HK Wi-Fi Security Survey 2008
2008 無線網絡應用保安普查

Presented by:

Mr. Ken K.K. Fong

Vice Chairman,

Hong Kong Wireless Technology Industry Association (WTIA)

Contact: ken@hkwtia.org

Presented by:

Mr. Alan Ho

Vice Chairperson,

Professional Information Security Association (PISA)

Contact: alan.ho@pisa.org.hk

2009.02.28

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

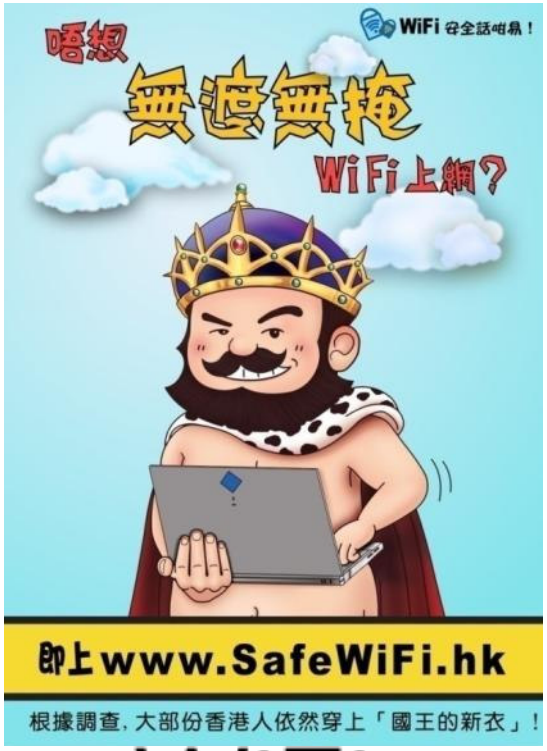
OFTA

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.



Introduction to WTIA

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

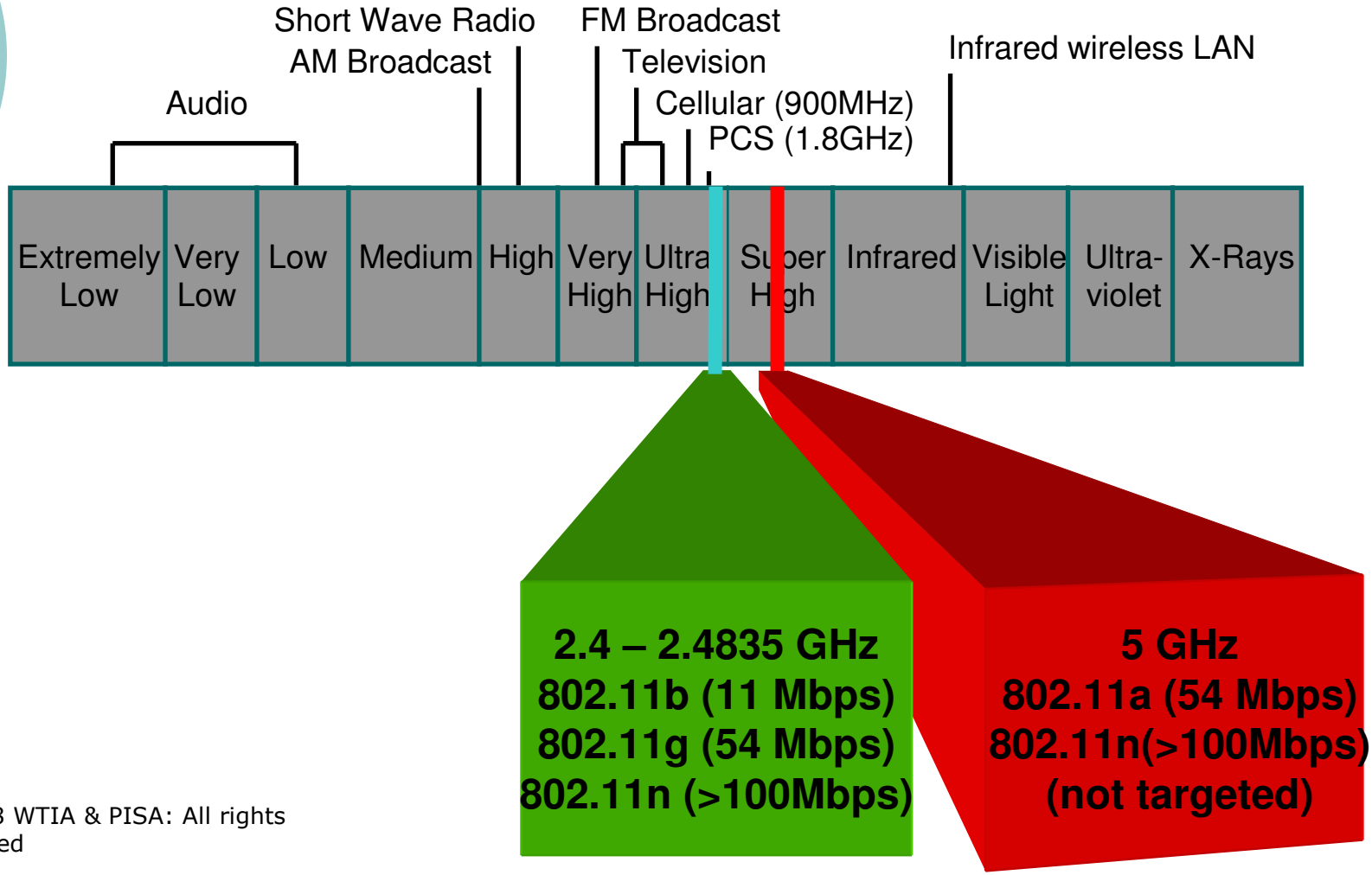
Hong Kong
Wi-Fi Security Survey

- 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

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 Focused in 2.4G License Free Spectrum



