HK Wi-Fi Security Survey 2009
2009 無線網絡應用保安普查

Presented by:

Mr. Ken K.K. Fong

Chairman,

Hong Kong Wireless Technology Industry Association (WTIA)

Contact: kenfong@hkwtia.org

Presented by:

Mr. Alan Ho

Hon. Secretary and Treasurer,

Professional Information Security Association (PISA)

Contact: alan.ho@pisa.org.hk

2010.03.27

Organizers

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

Sponsor

OFTA

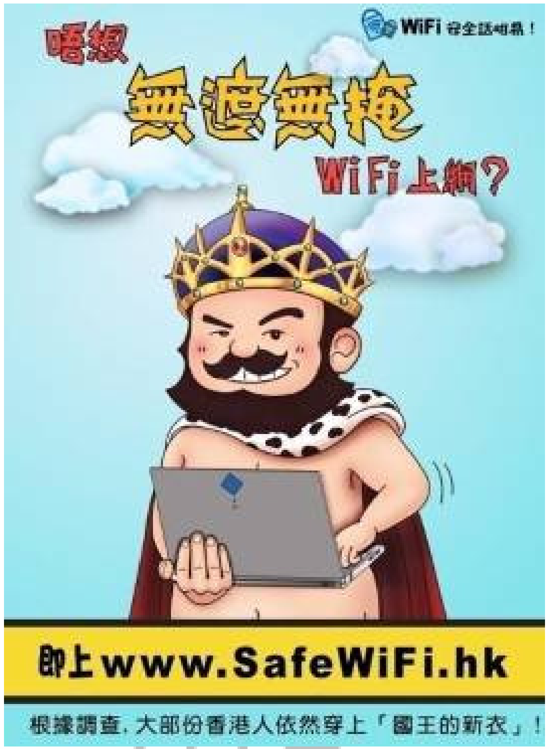
電訊管理局

WiFi

安全話咁易

About SafeWiFi.HK

- Public Awareness Campaign on WiFi Safety
- portal website www.SafeWiFi.hk to provide affluent knowledge about Wi-Fi Security.
- WTIA & PISA conduct survey about Wi-Fi Security and promote the importance of Wi-Fi Security. For more information, please visit www.safewifi.hk.



WiFi
安全話咁易

Introduction to WTIA

WTIA
香港無線科技商會

Hong Kong Wireless Technology Industry Association

www.hkwtia.org

Objectives of WTIA

Not-for-Profit Corporation registered in HK since 2001 with objectives:

- To promote the development, usage and awareness of wireless technology applications in Hong Kong
- To represent and safeguard the interests and opinions of the wireless technology to the Government and other international parties
- To enhance communication and partnership between different types of companies in the wireless technology industry

Activities of WTIA

- has over 150 local and overseas company members, including mobile network operators, mobile device manufacturers, wireless technology providers, system integrators, wireless application services developers, consultancy firms, etc.
- has organized different types of activities, including conference, seminar, workshop, competition, exhibition, etc. to accelerate the industry development.
- operate the Wireless Development Centre (WDC) at Cyberport

Introduction to PISA

Professional Information Security Association

(PISA)

專業資訊保安協會

www.pisa.org.hk

About 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

Mission of PISA

- 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

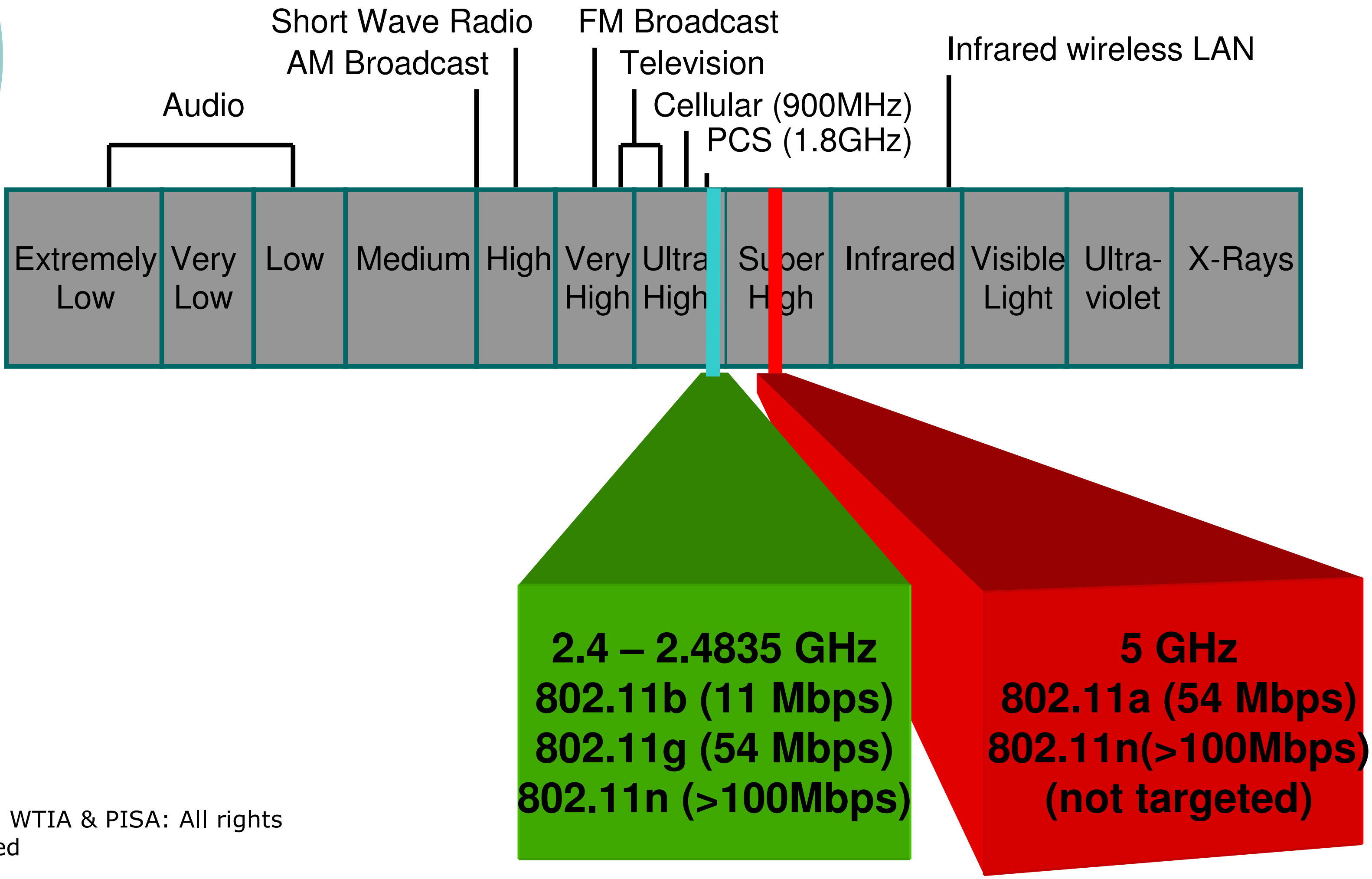
Hong Kong Wi-Fi Security Survey

- Nickname - HK War Driving
- WTIA and PISA Board and Neutral Definition: non-intrusive collection of “**Wireless LAN**” **or “Wi-Fi"** information including network name, signal, location by using a device capable of WLAN signal receiver and moving from one place to another

Potential Risk of Unsecured WiFi

- Security – unsecured WiFi Network
  - Resources
  - Legal
    - Illegal download and transaction by unauthorized users
- Privacy – leak of personal information

Our Focused in 2.4G License Free Spectrum



Is this legal?

- there are always two sides
- Simply driving around a city searching for the existence of wireless networks in a non-intrusive way, with no ulterior motive cannot be illegal.
- However, if you are searching for a place to steal internet access, or commit computer crimes then the wardriving you performed was done in a malicious manner and could be treated as criminal offense.

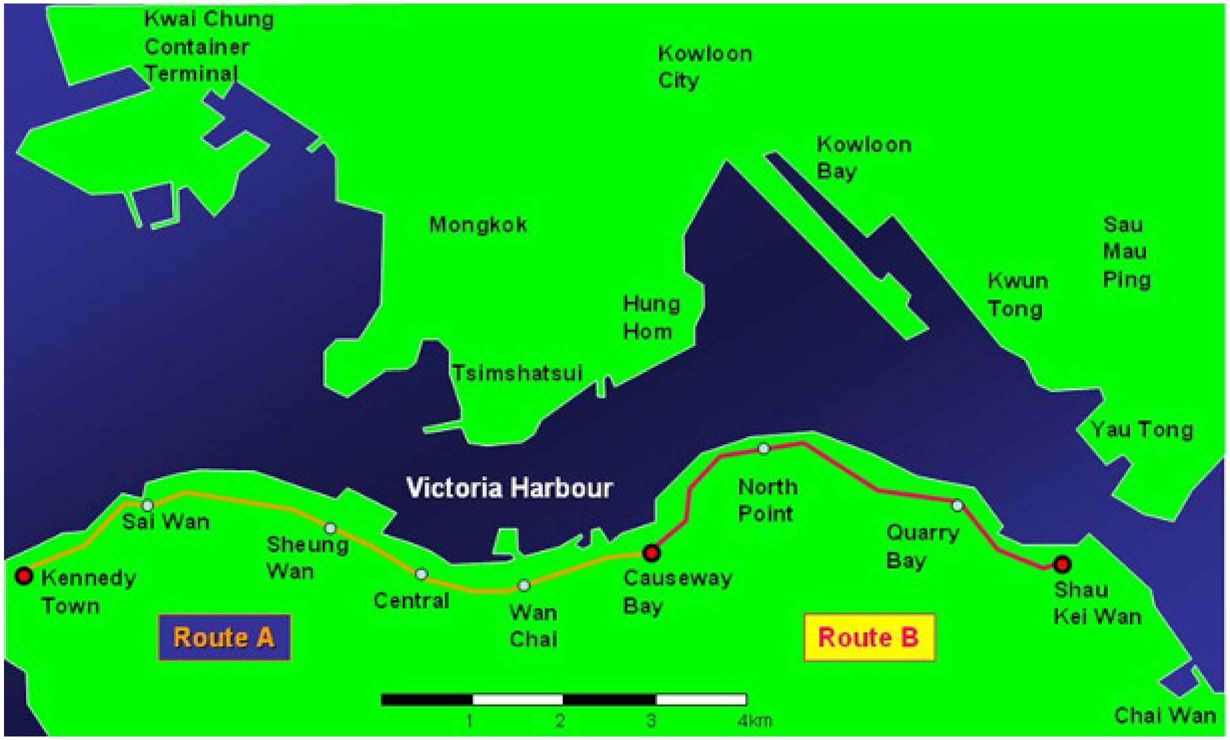
Our Code of Ethics in WD

- Our Objective of the Survey is to study the WLAN Security status and to arouse the public awareness in the WLAN Security
- We do not publicize the exact location and owner of the individual insecure APs. We Publicize only the consolidated figures
- We do not connect to any insecure AP to further explore their vulnerability
- We do not interfere/jam any wireless traffic

