破解WEP (1/2)

- 透過VMWare啟動CDLinux
- 執行minidwep-gtk程式

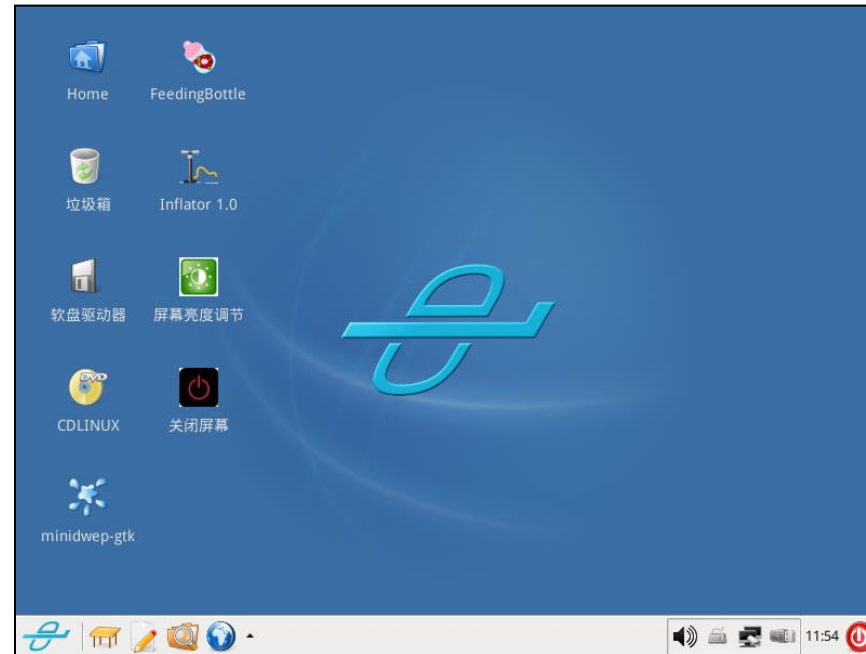
```
GRUB4DOS 0.4.4 2009-02-21, Memory: 637K / 253M, MenuEnd: 0x46D9E

Safe Graphics Mode
Normal, please select a language:
>
(de_DE) Deutsch           Willkommen         Deutschl and
(en_CA) English           Wel come         Canada
(en_GB) English           Wel come         Great Britain
(en_US) English           Wel come         United States
(fr_CA) French            Bienvenue        Canada
(fr_CH) French            Bienvenue        Suisse
(fr_FR) French            Bienvenue        France
(ru_RU) Russian          Добро пожаловать Россия
(zh_CN) Chinese           欢迎            中国大陆
(zh_TW) Chinese           歡迎            中國台灣
>
MemTest86+: a thorough, stand alone memory tester for x86

CDlinux

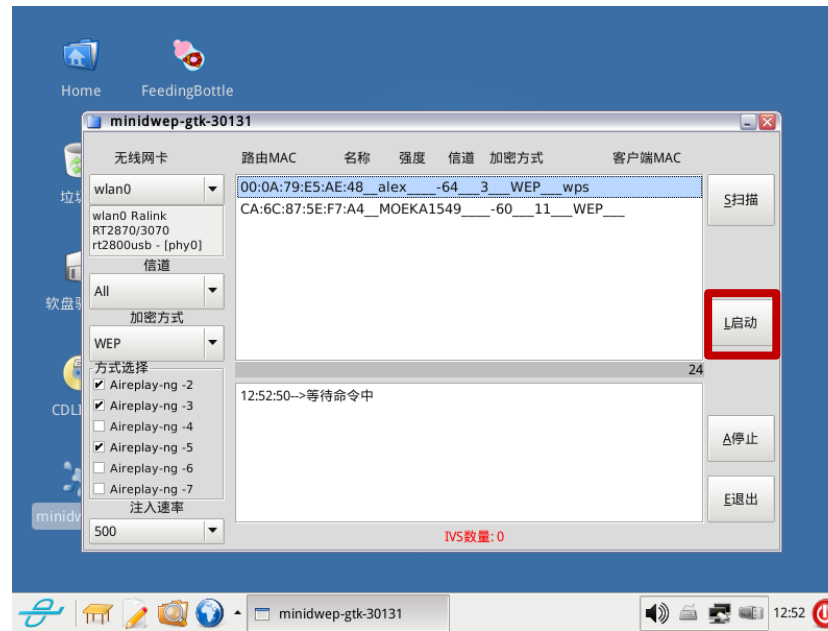
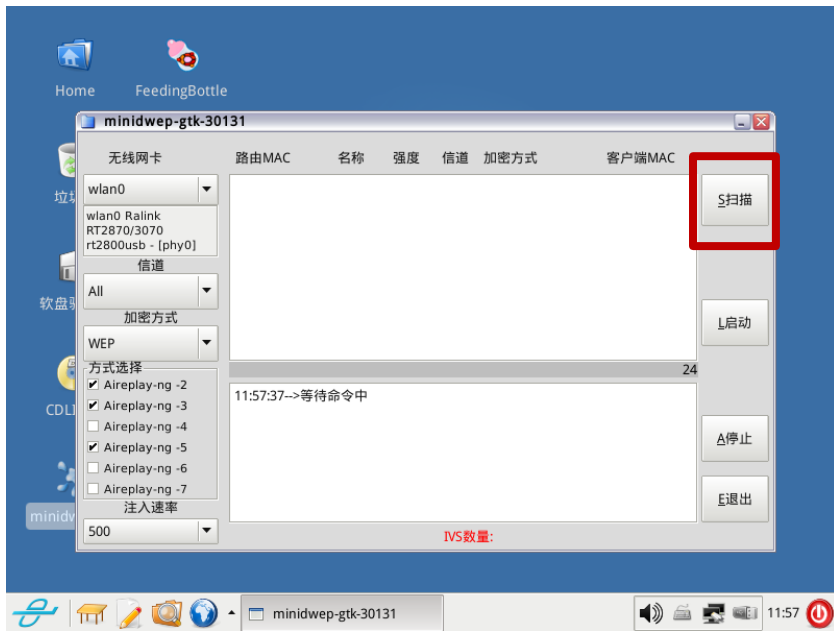
Use the ↑ and ↓ keys to highlight an entry. Press ENTER or 'b' to boot.
Press 'e' to edit the commands before booting, or 'c' for a command-line.

The highlighted entry will be booted automatically in 2 seconds.
```



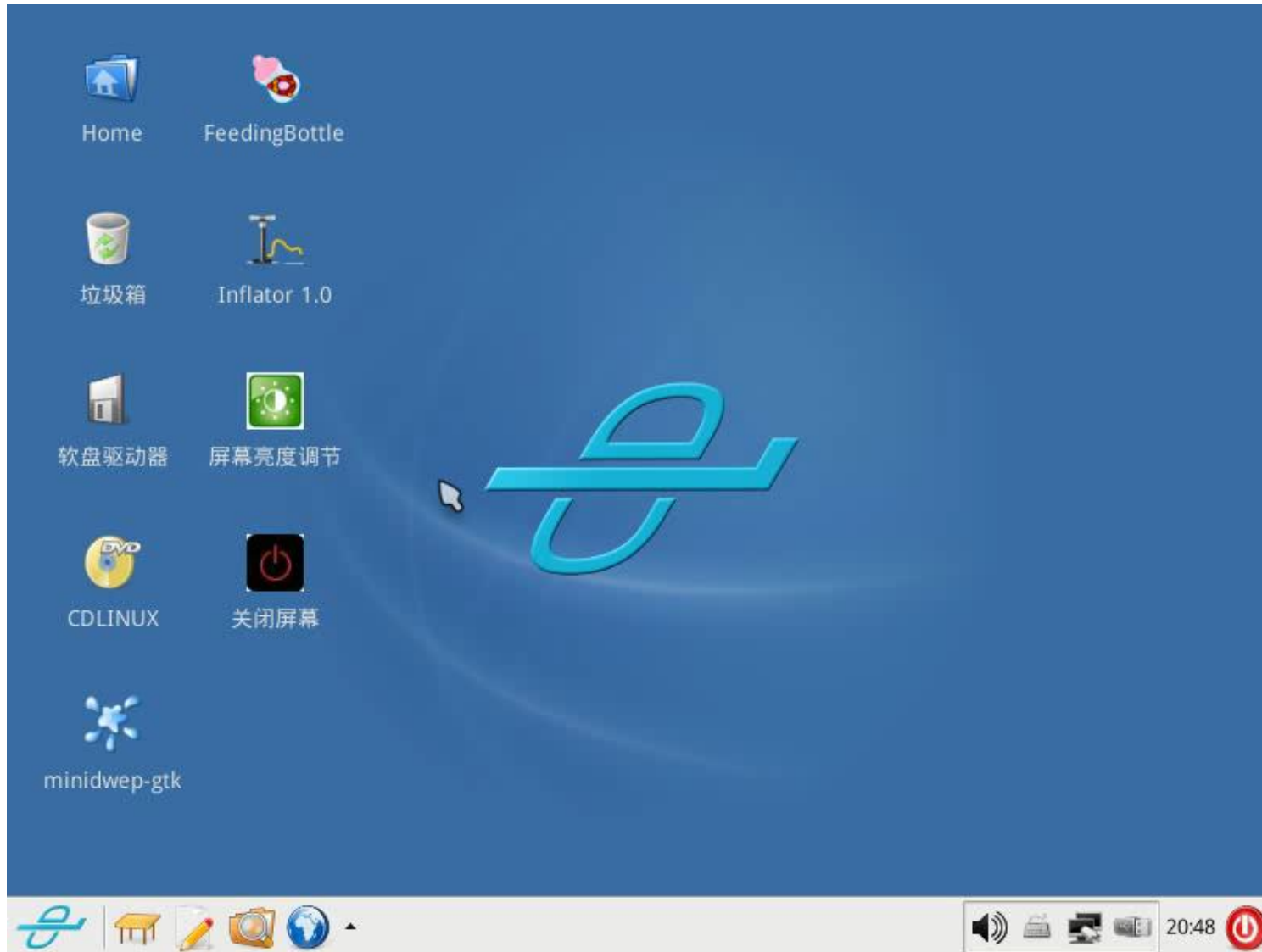
實戰破解WEP (2/2)

- 點擊掃描進行偵測無線網路
- 點擊啟動進行攻擊WEP



WEP破解Demo (1/2)

- 影片

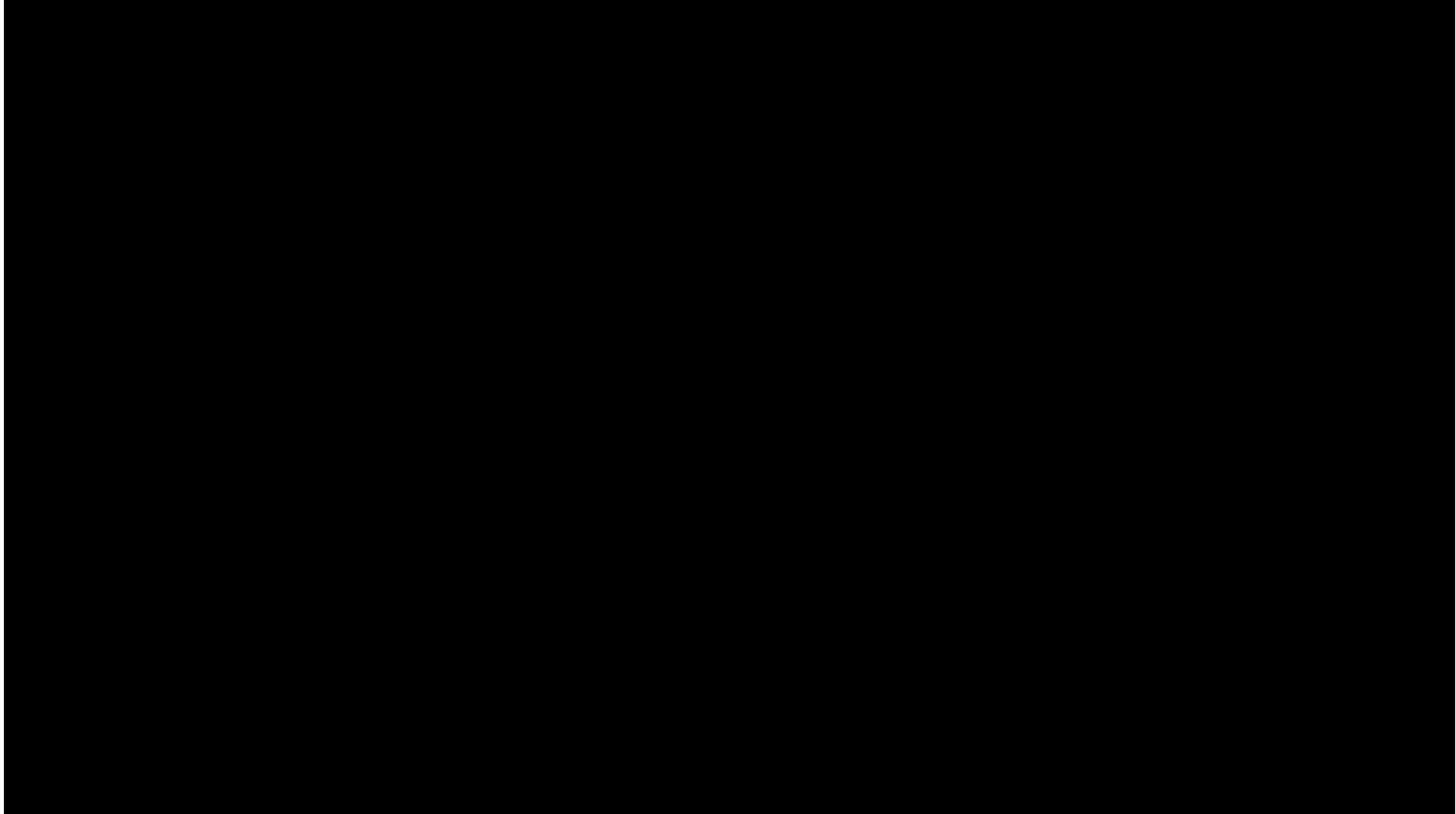


WEP破解Demo (2/2)

- 透過快速重送封包，可以很快取得IV
- 收集到8000個IV左右時會進入破解模式，尋找正確Key
- 攻擊者只要待在AP訊號範圍內，不用管有沒有使用者
- 整個過程約3分鐘

