Hong Kong and Macau Wi-Fi Security Survey (War Driving) 2007

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

Chairperson,

Professional Information Security Association (PISA)

Contact: alan.ho@pisa.org.hk

Organizers

Professional Information Security Association

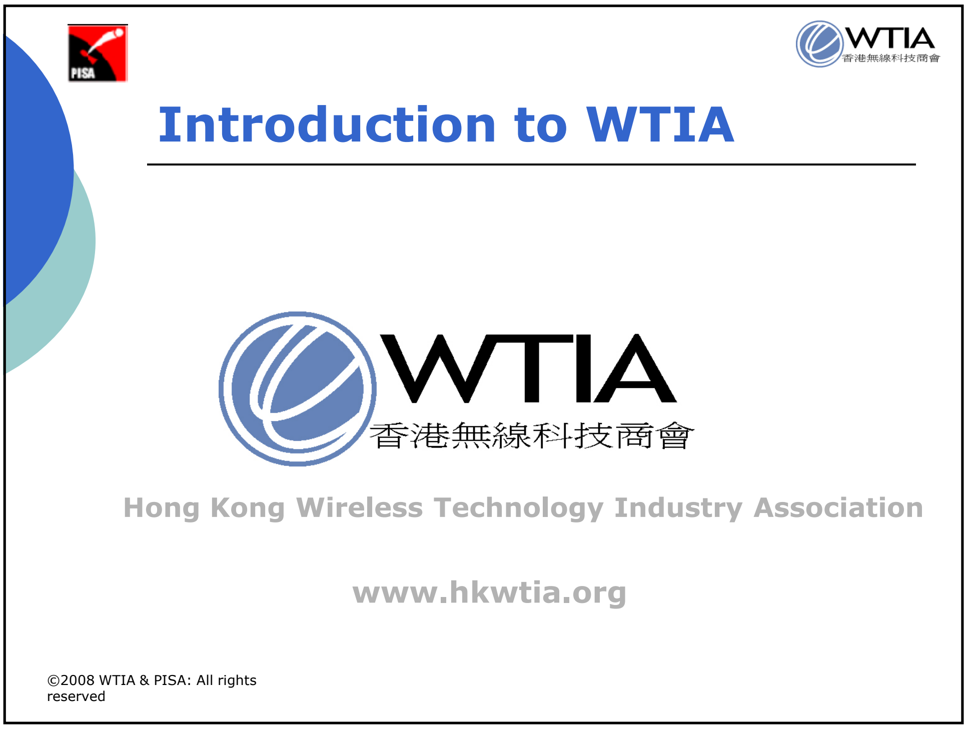
(PISA)

專業資訊保安協會

Hong Kong Wireless Technology Industry Association

(WTIA)