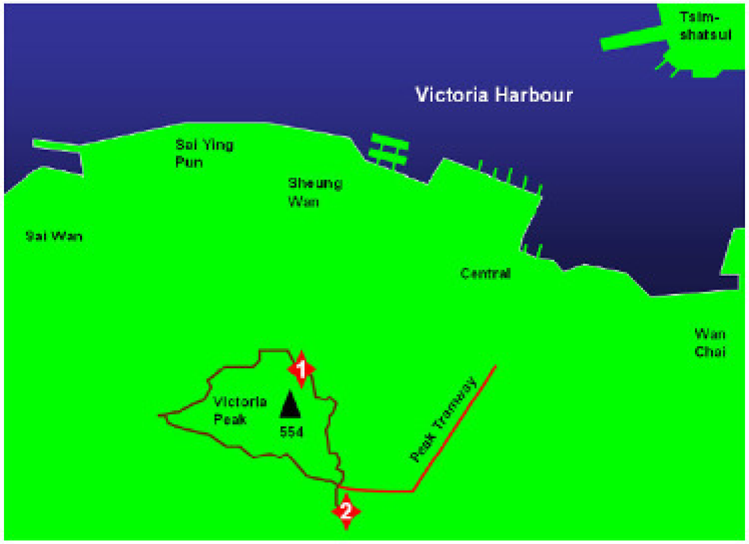
History of PISA/WTIA War Driving

Year	Tramway	Others
2002	Route A	N/A
2003	Route A + B	Victoria Peak War Driving – Long Distance
2004	Route A + B	Victoria Harbour War Sailing - Ferry
2005	Route A + B	Kowloon – Car and Bus
2006	Route A + B	Hong Kong Island round trip – Mini Bus
2007	Route A + B	Macau War Driving
2008	Route A + B	War driving in Victoria Harbour, Kowloon, New Territories and Macau
2009	Route A + B	War driving in Kowloon, New Territories and public/private housing estates

War Tramming Route A & B



War Driving 2003

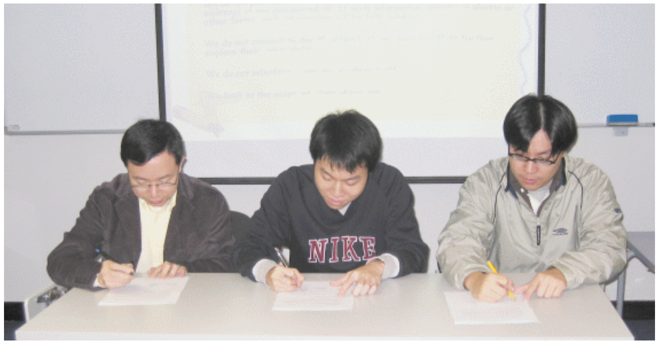


Two Checkpoints on the Victoria Peak

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

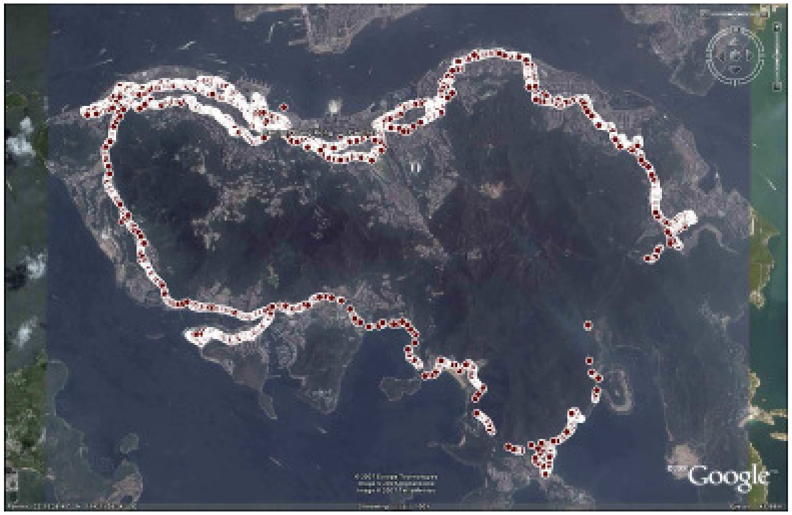
War Driving 2004

STAR FERRY'S HARBOUR TOUR
天星渡海遊
KOWLOON PENINSULA
VICTORIA HARBOUR



War Driving 2005

War Driving 2006



War Driving 2007

A Tales of Two Cities :
WD in HK and Macau

Hong Kong WiFi Security Survey (War Driving) 2008

The most comprehensive war-driving survey in Hong Kong: covering HK Island (Tramway), Kowloon, New Territories and Victoria Harbour

Hong Kong WiFi Security Survey (War Driving) 2009

HK, Kowloon & NT + public/private housing estates

Objectives of WD2009 - HK

- To study the current WLAN security status of HK
- To benchmark the results with previous figures from 2002 to 2008 in HK
- To conduct a non-intrusive WLAN security field study with responsible disclosure of information
- To arouse public awareness in WLAN security in both HK
- To compare the usage of encryption methods between two different type of estates
- To benchmark the results with neighboring area. e.g. Macau

Equipment Used:

- *Hardware:*
  - Notebook computers
  - Smartphone
  - WLAN cards, antennae and GPS