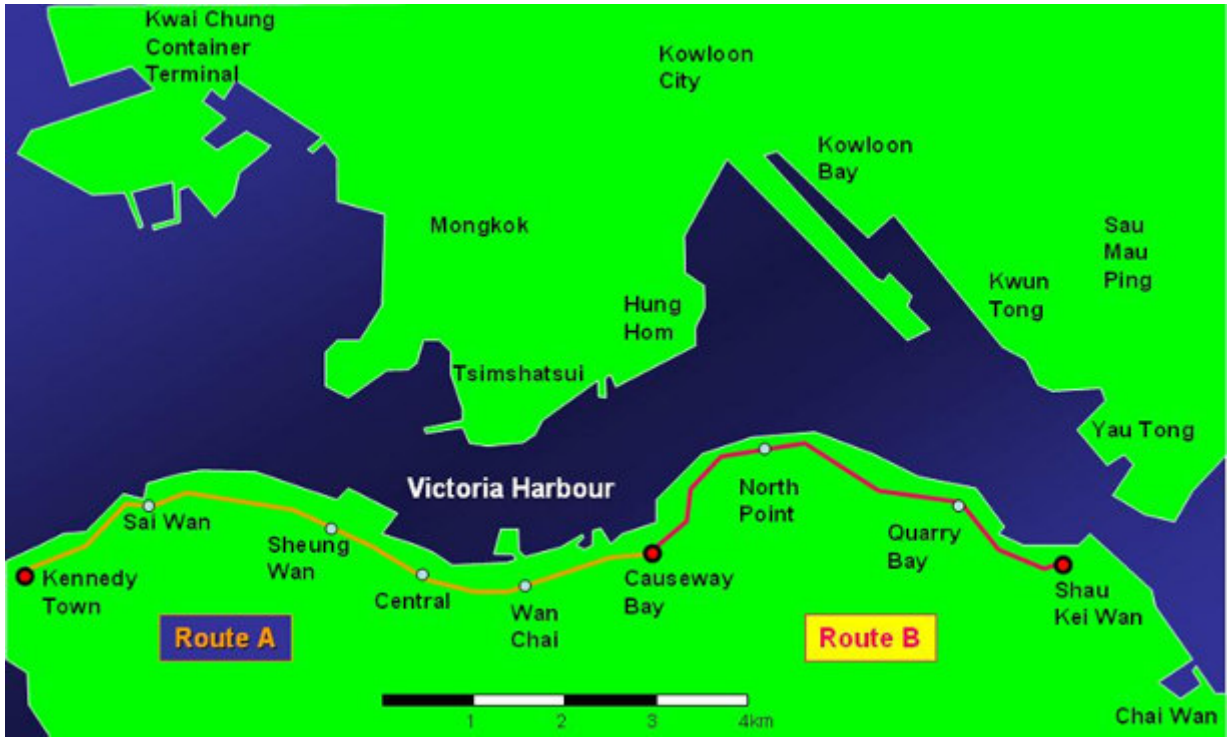
Our Code of Ethics in WD

- 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

War Tramming Route A & B

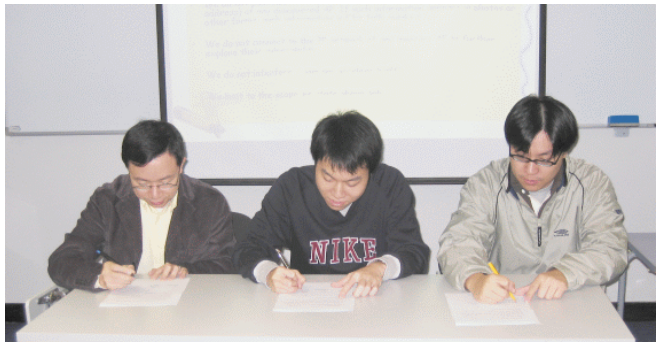


War Driving 2003

Two Checkpoints on the Victoria Peak

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

War Driving 2004



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




Objectives of WD2008 - HK

- To study the current WLAN security status of HK
- To benchmark the results with previous figures from 2002 to 2007 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 benchmark the results with neighboring area. e.g. Macau

Equipment Used:

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

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

Part 1: The Hong Kong Side

Day 1: Victoria Harbour War Sailing

25 Oct 2008 (Saturday) 12:45pm-3:30pm

Day 2: HK Island War Tramming

9 Nov 2008 (Sunday) 10:00am-1:00pm

Day 3: New Territories War Driving

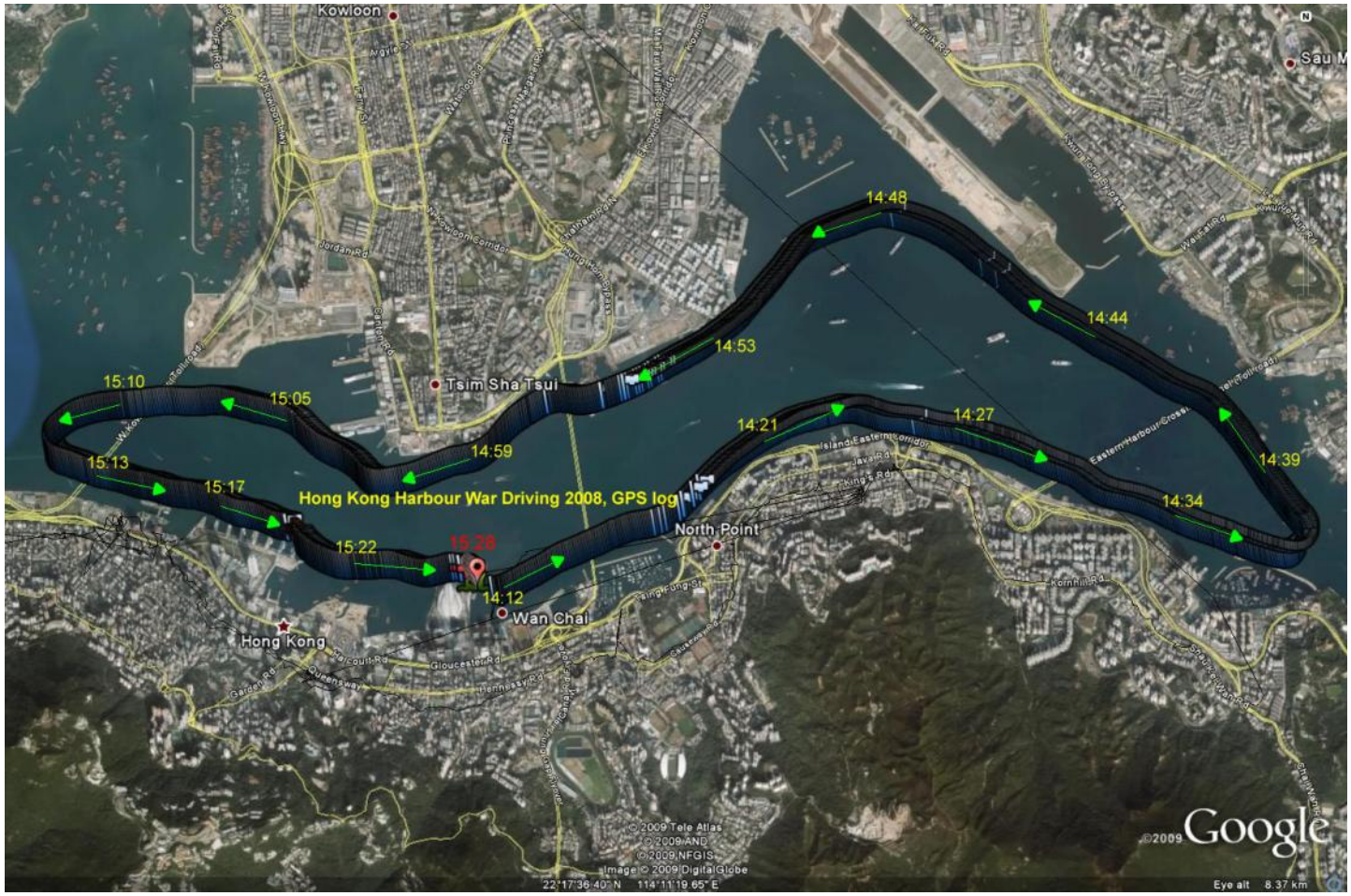
23 Nov 2008 (Sunday) 10:00am-2:00pm

Day 4: Kowloon War Driving

7 Dec 2008 (Sunday) 2:00pm-6:00pm

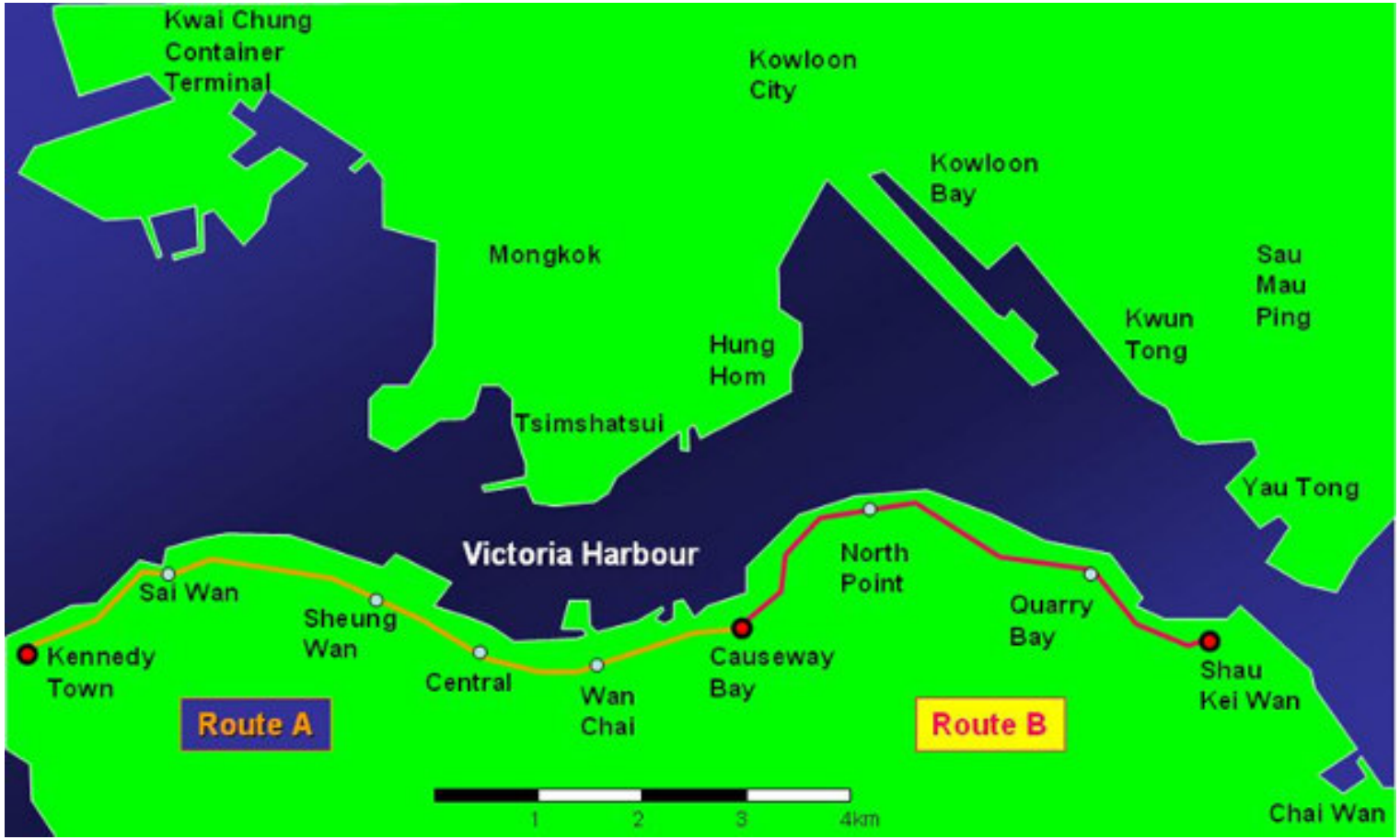
Day 1: Victoria Harbour

Day 1: Victoria Harbour



Day 2: HK Island Tramway

Day 2: HK Island Tramway



Day 2: 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 2007 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 3: New Territories

Day 3: New Territories

Day 4: Kowloon

Day 4: Kowloon

Part 2: Extra ~ Macau War Driving

Macau Bus Route 6 & 15

27 Sep 2008 (Saturday) 10:00am-5:00pm

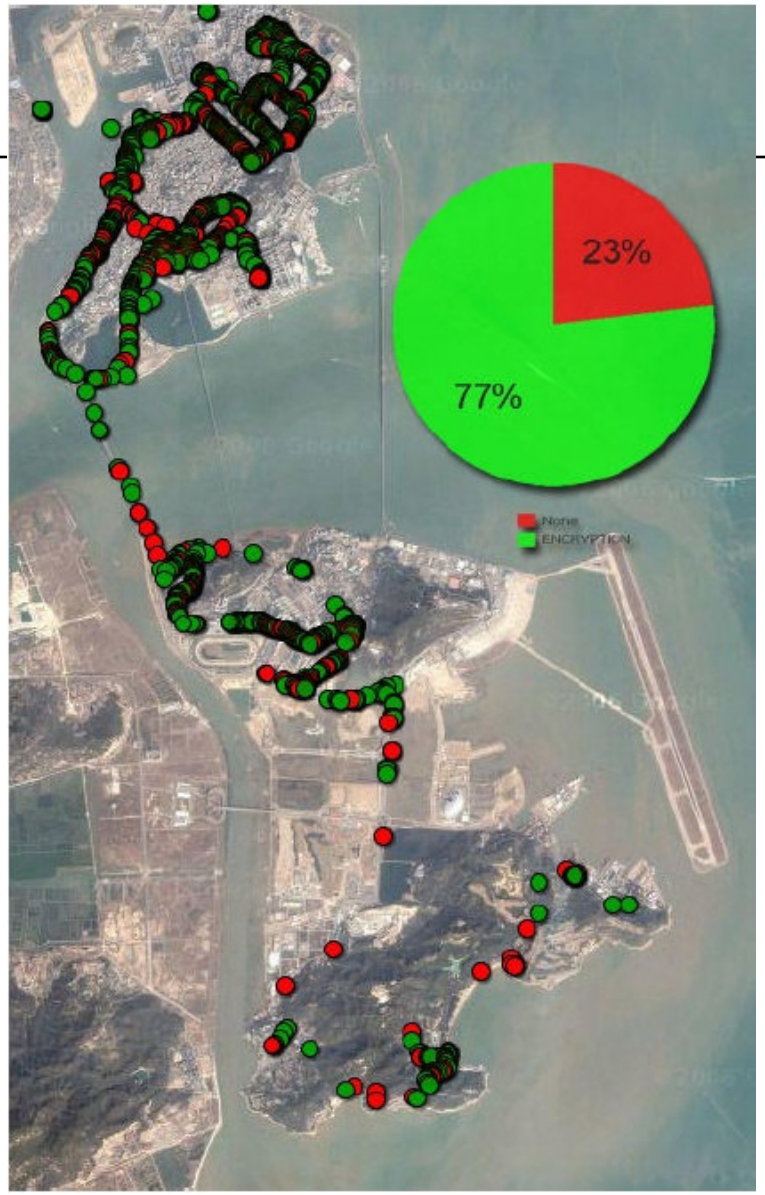
Co-organizing with
- ISACA Macau Chapter
- MANETIC
- Electronic Commerce Association of Macau

Macau

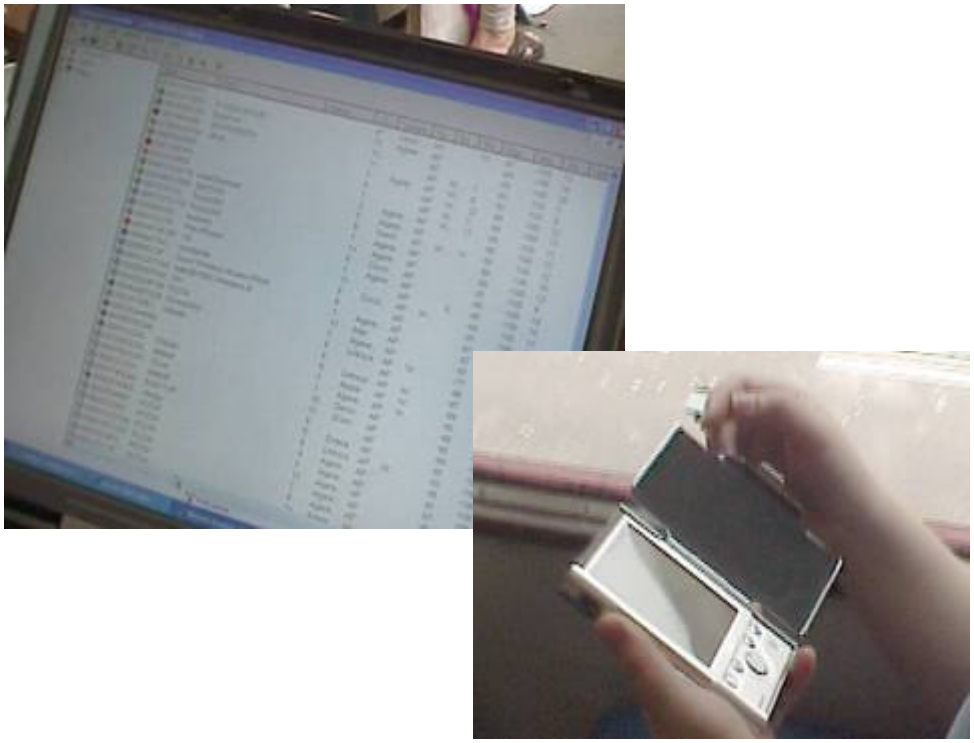
Macau

Bus Route 6 & 15

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

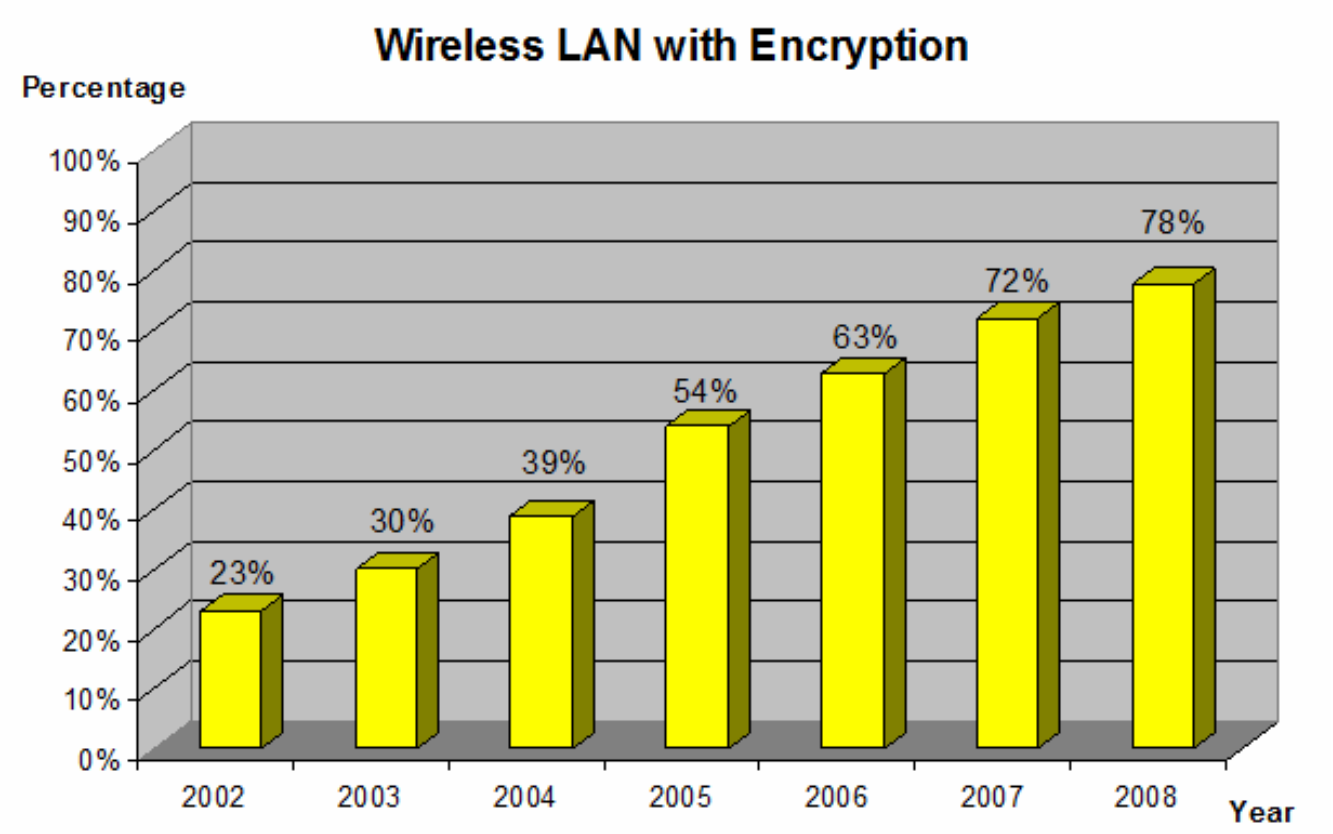


Summary of Findings



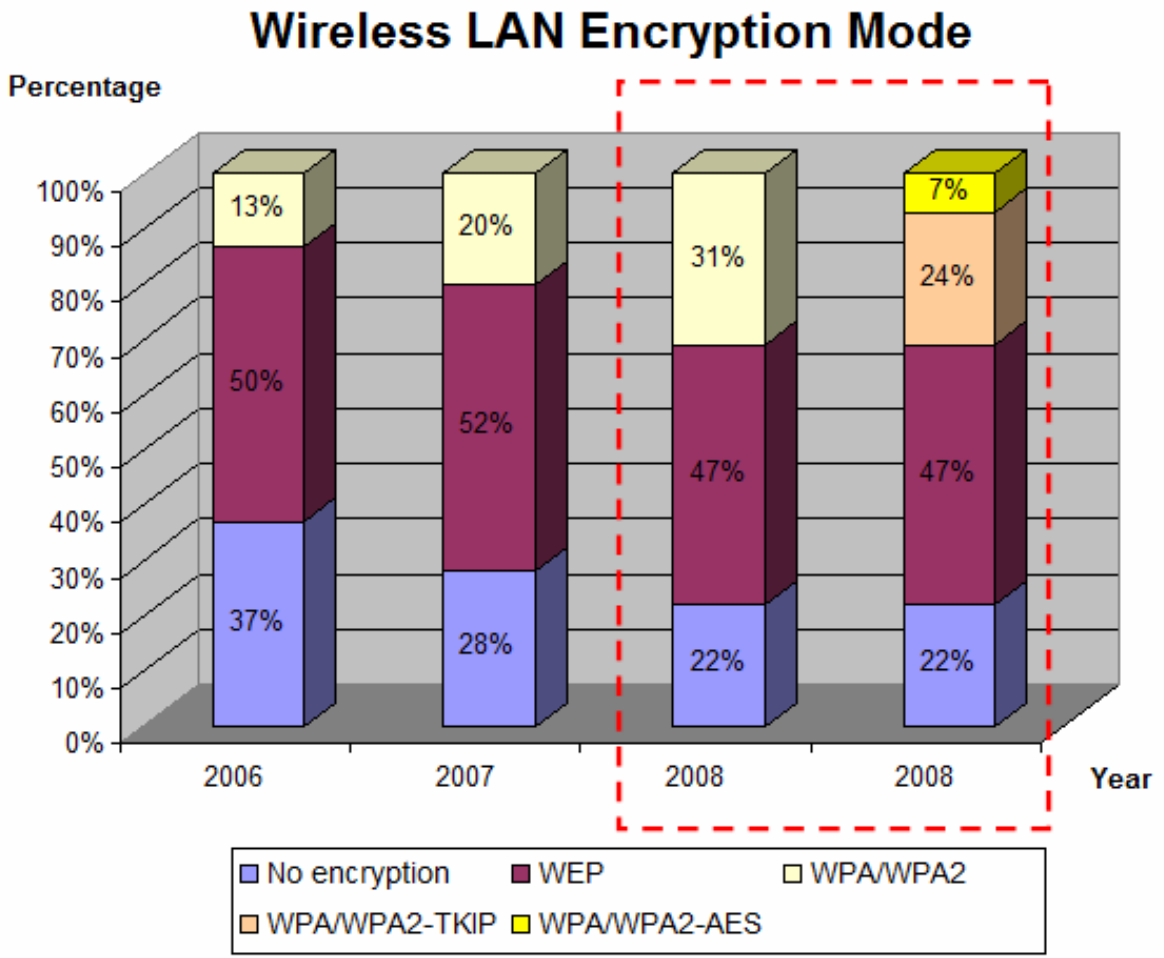
HK: Encryption Mode

- Increasing adoption of encryption settings



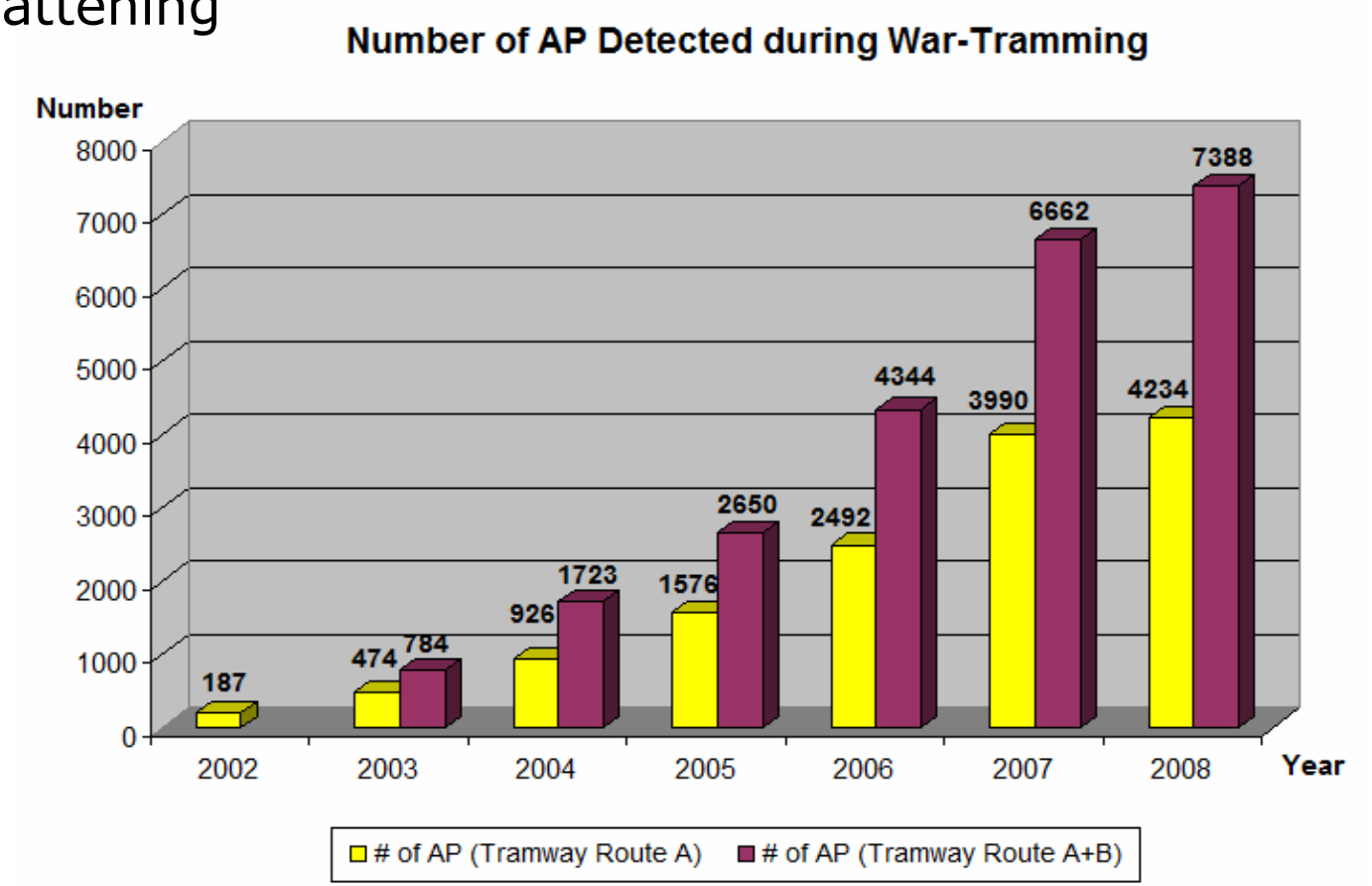
HK: Encryption Mode

- 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 7% WLAN is adopting this highly secured encryption mode)



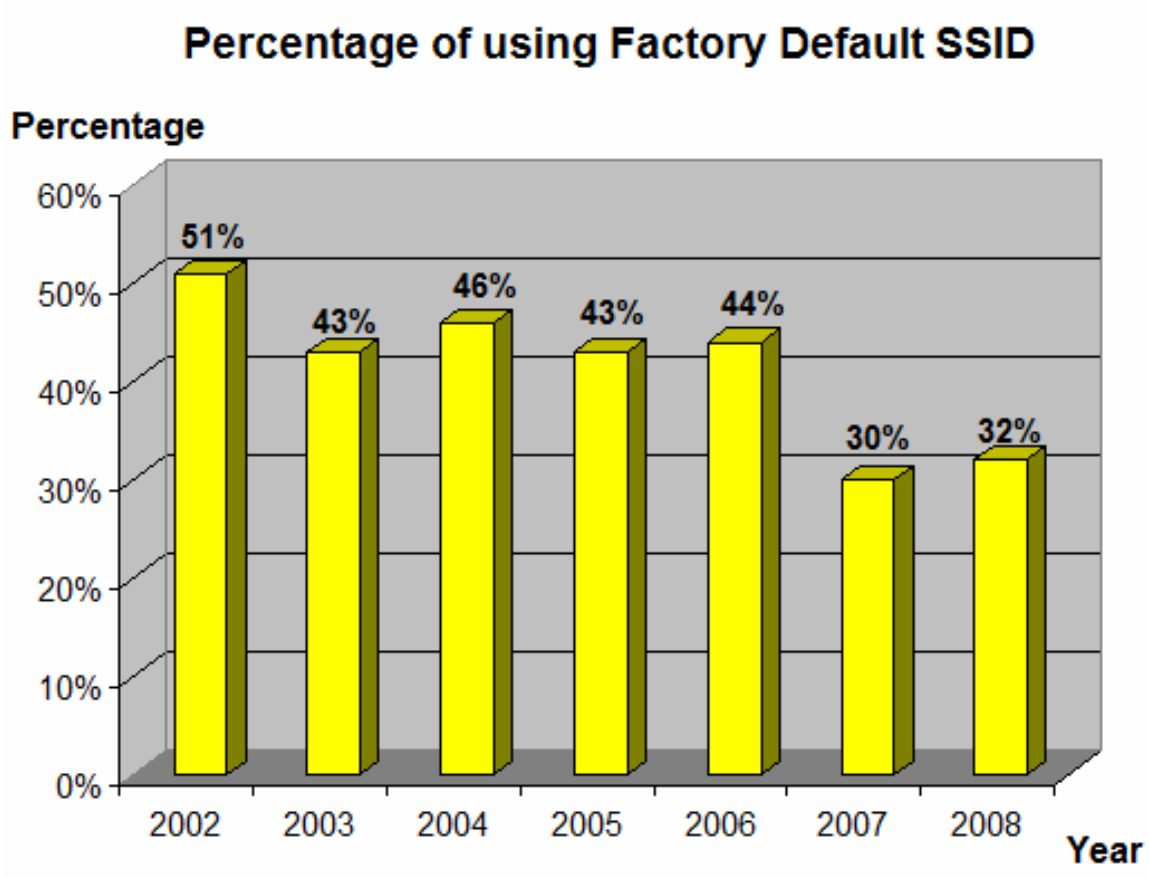
HK: Number of APs

- On average, growth rate is about 40%; the trend is flattening



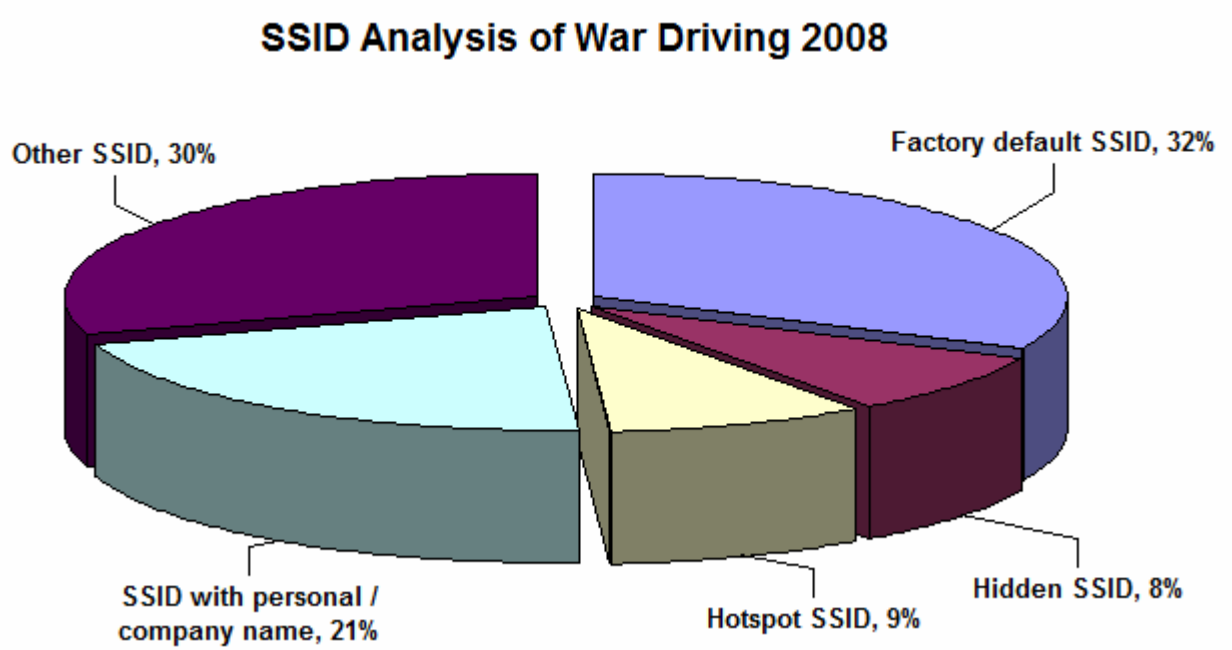
HK: Factory Default SSID

- Refer to default pre-set or generated SSID



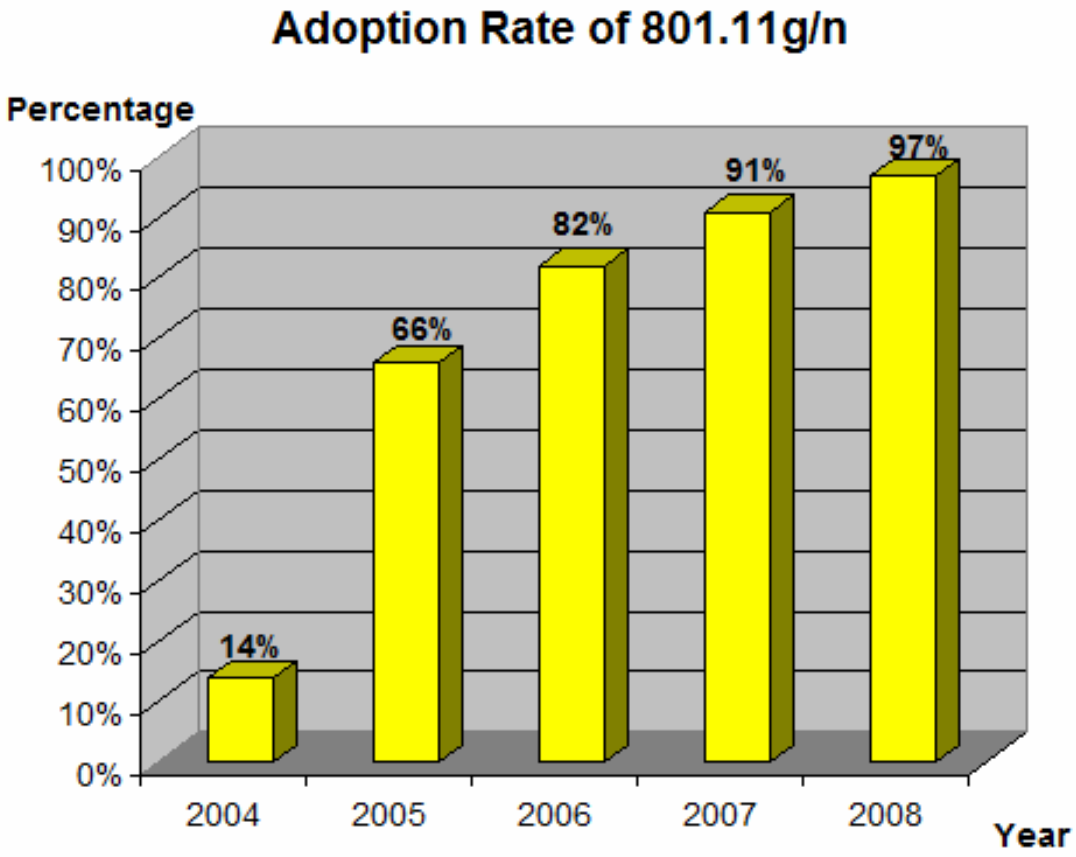
HK: SSID Analysis

- In 2008's SSID analysis, about 30% of users have not changed the default SSID and this may mean other system settings are also not changed (including the administrator password)
- About 20% SSID were associated with personal or organisation name
- enabling the hidden SSID function and change SSID not to associate your identity/name



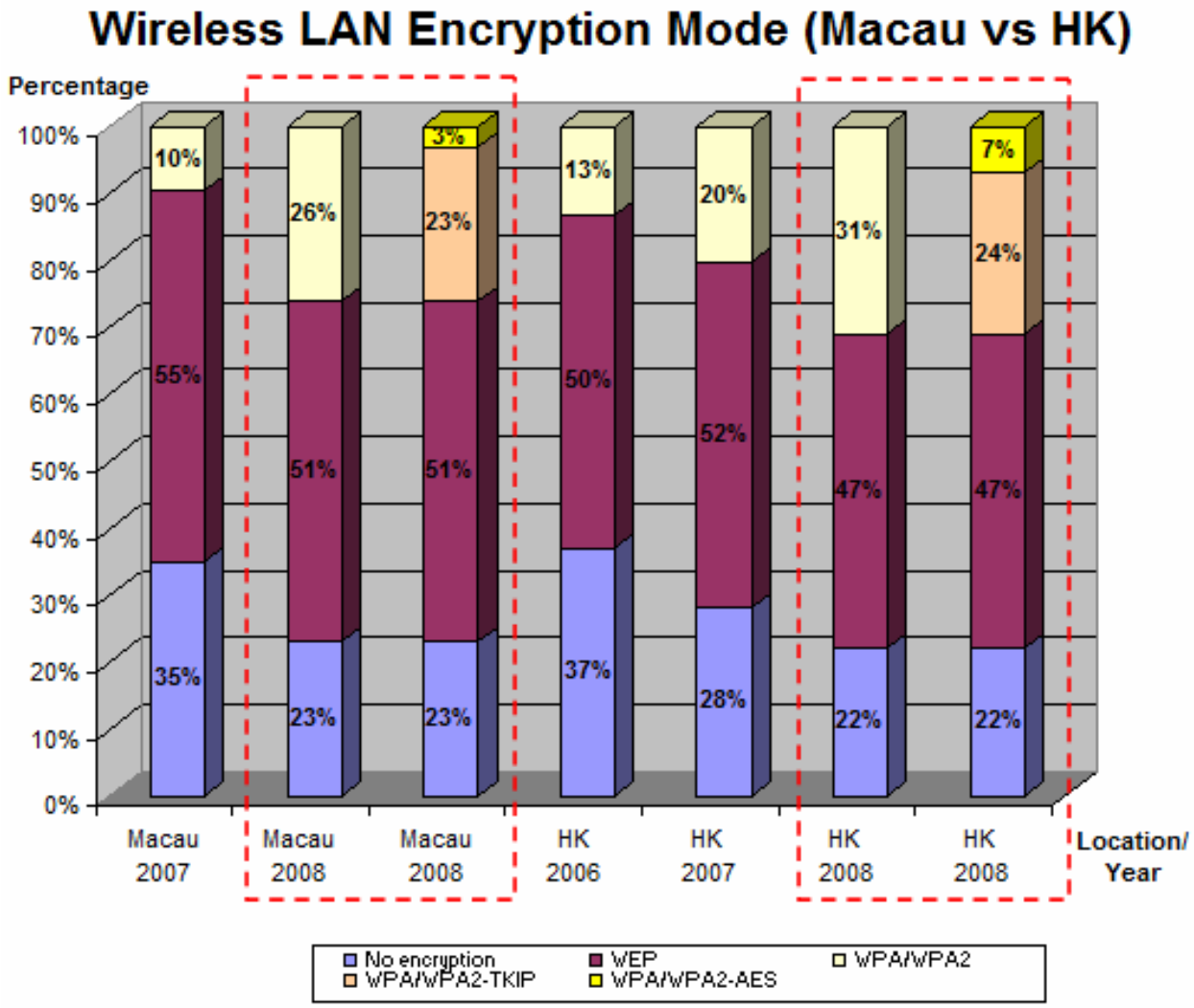
HK: Adoption of 802.11g/n

- Over 90% are 802.11g/n APs



Macau vs HK

- In general, the figures are similar and improving



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 hours

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.

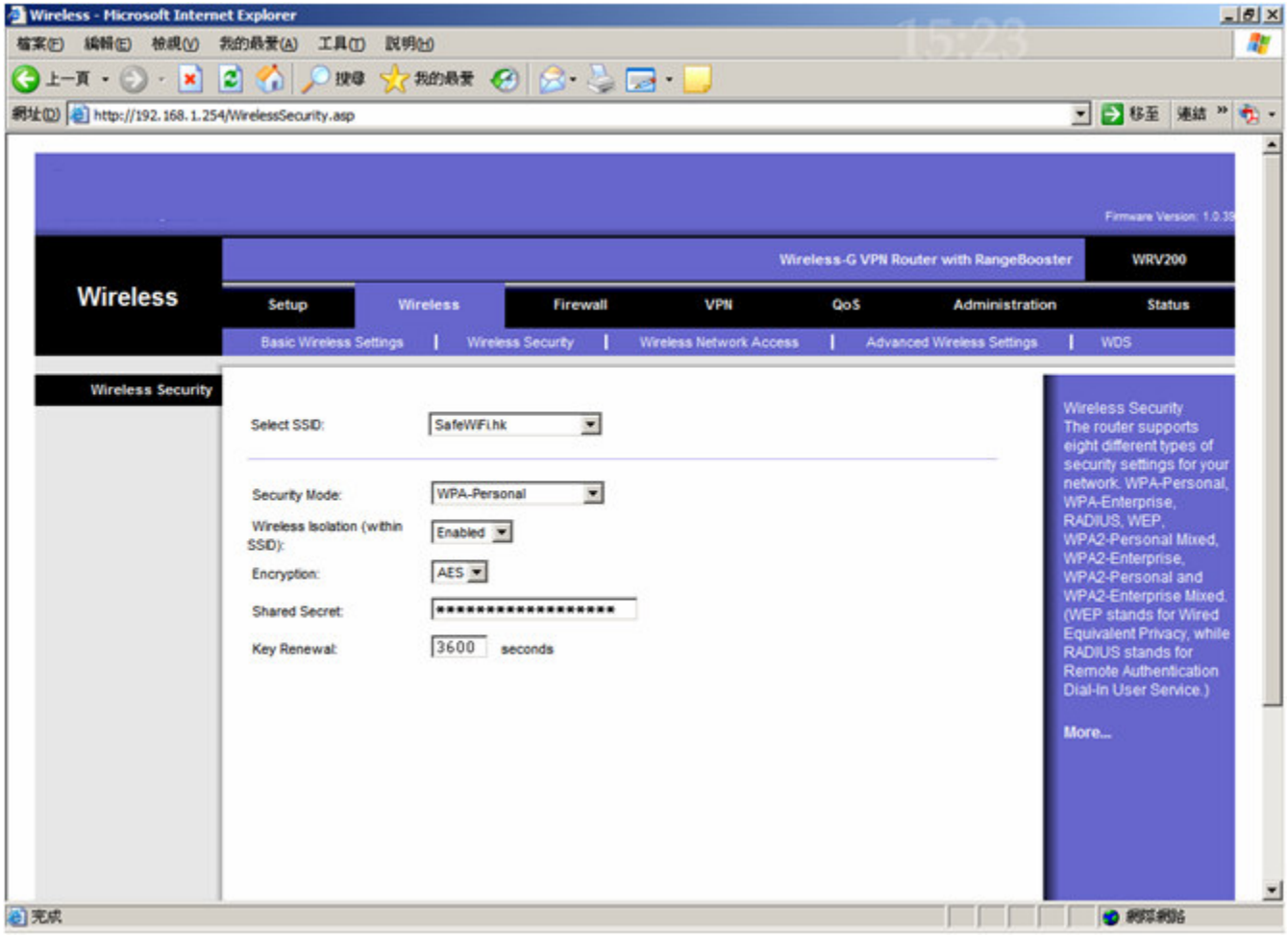
Overview of Wi-Fi Encryption Modes

- 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.

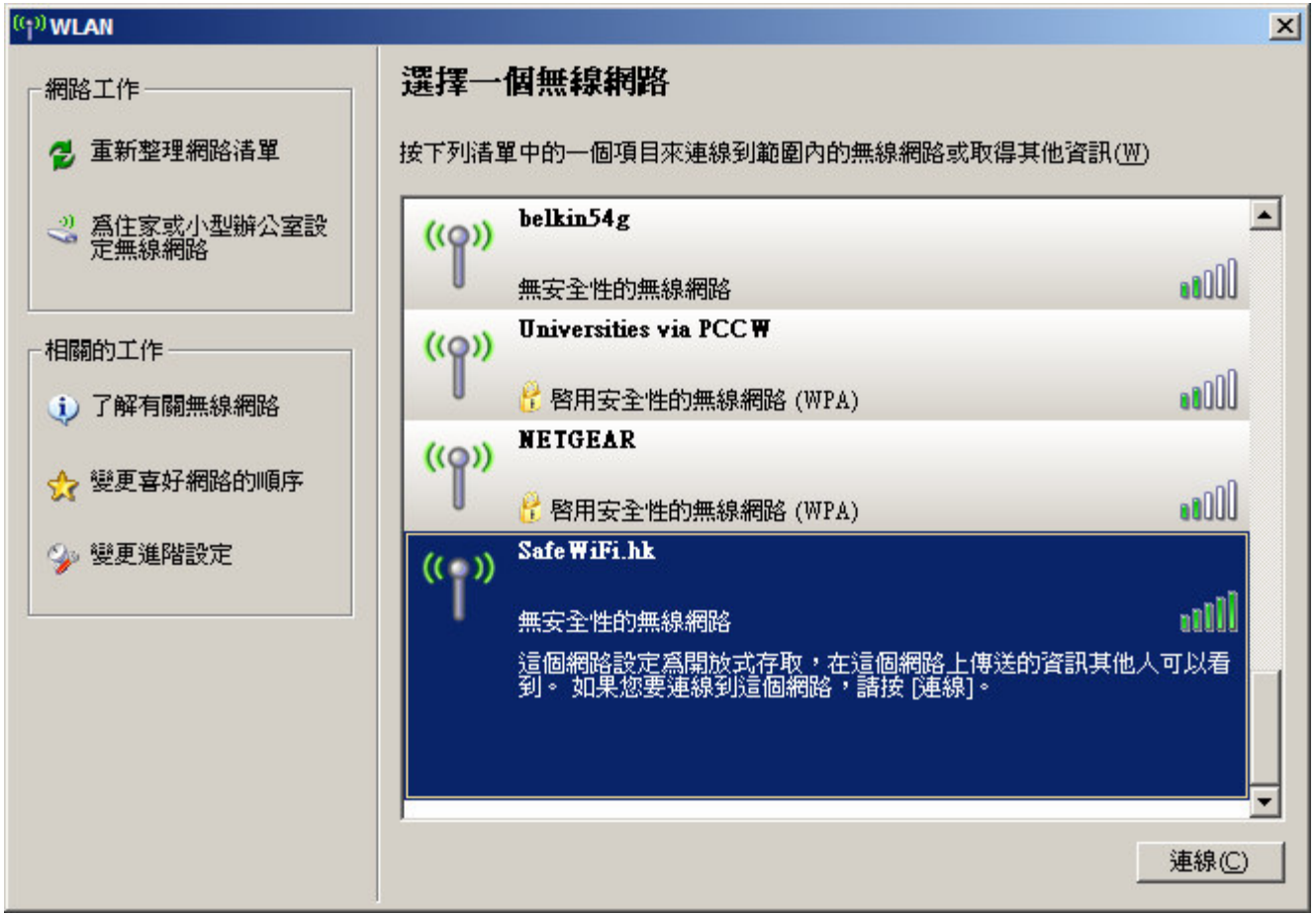
Tips and Recommendation

- 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

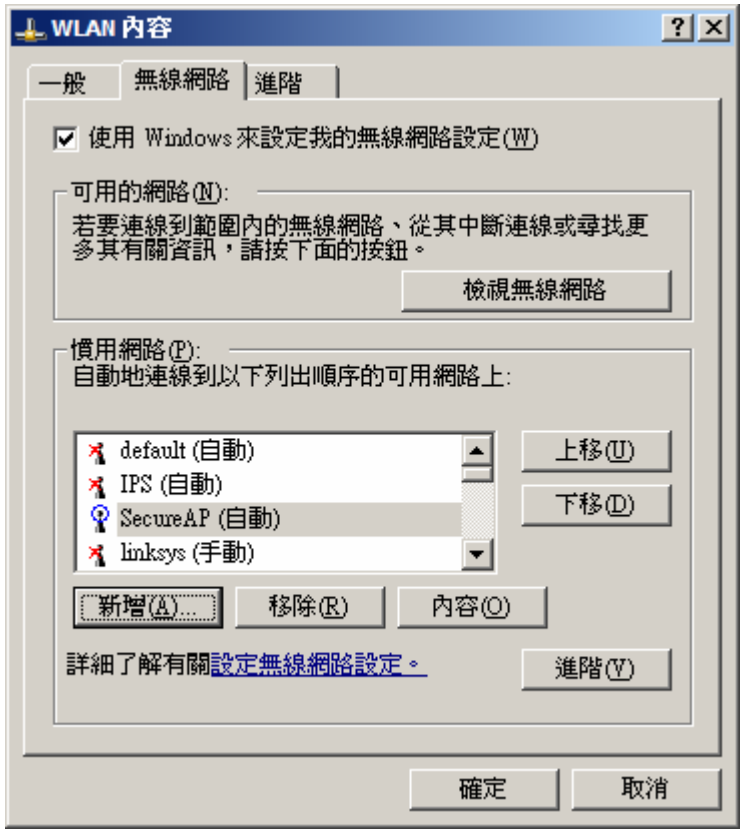
AP- WPA AES Setting



PC – WPA AES Setting



PC – WPA AES Setting



For More Information

- visit Safewifi.hk **WiFi** 安全話咁易
- Seminar on Protecting Your WiFi Network and Utilization" on 28 Feb 2009 (Sat) 「**WiFi** 保安大搜查 – **WiFi**網絡及應用保衛戰」

Acknowledgement

- **All WD2008 Team Members including**

PISA

Alan Ho (Convener) , Alan Tam, Billy Yung, CK Huen, Howard Lau, Jim Shek, Sang Young, SC Leung, Thomas Tsang, Warren Kwok

WTIA

Ken Fong (Convener) , Eric Leung, Jacky Cheng, Joseph Leung,, Kenny Chiu, 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