香港無線科技商會

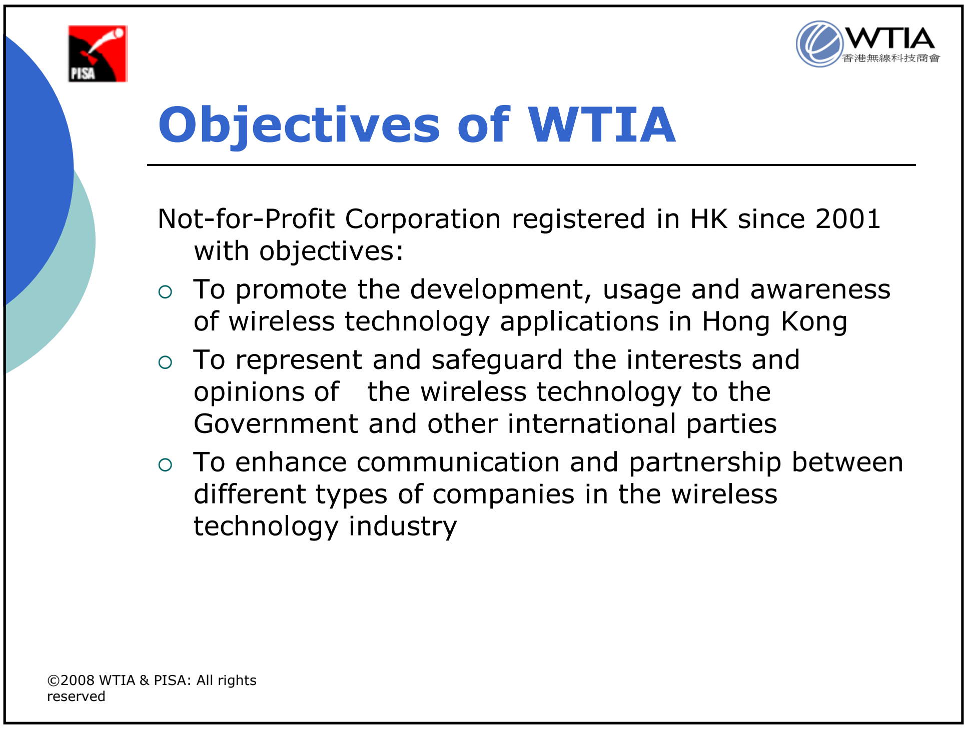


Introduction to WTIA

WTIA
香港無線科技商會

Hong Kong Wireless Technology Industry Association

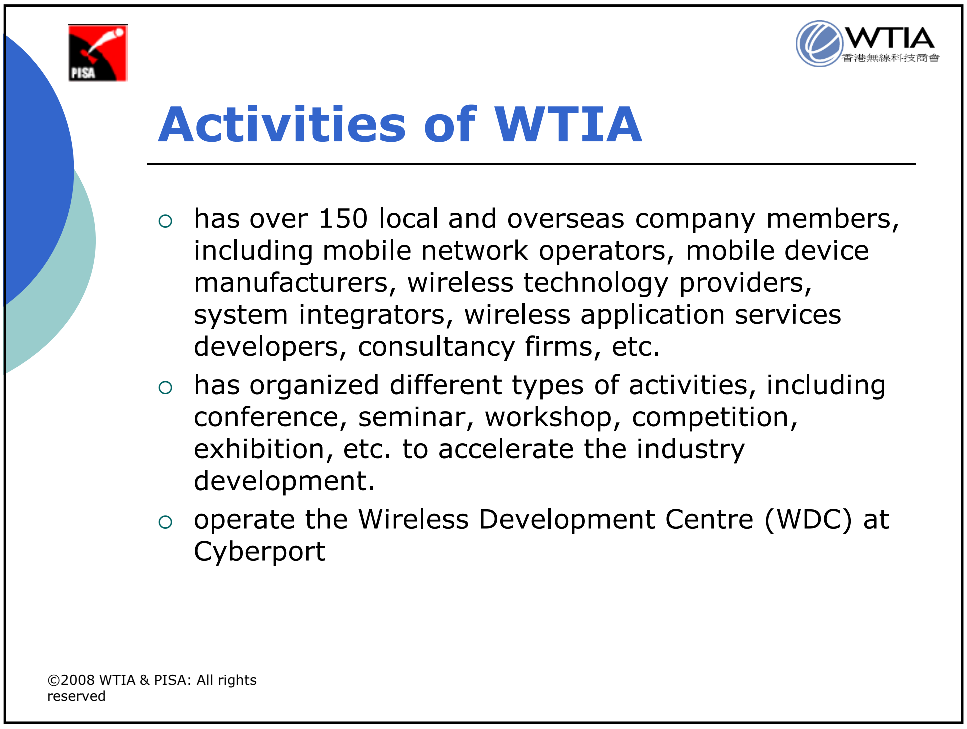
www.hkwtia.org



Objectives of WTIA

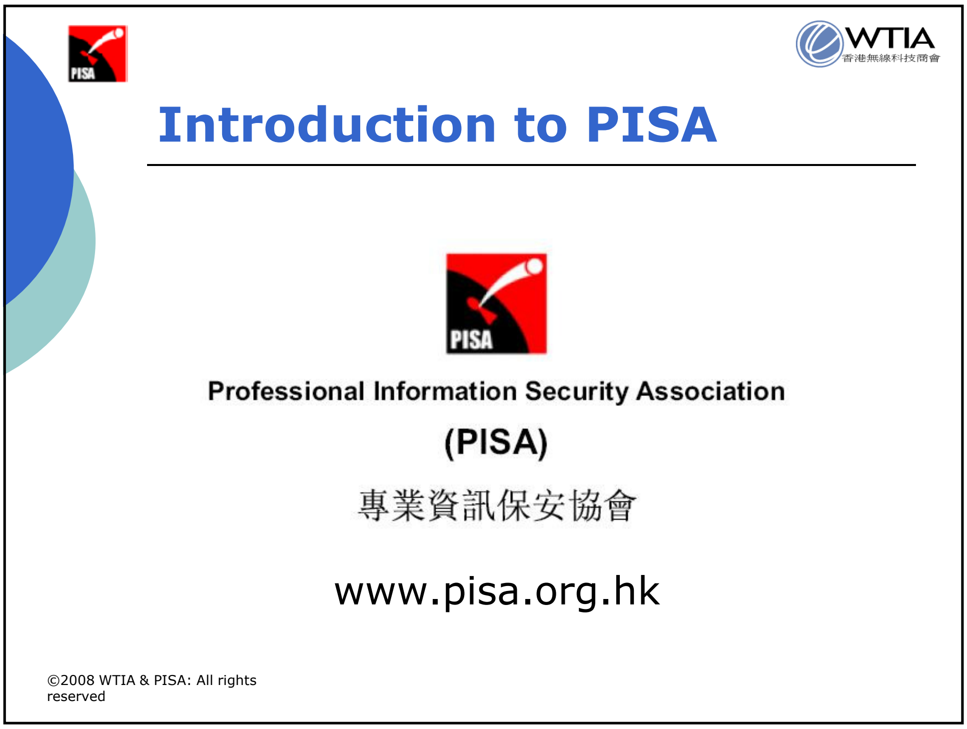