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

Part 1: The Hong Kong Side

Day 1: HK Island War Tramming

29 Nov2009 (Sunday) 10:00am-1:00pm

Day 2: New Territories War Driving

13 Dec 2009 (Sunday) 10:00am-1:00pm

Day 3: Kowloon War Driving

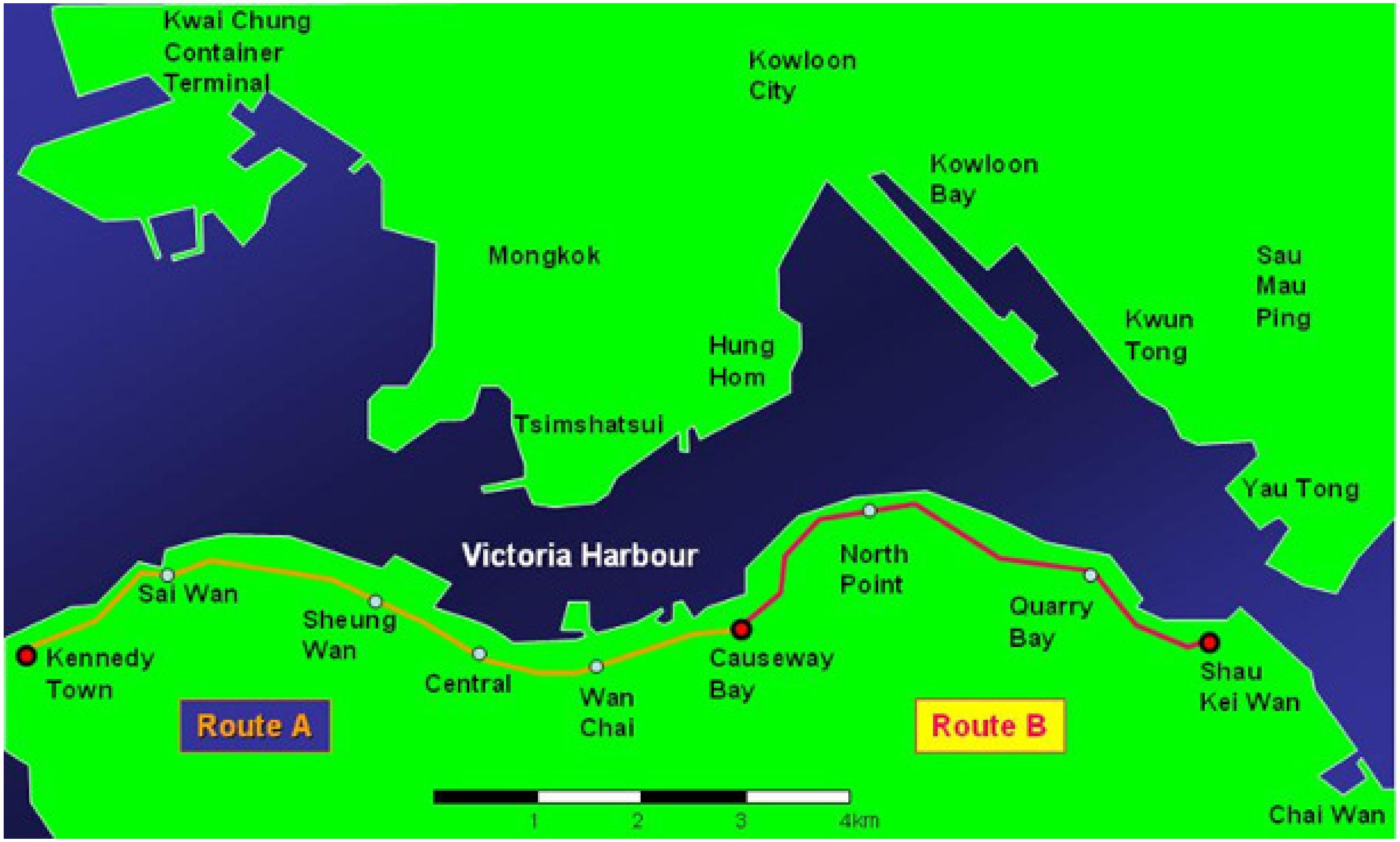
27 Dec 2009 (Sunday) 9:30am-1:30pm

Day 4: Public/private housing estates

21 Feb 2010 (Sunday) morning

Day 1: HK Island Tramway

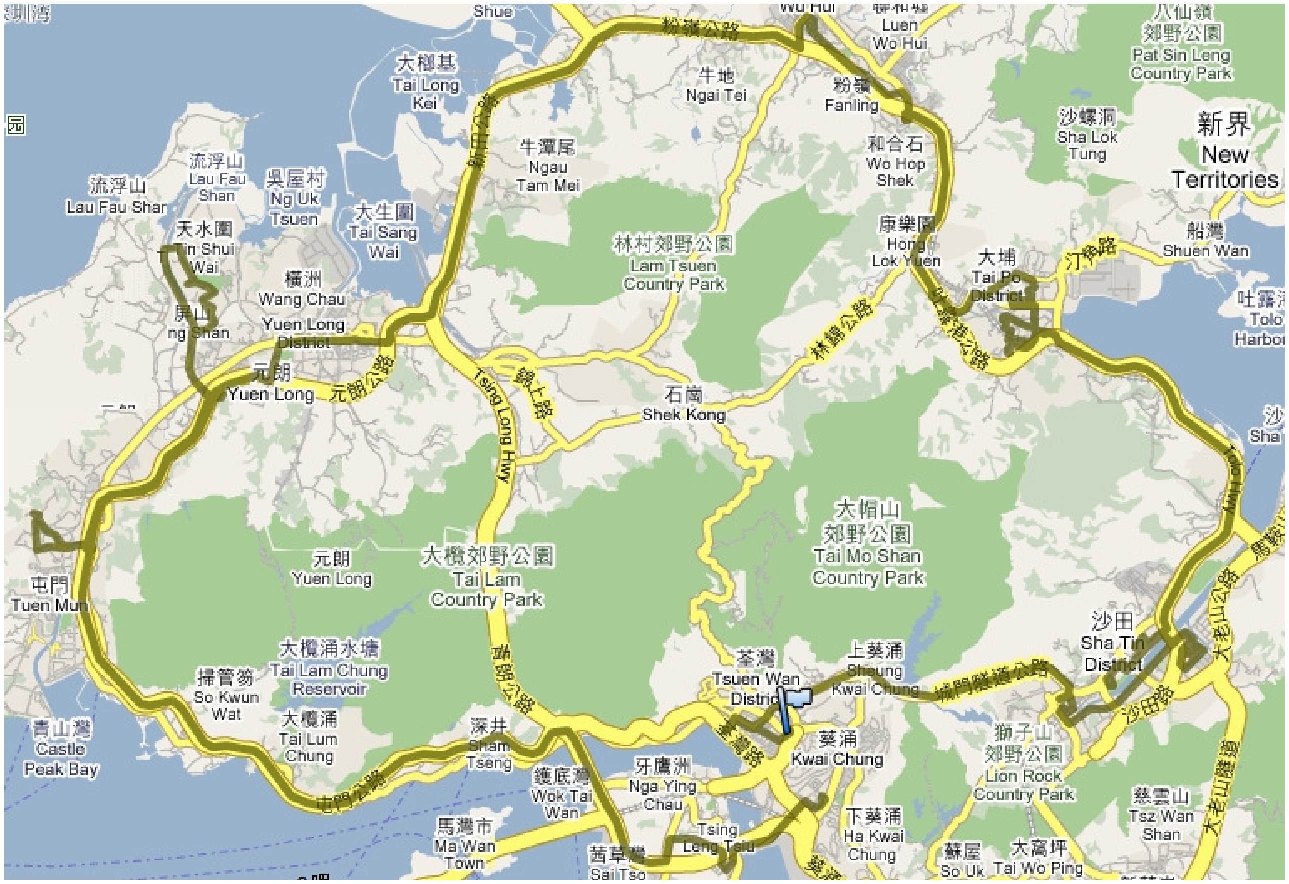
Day 1: HK Island Tramway



Day 1: HK Island Tramway

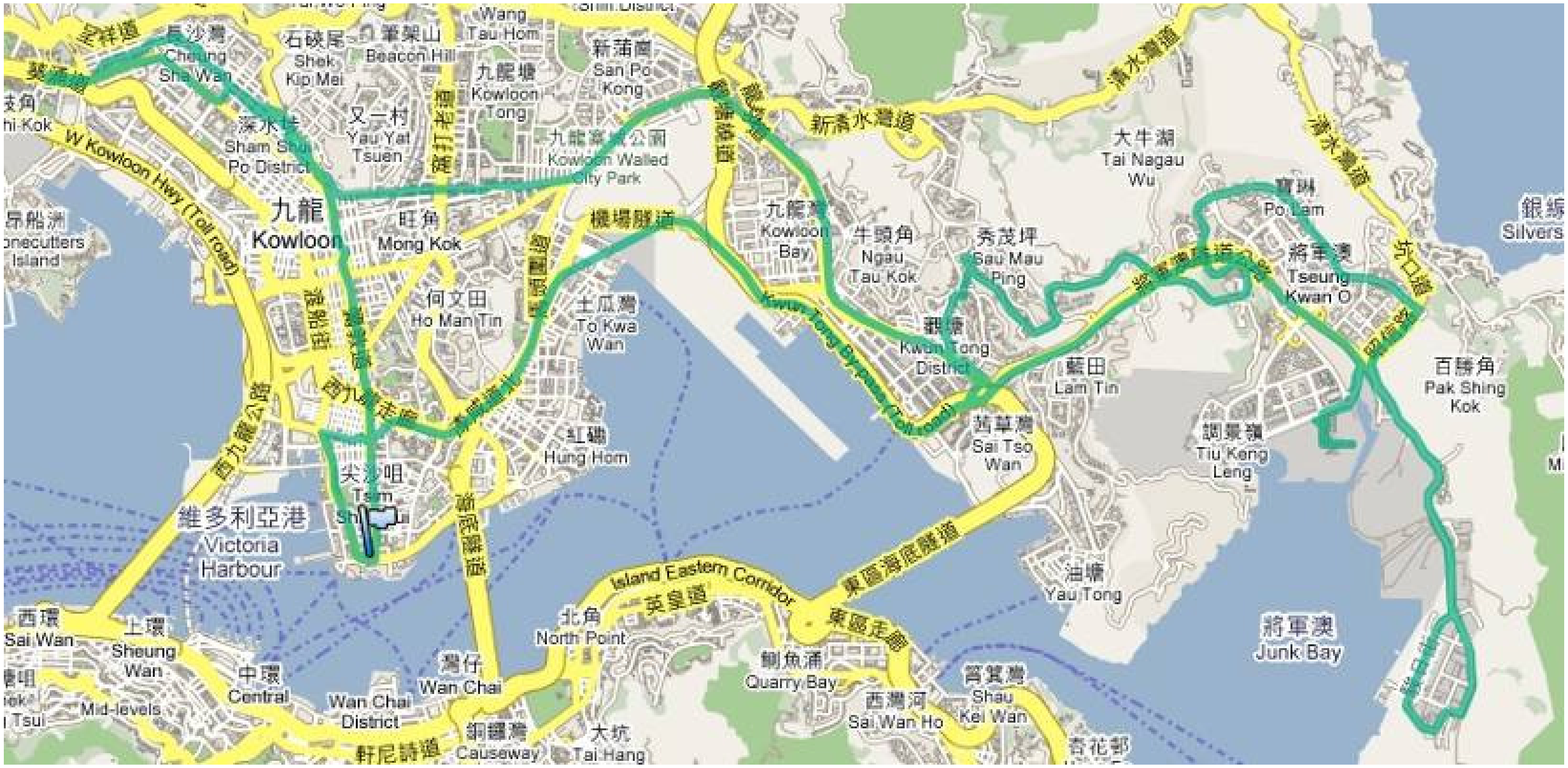
- War Driving on a tram had been proved to be a very effective way because trams run at a moderate speed (30-50km/h) in the middle of the road, allowing very good coverage of signals from the both sides.
- By War Driving on a tram, we benchmark the results with that of previous war driving studies from year 2002 to 2008 along the tramway
  - Route A - from Kennedy Town to Causeway Bay
  - Route B - from causeway Bay towards Shau Kai Wan
- This A+B route covers the whole tram way and is equivalent to the whole business corridor of the Hong Kong Island

Day 2: New Territories



Day 3: Kowloon

Day 3: Kowloon



Day 4: Housing Estates

- Conducted a war-driving in public and private housing estates
- To compare the wireless LAN usage between two different type of estates.
- To compare the usage of encryption methods between two different type of estates.

Part 2: Extra ~ Macau War Driving

Macau Bus Route 6 & 15

12 Sep 2009 (Saturday) 10:00am-5:00pm

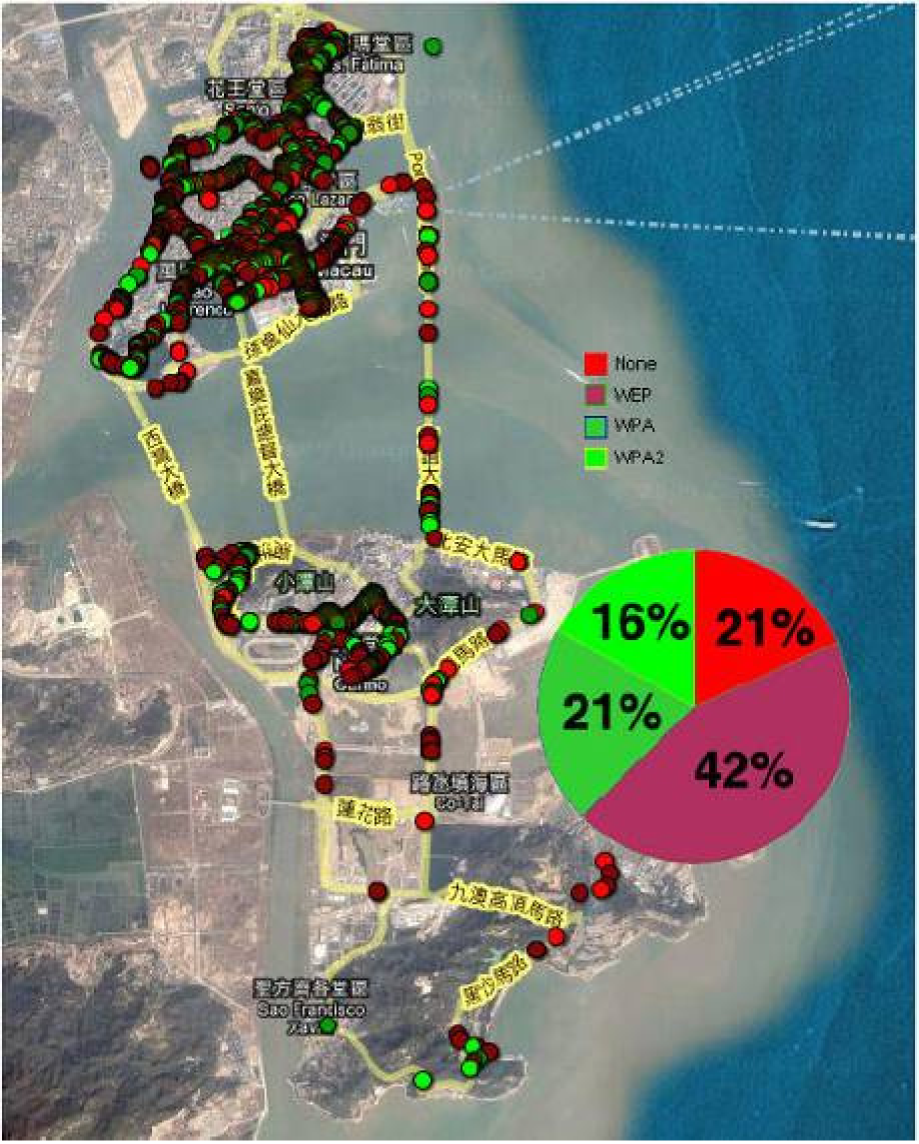
Co-organizing with
- ISACA Macau Chapter
- MANETIC
- Electronic Commerce Association of Macau

Macau

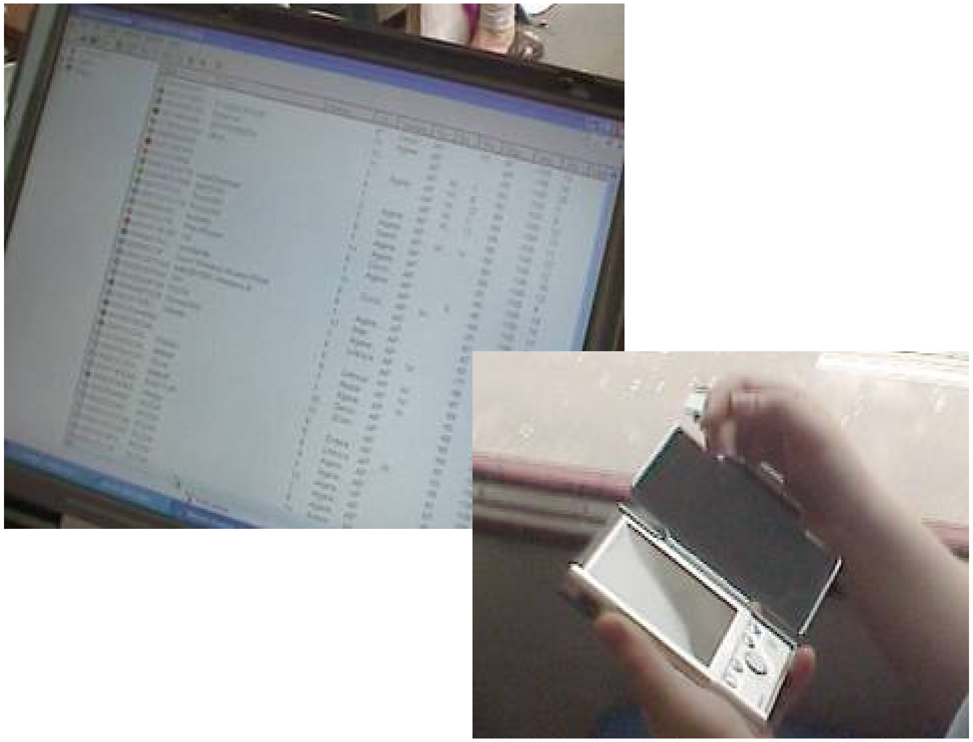
Macau

Bus Route 6 & 15

Covering main districts in Macau as well as Coloane and Taipa Islands

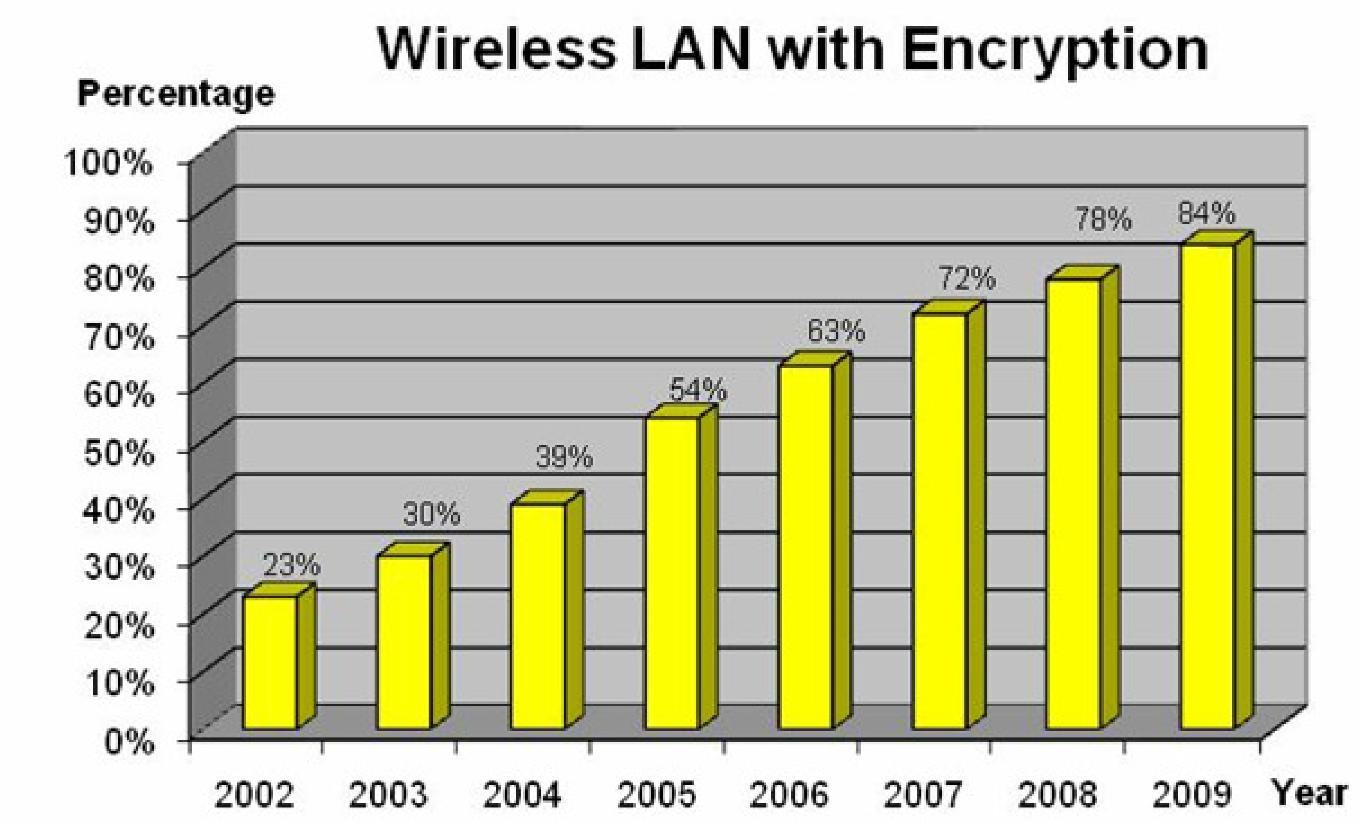


Summary of Findings



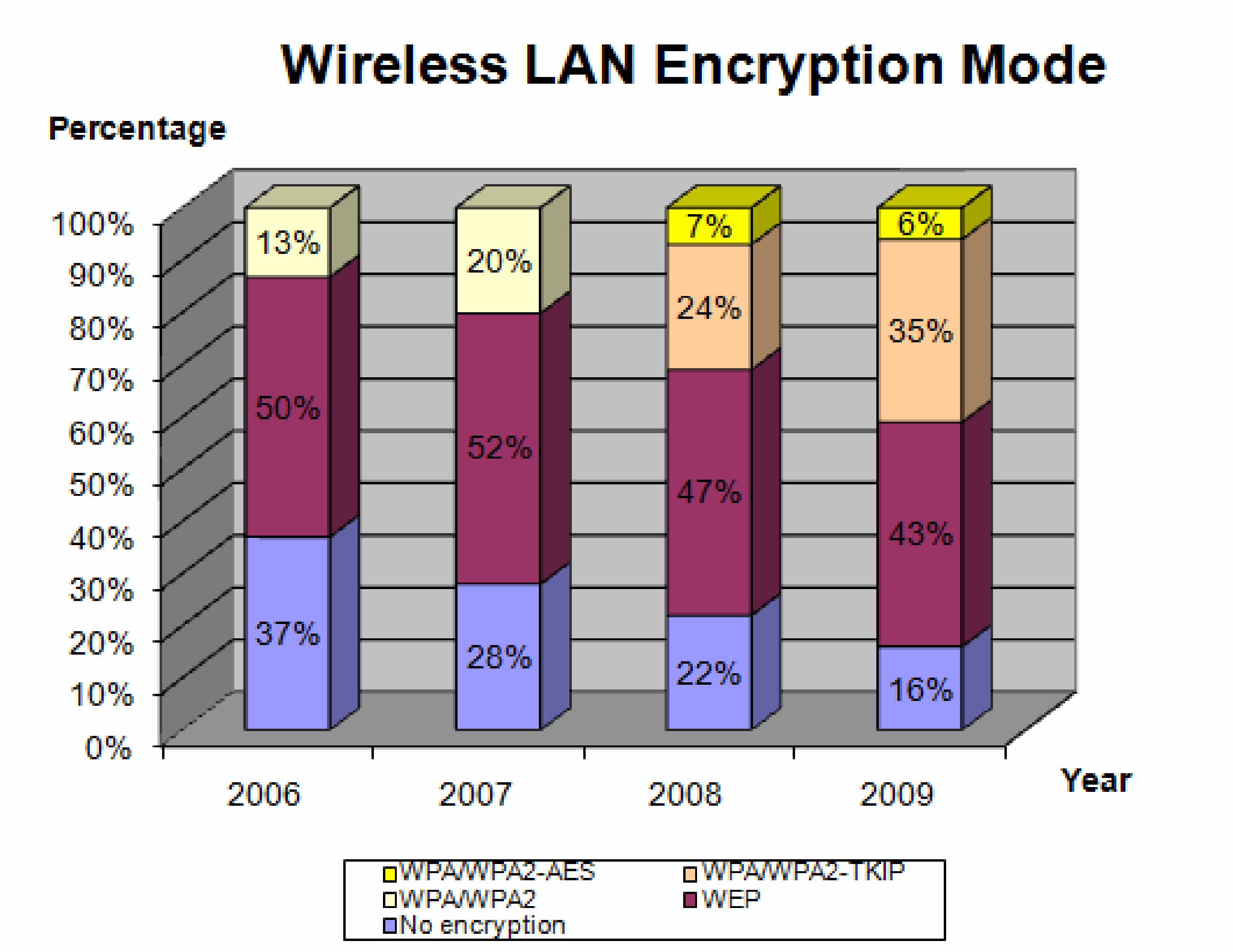
HK: Encryption Mode

- Increasing adoption of encryption settings



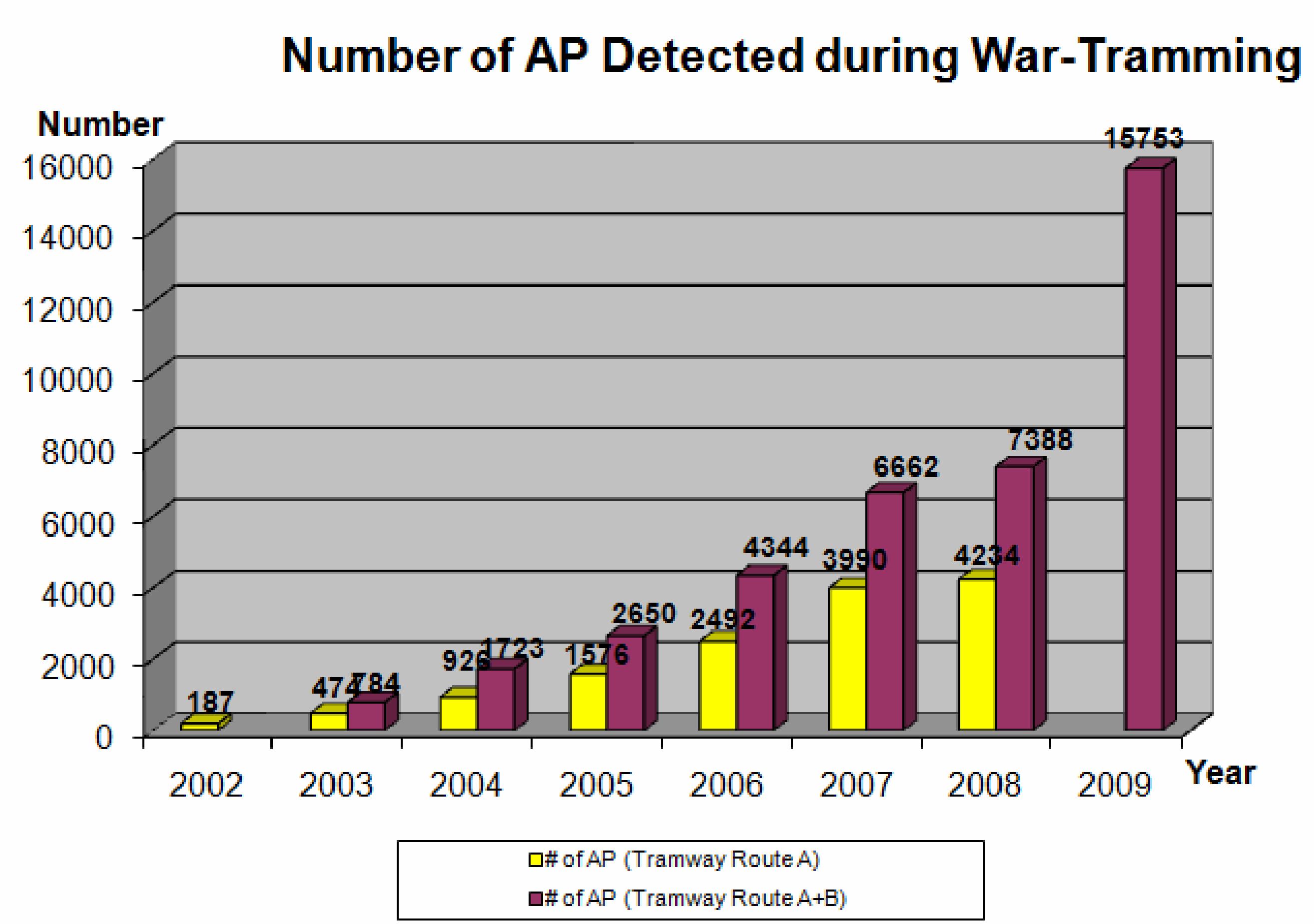
HK: Encryption Mode

- Though encrypted, use of WEP was high
- WEP is nowadays not secure
- WPA/WPA2-TKIP was recently found loopholes and can be hacked
- WPA/WPA2-AES should be used (only 6% WLAN is adopting this highly secured encryption mode)



