2011香港無線局域網
安全調研報告簡介
HK WiFi Security Survey 2011

講者：方健僑先生 Ken Fong
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2002-2011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

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WTIA

- 香港無線科技商會(WTIA)成立於2001年，其中旨包括：
- 代表無線科技行業向政府及國際組織發表意見，為業界維護本身的權益
- 推動香港無線科技應用的發展、使用及認知
- 促進業界不同種類公司間的溝通及合作
- 提升在無線科技應用方案中軟體及硬體的專業標準

有關WTIA

- 香港無線科技商會(WTIA)現有超過170個來自本地及外地的公司會員，包括流動網路營運商、流動器材生產商、軟硬體經銷商、系統集成商、無線應用開發商，流動內容供貨應商等。

- 商會積極與政府、其他商會和商業機構保持緊密合作，統籌並舉辦不同類型產品和技術的重要推廣活動以促進業界的發展。

有關 PISA

Professional Information Security Association

(PISA)

專業資訊保安協會

www.pisa.org.hk

有關 PISA

- A not-for-profit organization for local information security professionals found in 2001
- Focus on developing the local information security market with a global presence in the industry

有關 PISA

Mission

- to facilitate knowledge and information sharing among the PISA members
- to promote the highest quality of technical and ethical standards to the information security profession,
- to promote best-practices in information security control,
- to promote security awareness to the IT industry and general public in Hong Kong

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

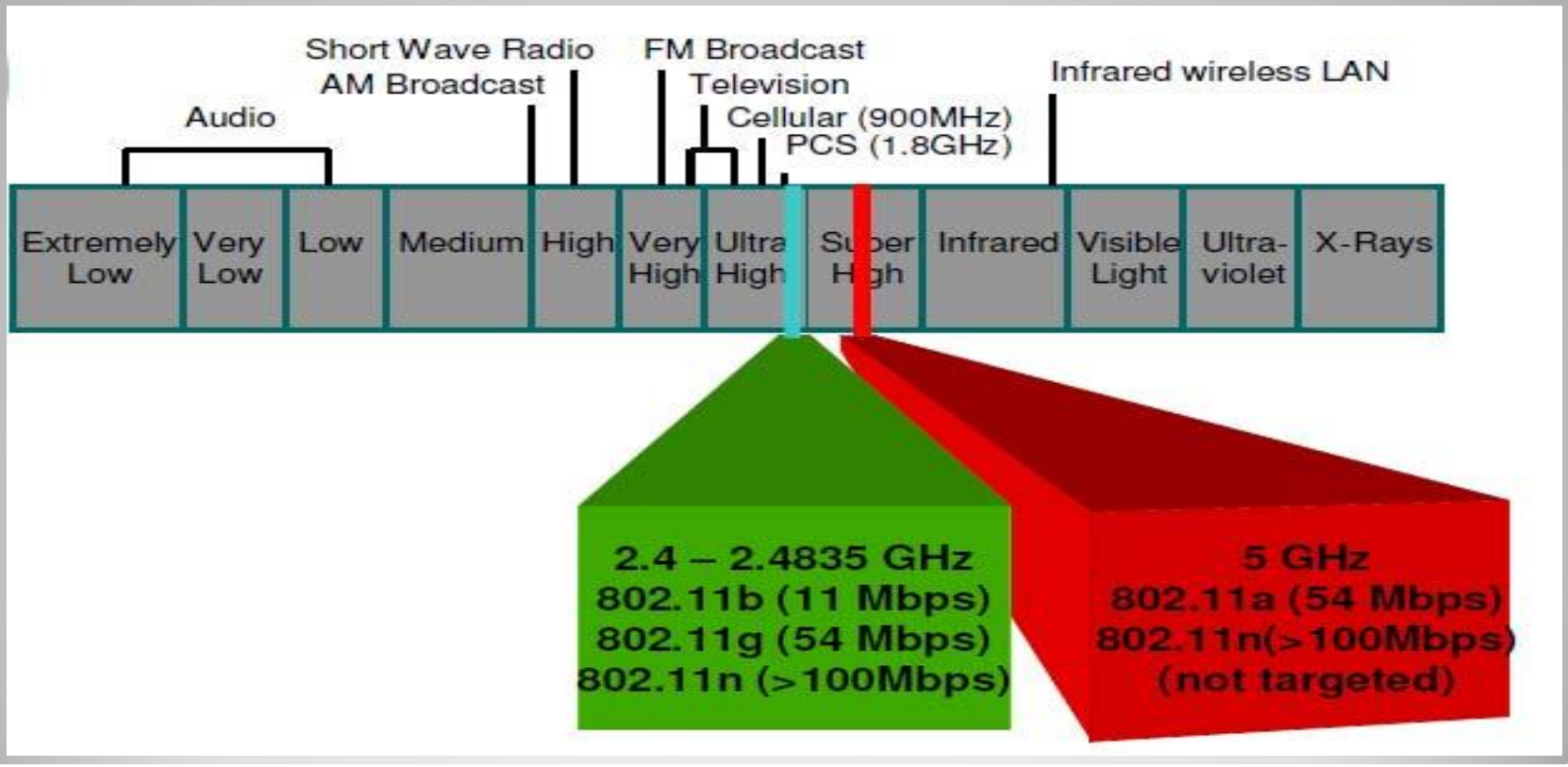
無線局域網的保安危機

- 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

本報局中無線局域網的保安設定

- WEP
- WPA/WPA2 - TKPI
- WPA/WPA2 – AES
- 802.11i

2.4G 免授權頻普- 我們的焦點



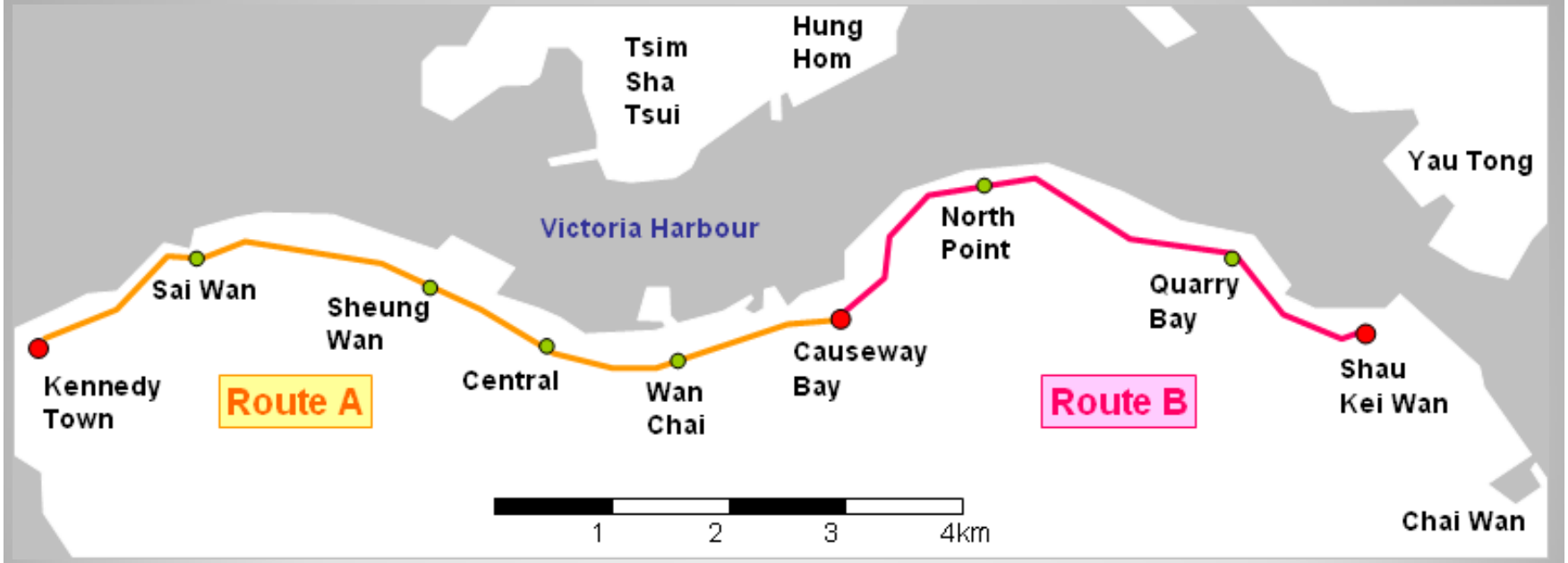
調研局域網的道德守則

- 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

War Tramming路線 A & B



War Driving 2003

Two Checkpoints on the Victoria Peak

Point <1> Peak-West Point <2> Peak-East (near Peak Tram Station)

War Driving 2004

War Driving 2005

War Driving 2006

War Driving 2007

港澳兩地的
無線局域網

香港無線網路應用保安普查 (War Driving)2008

香港最全面的War-driving普查：
覆蓋香港島(電車沿線)、九龍、新界及維多利亞港一帶




香港無線網路應用保安普查 (War Driving)2009

覆蓋香港(電車沿線) 、九龍、新界路線及公共與私人屋苑

香港無線網路應用保安普查 (War Driving)2011

覆蓋香港(電車沿線) 路線及公屋，居屋及私人屋苑

香港無線網路應用保安普查 (War Driving)2011 –宗旨

- 瞭解無線局域網的保安狀況
- 利用2002-2011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

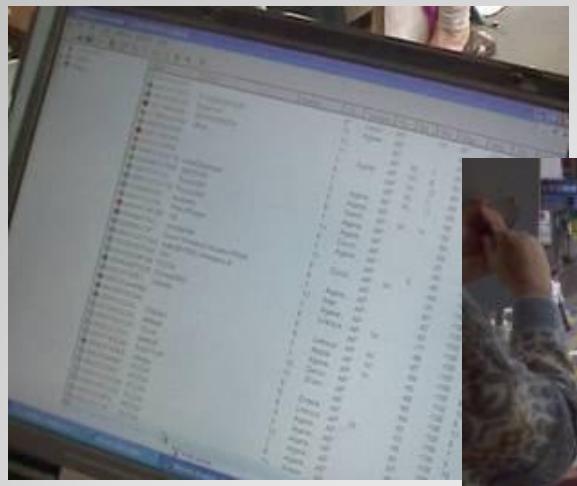
硬體：

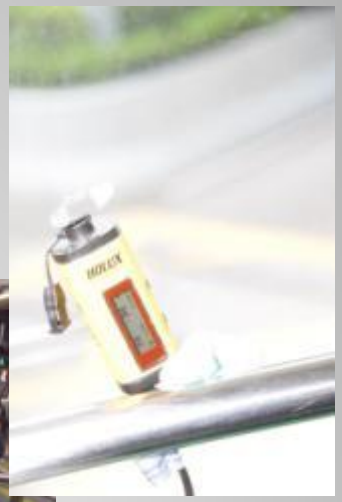
- 筆記簿電腦
- 智慧型電話
- WLAN Card、天線及全球定位系統（GPS）

軟體：

- Vistumbler
- (http://vistumbler.sourceforge.net)
- WiFi Hopper (http://www.wifihopper.com)

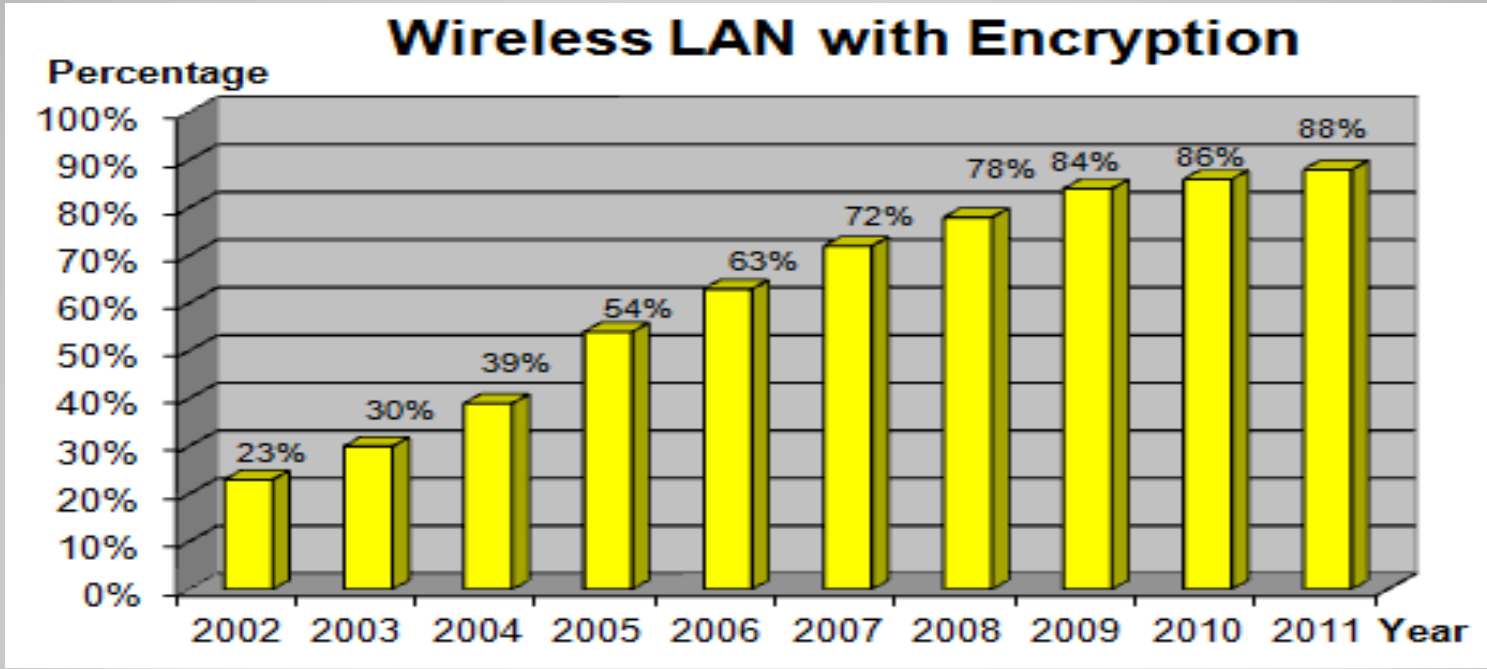
調研發現





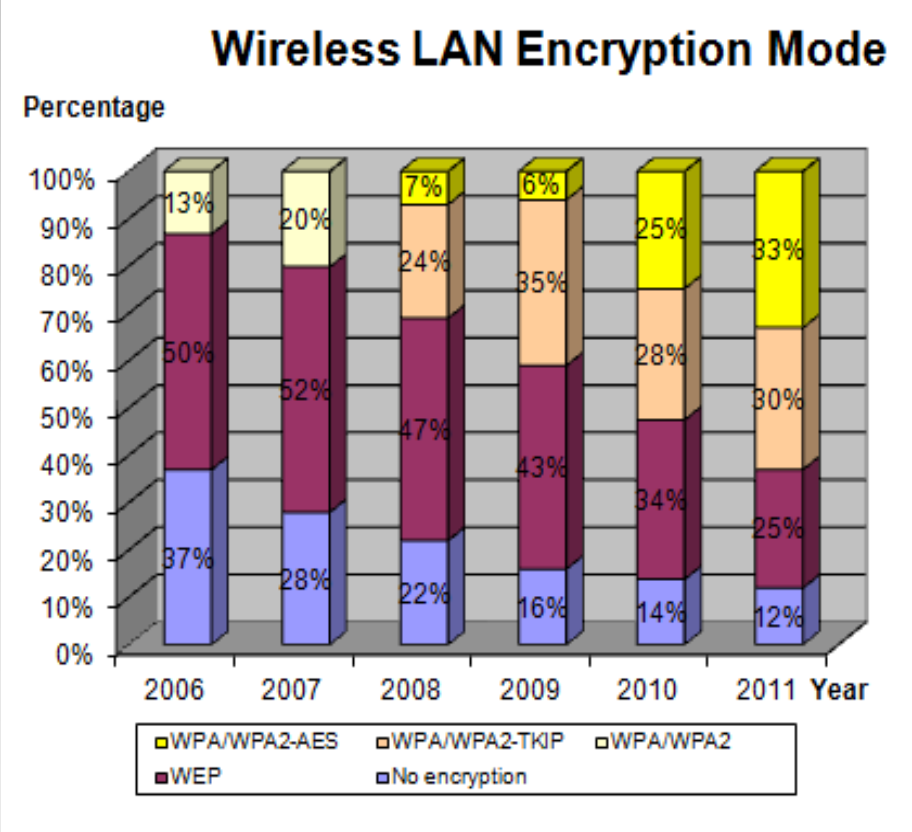
香港：加密模式

採用加密設定的增長趨勢

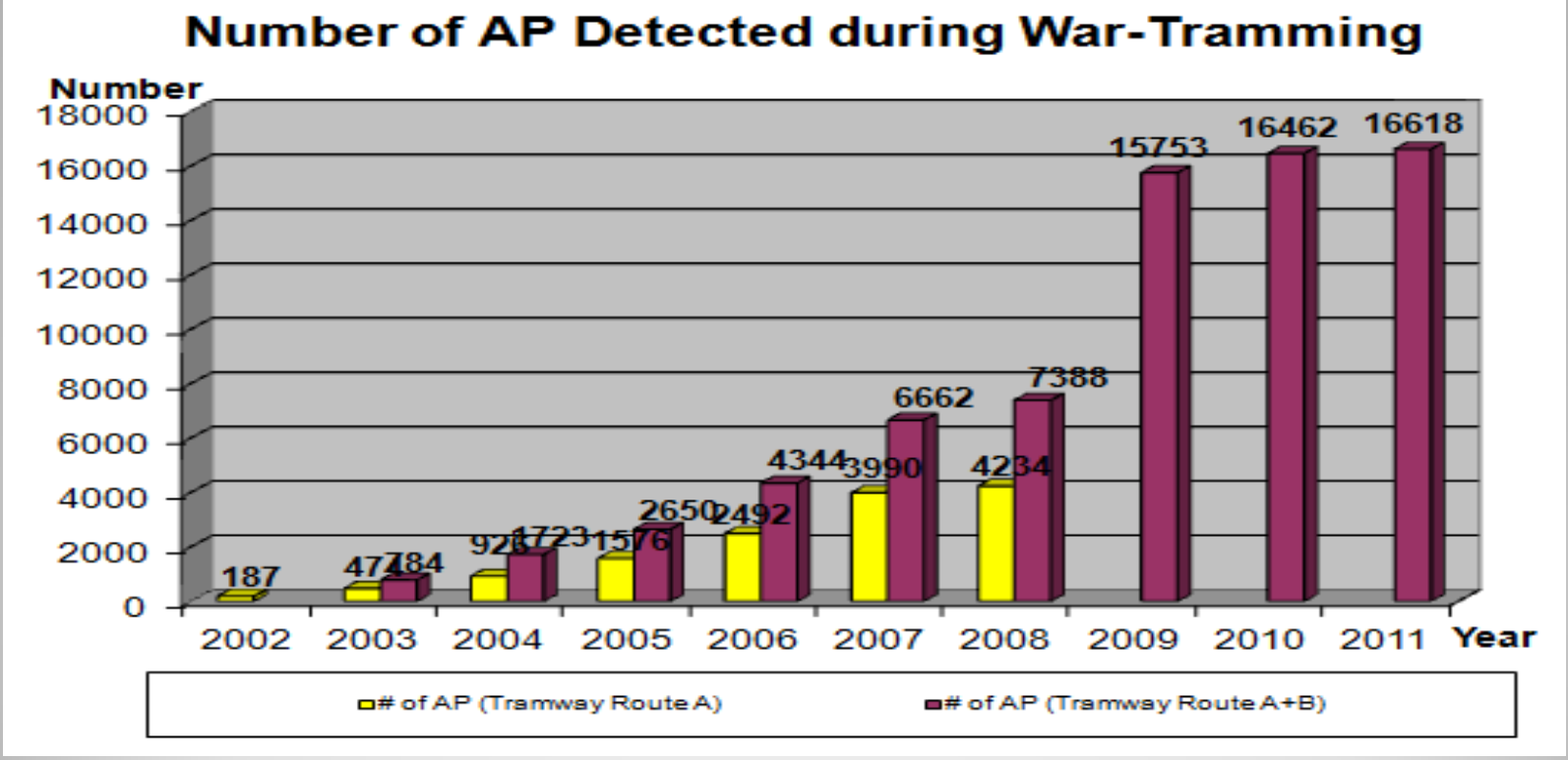


香港：加密模式

- 儘管使用加密比率高
- 可是WEP已變得不夠安全
- WEP / WPA-TKIP亦有漏洞，有可能被非法入侵
- 鼓勵使用WPA/WPA2-AES
- (目前有33% WLAN採用此高度安全的加密技術)

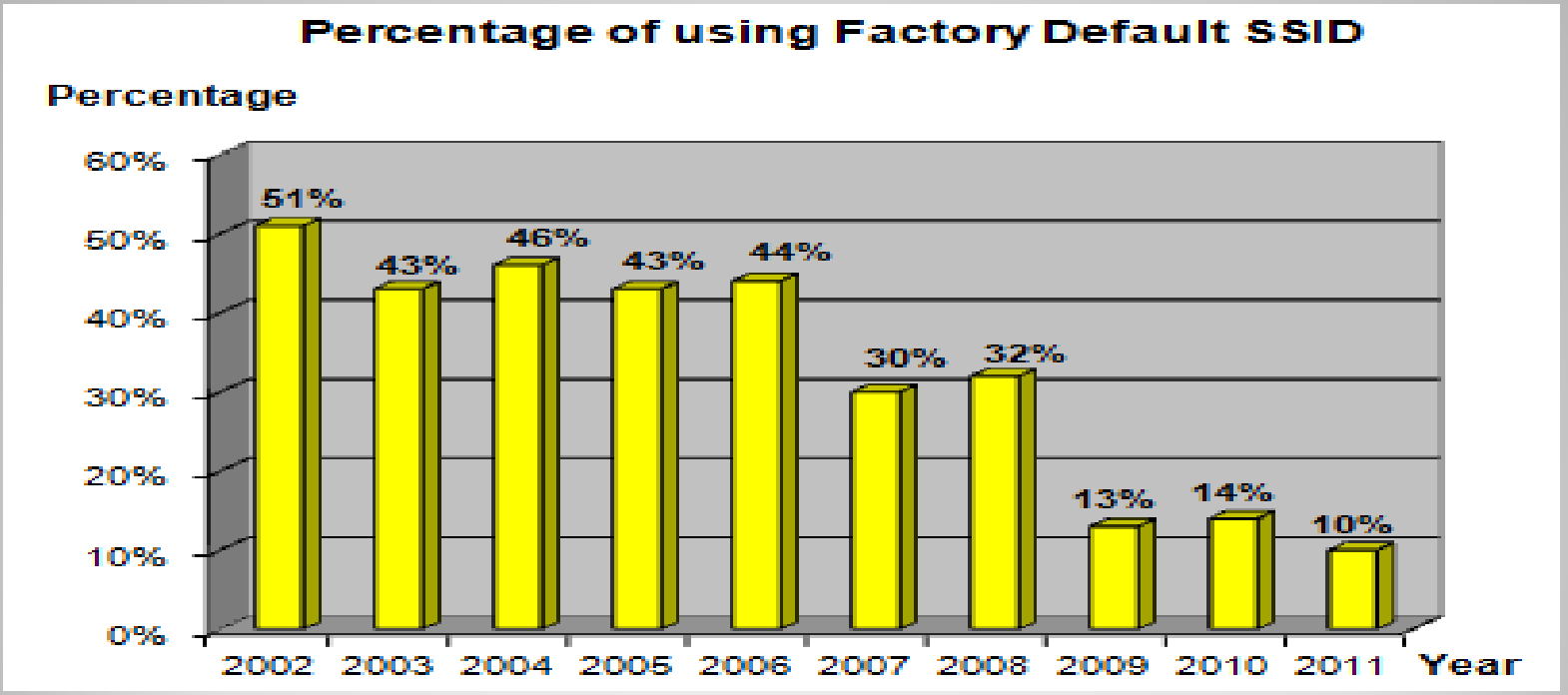


香港：無線接入口數目

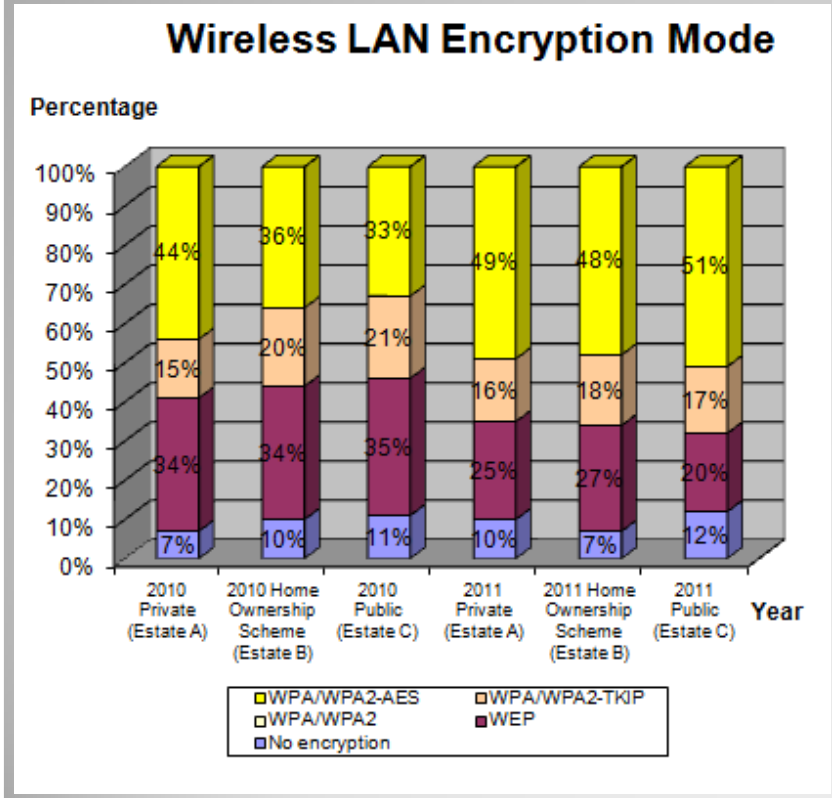


香港：出廠設定

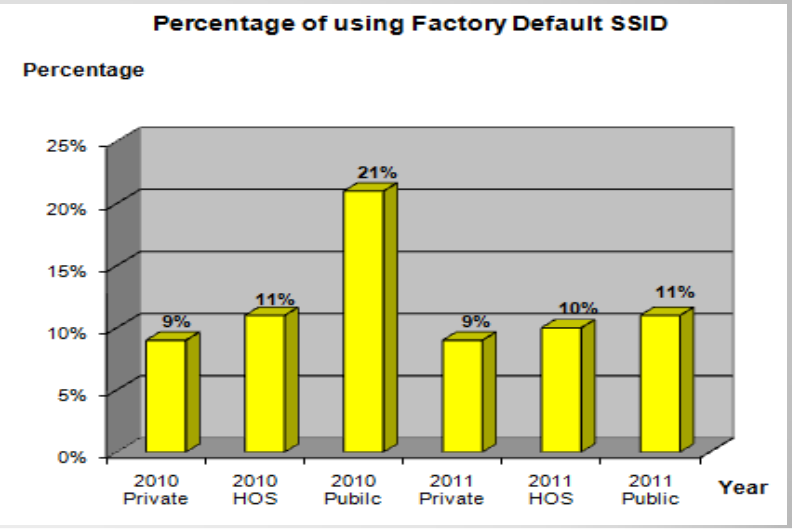
按出廠設定的SSID



香港：比較公共與私人屋苑



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 (2010)	2626	1952	565



HK WiFi Security Index
香港無線網絡安全指數

香港無線網絡安全指數 HK WiFi Security Index

- 指數是由香港無線科技商會（WTIA）及專業資訊保安協會（PISA）以多年來在War Driving 查收集的數據分析編制。
- 指數是一個單指標，容易了解香港WiFi安全趨勢
- 每年指數的範圍從0-100。
- 以每年電車路War Driving 查收集的數據作為計算的基礎

香港無線網絡安全指數 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

香港無線網絡安全指數 HK WiFi Security Index

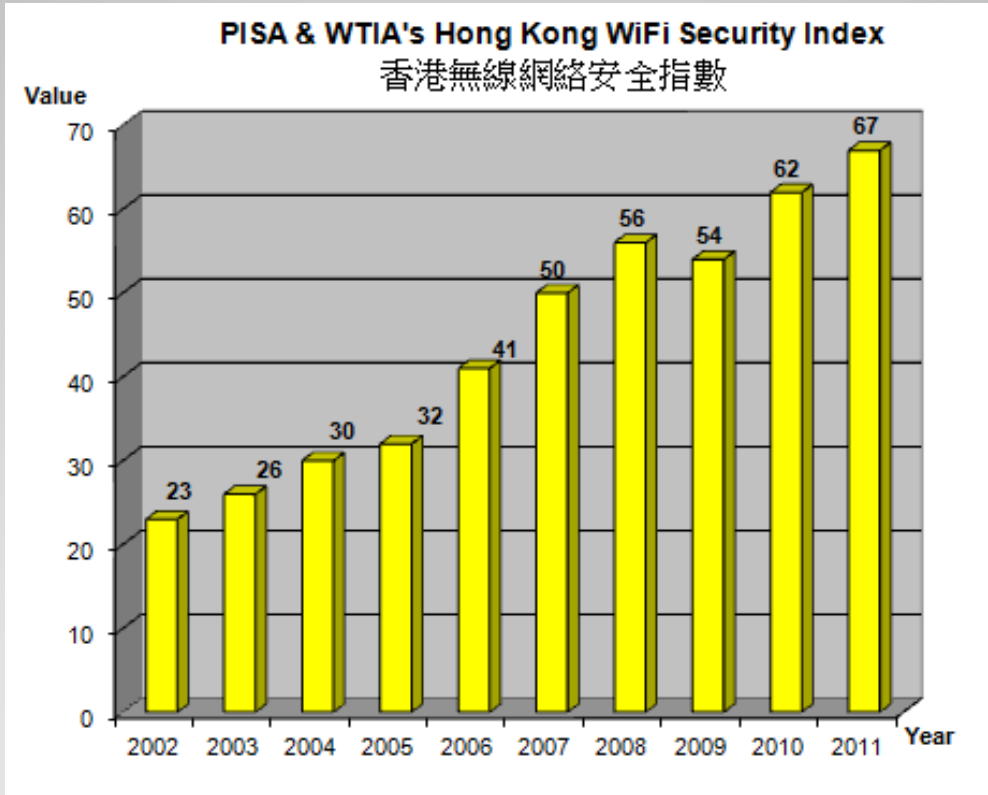
		2002 (%)	Weight	2003 (%)	Weight	2004 (%)	Weight	2005 (%)	Weight	2006 (%)	Weight	2007 (%)	Weight	2008 (%)	Weight	2009 (%)	Weight	2010 (%)	Weight	2011 (%)	Weight
Public Awareness	Encryption Applied	23	20%	30	20%	39	20%	54	20%	63	20%	72	20%	78	20%	85	20%	86	20%	88	20%
Best Practice	Non default SSID*	49	20%	57	20%	54	20%	57	20%	56	20%	70	20%	80	20%	88	20%	86	20%	91	20%
Technology Merit			60%		60%		60%		60%		60%		60%		60%		60%		60%		60%
	WEP	23	L3	30	L4	39	L4	54	L5	50	L5	52	L5	43	L5	45	L6	34	L6	25	L6
	WPA or WPA2									13	L1	20	L1								
	WPA/WPA2-TKIP													29	L2	33	L4	28	L4	29	L4
	WPA/WPA2-AES													5	L1	7	L1	25	L1	33	L1
			100%		100%		100%		100%		100%		100%		100%		100%		100%		100%
香港無線網絡安全指數	HK WiFi Security Index**	23		26		30		32		41		50		56		54		62		67	

*Non default SSID means the SSID is configured as non-factory-default, non-hotspot or hidden

*Non default SSID means the SSID is configured as non-factory-default, non-hotspot or hidden

**The PISA and WTIA "Hong Kong WiFi Security Index" was calculated based on the tramway war-driving statistics

香港無線網絡安全指數 HK WiFi Security Index



提問環節

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

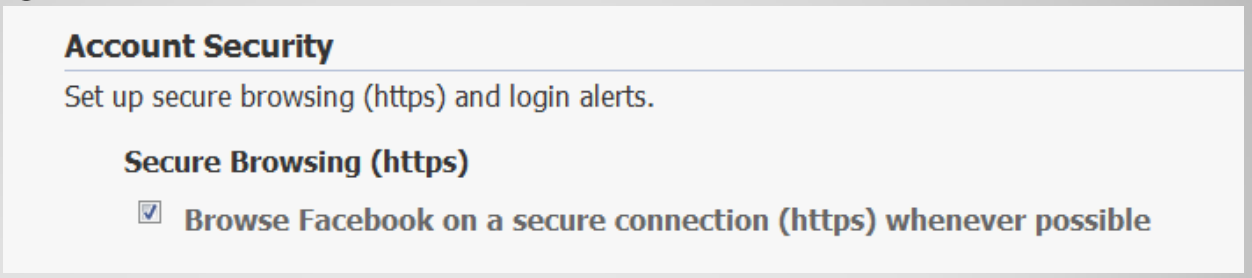
- Enable encryption mode and use WPA/WPA2-AES
- Though MAC address can be spoofed, recommend to enable MAC Address Filtering
- Though hidden SSID can be seen with a suitable tool, recommend to hide SSID
- Change SSID to not easily identifiable
- Do not just use the “off-the-shelf” settings, need to review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

Tips and Recommendation

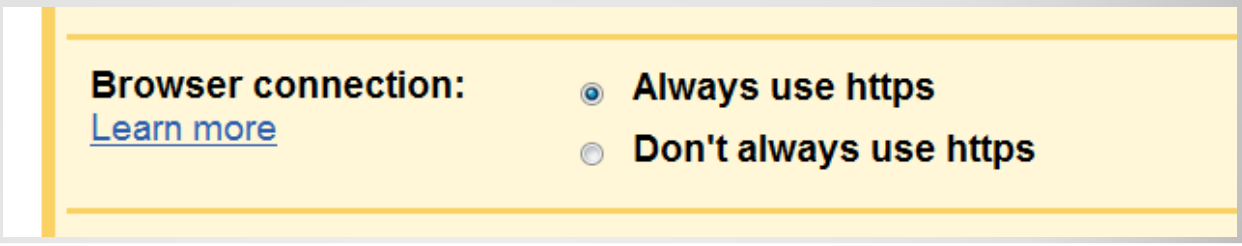
- Hotspot
  - Use secured channels to handle sensitive data (e.g. email, online transactions)
  - Some hotspot service provider(s) provide both secured and unencrypted channels
  - HK government Wi-Fi – both secured and unencrypted channels are available. (Secured channel: "freegovwifi-e" using WPA encryption)
  - 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



鳴謝

WD2011 Team Members including

WTIA

- Ken Fong (Convener) , Eric Leung, Eric Lo, Jacky Cheng, Joseph Leung, Lawrence Li, Michael Kan, Voker Lam

PISA

- Alan Ho (Convener) ,Chun Fai Li, Jim Shek, Leo Sin, Sang Young, SC Leung, Thomas Tsang, WS Lam

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 2002-2008 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

— 謝謝 —

www.hkwtia.org

kenfong@hkwtia.org

www.pisa.org

jim.shek@pisa.org.hk