利用Kali Linux破解WEP Demo

- 使用wifite工具來破密



實戰破解WPA/WPA2

- 透過選擇加密方式切換到WPA/WPA2

切換加密方式

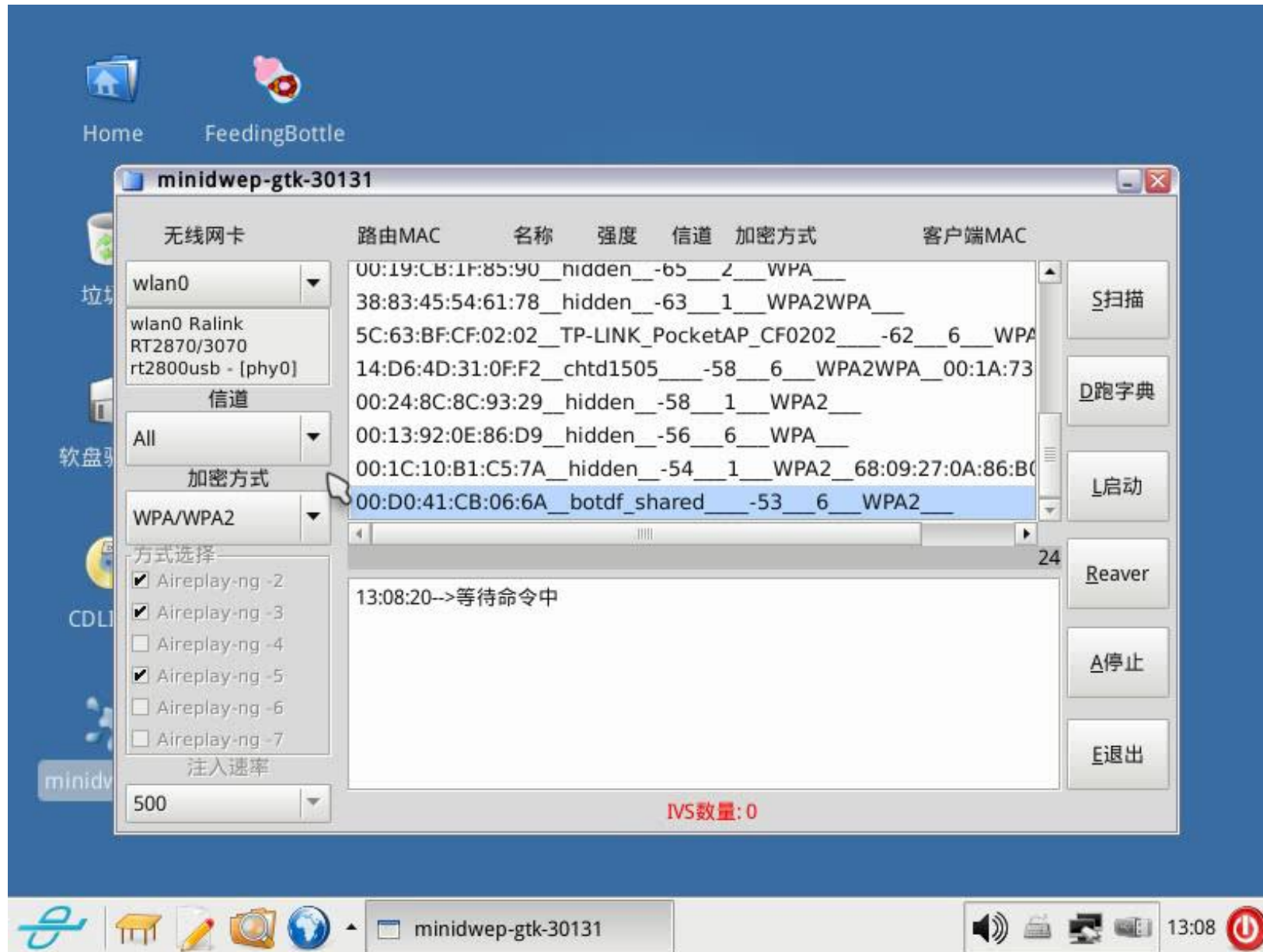
WPA/WPA2破解

WPS破解

无线网卡	路由MAC	名称	强度	信道	加密方式	客户端MAC
wlan0	74:EA:3A:E5:5F:42	TPLINK	-72	2	WPA2WPA	wps
wlan0 Ralink	40:4A:03:52:99:F1	hidden	-72	1	WPA	
RT2870/3070	50:67:F0:38:5D:11	Travis	-72	1	WPA2	
rt2800usb - [phy0]	00:22:15:36:25:3D	WL520GC_MNPy	-71	1	WPA	
	50:67:F0:61:78:DB	P876	-68	6	WPA	
	1C:AF:F7:1B:89:D2	hidden	-70	1	WPA2	
	BC:AE:C5:C4:D0:A8	hiVideo_AP	-68	1	WPA2WPA	wps

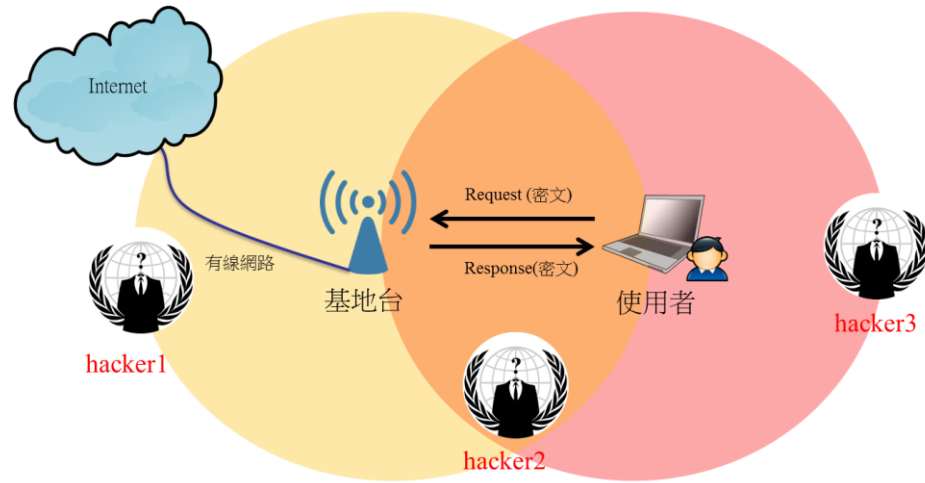
WPA/WPA2破解Demo (1/3)

- 影片



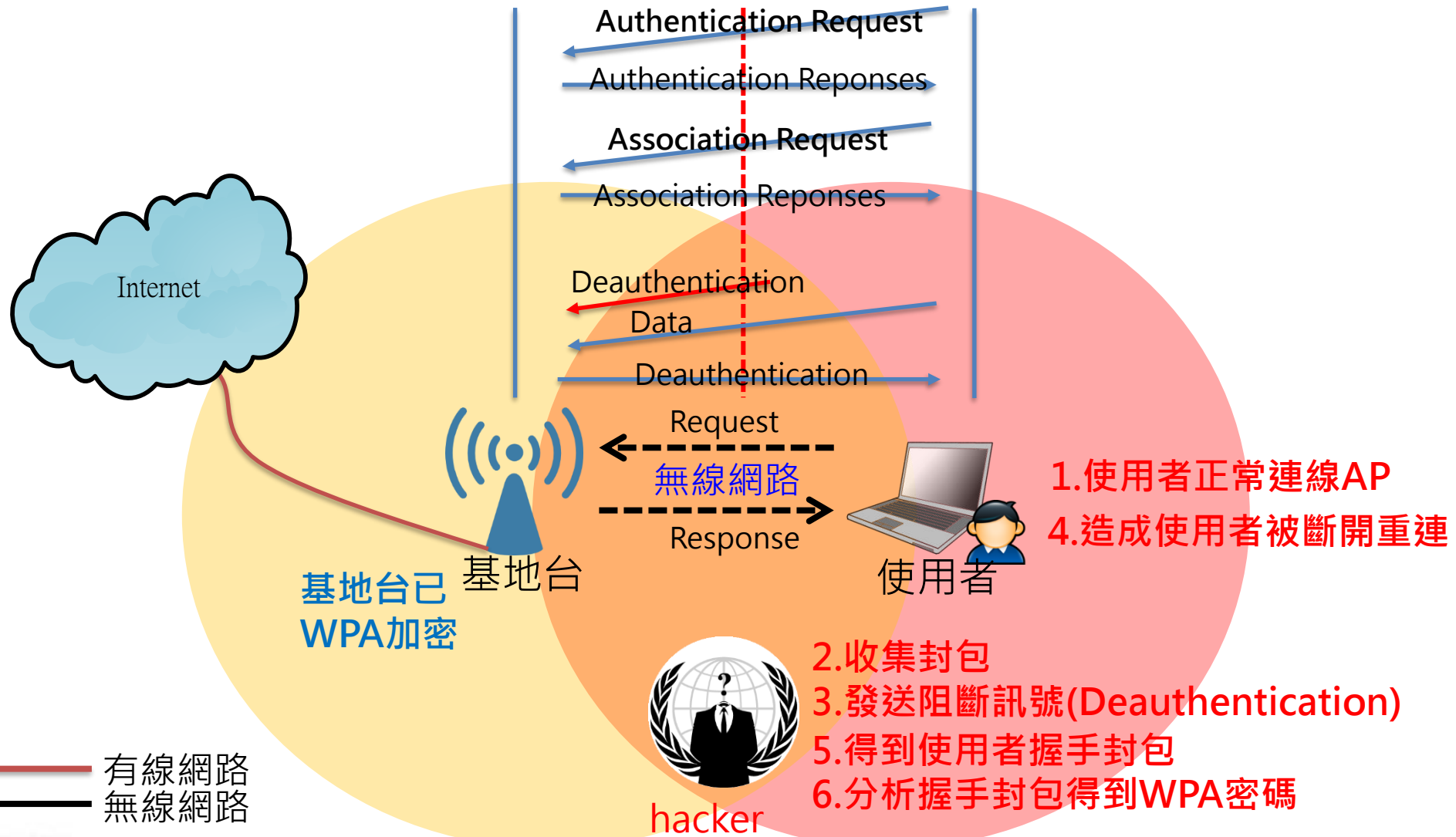
WPA/WPA2破解Demo (2/3)

- 攻擊者必須位於hacker2，也就是同時可以涵蓋使用者與AP的訊號範圍的位置



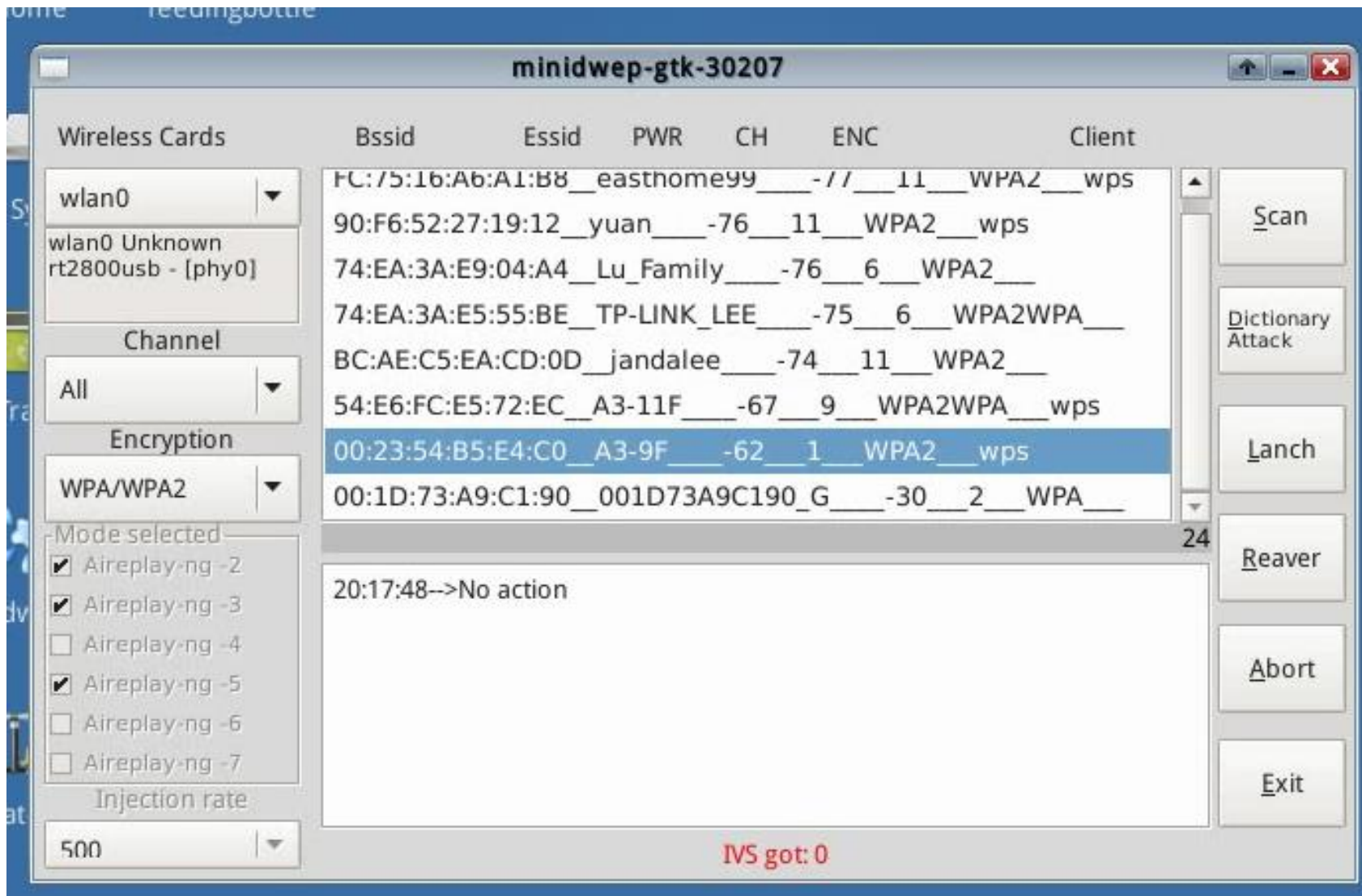
- 送出Deauthentication封包令使用者斷線並伺機取得握手封包
- 對取得之握手封包進行暴力破解，時間從數天至數月，看密碼強度

WPA/WPA2破解Demo (3/3)



WPS Demo (1/2)

- 影片



WPS Demo (2/2)

- 攻擊者只需在有AP訊號範圍，不用有使用者
- 一般破解時間約在8小時左右

WPA3 Timing Attack



WPA3 Timing Attack



Attacker knows password = 3 iterations



HAK5

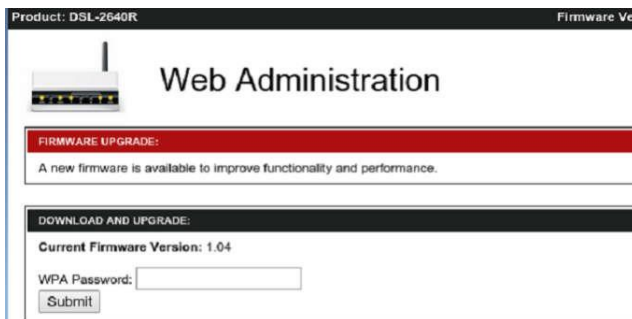
Wi-Fi中間人釣魚攻擊工具：Wifiphisher

- 開源無線安全工具Wifiphisher能夠對WPA加密的AP無線熱點執行**自動化釣魚攻擊**，取得帳戶密碼
- 由於利用了社工原理實施中間人攻擊，Wifiphisher在攻擊時無需進行暴力破解

1. 首先解除攻擊者與AP之間的認證關係

3. 向攻擊者將推送一個以假亂真的路由器設定頁面（釣魚）

2. 受攻擊者登錄假冒AP



```
[+] Ctrl-C at any time to copy an access point from below
num ch  ESSID
-----
1  - 1 - xasaki
2  - 1 - conn-xf41c18
3  - 1 - Thomson06D09C
4  - 6 - BIG BOOBS
5  - 6 - Wind WiFi 5V4Weg
6  - 6 - Petter Pan
7  - 6 - CONNX 1
8  - 6 - CONN-X_6486
9  - 6 - OTENET_6364
10 - 7 - conn-xe0fc94
11 - 9 - hol wifi
12 - 11 - man-max
13 - 11 - @Agra
```



WiFi 干擾裝置

- <https://www.mgteurope.com/>

MGT europe Home About Us Products News Contact Us Sign Up Log In

MGT GHOST-SYSTEM NEW 2022

Digital Audio Transmission System

MGT GHOST-SYSTEM

NEW TINY Digital Audio Transmission System

- ✓ Voice transmitted in stereo mode.
- ✓ High-quality digital coding.
- ✓ Low current use (40mA-Tx).
- ✓ Mics with high sensitivity.
- ✓ Crypto digital transmission.

MGT PIXEL-NANO-3G

GSM Audio Transmitter

MGT PIXEL-NANO-3G

3G GSM, NEW Listening Audio System with ONE CALL

- ✓ SMS tracking with a tiny GPS antenna.
- ✓ Small 3G GSM dimensions.
- ✓ It supports 2G GSM networks.
- ✓ Audio quality very clear.
- ✓ GSM Audio Transmitter

MGT RM2033

Digital Room Monitoring System

MGT RM2033

TWO-CHANNEL DIGITAL ROOM MONITORING

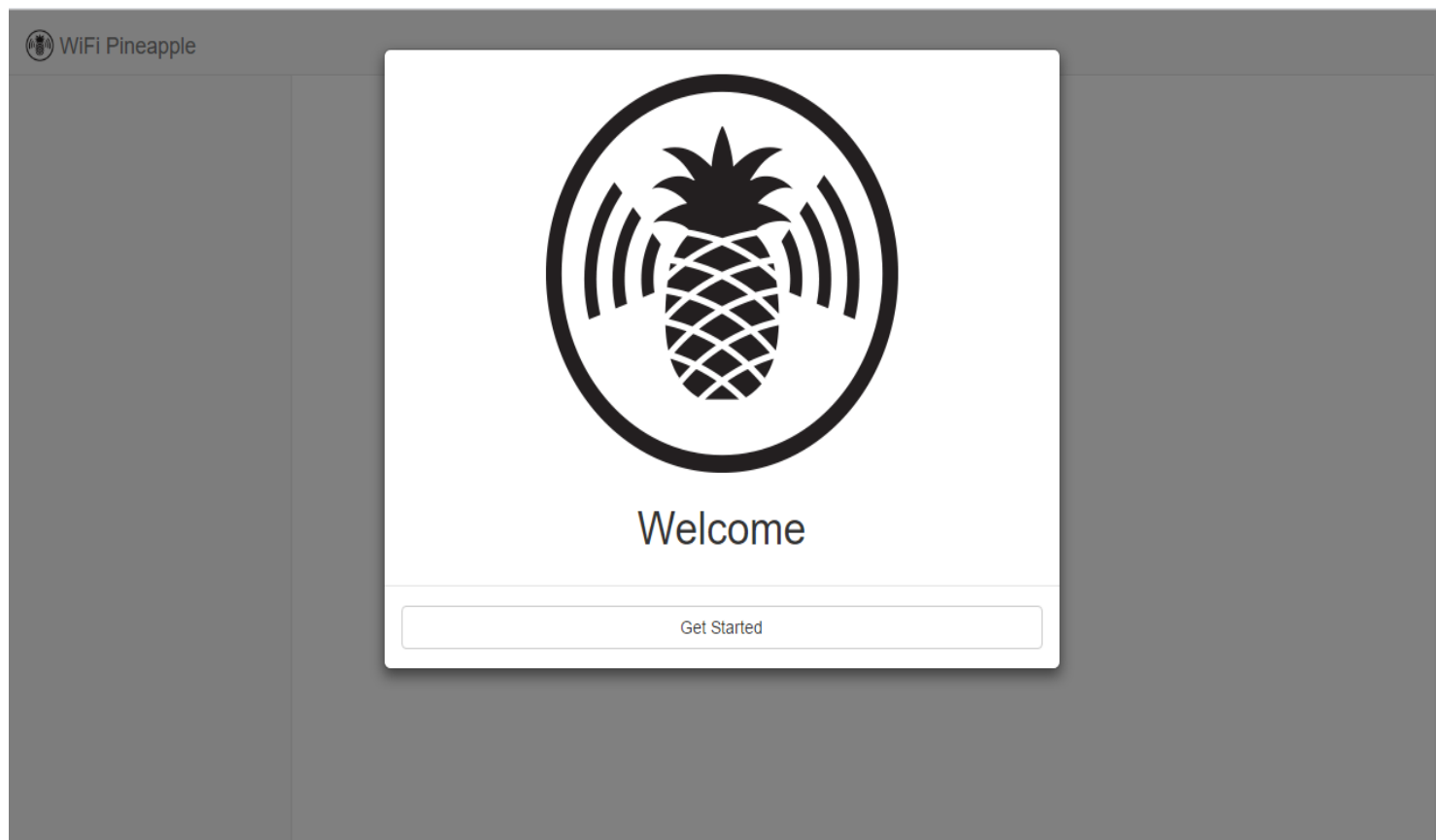
- ✓ Audio-secure digital transmission with jamming-prof.
- ✓ Detection is strongly restricted.
- ✓ LF-amplifier output for each channel is available.
- ✓ Room Monitoring Surveillance Systems
- ✓ Digital Room Monitoring Surveillance Systems

WE ARE SPECIALIST IN COVERT SOLUTIONS

<p>MGT- P6 GPS Jammer</p>  <p>Range : 10 ~ 20 meters 4 antennas 3G: 2110 ~ 2170MHz Wi-Fi / Bluetooth: 2400 ~ 2485MHz</p>	<p>MGT- 04 Wi-Fi Jammer</p>  <p>Range : 5 ~ 80 meters 4 antennas</p>	<p>MGT- MP200 Jammer</p>  <p>Range: 50 - 75m Barrage + DDS sweep jamming 20 to 2500 MHz. Omni-directional antennas</p>
<p>MGT- 03 Jammer</p>  <p>Range : 20 ~ 40 meters External antennas</p>	<p>MGT- P6 Wi-Fi Jammer</p>  <p>Range : 10 ~ 20 meters iDen - CDMA - GSM: 850 ~ 960MHz DCS - PCS: 1805 ~ 1990MHz 3G: 2110 ~ 2170MHz Wi-Fi / Bluetooth: 2400 ~ 2485MHz 4 antennas</p>	<p>MGT- 3x13 Jammer</p>  <p>Range : 50 ~ 120 meters 3 frequency bands jammed</p>

WiFi Pineapple

- <https://www.wifipineapple.com/>



WiFi Pineapple 攻擊模組

WiFi Pineapple ✕

Dashboard

Recon

Clients

Filters

Modules ▾

Manage Modules

nmap

PineAP

Tracking

Logging

Reporting

Networking

Configuration

Advanced

Help

Available Modules Refresh

Module	Version	Description	Author	Size	Type	Action
DWall	1.1	Display's HTTP URLs, Cookies, POST DATA, and images from browsing clients as a stream. Wall of Sheep style.	sebkinne	6.25kb	GUI	<input type="button" value="Install"/>
Deauth	1.4	Deauthentication attacks of all devices connected to APs nearby	whistlemaster	7.21kb	GUI	<input type="button" value="Install"/>
Evil Portal	2.1	An Evil Captive Portal.	newbi3	39.97kb	GUI	<input type="button" value="Install"/>
SSLSplit	1.0	Perform man-in-the-middle attacks using SSLSplit	whistlemaster	6.89kb	GUI	<input type="button" value="Install"/>
Status	1.1	Display status information of the device	whistlemaster	43.56kb	GUI	<input type="button" value="Install"/>
ettercap	1.4	Perform man-in-the-middle attacks using ettercap	whistlemaster	8.27kb	GUI	<input type="button" value="Install"/>
Site Survey	1.2	WiFi site survey	whistlemaster	10.23kb	GUI	<input type="button" value="Install"/>
urlsnarf	1.4	Output all requested URLs sniffed from http traffic using urlsnarf	whistlemaster	5.95kb	GUI	<input type="button" value="Install"/>
Occupineapple	1.5	Broadcast spoofed WiFi SSIDs	whistlemaster	11.52kb	GUI	<input type="button" value="Install"/>
tcpdump	1.4	Dump traffic on network using tcpdump	whistlemaster	6.45kb	GUI	<input type="button" value="Install"/>
DNSspooF	1.3	Forge replies to arbitrary DNS queries using DNSspooF	whistlemaster	6.39kb	GUI	<input type="button" value="Install"/>
SignalStrength	1.0	Displays signal strength for wireless cells that are within range. Can be used to physically locate cells.	r3dfish	16.42kb	GUI	<input type="button" value="Install"/>
RandomRoll	1.1	This module allows you to troll unsuspecting clients connected to your WiFi Pineapple	foxtrot	20403.63kb	GUI	<input type="button" value="Install"/>

使用Kali Linux檢測KRACK

To install the git-master version of Kismet on Kali Linux, follow these steps

First, tell networkmanager to ignore the Wi-Fi device by adding these lines:

```
[keyfile]
unmanaged-devices=interface-name:wlan0
```

to

```
/etc/NetworkManager/NetworkManager.conf
```

Then, restart NetworkManager:

```
root@kali:~# systemctl restart NetworkManager
```

Next, install updates and the git-master version of Kismet:

```
root@kali:~# apt update
root@kali:~# apt upgrade
root@kali:~# git clone https://www.kismetwireless.net/git/kismet.git
root@kali:~# apt install build-essential libmicrohttpd-dev libnl-3-dev libnl-genl-3-dev libcap-dev libpcap
root@kali:~# cd kismet
root@kali:~# ./configure
root@kali:~# make
root@kali:~# make suidinstall
root@kali:~# /usr/local/bin/kismet_capture_tools/kismet_cap_linux_wifi --list
root@kali:~# kismet -c wlan0
```

Next you can browse to <http://localhost:2501> to view the Kismet interface and any alerts. Be sure to log in with the credentials found in

```
~/kismet/kismet_httpd.conf
```

The screenshot shows the Kismet web interface in a browser window. The main content area displays a table of detected Wi-Fi devices with columns for Name, Type, Phy, Signal, Channel, and Last Seen. An alert panel on the right shows a message: "This is the first time you have run Kismet on this account. A new password has been automatically generated, and is in [redacted] kismet/kismet_httpd.conf. You will need this password to configure Kismet from the web interface." Below the table, a terminal window shows a list of detected packets with columns for Messages, Channels, and packet details.

Name	Type	Phy	Signal	Channel	Last Seen
		IEEE802.11	-94	2.462 GHz	Oct 18 2017 19:56:32
	Wi-Fi Bridged Device	IEEE802.11	-81	2.447 GHz	Oct 18 2017 19:56:36
	Wi-Fi Client	IEEE802.11	-43	9	Oct 18 2017 19:56:49
	Wi-Fi Bridged Device	IEEE802.11	-32	2.462 GHz	Oct 18 2017 19:56:42
	Wi-Fi Bridged Device	IEEE802.11	-85	2.412 GHz	Oct 18 2017 19:57:28
	Wi-Fi AP	IEEE802.11	-83	11	Oct 18 2017 19:57:38
	Wi-Fi AP	IEEE802.11	-90	9	Oct 18 2017 19:57:35
	Wi-Fi Bridged Device	IEEE802.11	-90	2.442 GHz	Oct 18 2017 19:57:23
	Wi-Fi Bridged Device	IEEE802.11	-85	2.447 GHz	Oct 18 2017 19:56:31
	Wi-Fi Bridged Device	IEEE802.11	-93	2.412 GHz	Oct 18 2017 19:57:22

The screenshot shows the Alerts panel in the Kismet web interface. It displays two alerts:

- Oct 18 2017 19:48:59 NONCEREUSE**
WPA EAPOL RSN frame seen with a previously used anonce; this may indicate a KRACK-style WPA attack (anonce: 86466611F86F24A69BBBC059B5A6220EF95D072BCA86499641C9A6E50EB28B8D)
- Oct 18 2017 19:45:14 CHANCHANGE**
IEEE80211 Access Point BSSID F0A8B04A6E07E SSID "Poland's Truth" changed advertised channel from 6 to 1 which may indicate AP spoofing/impersonation



無線網路金鑰被破解了會怎樣？

透過金鑰可以解析加密後的無線封包

- 透過**加密方式**使得廣播的封包就算被聽到也無法理解
- 但是當駭客得到**金鑰**之後，一切又都聽得懂了!



監聽無線網路封包的工具

- 在擁有無線網路加密金鑰之後，可以透過下列工具聽取無線網路封包：
 - Commview For Wifi 7.3
 - 支援Intel 網卡，許多筆電內建這張網卡，因此一般筆電也可以聽封包
 - AiropEEK
 - 支援歐美大廠的網卡Atheros、Cisco、Proxim、3com
 - Aircap Nx
 - 有良好的開發工具，Aircap <http://www.airpcap.nl/airpcap-nx.htm>
 - ，但是只支援自己的卡










Acrylic Wi-Fi Sniffer

Acrylic Wi-Fi Sniffer

We have recently launched a new tool that represents a radical evolution in the capture of WiFi traffic, previously done with Aircap cards in Windows. Using our [WiFi Sniffer](#) you can obtain all the information provided by AirPCAP cards including SNR values, and additionally, capture all traffic transmitted on **802.11ac** networks in all channel widths (20/40/80/160MHz).

The list of compatible cards is as follows:

Device		Channel width (MHz)				Bandwidth (GHz)		SNR	Compatibility
		20	40	80	160	2.4	5		
ALFA Network AWUS1900		✓	✓	✓	✓	b/g/n	a/n/ac	✓	Recommended
COMFAST CF-958AC		✓	✓	✓	✓	b/g/n	a/n/ac	✓	Recommended
ASUS USB-AC68		✓	✓	✓	✓	b/g/n	a/n/ac	✓	Recommended
D-Link DWA-192		✓	✓	✓	✓	b/g/n	a/n/ac	✓	Recommended
Edimax EW-7833UAC		✓	✓	✓	✓	b/g/n	a/n/ac	✓	Recommended
TP-LINK Archer T9UH		✓	✓	✓	✓	b/g/n	a/n/ac	✓	Recommended
ALFA AWUS036ACH		✓	✓	✓		b/g/n	a/n/ac	✓	Very Good
HP-Pavilion 802.11 n WLAN		✓	✓			b/g/n	-		Good
Sweex LW153 802.11n Adapter		✓	✓			b/g/n	-		Good
Sweex LW164 Wireless 150N Nano		✓	✓			b/g/n	-		Good

War-Driving

- 所謂War-Driving，就是帶著無線電腦或無線電裝置，利用掃描程式，在戶外沿著街道行走，以搜尋、找出、辨識無線網路存取點 (Access Point)
- 這種為戶外無線網路進行的測試調查在外非常普遍及受重視，主要目的是檢測無線網路於公眾環境的連接情況，檢測無線網路的可靠性及安全性
- 另一方面，利用War-Driving技術，可檢測及分析無線網路的覆蓋程度，方便用戶尋找最佳及最穩定的網路存取點

War-Driving

Mem: 26% CPU: 02% ↑0.00B ↓0.00B 12月2日 周日 下午 1:57

```
1 select a.bssid , a.lat,a.lon ,b.ssid ,b.capabilities from location a ,network b where a.bssid = b.bssid group by a.bssid
```

Duration: 0.029 seconds * Col: 121 Row: 1/

Full View Item View Script Output

	bssid	lat	lon	ssid	capabilities
1	00:0a:c2:31:4d:ad	31.266503	121.438306	ChinaNet-67cY	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]
2	00:1d:0f:97:1b:88	31.266503	121.438306	TP-LINK	[ESS]
3	00:23:cd:85:3e:18	31.266503	121.438306	ahl007	[WEP][ESS]
4	00:23:cd:e1:6a:a8	31.26671753	121.4385221	fying	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP-preauth][ESS]
5	00:25:86:3c:10:30	31.266943	121.4395591	TP-LINK_3C1030	[WPA2-PSK-CCMP-preauth][ESS]
6	00:25:86:82:41:16	31.266943	121.4395591	MERCURY_824116	[WPA2-PSK-TKIP-preauth][ESS]
7	00:27:19:5e:f9:62	31.266503	121.438306	TP-LINK_5EF962	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP-preauth][ESS]
8	00:27:19:98:1b:5c	31.2667301	121.4388318	TP-LINK_981B5C	[WEP][ESS]
9	00:27:19:a2:e6:08	31.266943	121.4395591	MERCURY_EMMA	[WEP][ESS]
10	0c:4c:39:3d:89:7c	31.266503	121.438306	ChinaNet-ycl1	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]
11	0c:4c:39:3d:90:fc	31.266503	121.438306	ChinaNet-ycl2	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]
12	14:e6:e4:37:09:32	31.26671753	121.4385221	msc	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]

Query OK
Row(s) returned: 99
select a.bssid , a.lat,a.lon ,b.ssid ,b.capabilities from location a ,network b where a.bssid = b.bssid group by a.bssid

War-Driving 工具 – WiGLE (1/2)

- https://play.google.com/store/apps/details?id=net.wigle.wigleandroid&hl=zh_TW&gl=US

Google Play 遊戲 應用程式 影視 圖書 兒童

WiGLE WiFi Wardriving

WiGLE.net

4.3★
4740 則評論

50萬+
次下載

E
適合所有人

安裝

應用程式支援

同類型應用程式

- WiFiman
Ubiquiti Inc.
4.7★
- NetSpot WiFi Heat Map Analyzer
Etwok, Inc.
4.0★
- Wi-Fi Toolkit
TP-LINK GLOBAL INC.
4.2★
- NETGEAR Nighthawk WiFi Router
NETGEAR, Inc.
4.3★
- Net Signal Pro:WiFi & 5G Meter
Phuongpn
4.7★ US\$0.49

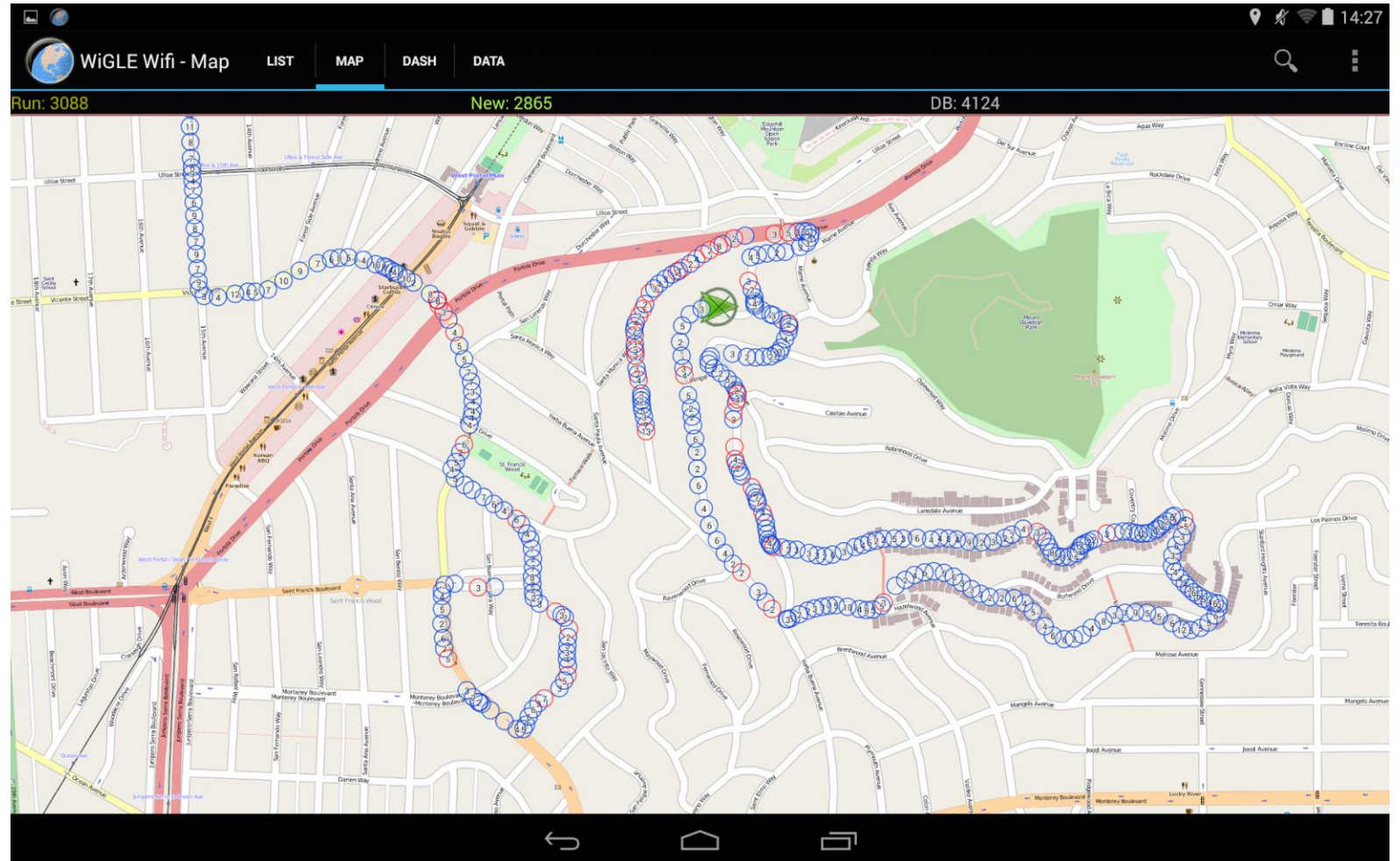
關於這個應用程式 →

開源網絡觀察，定位，並顯示客戶端從無線網絡的世界上最大的可查詢數據庫。可用於現場調查，安全分析，競爭與您的朋友。收集的個人研究或上傳到網絡<https://wigle.net>。自2001年以來威格爾一直收集和映射網絡數據，並且目前有超過350米網絡。威格爾是*不*網絡可以使用的列表。

*使用GPS來估算觀察網絡的位置
*記錄到本地數據庫觀察跟蹤發現你的網絡...

更新日期
2024年4月25日

War-Driving工具 – WiGLE (2/2)



WarKittteh – 貓也可以... !?

家貓功能再進化：WiFi 偵測器

由 Casper 於 六, 2014/08/09 - 11:03am 發表

80 3 1
讚 8+1 推文
分享

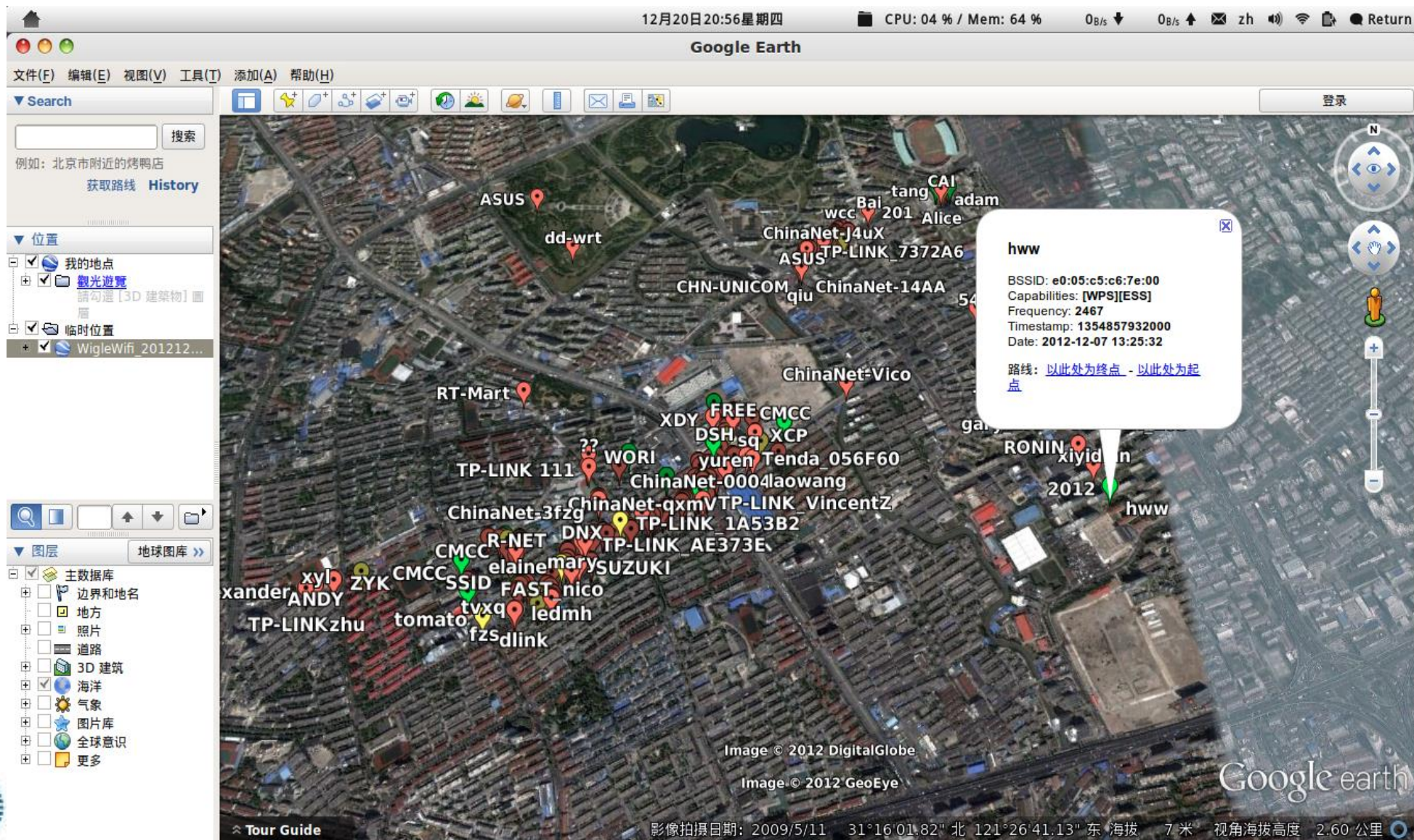


圖片引用來源：[Flickr](#)；原文引用來源：[The Verge](#)

安全專家 Gene Bransfield 最近想到了一個有趣的方法，來偵測住家附近未受安全保護的 WiFi 熱點，他在自家小貓（上圖為示意圖，非本貓）Coco 的頸環當中，塞了一張 WiFi 網路卡、GPS 模組、電池，以及一片 Spark Core 晶片，再用自己撰寫的程式進行 WiFi 熱點訊號搜尋任務，同時還可以紀錄該熱點是否有用任何密碼保護，或者那些還在使用容易受破解的 WEP 加密。



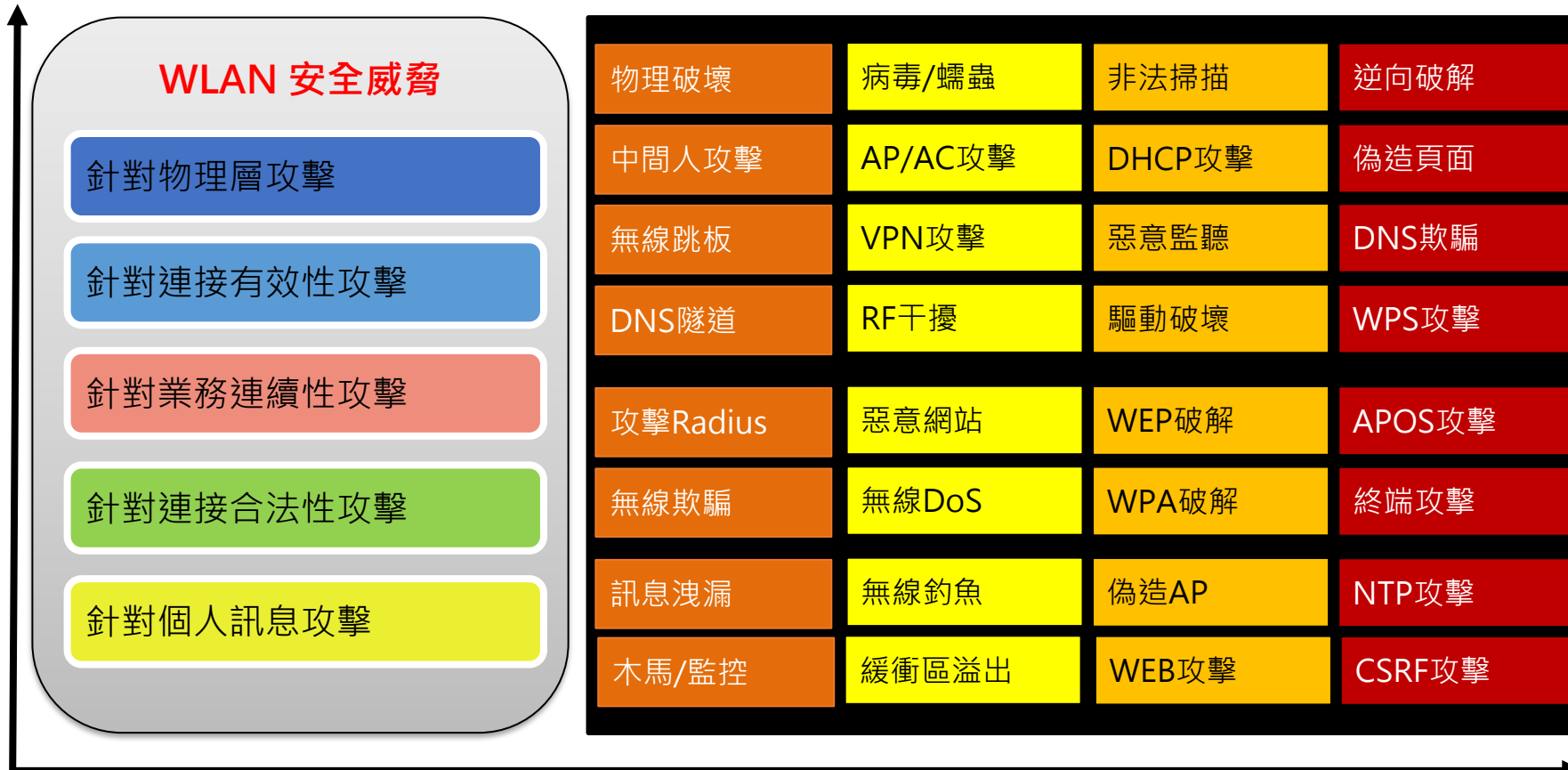
結合無線訊號與GPS座標



最強大的War-Driving

- Wi-Fi 定位：靠的是偵測附近周圍所有的無線網路基地台 (Wi-Fi Access Point) 的 MAC Address (類似 10-78-D2-93-58-C2 這樣的格式)，去比對資料庫中該 MAC Address 的座標，交叉連集出所在地。此法尚需有網路連線做資料庫查詢才能完成定位
- 這份無線網路基地台 MAC Address 對應到經緯度的資料庫，是怎麼建立起來的呢？
 - 基礎建設靠的是 Google 街景車。Google 街景車除了拍下街景以外，另外還做了兩件事情：
 - 沿路蒐集所有公開的無線網路 MAC Address，與當時的經緯度一併記錄
 - 根據拍下的街景來建立建築物 3D 模型資料
 - 資料來源：[Google blog](#)

無線網路威脅



通訊標準弱點 – FragAttacks漏洞

- 2021年，比利時資安研究人員 Mathy Vanhoef發表論文指出，發現多個 802.11 Wi-Fi 無線網路連線標準資安漏洞
- 可用於挾持物聯網與各種電腦、行動裝置，而且即使套用最新加密連線協定如 WPA3 也一樣有效，其中有些漏洞存在長達 24 年之久
- 稱為 Frag Attacks (Fragmentation and Aggregation Attacks)，攻擊者只要位在有效的 Wi-Fi 通訊範圍內，即可透過這種攻擊手法取得資訊，或是在受害裝置上執行惡意軟體
- 只是這種攻擊方法相當複雜，不易實作
- 資安漏洞共有 12 個，分為3種類別：Wi-Fi 標準設計上的漏洞有3個；存於 Wi-Fi 標準的實作上有4個；其他實作層面的漏洞則有5個
- 解決/緩解方法：使用HTTPS加密連線，盡可能安裝所有可用的更新

所有Wi-Fi裝置皆存在FragAttacks漏洞，可被駭客用來竊取個人資訊和攻擊裝置

研究人員發現，所有的Wi-Fi裝置皆至少存在一個FragAttacks系列漏洞，而絕大多數的裝置則受多個漏洞影響

文/ 李建興 | 2021-05-12 發表

讚 476 分享

.....

FragAttacks一系列的漏洞，其中3個來自Wi-Fi標準中的設計缺陷，所以大多數的裝置都受到影響，而更重要的是，Mathy Vanhoef還發現了一些漏洞，這些漏洞是由Wi-Fi產品中普遍存在的程式錯誤引起。經證實，每個Wi-Fi產品都至少受一個FragAttacks漏洞影響，並且絕大多數的產品都存在多個漏洞。

這些漏洞影響所有Wi-Fi的安全協定，包括最新的WPA3規範，甚至是Wi-Fi最初的安全協定WEP都在影響範圍中，也就是說，從1997年Wi-Fi發布一樣，這些設計缺陷已經成為Wi-Fi的一部分。值得慶幸的是，設計缺陷難以被駭客利用，Mathy Vanhoef提到，因為這些設計缺陷必須要有用戶參與，才有可能被濫用，又或是只有在使用不常見的網路配置時，才有可能被實現。

因此FragAttacks漏洞最大的隱憂，還是在Wi-Fi產品的程式錯誤，其中幾個漏洞可輕易地被惡意攻擊者利用。

FragAttacks漏洞包括了一個明文注入漏洞，惡意攻擊者可以濫用實作缺陷，將一些惡意內容注入到受保護的Wi-Fi網路中，尤其是攻擊者可以注入一個精心建構的未加密Wi-Fi訊框 (Frame)，像是透過誘使客戶端使用惡意DNS伺服器，以攔截用戶的流量，或是路由器，也可能被濫用來繞過NAT或防火牆，進而使攻擊者之後可以攻擊本地端中的Wi-Fi裝置。

另外還有一些實作漏洞，例如即便發送者未通過身分驗證，部分路由器也會將交握訊框發送給另一個客戶端，這個漏洞讓攻擊者不需要用戶交握，即可執行聚合攻擊注入任意訊框。還有一個極為常見的實作錯誤，便是接收者不檢查所有片段是否屬於同一訊框，這代表攻擊者可以混和兩個不同訊框的片段，來偽造訊框。

即便部分裝置不支援分段或是聚合功能，但是仍然容易受到攻擊，因為這些裝置會將分段的訊框，當做完整的訊框進行處理，在部分情況這可能會被濫用來注入資料封包。

設備漏洞 – 智慧燈泡漏洞讓駭客取得Wi-Fi密碼

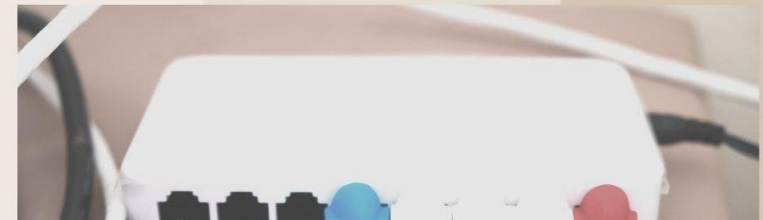
- 2023年，義大利與英國資安研究人員聯合發表研究報告，指出TP-Link 智慧燈泡 Tapo L530E 與其控制用行動軟體 Tapo App，內含 4 個嚴重漏洞，駭侵者可藉以竊取使用者設定的 **Wi-Fi 連線密碼**
 - 其中一個漏洞可讓鄰近攻擊者取得 Tapo 系統的使用者密碼，以控制 Tapo 系列裝置
 - 一個漏洞是硬式編碼（hard-coded）在程式碼中的共享密碼，僅使用很短的 checksum 加密，入侵者可透過暴力破解取得這些密碼
 - 另一個漏洞是在進行加密時缺少隨機性，因此其加密方式可預測得知
 - 第四個漏洞是訊息在執行期間的有效期限長達 24 小時，使得入侵者可以在期間內不斷重播訊息
- 使用各類 IoT 裝置的使用者或系統管理者，必須隨時保持這些裝置與其軟體**維持在最新版本**，且應在**原廠發表資安修補時立即更新**



設備漏洞 – 多款家用路由器發現資安漏洞

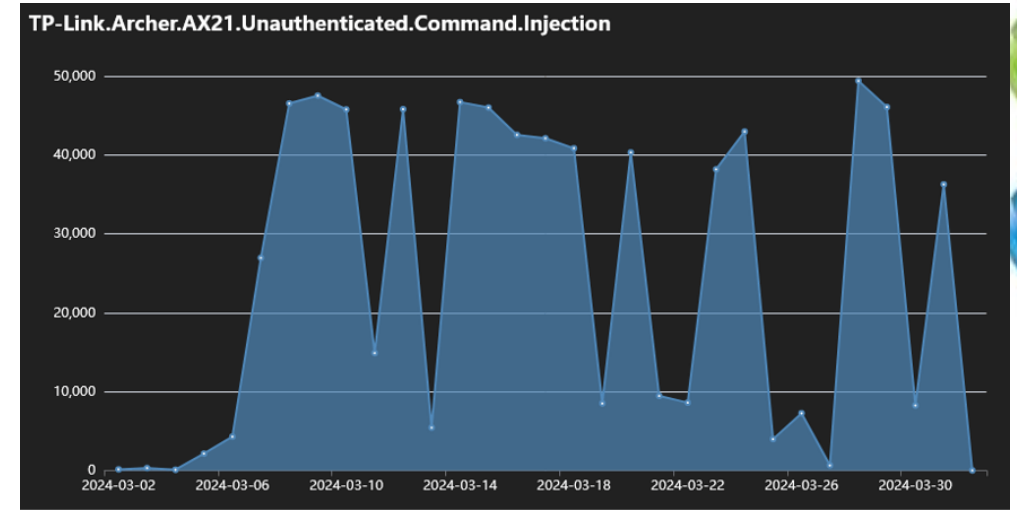
- 2021年，資安廠商 IoT Inspector 與德國資訊科技媒體 CHIP，蒐集市面上十分熱門的家用無線路由器來進行測試，其中也包括數個台灣廠商的產品
 - Asus ROG Rapture GT-AX11000：25 個
 - AVM FritzBox 7530AX：20 個
 - AVM FritzBox 7590AX：18 個
 - D-Link DIR-X5460：26 個(D-Link 支援公告請點此)
 - Edimax BR-6473AX：25 個
 - Linksys Velop MR9600：21 個
 - Netgear Nighthawk AX12：29 個
 - Synology RT-2600AC：30 個
 - TP-Link Archer AX6000：32 個
- CHIP 測試的都是市場上的最新機種，廠商送測時也均更新至最新版本
- 使用家用路由器應時常注意並安裝更新
- 主要問題
 - 韌體採用的 Linux 作業系統版本太過老舊
 - 多媒體與 VPN 功能使用的程式碼太過老舊
 - 採用的 BusyBox 程式版本太舊
 - 使用容易遭到破解的管理者密碼
 - 在韌體程式碼中以明文寫入登入資訊

多款家用路由器發現資安漏洞
國內廠商已釋出更新檔
建議用戶盡速進行更新



設備漏洞 – 路由器漏洞遭濫用導致設備被綁架

- 2023年3月TP-Link修補旗下無線路由器Archer AX21命令注入漏洞CVE-2023-1389（CVSS風險評分為8.8），隨後就傳出被用於散布殭屍網路病毒Mirai，如今有更多經營殭屍網路的駭客加入漏洞利用的行列
- 資安業者Fortinet指出，他們最近發現有6種殭屍網路病毒利用上述漏洞，自今年3月開始，試圖利用該漏洞的攻擊行動大多一天超過4萬次，到了3月底更出現接近5萬次的高峰
 - 包括Moobot、Miori、Condi，Go語言打造的AGoent，以及Gafgyt和Mirai變種病毒
- Gafgyt、Condi用來發動DDoS攻擊
 - Gafgyt植入路由器並與C2建立連線，就會持續接收PING命令，並等待C2下達攻擊命令，該病毒能執行4種類的DDoS攻擊
 - Condi則是在感染途徑上，透過指令碼存取多種通訊協定，從而增加成功感染的機會。此外，這種殭屍網路病毒的開發者，也標榜它能夠發動多種類型的洪水攻擊



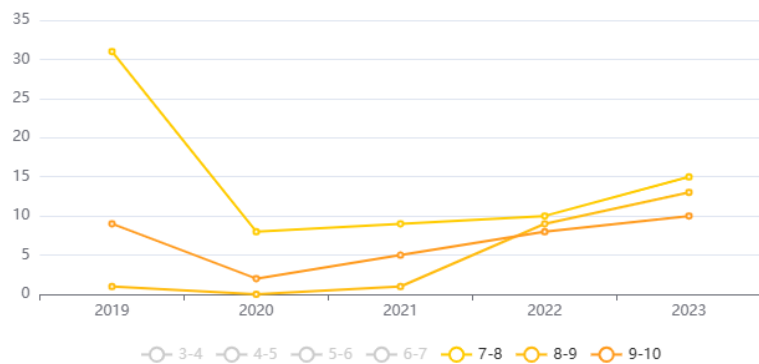
無線基地台本身漏洞

資料來源: <https://www.cvedetails.com/>

Asus: CVSS Scores Between 2019-01-01 and 2023-12-31

Period Group By Year

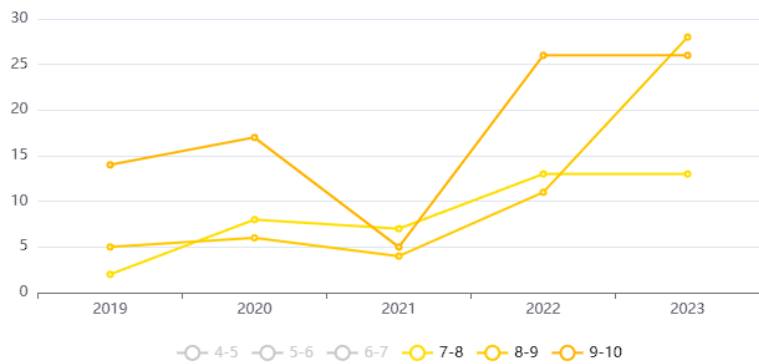
Vulnerabilities by max CVSS base scores



Tp-link: CVSS Scores Between 2019-01-01 and 2023-12-31

Period Group By Year

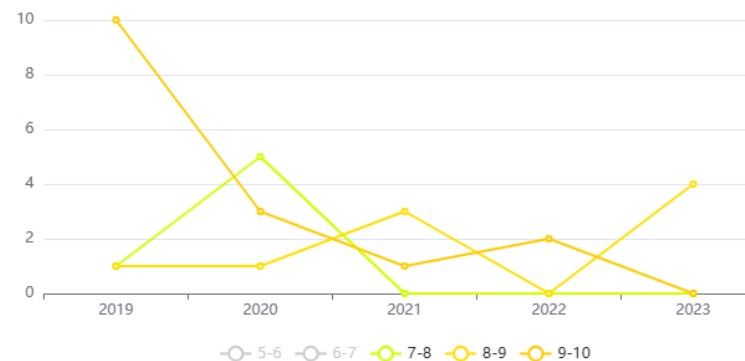
Vulnerabilities by max CVSS base scores



D-link: CVSS Scores Between 2019-01-01 and 2023-12-31

Period Group By Year

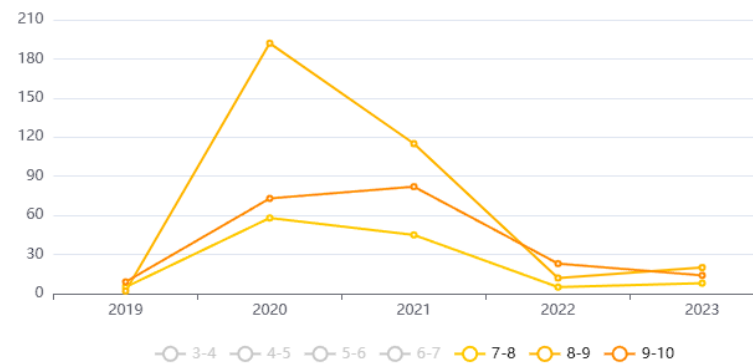
Vulnerabilities by max CVSS base scores



Netgear: CVSS Scores Between 2019-01-01 and 2023-12-31

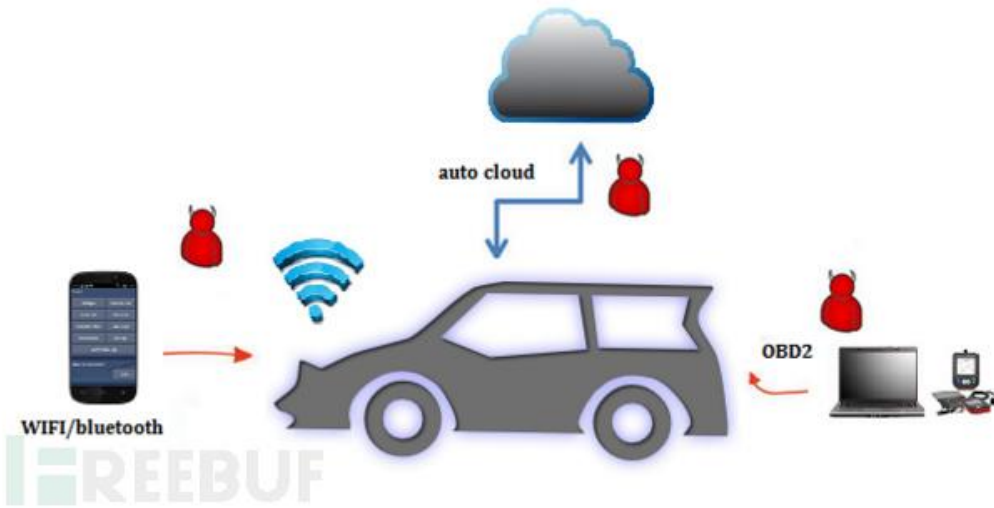
Period Group By Year

Vulnerabilities by max CVSS base scores



汽車攻擊離你很近：一分鐘變身汽車駭客

- 從車外攻擊：攻擊者無需坐在車裡，在車外就可以通過手機Wi-Fi甚至行動網路，讓被攻擊者的汽車在駕駛途中熄火，遙控打開其後備箱進行偷盜，模擬電子鑰匙打開車門車窗（租車公司痛點）等動作



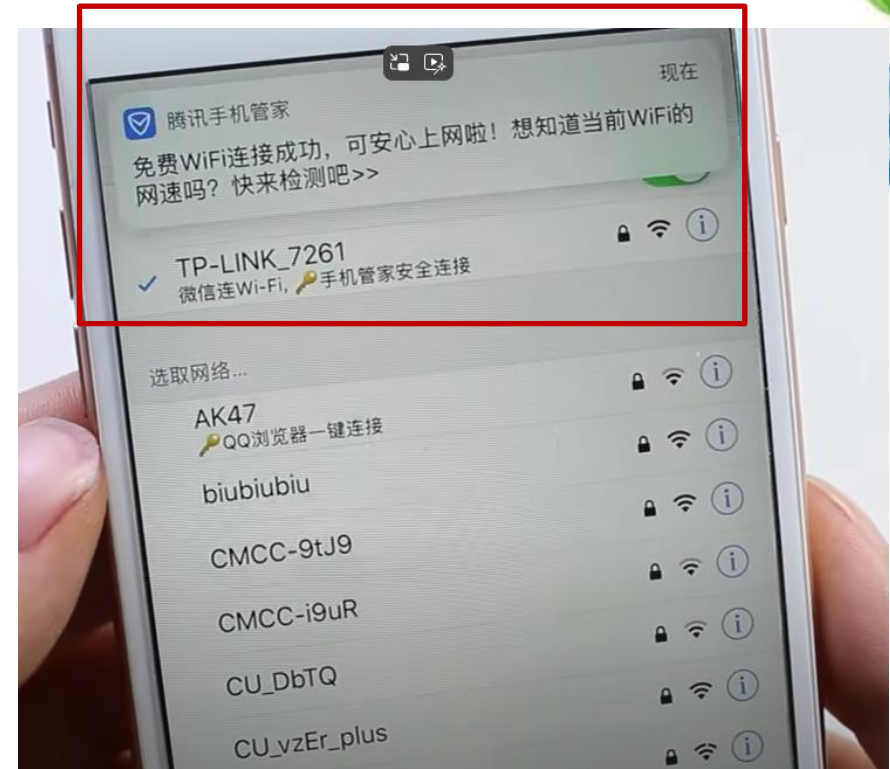
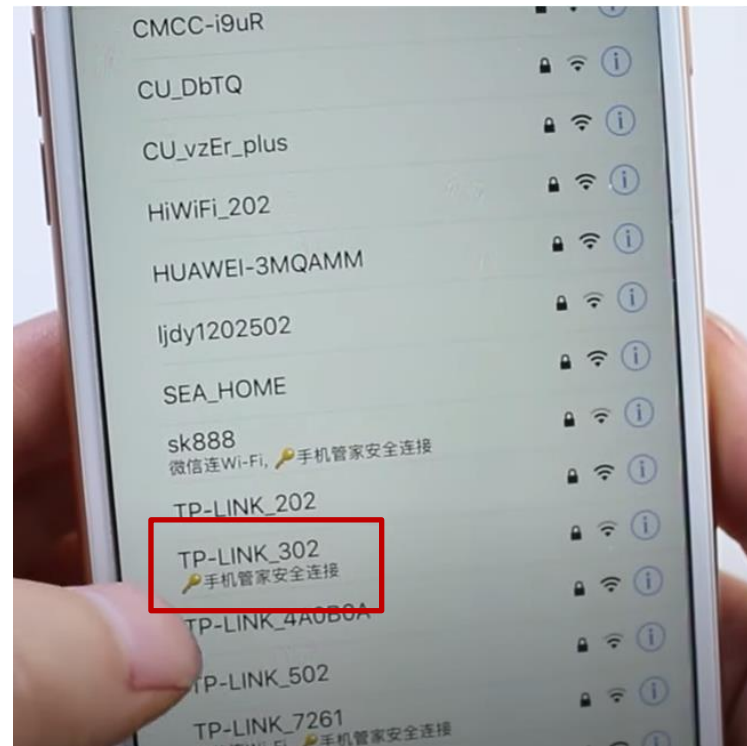
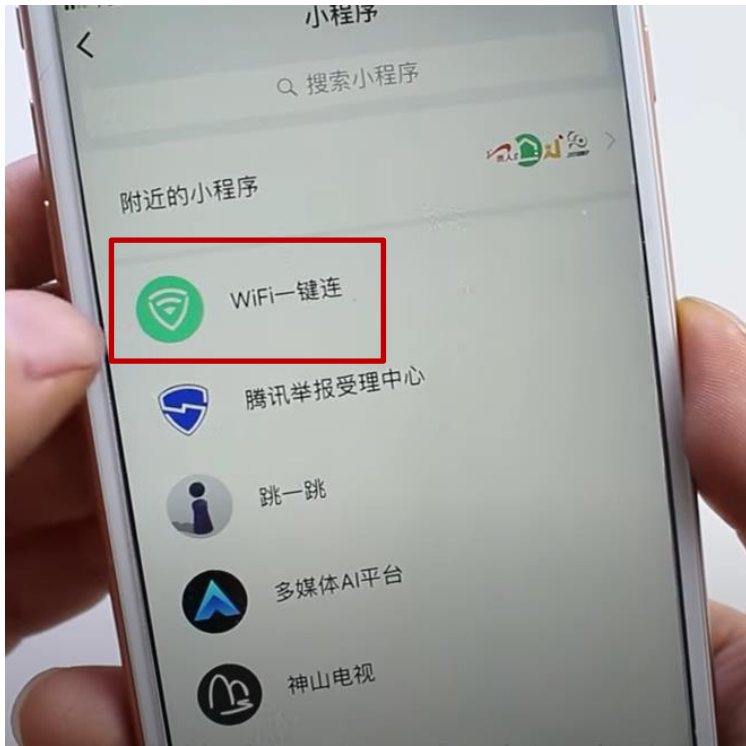
資料來源: FreeBuf

WiFi萬能鑰匙

- WiFi萬能鑰匙PC是一款自動連接用戶共用的免費WiFi熱點軟體，是無線路由器流量分享、連接管理必備利器，非密碼破解工具
- 會自動把已知WiFi密碼分享給他人使用
- 不僅有PC版，也有iOS跟Android版本
- 不要裝!!!



微信內Wi-Fi一鍵連 (不需密碼)





4. 如何強化無線網路安全



如何加強無線網路安全 – 個人篇

如何強化無線網路安全 – 一個人(1/2)

- 避免連接**未加密**的無線網路AP
 - 使用未加密連線時有可能會遭受駭客竊聽流量，趁機盜取重要資訊
 - 未加密的AP也可能是所謂的惡意AP，有可能是有心人士刻意提供免費網路給其他人用，卻刻意記錄所有經過的流量，趁機取得資訊
- 避免使用**WEP**加密無線網路
 - 只需3分鐘不到就可以破解WEP網路，基本上已經可以認定為不具備安全性
- 立即關閉**WPS**
 - WPS的新漏洞，WPS網路在一天之內就可以被破解，與真正破解WPA/WPA2的時間比起來，算是非常短，建議立即關閉

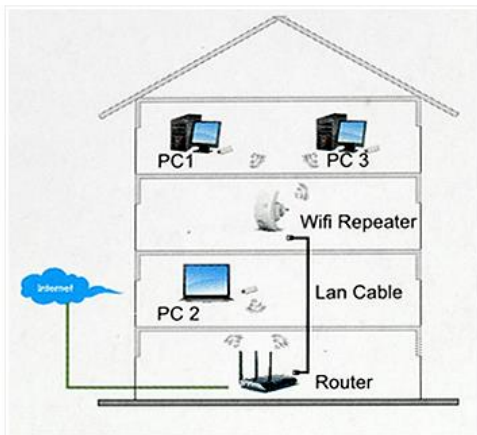
你家的Wi-Fi路由器還沒設密碼嗎？當心成盜刷集團幫兇



根據蘋果日報的報導，一名新竹的林姓女子接到警方的傳喚，被懷疑涉及網路上多起信用卡的盜刷案件，並且家中的網路設備也同時被查扣。莫名其妙的林姓女子就這麼惶恐的度過了好幾天，一直到最後警方才確認林姓女子其實也是受害者，起因在於家中無線網路沒有設密碼，因此遭到歹徒的盜用。

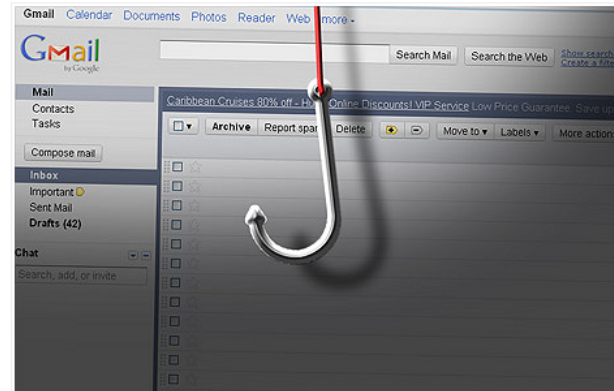
雖然大家都知道家中的無線AP應該要設密碼，但是大概十個家庭裡頭有八家都嫌麻煩，不是想「反正我家電腦也沒什麼機密資料，應該沒有駭客會這麼湊巧住在我家隔壁，想來入侵我家的電腦吧？」就是覺得「每次朋友來要用Wi-Fi，都還要記密碼好麻煩，有人要用就大方分享給他們用吧！」

的確，在過去大家覺得要駭電腦好像是很難的一件事，而且Wi-Fi的訊號範圍有限，左鄰右舍大家都是好鄰居，應該不會有人想要盜用我們的無線訊號。但如果你這麼想，就大錯特錯了。



▲ 很多人懂得怎麼在自己家架設無線網路，甚至還知道怎麼串接，但是卻懶得設定密碼。

根據蘋果日報的報導，國內警方從六月份開始，陸續接到有民眾指出自己的信用卡遭到盜刷。深入調查發現，歹徒是利用釣魚網站偽裝成國內知名的購物網站，然後透過釣魚信件來跟民眾宣傳說有週年慶好康活動，誘騙民眾到這個假的購物網站去消費刷卡。因此，當民眾在線上登入自己的資料，歹徒也就取得了民眾信用卡的資訊。之後這些資料被歹徒用來購買遊戲點數的儲值卡以及線上遊戲點數，拿去出售圖利。



在追查這個詐騙集團的時候，由於釣魚網站都是設在國外調查不易，警方轉而利用歹徒盜刷購買點數卡時留下的IP位址，來鎖定追查盜刷集團，打算查出IP位址的真實所在地，查出幕後的犯人。

透過這個方式，警方依照刷卡時的IP鎖定了六個嫌犯，但是卻發現這六名「嫌犯」都只是單純的上班族、家庭主婦，甚至對於網路也沒什麼概念，一點都不像高科技的駭客。最後警方才發現，這些人的共通點都是：家中的無線AP沒有設密碼。

不過，還好警方又從另外的管道，找到了真正的歹徒。警方透過盜刷信用卡所購買的電話卡資料，追查到了真正的歹徒，才發現這個歹徒是那六名「嫌犯」中一名林姓女子的鄰居。證實了這名歹徒是利用登入鄰居的無線網路，去連上真正的購物網站，利用竊取得來的信用卡資料進行刷卡購買點數卡、遊戲卡的動作。



如何強化無線網路安全 – 一個人(2/2)

- 使用WPA/WPA2時加上**強密碼**
 - 破解WPA/WPA2的限制較多，駭客需要同時影響客戶端與AP才能進行破解，且運算需要較多時間，因此使用較強的密碼可以避免被破解
- 可以的話使用**WPA 3 Personal**
- 存取**白名單**
 - 可以在AP加上網路卡號白名單，限制可以存取無線網路的機器，就算對方破解加密，也無法使用網路(但是仍可以竊聽封包)
- 定期檢查並套用路由器/AP**更新**

駭客會嘗試透過無線網路竊取資訊



在外使用無線網路很危險

荷蘭記者口述：危機四伏的公共WiFi

cindy 2014-11-05 共22485人圍觀，發現22個不明物體 專題 無線安全



黑客Wouter走進一家咖啡館，優雅的點了杯卡布奇諾。20分鐘之後，他已經知道咖啡館裡每個人的出生地、來自哪所學校以及他們在搜索引擎上最近瀏覽的內容.....

我是偶然在阿姆斯特丹市中心的一家咖啡館與Wouter認識的。Wouter Slotboom，34歲，是一名黑客。在他的雙肩包裡，永遠都裝著一部只有煙盒大小並且配有天線的黑色裝置。

Wouter Slotboom向我演示了黑客是如何截獲那些使用公共WiFi用戶的個人信息的：

那天陽光明媚，咖啡館裡幾乎坐滿了人。有的人在聊天、有的人在上網、有的人在玩手機.....Wouter找了一個位置坐下，從背包裡拿出了他的筆記本電腦和黑色裝置。點了兩杯咖啡並向服務員索取了咖啡館裡的公共WiFi密碼。

一切已經準備妥當，黑客行動即將上演。

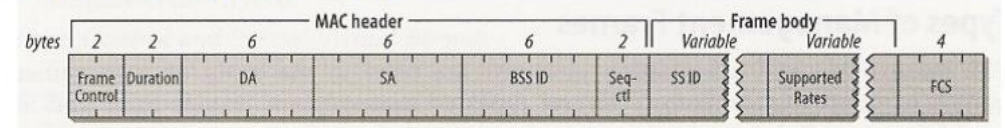
駭客會掃描同網段內的主機漏洞



駭客有辦法讓你自動連上陌生Wi-Fi

- 搭建一個你之前就連接過的Wi-Fi，**SSID**與加密方式與之前一樣，這樣你的設備搜到該Wi-Fi之後就會自動連接
- 解決方法
 1. 刪掉所有未開加密的**SSID**
 2. 在不用Wi-Fi的情況下關閉Wi-Fi連接

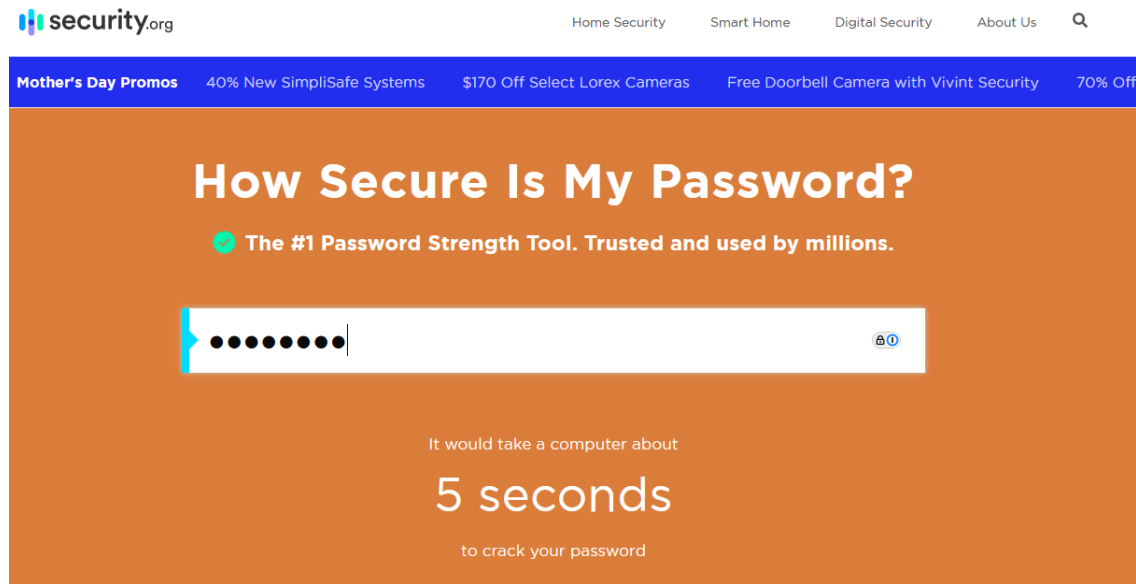
■ Probe Request Frame



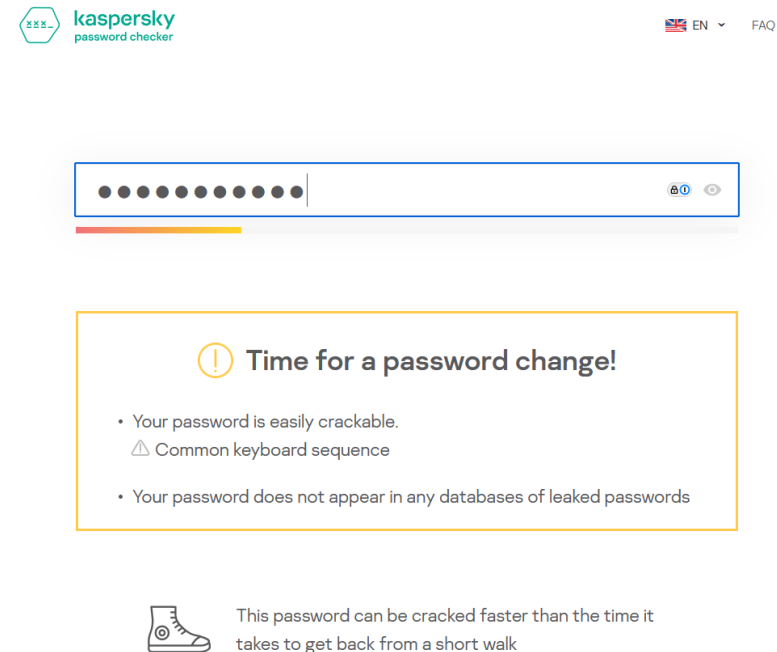
<https://wifipineapple.com>

駭客破解你的密碼要花多少時間?

- <https://password.kaspersky.com/>
- <https://www.security.org/how-secure-is-my-password/>
- 建議不要輸入自己的真實密碼!



The screenshot shows the security.org website interface. At the top, there's a navigation bar with 'Home Security', 'Smart Home', 'Digital Security', and 'About Us'. Below that, a blue banner advertises 'Mother's Day Promos' with various discounts. The main content area has a large orange background with the title 'How Secure Is My Password?' and a sub-headline 'The #1 Password Strength Tool. Trusted and used by millions.' A password input field is shown with a strength indicator. Below the field, it states 'It would take a computer about 5 seconds to crack your password'.

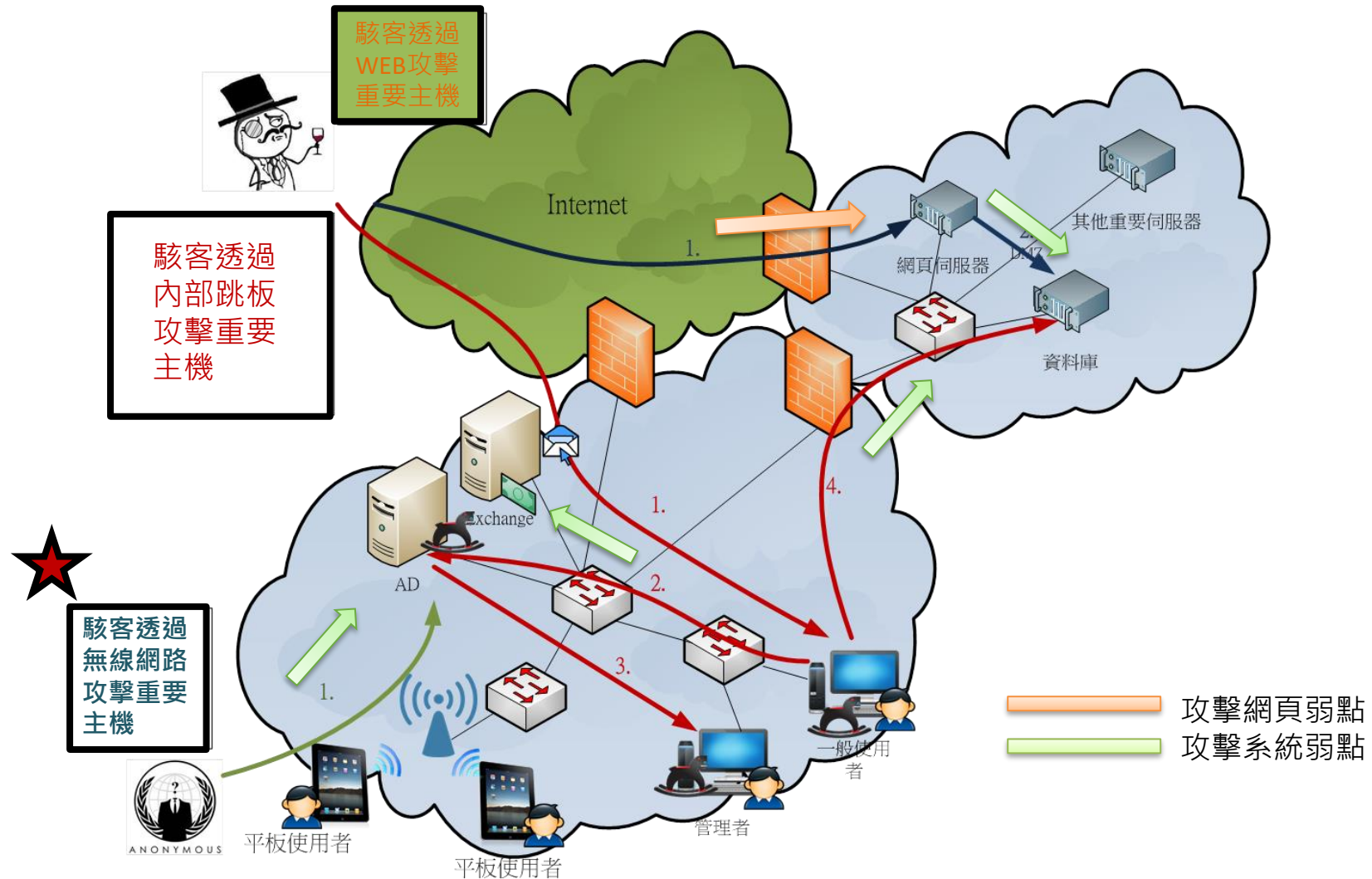


The screenshot shows the kaspersky password checker website. At the top right, there's a language selector set to 'EN' and a 'FAQ' link. The main content area features a password input field with a strength indicator. Below the field, a yellow box contains a warning icon and the text 'Time for a password change!'. A list of reasons is provided: 'Your password is easily crackable.', 'Common keyboard sequence', and 'Your password does not appear in any databases of leaked passwords'. At the bottom, a boot icon is accompanied by the text 'This password can be cracked faster than the time it takes to get back from a short walk'.



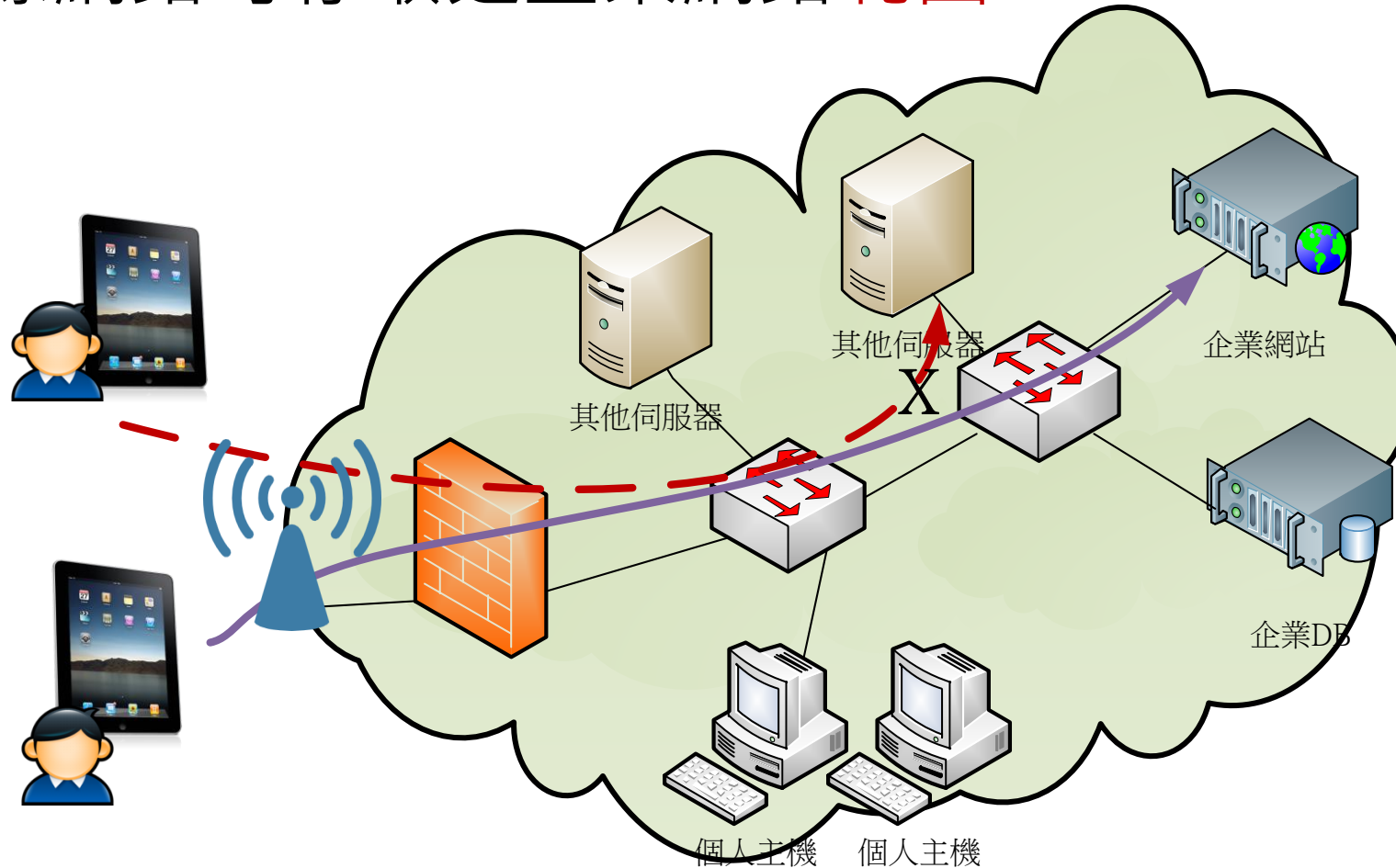
如何加強無線網路安全 – 企業篇

駭客入侵的示意圖



如何強化無線網路安全 – 企業(1/6)

- 限制無線網路可存取之企業網路範圍

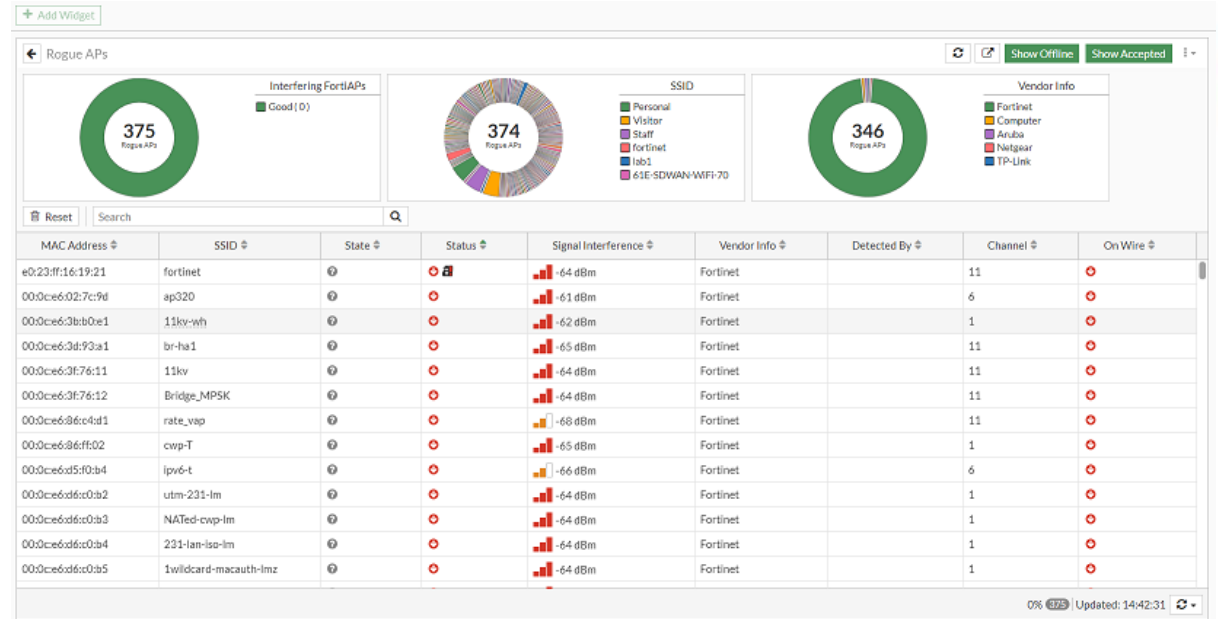


如何強化無線網路安全 – 企業(2/6)

- 使用**EAP**進行加密金鑰分配
 - 使用**PSK**的進行無線網路的金鑰共用缺點就是，就算用上**WPA2**只要對方有辦法取得握手封包，加上夠多的時間與運算能力，還是有機會解密
- 可以的話使用**WPA 3 Enterprise**
- 使用**VPN**
 - 透過在無線網路環境中使用**VPN**確保安全性
 - 但是有許多行動裝置並未內建**VPN**客戶端

如何強化無線網路安全 – 企業(3/6)

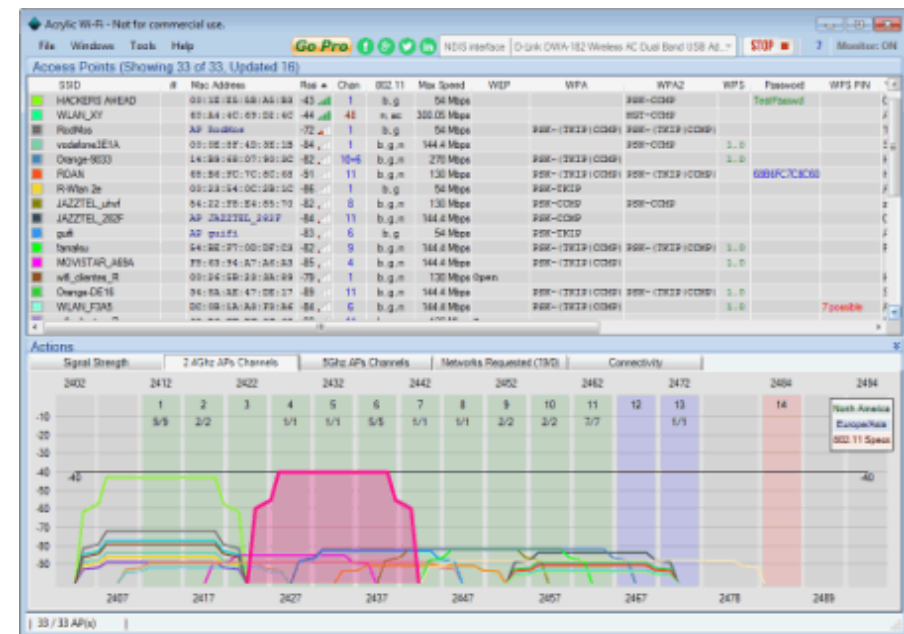
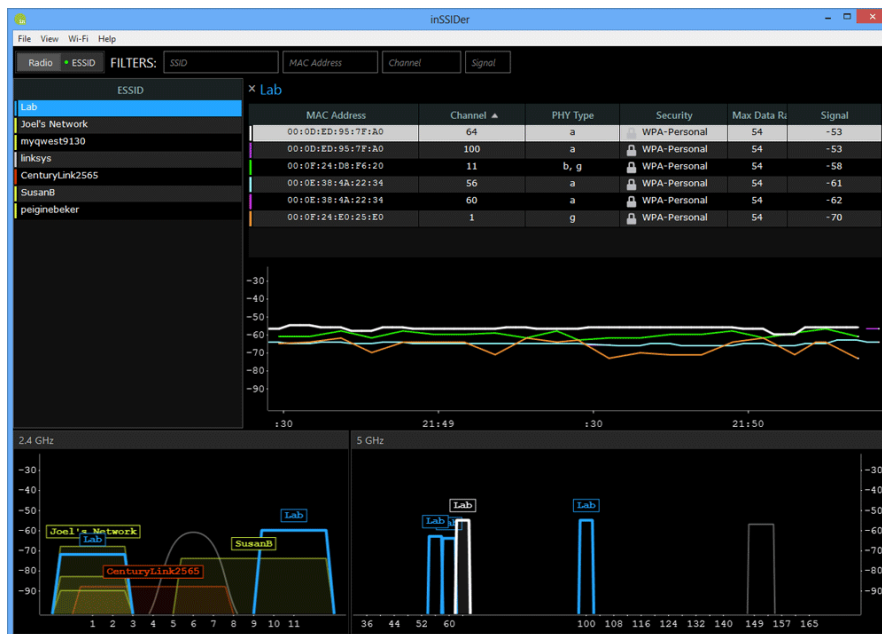
- 定期**檢測**是否有私架**AP**的情形
 - 所有的無線網路存取都應該要受到管控，私人架設的**AP**可能直接就進入到企業網頁內部，成為內控的隱憂
 - 就算有進行WPA/WPA2加密，仍可能遭受駭客破解入侵
 - 有些商用Wi-Fi解決方案可檢測企業區域內是否有私人**AP**存在



- 定期檢查並套用路由器/AP**更新**

如何強化無線網路安全 – 企業(4/6)

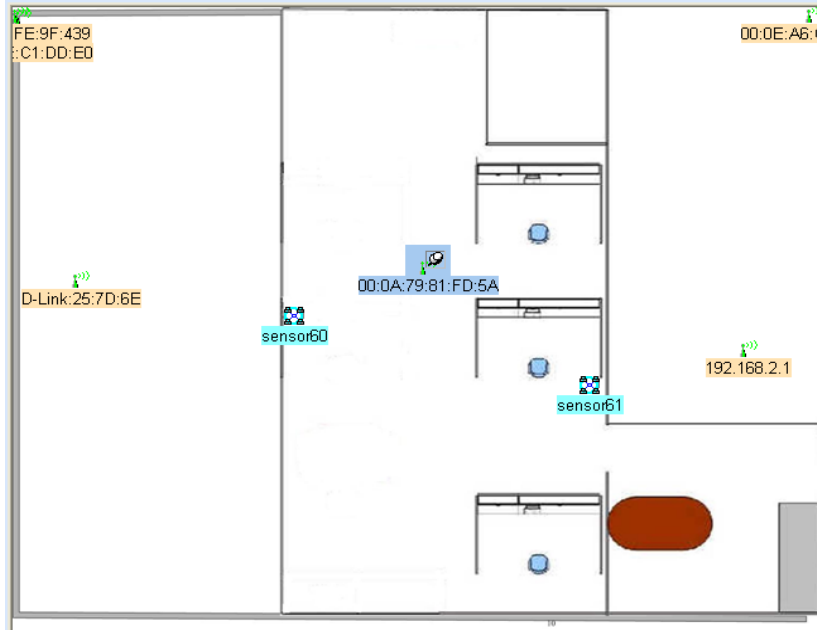
- 比較便宜的Wi-Fi檢測軟體
 - Inssider (\$20)
 - <http://www.inssider.com/>
 - Acrylic_WiFi_Free
 - <https://www.acrylicwifi.com/en/wlan-software/wlan-scanner-acrylic-wifi-free/>



如何強化無線網路安全 – 企業(5/6)

- 佈署無線網路**監控**系統

- 在企業內佈署固定式無線網路偵測裝置，並由中央控制系統統一整合資訊
- 及時告警，且可以三角定位立刻找出攻擊者位置(搭配平面圖)
- 阻斷非法使用者或AP(蓋台)



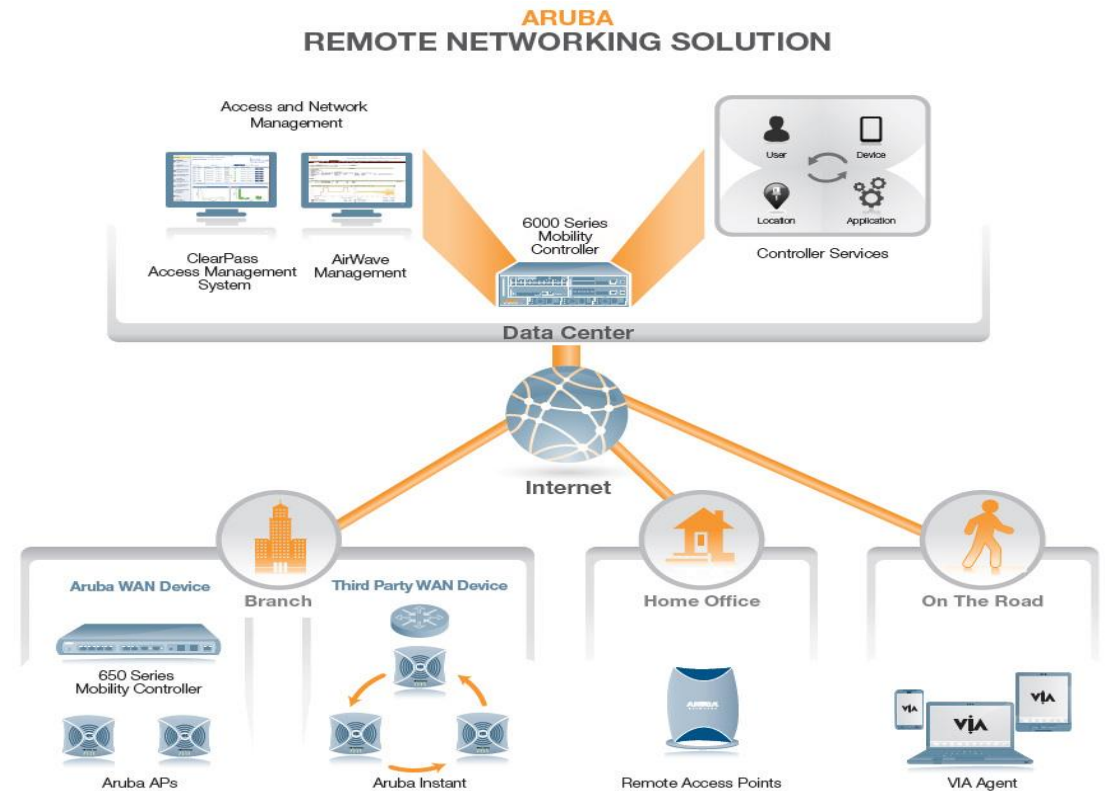
A screenshot of the AirMagnet software interface, displaying the AP List and Detail views. The AP List view shows a table of detected access points with columns for Display Name, MAC, VIP, Signal, SSID, Security, and Owner. The Detail view shows information for a specific AP, including its MAC address, SSID, and security settings.

Display Name	MAC	VIP	Signal	SSID	Security	Owner
WIFLY:FE:9F:43	FE:9F:439	M	2	g	N	N
WIFLY:FE:9F:42	FE:9F:42	M	2	g	N	N
WIFLY:FE:9F:41	FE:9F:41	M	2	g	N	N
WIFLY:FE:97:A3	FE:97:A3	U	2	g	Y	Y
WIFLY:FE:97:A2	FE:97:A2	OK	2	g		
WIFLY:FE:97:A1	FE:97:A1	U	2	g		
WIFLY:FE:97:A0	FE:97:A0	M	2	g	WIFLY	Open
WIFLY:FE:92:33	FE:92:33	R	10	g		
Proximi:6A:1E:4C	6A:1E:4C	M	9	FE:PH-POS		Open
Proximi:5A:2D:3D	5A:2D:3D	U	1	FE:GHQ		?
Proximi:59:D9:87	59:D9:87	U	7	K2		?
D-Link:25:7D:6E	25:7D:6E	M	6	NB Sports Pack 96S	WPA-P	
D-Link:23:E0:ED	23:E0:ED	U	6	angela	WEP	
Cisco-Linksys:77...	77...	OK	6	HomeStation	WEP	
Buffalo:5E:12:24	5E:12:24	U	7	0000B5E1224	WPA-P	
Buffalo:3D:E7:3C	3D:E7:3C	U	7	diffl/WLbuf	WEP	

ACL	非法	鄰近	監控中	不明	總計
蓋台	6	2	2	11	52
工作站	2	0	2	2	138
AdHoc	0	0	0	0	?

如何強化無線網路安全 – 企業(6/6)

- 如果有大規模佈署Wi-Fi需求可考慮企業解決方案
- 可同時處理多台 AP的連網認證，達到集中管理、設定的目的，包括政策設定與執行
- 對設有上百個 AP的環境來說，可以集中管理，降低管理成本，可協助中大型企業、教育等單位快速部署大規模、中央控管的高效能無線區域網路，並從單一個點執行全面的管理、升級及最佳化的無線網路



5. 結語

結語

- 無線網路的最大優勢就是**便利**，從此使用者不必受到網路線拘束，但也有竊聽、干擾、破解等問題存在
- 資安威脅層出不窮，**無線網路也不例外**
- 個人應養成良好**資安意識**與**使用習慣**，企業則應**妥善管理**以確保無線網路安全

報告完畢，敬請指教