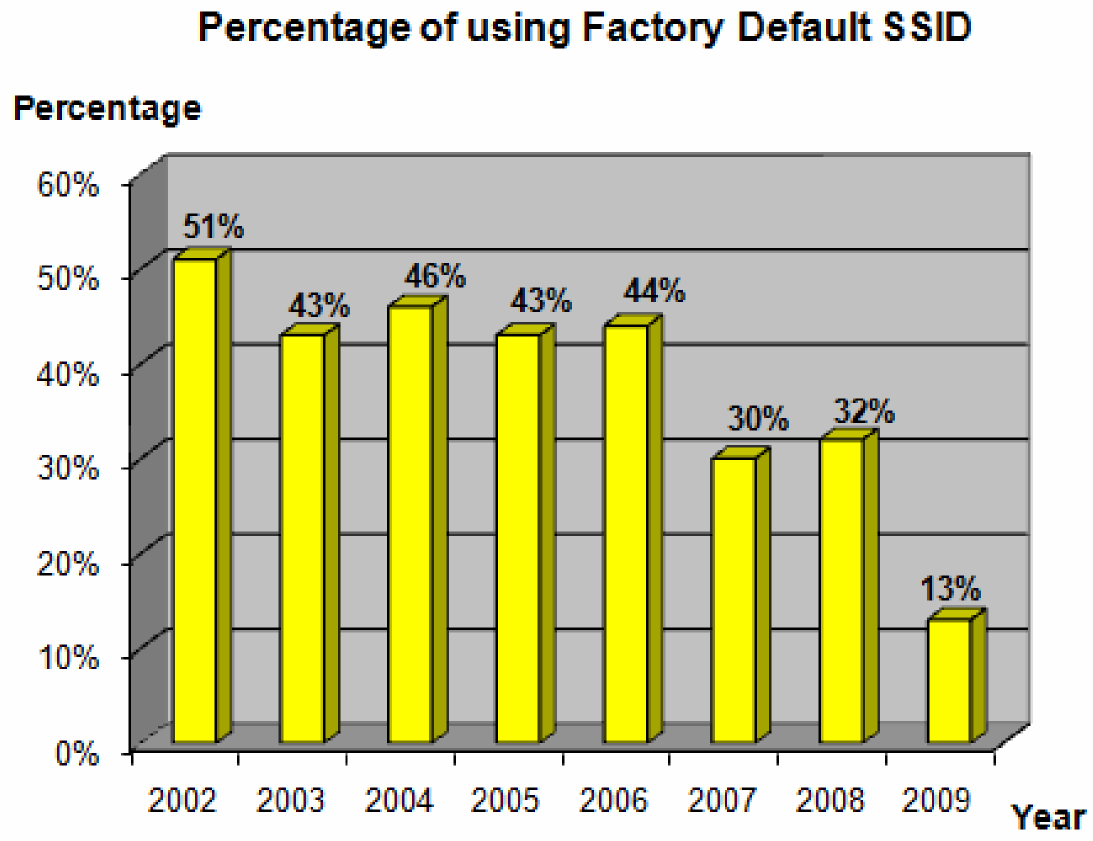
HK: Number of APs

- On a increasing trend



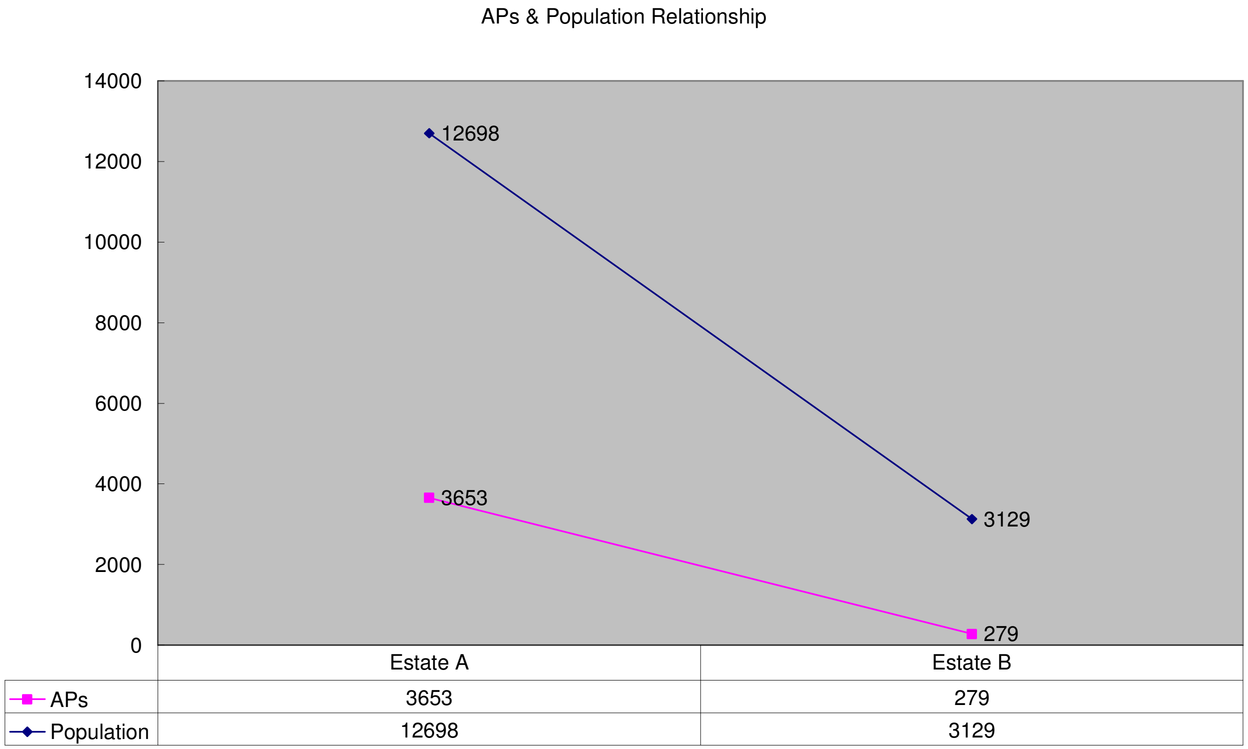
HK: Factory Default SSID

- Refer to default pre-set or generated SSID



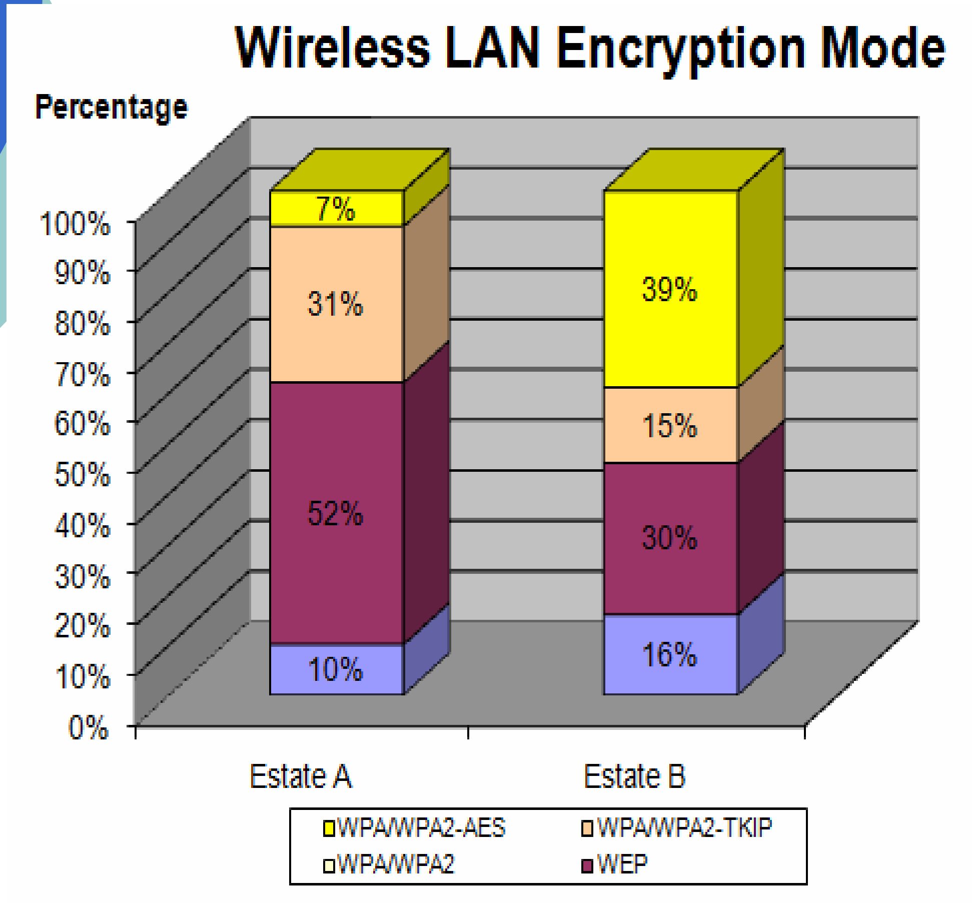
HK: Two Estates

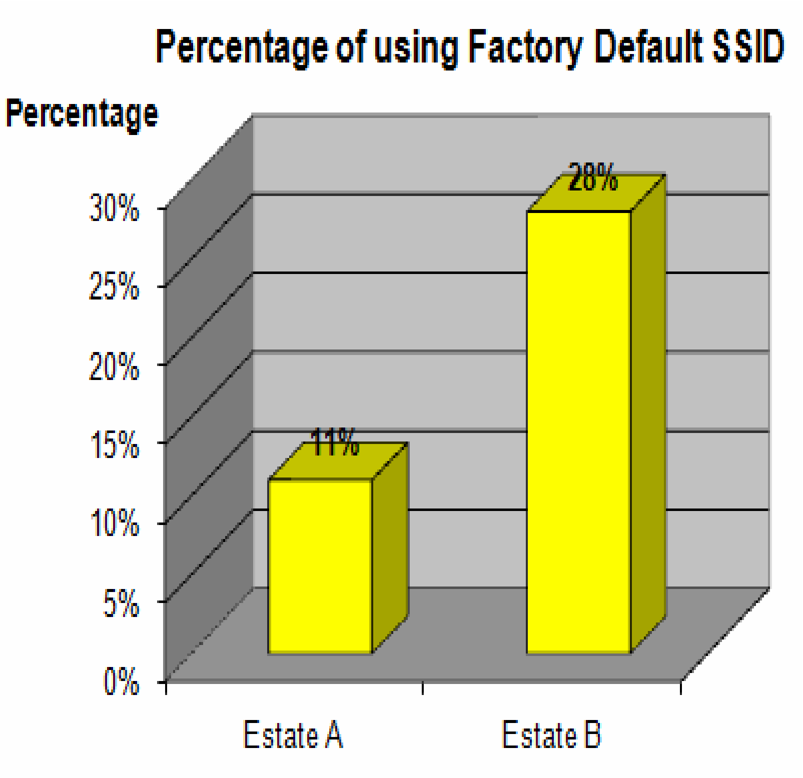
Estate A	Information	Estate B
Private Housing Estate	Type	Public Rental Housing Estate
Since 1977	Year	Since 1963
61	Number of Apartment Buildings	9
12,698	Apartment Flats	3,129


APs & Population Relationship

	Estate A	Estate B
■ APs	3653	279
◆ Population	12698	3129

HK: Two Estates

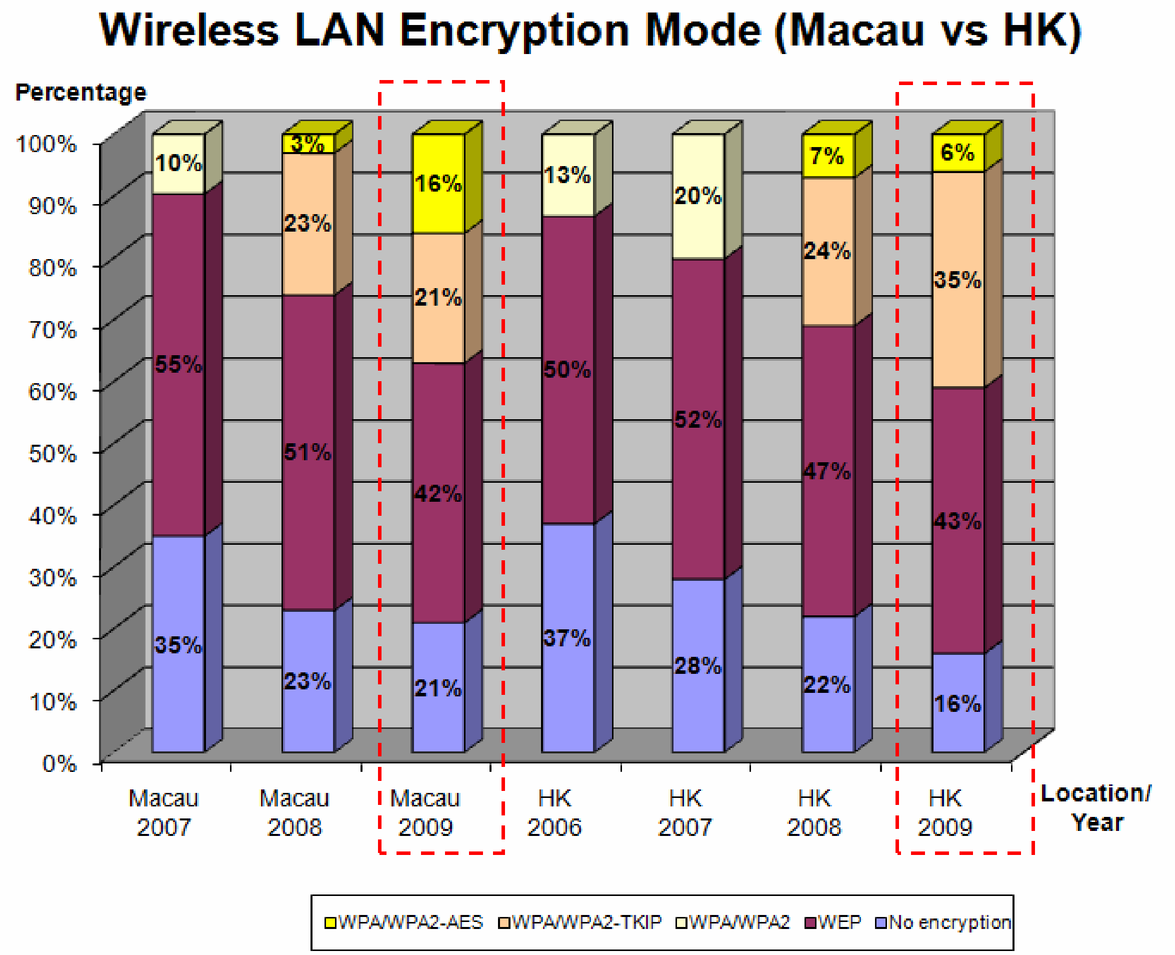

Wireless LAN Encryption Mode


Percentage of using Factory Default SSID

HK: Two Estates

- The more the population, the more the discovered Access Points. The younger the population, the more the discovered Access Points.
- The percentage of using encryption is higher in middle-class population than aging population. However, the percentage of more secured encryption mode is higher in the aging population. It can be considered that the adoption of wireless LAN is later in the aging population than the middle-class population.
- The percentage of protecting their SSID is higher in middle-class population than aging population.

Macau vs HK



- In general, the figures are similar and improving

HK WiFi Security Index

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

Index from 2002 to 2009

		2002 (%)	Weight	2003 (%)	Weight	2004 (%)	Weight	2005 (%)	Weight	2006 (%)	Weight	2007 (%)	Weight	2008 (%)	Weight	2009 (%)	Weight
Public Awareness	Encryption Applied	23	20%	30	20%	39	20%	54	20%	63	20%	72	20%	77	20%	85	20%
Best Practice	Non default SSID*	49	20%	57	20%	54	20%	57	20%	56	20%	70	20%	80	20%	88	20%
Technology Merit			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
	WPA or WPA2									13	L1	20	L1				
	WPA/WPA2-TKIP													29	L2	33	L4
	WPA/WPA2-AES													5	L1	7	L1
			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	

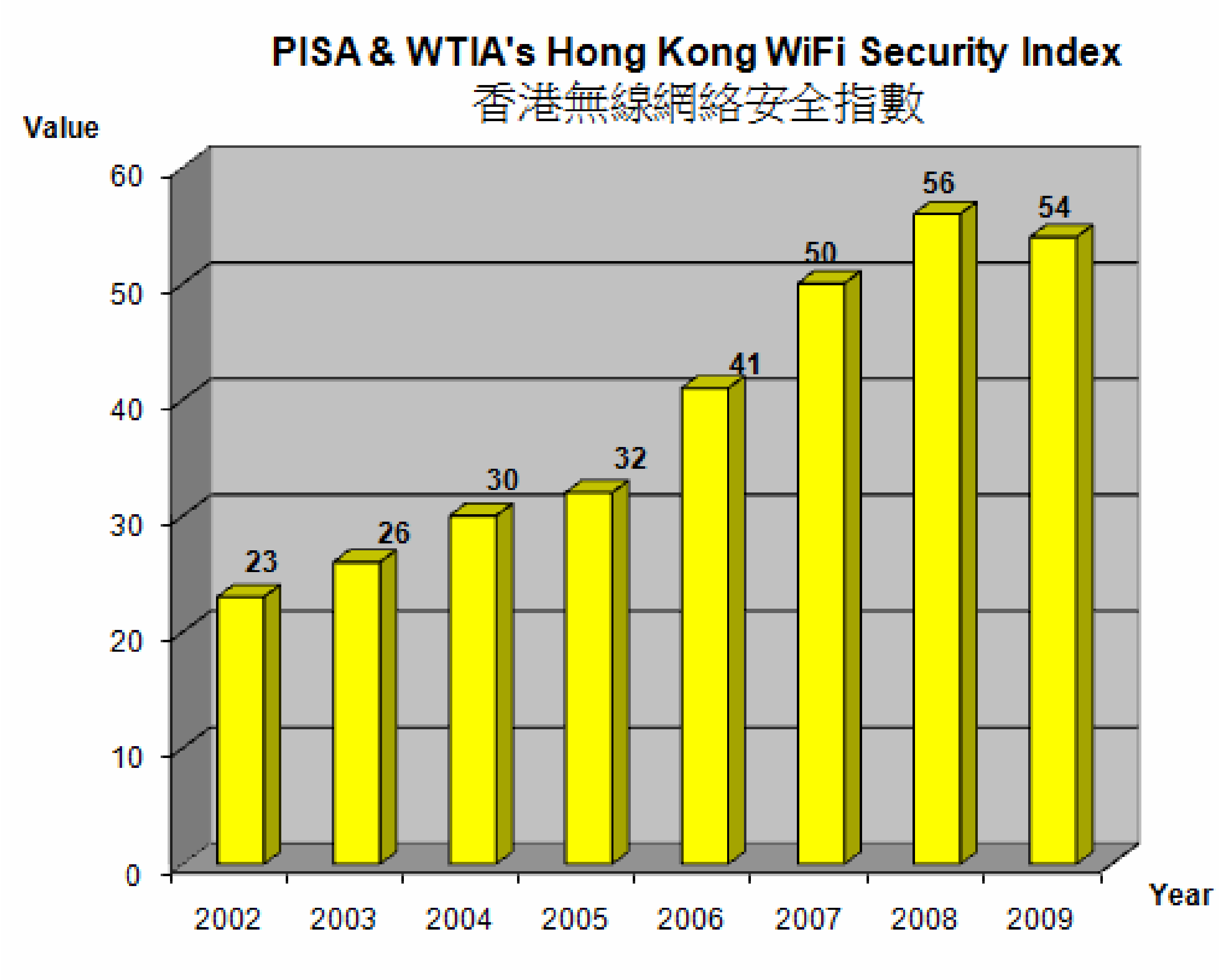
*Non default SSID means the SSID is configured as non-factory-default, non-hotspot or hidden

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

Remarks on Technology Merit

Criticality of vulnerability	**Score**	
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

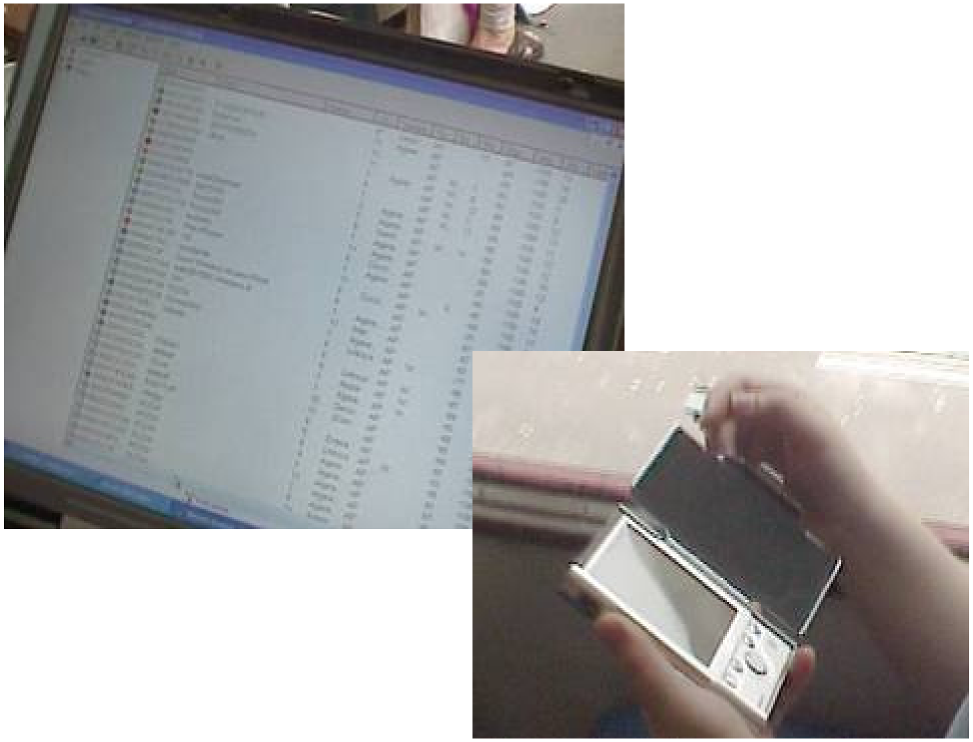
Implication of the Index



Implication of the Index

- A continuous improvement in the adoption of encryption
- A continuous improvement in the adoption of WPA/WPA2 against WEP
- WLAN security index also showed an improving trend but was slightly dropped in 2009. The reasons include
  - (a) the adoption of WEP is still high & the cracking tool is commonly available;
  - (b) the security of using WPA/WPA2-TKIP is decreasing.
- We recommend switching to WPA/WPA2-AES ASAP.

The WiFi Encryption and Recommendation



Overview of Wi-Fi Encryption Modes

- Open
- WEP (Wired Equivalent Privacy)
  - Shared Key: 64 or 128-bit WEP key – 26 hexadecimal character (0-9, A-F)
  - RC4 encryption
  - Security weakness
    - short key size
    - May have IV collisions or altered packets, this is a limitation in WEP design, longer key cannot help
    - May be cracked within a few minutes

Overview of Wi-Fi Encryption Modes

- WPA/WPA2 (Wi-Fi Protected Access)
  - WPA/WPA2 – WPA is based on draft 3 of 802.11i standard; WPA2 is based on the final draft of 802.11i
  - Mode:
    - Personal or PSK (Pre-shared key)
      - Pre-shared key can be a string of 8 to 63 char
        - Recommend using longer and complex key (alphabet, number, symbol) and do not use dictionary word
    - WPA-Enterprise
      - 802.1X authentication / RADIUS
      - Individual user has his/her own password. Much safer than Pre-shared key.

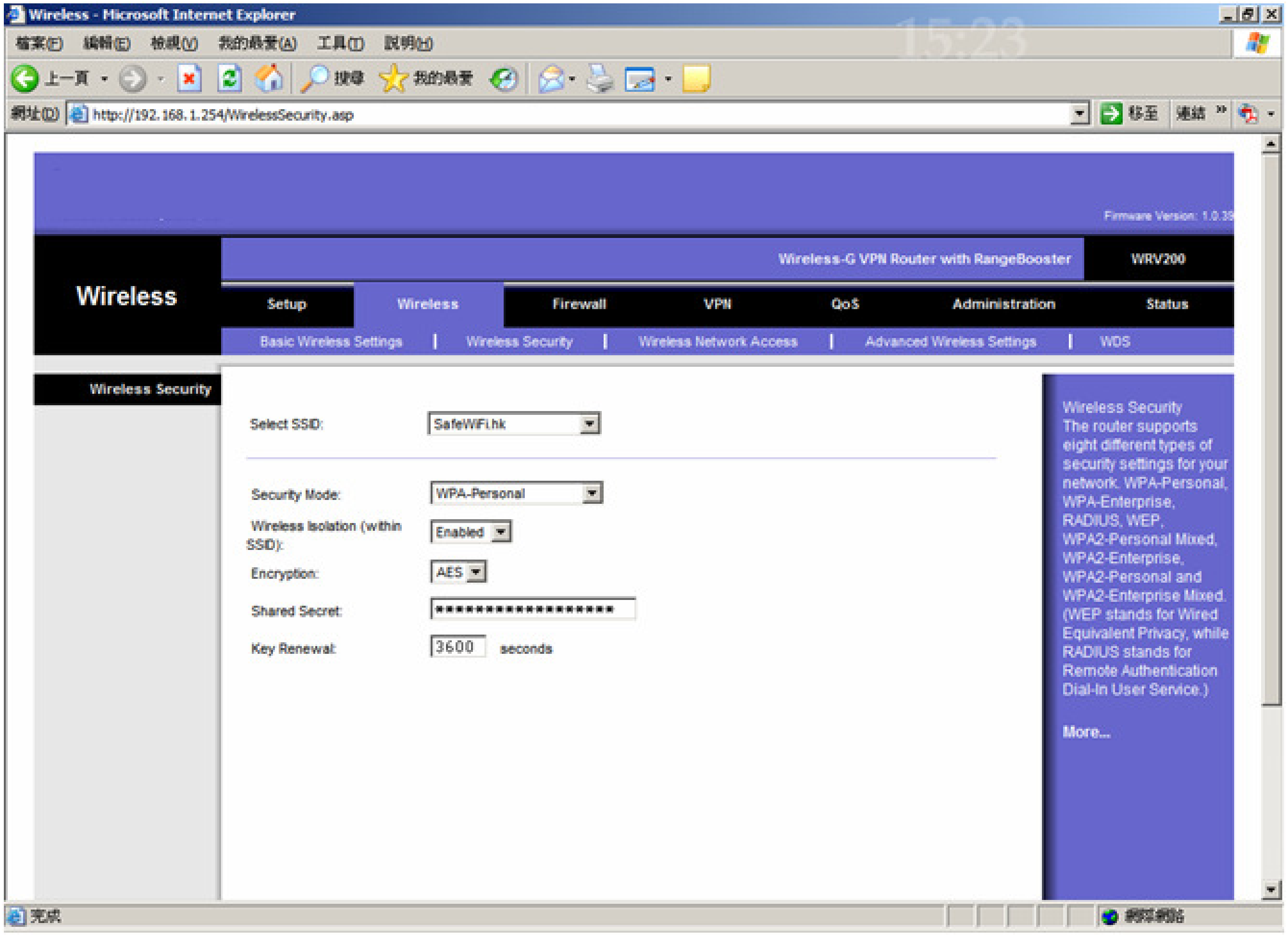
Overview of Wi-Fi Encryption Modes

- WPA/WPA2 (Wi-Fi Protected Access) – cont'd
  - TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) encryption
    - TKIP was implemented to solve WEP problem. AES is a newer implementation and design.
  - WPA/WPA2 is much more secure than WEP
  - However, recently, loopholes were found for WPA/WPA2-TKIP and can be hacked. Hence, we recommend using WPA/WPA2-AES.

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
- Consider to use VPN over public hotspots

AP- WPA AES Setting


Wireless - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
http://192.168.1.254/WirelessSecurity.asp
移至
連結
Firmware Version: 1.0.39
Wireless-G VPN Router with RangeBooster
WRV200
Wireless
Setup
Wireless
Firewall
VPN
QoS
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Network Access | Advanced Wireless Settings | WDS
Wireless Security
More...
完成
網際網路

Select SSID: SafeWiFi.hk

Security Mode: WPA-Personal

Wireless Isolation (within SSID): Enabled

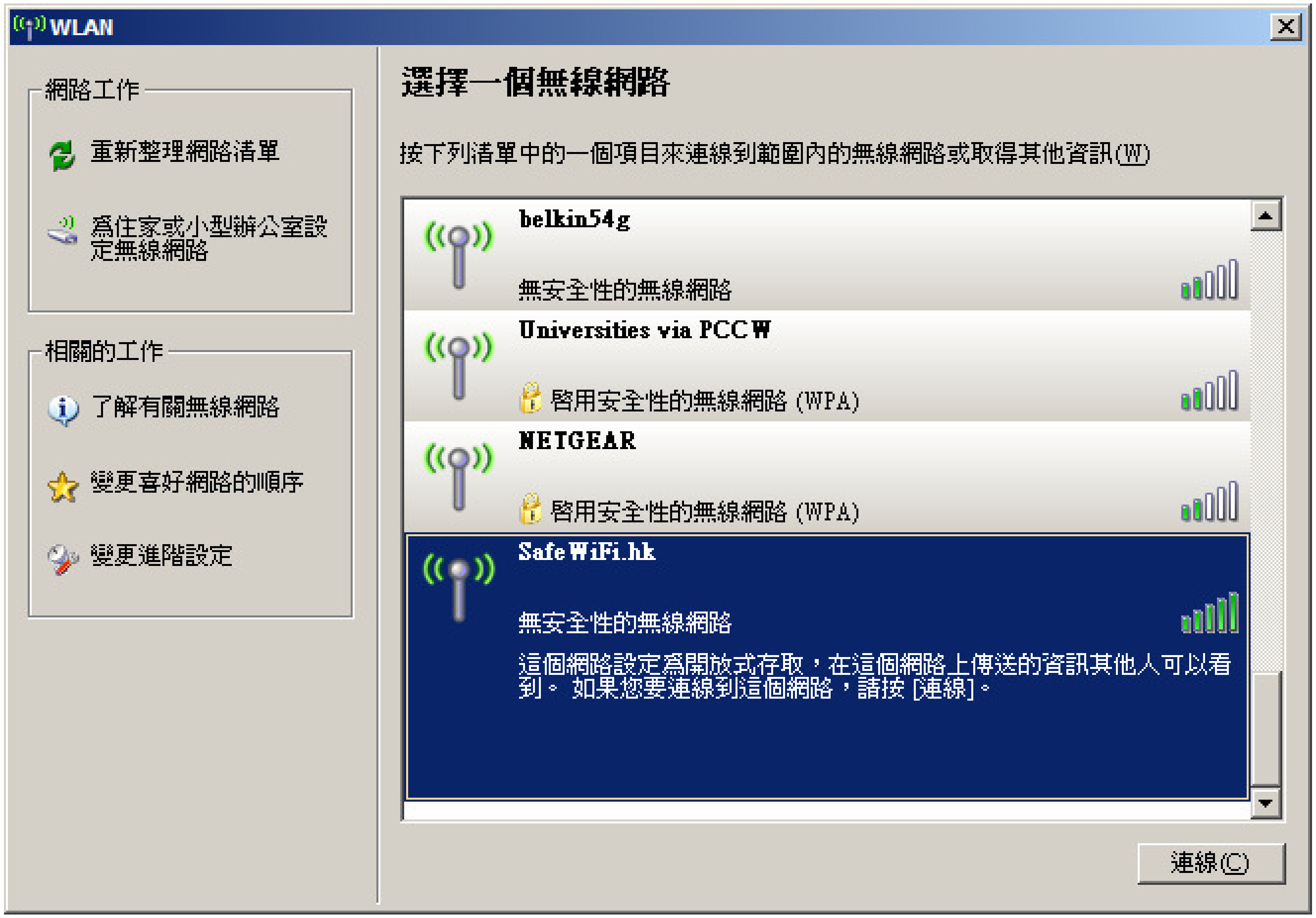
Encryption: AES

Shared Secret: ********************

Key Renewal: 3600 seconds

Wireless Security
The router supports eight different types of security settings for your network. WPA-Personal, WPA-Enterprise, RADIUS, WEP, WPA2-Personal Mixed, WPA2-Enterprise, WPA2-Personal and WPA2-Enterprise Mixed. (WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.)

PC - WPA AES Setting


WLAN

網路工作

重新整理網路清單

為住家或小型辦公室設定無線網路

相關的工作

了解有關無線網路

變更喜好網路的順序

變更進階設定

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)

belkin54g
無安全性的無線網路

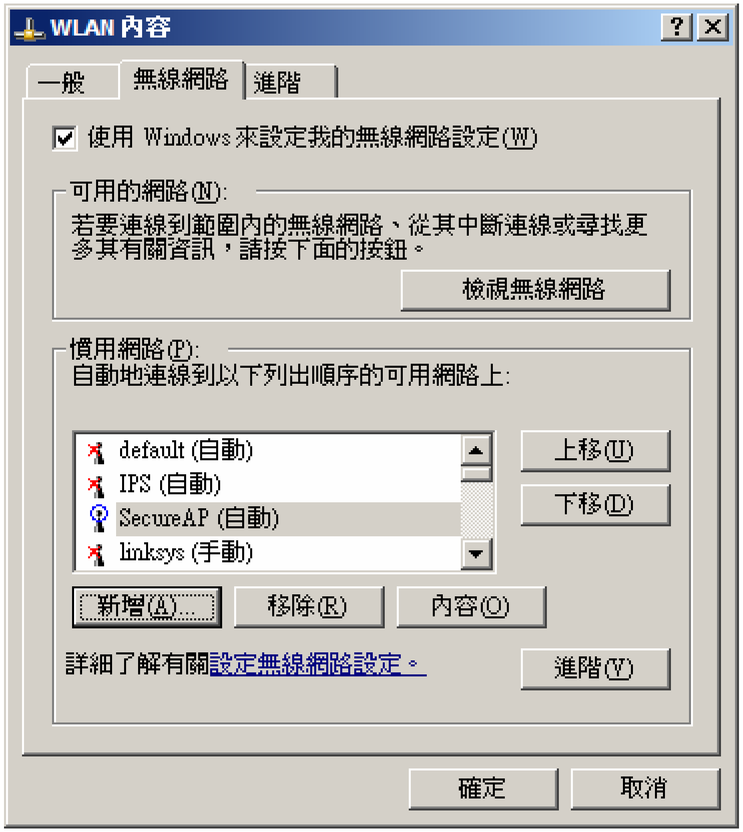
Universities via PCCW
啟用安全性的無線網路 (WPA)

NETGEAR
啟用安全性的無線網路 (WPA)

SafeWiFi.hk
無安全性的無線網路
這個網路設定為開放式存取，在這個網路上傳送的資訊其他人可以看到。 如果您要連線到這個網路，請按 [連線]。

連線(C)

PC - WPA AES Setting



WLAN 內容

☑ 使用 Windows 來設定我的無線網路設定(W)

可用的網路(N):

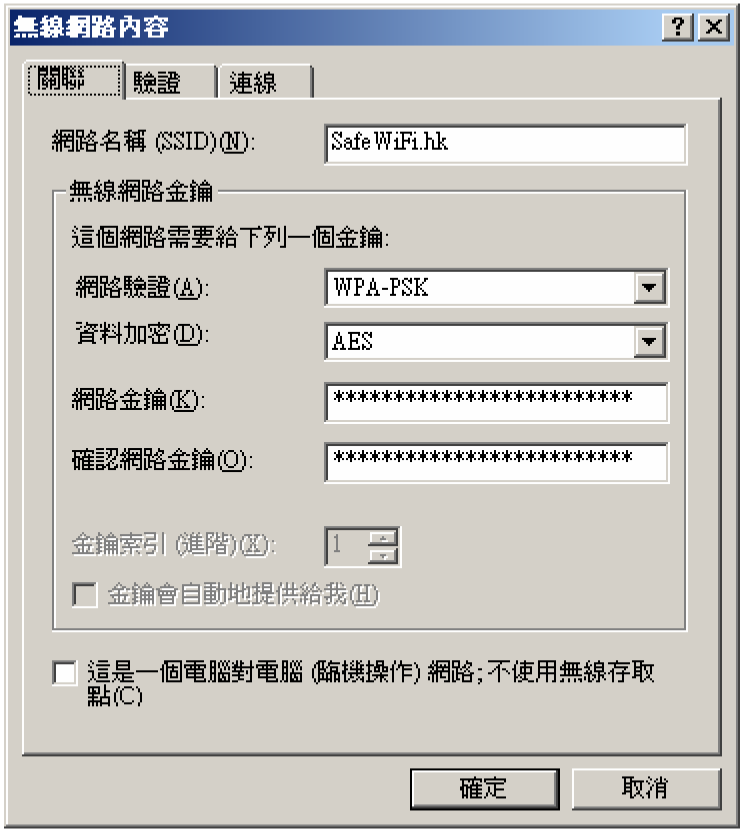
若要連線到範圍內的無線網路、從其中斷連線或尋找更多其有關資訊，請按下面的按鈕。

慣用網路(P):

自動地連線到以下列出順序的可用網路上:

- default (自動)
- IPS (自動)
- SecureAP (自動)
- linksys (手動)

詳細了解有關設定無線網路設定。



無線網路內容

網路名稱 (SSID)(N): Safe WiFi.hk

無線網路金鑰

這個網路需要給下列一個金鑰:

網路驗證(A): WPA-PSK

資料加密(D): AES

網路金鑰(K): ************************

確認網路金鑰(O): ************************

金鑰索引 (進階)(X): 1

□ 金鑰會自動地提供給我(H)

□ 這是一個電腦對電腦 (臨機操作) 網路; 不使用無線存取點(C)

For More Information

- visit Safewifi.hk **WiFi** 安全話咁易
- Seminar on Protecting Your WiFi Network and Utilization” on 27 Mar 2010 (Sat) 「**WiFi**網絡及應用保衛戰研討會**2010**」

WiFi網絡及應用保衛戰研討會2010

- 2010年3月27日(星期六) -下午2:20至 5:20
- 九龍塘達之路72号創新中心地下1B室
- 研討會時間表
  - 歡迎辭：「 WiFi安全話咁易」運動簡介
  - 開幕致辭
  - 香港WiFi保安調查2009：結果及啟示
  - 最新「無線入侵防禦」技術
  - **即場示範**：怎樣防範最新WiFi保安破解術 – 蹭網卡？
  - 嘉賓座談會：WiFi保安於香港及全球的最新趨勢
  - 抽獎環節

Question?

Acknowledgement

-All WD2009 Team Members including

PISA

Alan Ho (Convener) , Alan Tam, Charles Mok, Chee Huen, Frank Chow, George Chung, Howard Lau, Jim Shek, Sang Young, SC Leung, Thomas Tsang, Warren Kwok, WS Lam

WTIA

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

Important Notice

- Copyright

  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

  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

Thank You