Not-for-Profit Corporation registered in HK since 2001 with objectives:

- 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



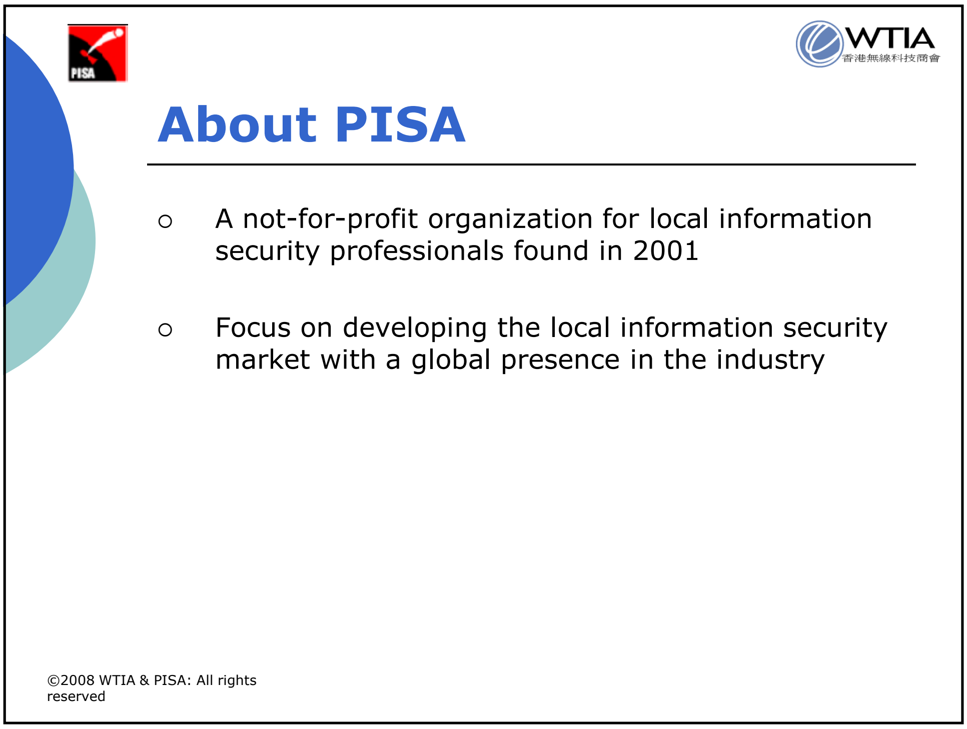
Introduction to PISA

Professional Information Security Association

(PISA)

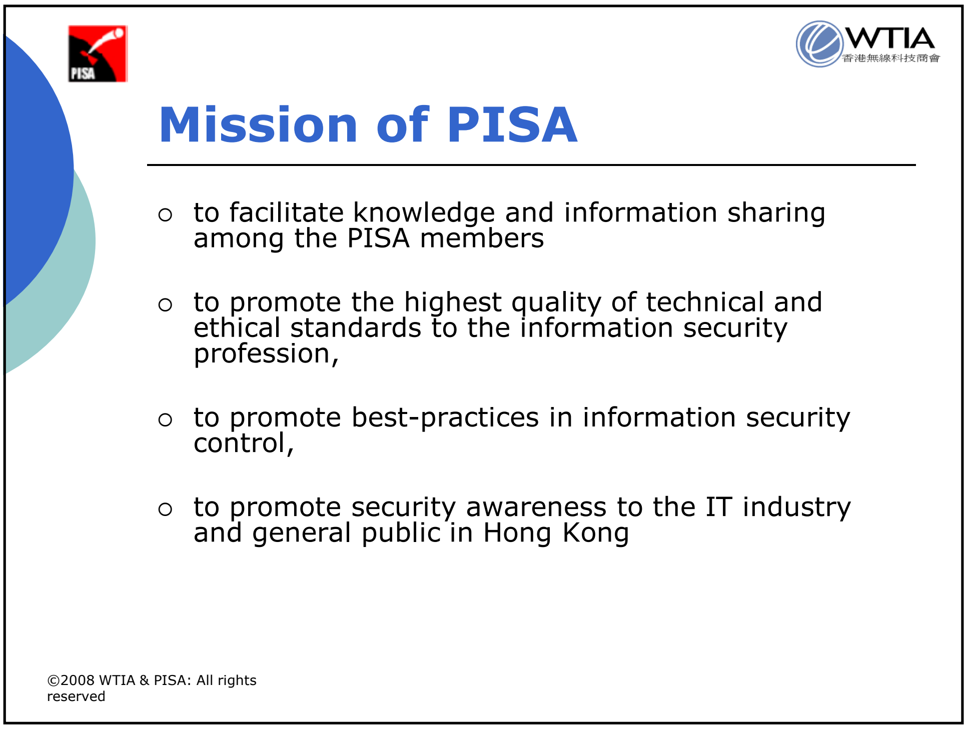
專業資訊保安協會

www.pisa.org.hk



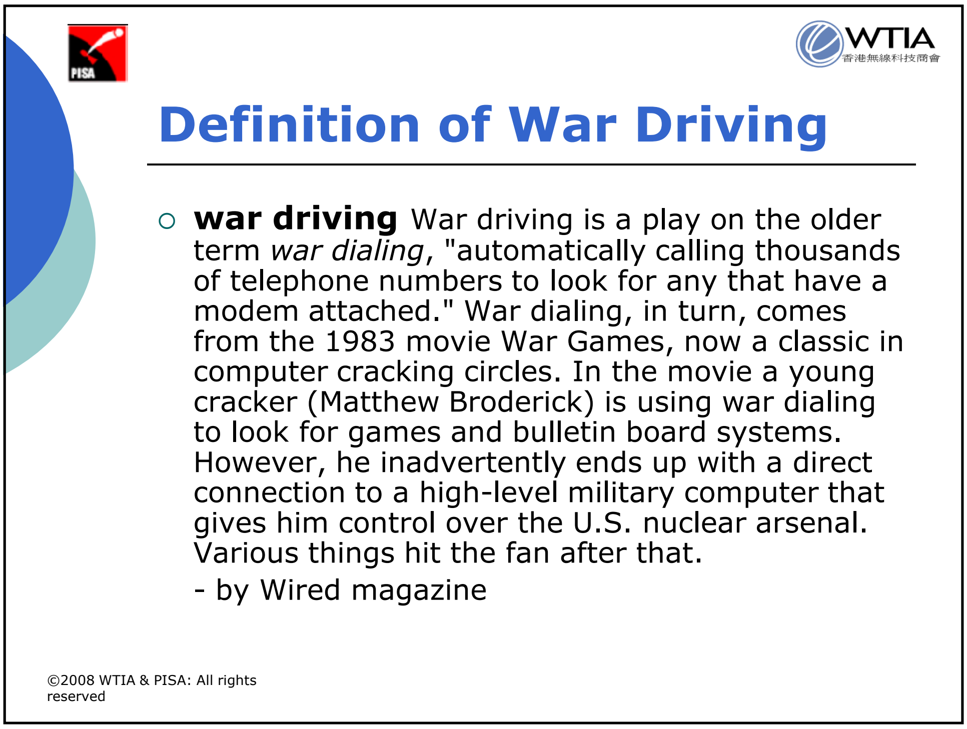
About PISA

- 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

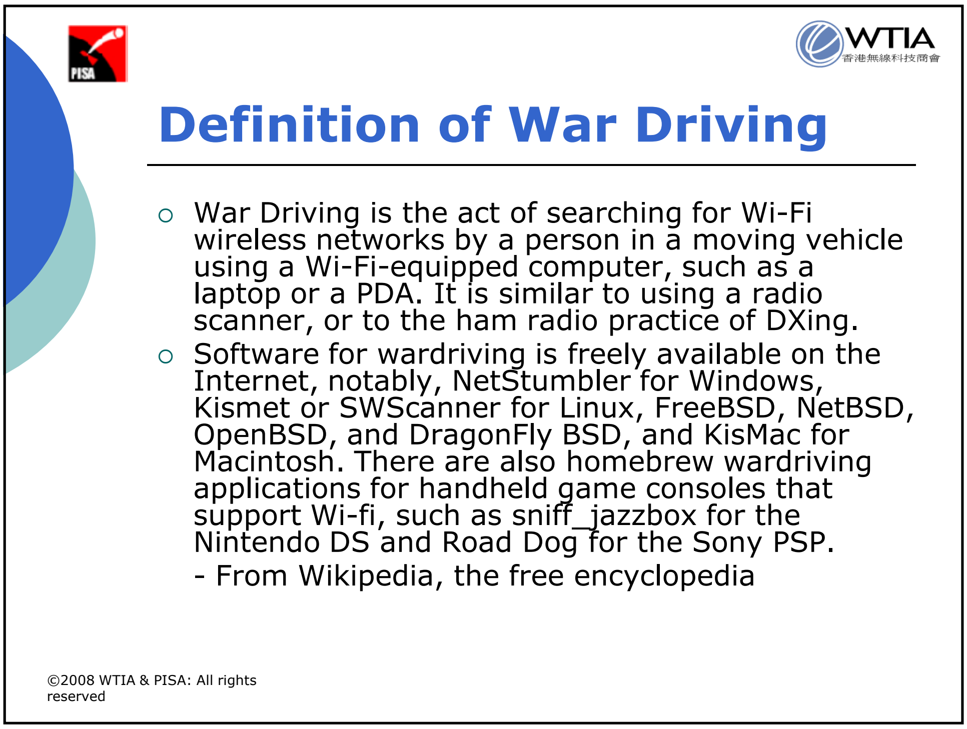
- to facilitate knowledge and information sharing among the PISA members
- to promote the highest quality of technical and ethical standards to the information security profession,
- to promote best-practices in information security control,
- to promote security awareness to the IT industry and general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



Definition of War Driving

- **war driving** War driving is a play on the older term *war dialing*, "automatically calling thousands of telephone numbers to look for any that have a modem attached." War dialing, in turn, comes from the 1983 movie War Games, now a classic in computer cracking circles. In the movie a young cracker (Matthew Broderick) is using war dialing to look for games and bulletin board systems. However, he inadvertently ends up with a direct connection to a high-level military computer that gives him control over the U.S. nuclear arsenal. Various things hit the fan after that.

  - by Wired magazine



Definition of War Driving

- War Driving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle using a Wi-Fi-equipped computer, such as a laptop or a PDA. It is similar to using a radio scanner, or to the ham radio practice of DXing.
- