2015-16香港無線局域網
安全調研報告簡介
HK WiFi Security Survey 2015

講者：羅國明先生 Roy Law
香港無線科技商會

講者：石裕輝先生 Jim Shek
專業資訊保安協會

資料來源：香港無線科技商會及專業資訊保安協會於2002-201年進行之無線網路應用保安普查報告

主辦機構

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

Hong Kong Wireless Technology Industry Association (WTIA)
香港無線科技商會

贊助

通訊事務管理局 COMMUNICATIONS AUTHORITY

Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region

WiFi 安全話咁易

關於SafeWiFi.HK

- 提高市民對Wi-Fi保安的意識
- 網站：www.SafeWiFi.hk提供豐富的Wi-Fi安全知識
- WTIA 與PISA攜手進行香港無線局域網安全調查及其他推廣活動

有關WTIA

Hong Kong Wireless Technology Industry Association
www.hkwtia.org

有關 PISA

www.pisa.org.hk

facebook.com/PISAHKG

無線局域網安全調研報告

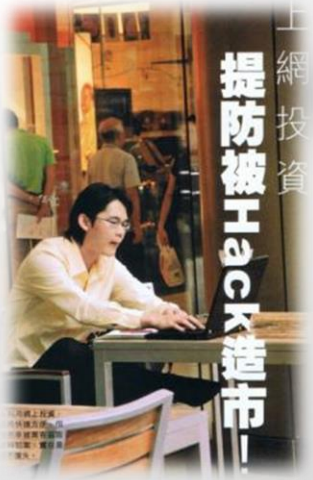
- HK Wi-Fi Security Survey
- 昵稱：HK War Driving
- WTIA、PISA 之中立定義：

  利用無線裝置以非闖入方式沿街掃描無線局域網；

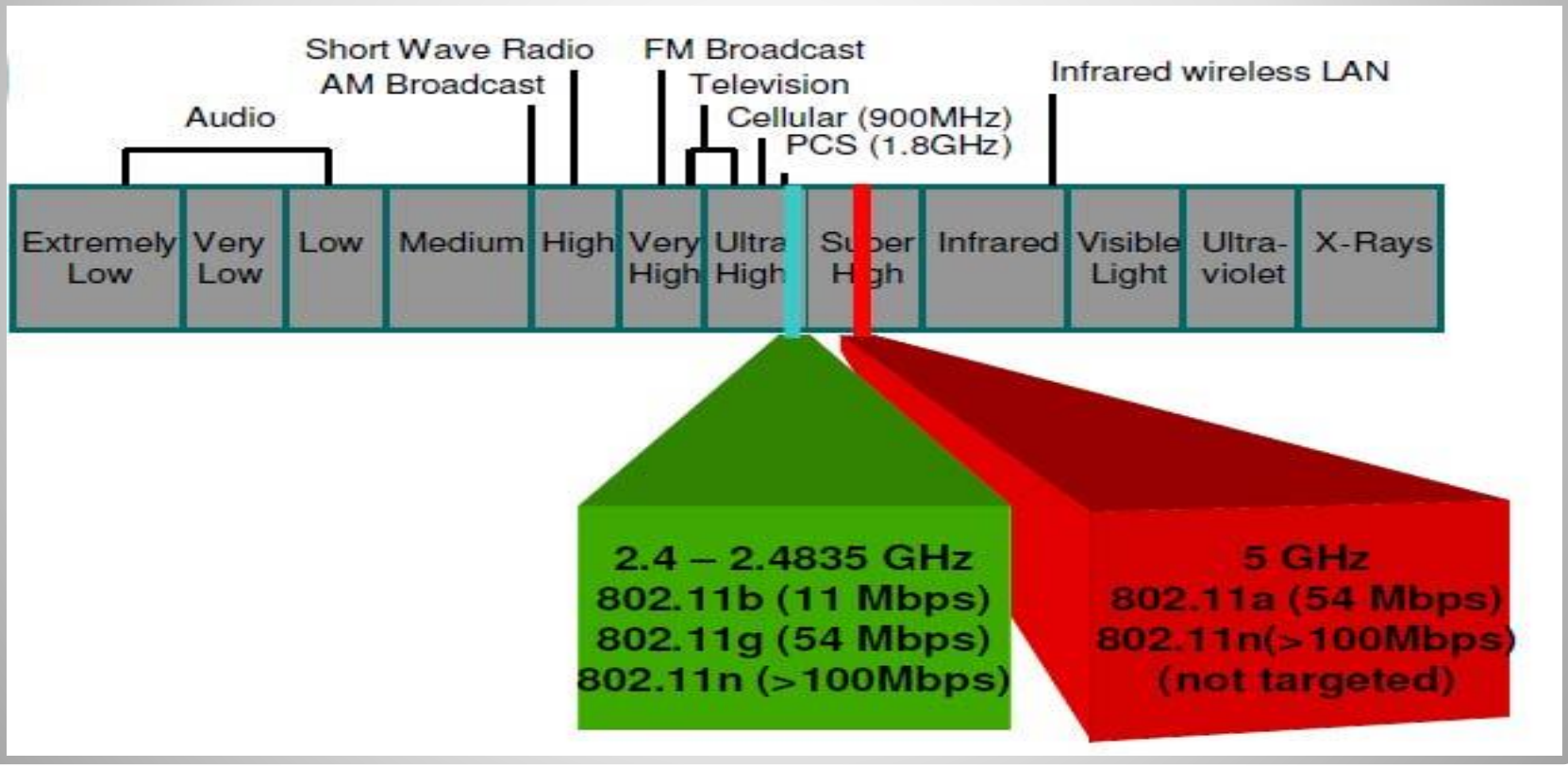
  搜尋網路的名稱、訊號及位置

無線局域網的保安危機

- 訊息可能被截取
- 導致個人資料被盜
- 被駭客入侵網路及電腦
- 被利用作非法用途



2.4G 免授權頻普- 我們的焦點



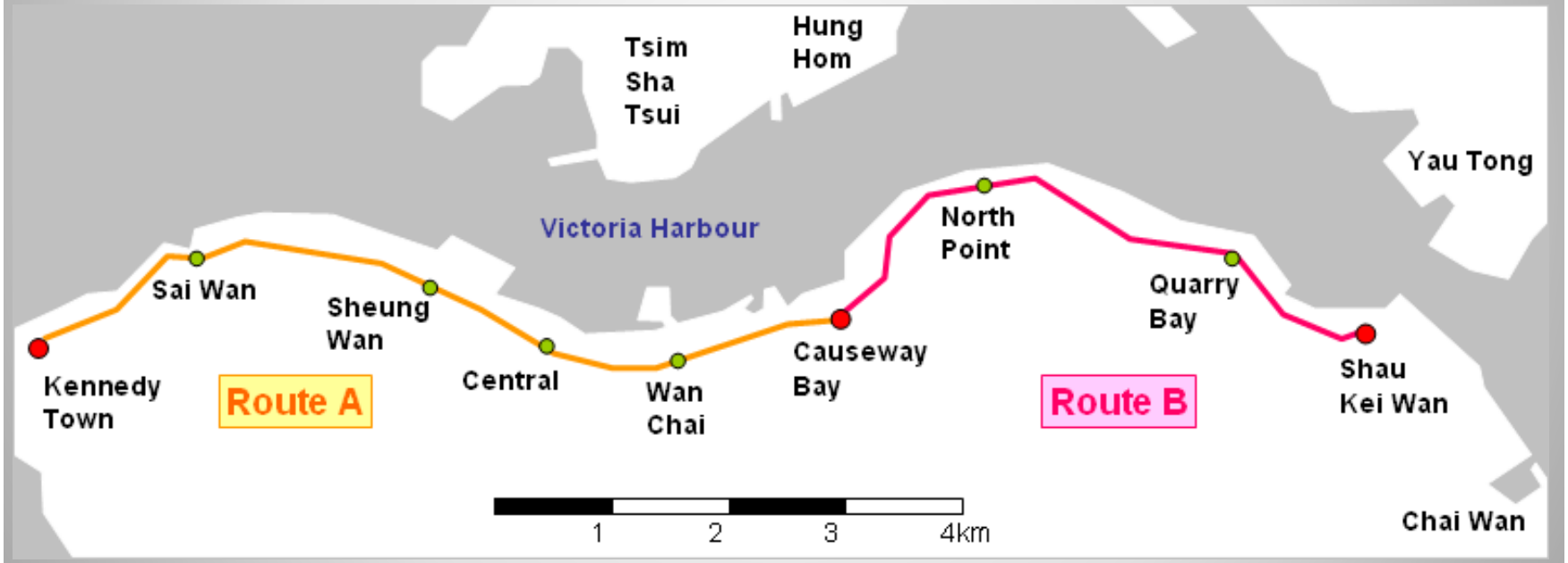
調研局域網的道德守則

- 以研究為示旨，瞭解無線局域網的保安狀況以提高市民對無線局域網的保安意識
- 不公開個別欠安全的接入點之所在位置和用戶名稱-只公佈綜合資料
- 不連接入欠安全之接入點，更不進一步搜尋其弱點
- 不妨礙/堵塞任何無線局域網

歷屆WTIA/ PISA War Driving

年份	電車路線	其他路線
2002	路線A (Route A)	N/A
2003	路線A&B(Route A&B)	香港山頂–長距War Driving
2004	路線A&B(Route A&B)	維港渡輪-War Sailing
2005	路線A&B(Route A&B)	九龍-汽車及巴士
2006	路線A&B(Route A&B)	香港島環島遊-小巴
2007	路線A&B(Route A&B)	澳門
2008	路線A&B(Route A&B)	山頂，九龍，新界及澳門
2009	路線A&B(Route A&B)	九龍，新界，公共及私人屋苑
2010	路線A&B(Route A&B)	公屋，居屋及私人屋苑
2011	路線A&B(Route A&B)	公屋，居屋及私人屋苑
2012	路線A&B(Route A&B)	公屋，居屋及私人屋苑，直升機
2013	路線A&B(Route A&B)	公屋，居屋及私人屋苑，直升機，維港渡輪
2014	路線A&B(Route A&B)	公屋，居屋及私人屋苑
2015	路線A&B(Route A&B)	公屋，居屋及私人屋苑

War Tramming路線 A & B



歷屆War Driving

2003

2004

2007 –
港澳兩地的無線局域網

2010

2015

2012

香港無線網路應用保安普查 (War Driving)2015 –宗旨

- 瞭解無線局域網的保安狀況
- 利用2002-2015歷年的資料，評估成效
- 進行非闖入方式無線局域網之研究
- 提高市民對無線局域網的保安意識
- 比較公屋，居屋及私人屋苑使用加密的方法

配備應用

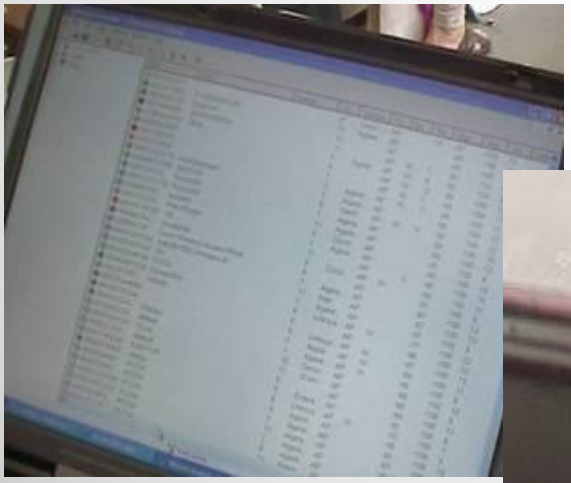
硬體：

- Android電話或平板電腦

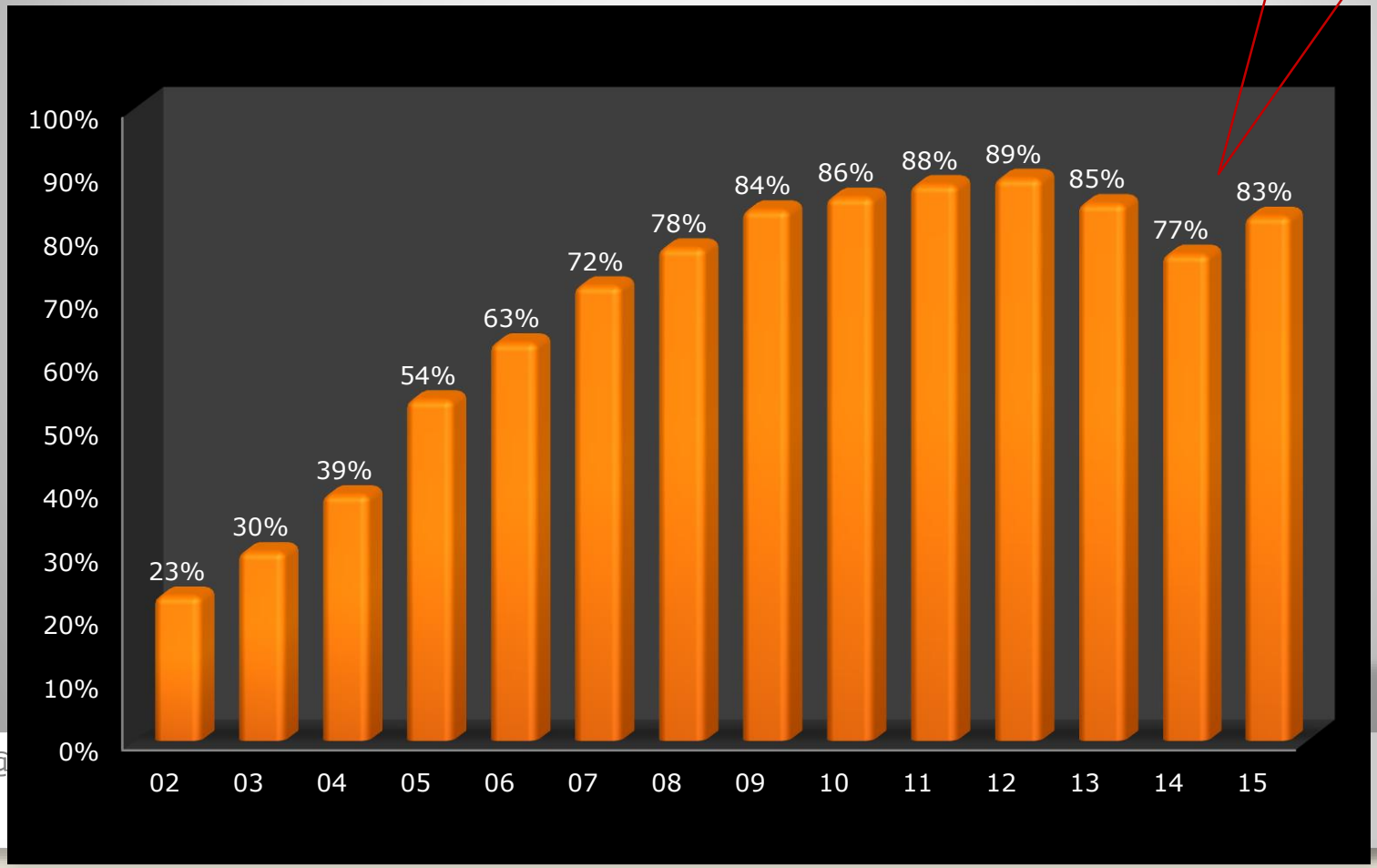
軟體：

- WigleWifi Wardriving for Android OS (https://play.google.com/store/apps/details?id=net.wigle.wigleandroid)

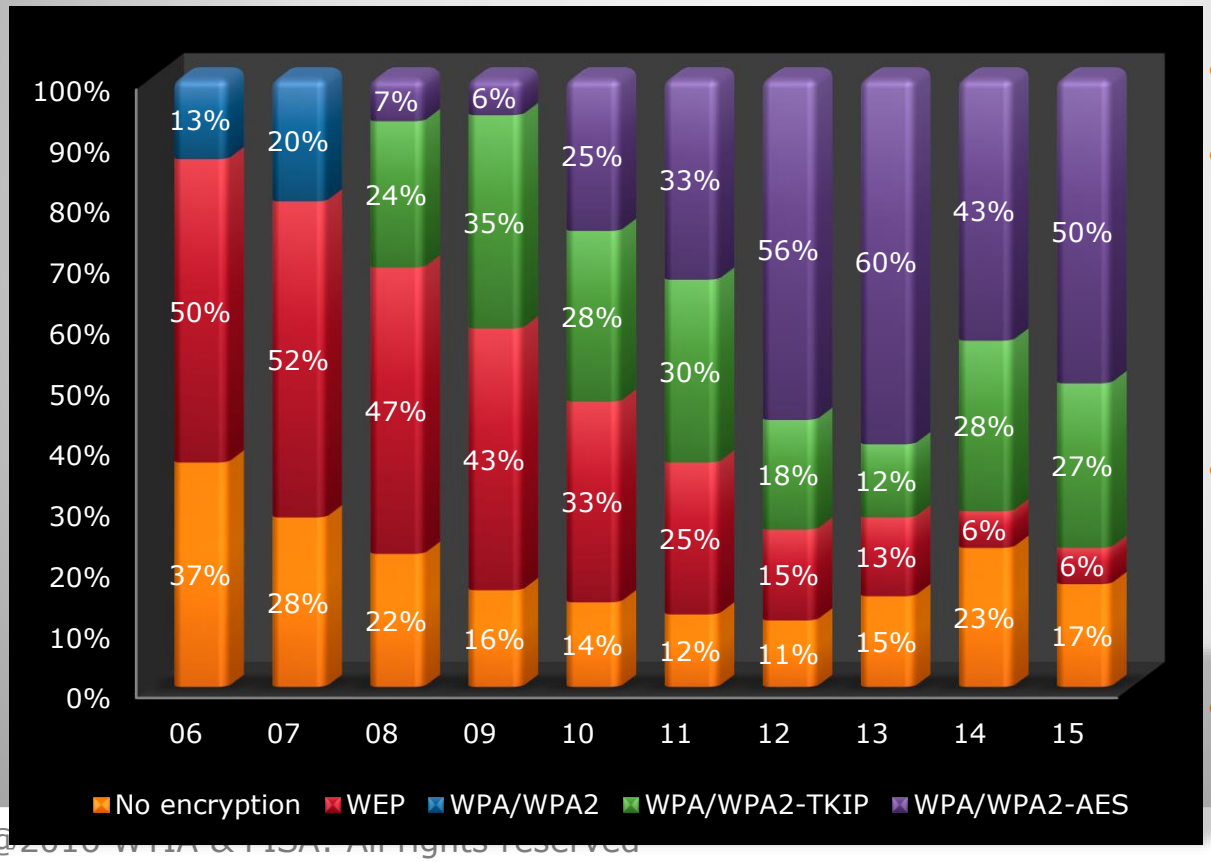
調研發現



採用加密設定的增長趨勢



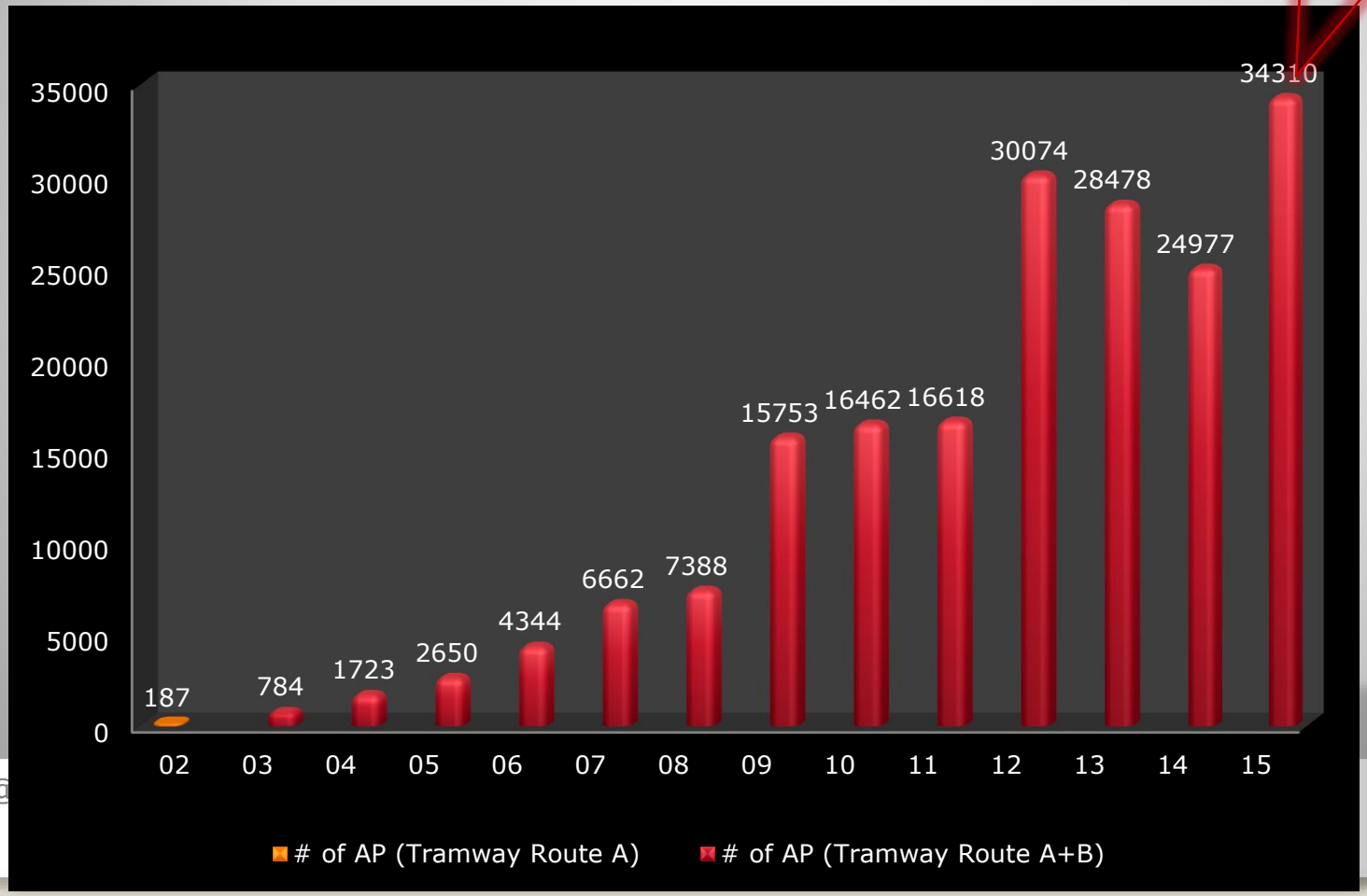
加密模式使用分佈



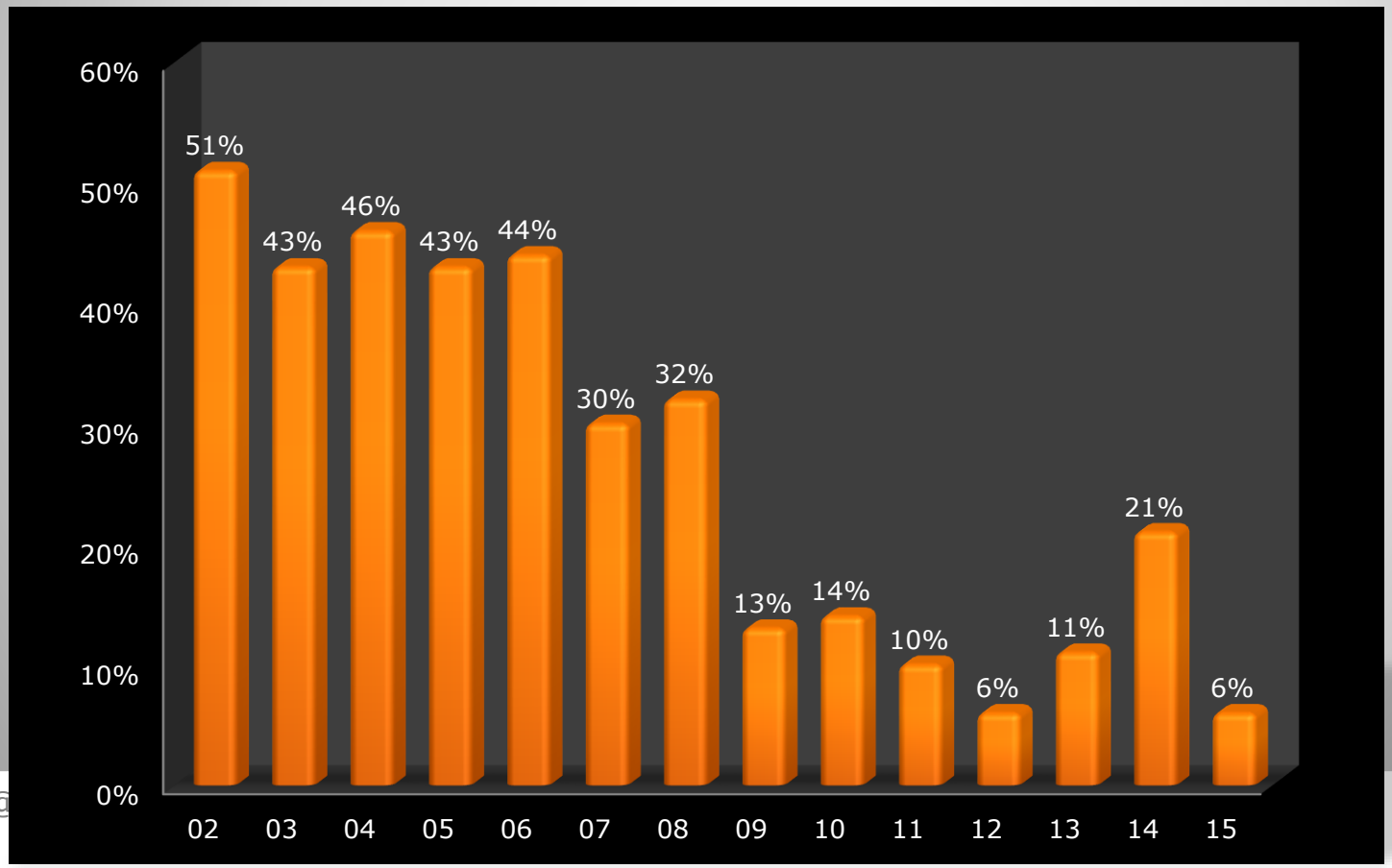
- 儘管使用加密比率高
- WEP已變得不夠安全(目前有6% WLAN採用WEP;**較前年13%大爲改善**)
- WEP/WPA-TKIP亦有漏洞，有可能被非法入侵
- 鼓勵使用WPA2-AES

無線接入口數目

New Record &
Using Android Only



SSID出廠設定

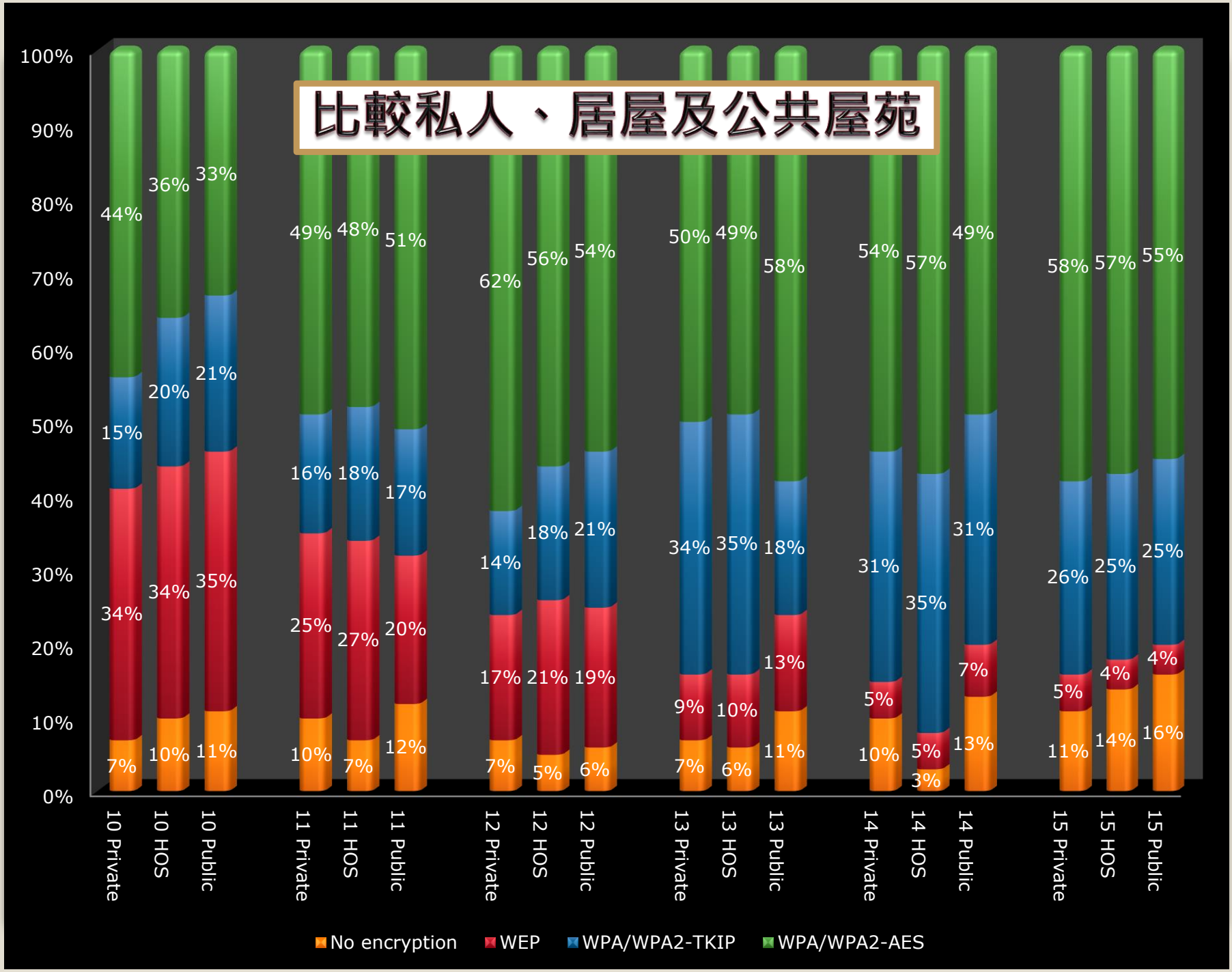

60%
50%
40%
30%
20%
10%
0%
51%
43%
46%
43%
44%
30%
32%
13%
14%
10%
6%
11%
21%
6%
02
03
04
05
06
07
08
09
10
11
12
13
14
15

比較私人、居屋及公共屋苑

Information	Estate A	Estate B	Estate C
Type	Private Housing Estate	Home Ownership Scheme	Public Rental Housing Estate
Year	Since 1977	Since 1993	Since 1963
Number of Apartment Buildings	61	12	9
Apartment Flats	12,698	4,200	3,129
Access Point(2014)	4224	2127	1990

Wi-Fi Protected Setup (WPS) flaw

- Wi-Fi Protected Setup (WPS) is a computing standard that attempts to allow easy establishment of a secure wireless home network. A major security flaw was revealed in December 2011 that affects wireless routers with the WPS feature.
- We also aim to indentify the potential risk of WPS by also discovering the amount of WPS turn-on on the discovered AP. We test the WPS features for the target Access Point by using "WigleWifi Wardriving for Android OS".
- The percentage of enabling WPS of total Access Points was 34.67% for year 2013, 34.08% for 2014 and 28.82% for 2015. Improvement is identified in this area.


比較私人、居屋及公共屋苑
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
10 Private
10 HOS
10 Public
11 Private
11 HOS
11 Public
12 Private
12 HOS
12 Public
13 Private
13 HOS
13 Public
14 Private
14 HOS
14 Public
15 Private
15 HOS
15 Public
No encryption
WEP
WPA/WPA2-TKIP
WPA/WPA2-AES

HK WiFi Security Index
香港無線網絡安全指數

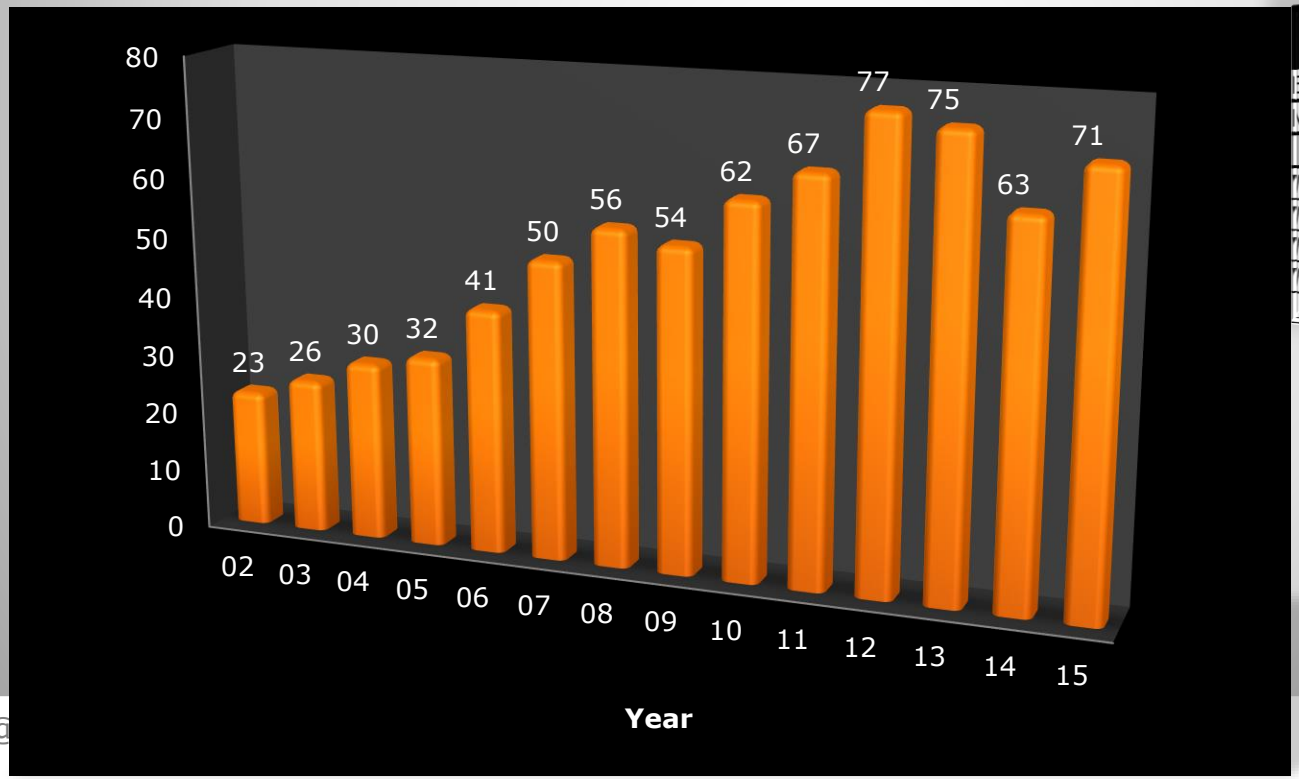
HK WiFi Security Index

- The index is compiled by the Hong Kong Wireless Technology Industry Association (WTIA) and Professional Information Security Association (PISA), analyzing data collected in War Driving surveys over the years.
- A single index for the easy interpretation of the WiFi Security Trend of Hong Kong
- Range from 0-100 indicating the level of WiFi security for representing year.
- Calculate based on tramway statistics

HK WiFi Security Index

Criticality of vulnerability	Score	Description
L1	100	No vulnerability found in the technology
L2	80	Found a vulnerability in theory (concept)
L3	60	A proof of concept verified the vulnerability exploitable
L4	50	Exploit is found conducted by skilful personnel but source code not widely distributed
L5	30	Source code of exploit is published to public
L6	20	Handy tool is available for script kiddies to use
L7	0	No encryption

HK WiFi Security Index
香港無線網絡安全指數



	2015 (%)	Weight
Encryption Applied	83	20%
Non default SSID*	93	20%
		60%
WEP	6	L6
WPA or WPA2		
WPA/WPA2-TKIP	27	L5
WPA/WPA2-AES	51	L1

Overview: Wi-Fi Encryption Modes

Encryption	Level of Security	Remark
None	Insecure	No encryption at all
WEP	Insecure	Shared password/key WEP key can be cracked in a few minutes Cracking tools are widely available Due to old design, security cannot be improved with a longer WEP key
WPA/WPA2 Personal TKIP	Comparatively still safe but recommend to use AES security mode	Shared password/key TKIP is theoretically can be cracked Tools are emerging but not widely used Recommend to use shorter Key Renewal time if AES option is not available
WPA/WPA2 Personal AES	Secure	Shared password/key No threat discovered at the moment
WPA/WPA2 Enterprise	Secure	Individual user ID & password with a backend authentication server (802.1X authentication / RADIUS) No threat discovered at the moment

Tips and Recommendation

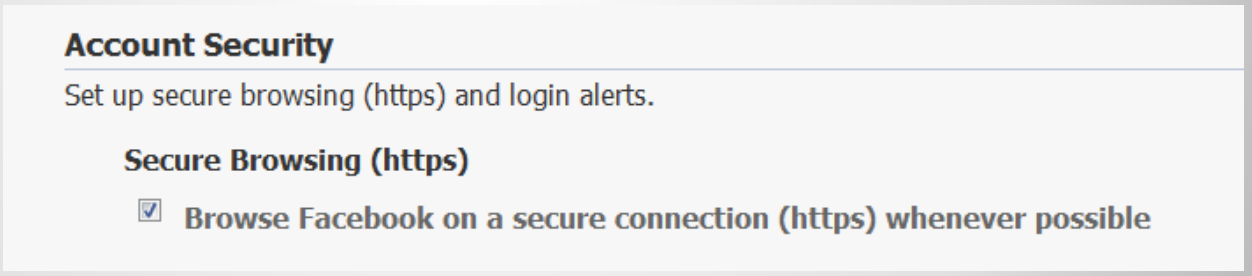
- Enable encryption mode and use WPA/WPA2-AES
- Though MAC address can be spoofed, recommend to enable MAC Address Filtering
- Though hidden SSID can be seen with a suitable tool, recommend to hide SSID
- Change SSID to not easily identifiable
- Do not just use the “off-the-shelf” settings, need to review
- Better not to put the AP near to the Windows to reduce chance of connection outside your home/office

Tips and Recommendation

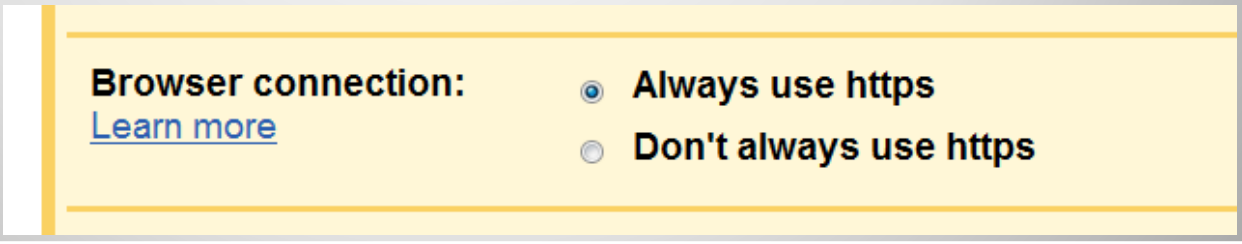
- Hotspot
  - Use secured channels to handle sensitive data (e.g. email, online transactions)
  - Some hotspot service provider(s) provide both secured and unencrypted channels
  - HK government Wi-Fi – both secured and unencrypted channels are available. (Secured channel: "freegovwifi-e" using WPA encryption)
  - Beware of rogue access points – be aware of any strange behaviours/response during the connections (remark: some enterprise wireless network systems can detect rogue access points)
  - Use VPN in case secured channel is not available

Tips and Recommendation

- May consider using 3G HSDPA thumb key (i.e. not using 802.11/Wi-Fi network) to handle sensitive data
- Use secure browsing features provided by applications
  - Facebook



  - Gmail



提問環節

— 謝謝 —

www.hkwtia.org
roylaw@hkwtia.org

www.pisa.org
jim.shek@pisa.org.hk

重要告示

Copyright（版權聲明）

Hong Kong Wireless Technology Industry Association (WTIA) and Professional Information Security Association (PISA) owns the right to use this material of Report on Hong Kong War Driving 2002-2015 in the presentation. Any party can quote the whole or part of this presentation in an undistorted manner and with a clear reference to WTIA and PISA.

Disclaimer（免責條款）

The report is to provide information on WLAN security status and risks in Hong Kong. It should not be used for malicious intent. Unauthorized Access to computer system is an offense. The author takes no liability to any act of the user or damage caused in making use of this presentation material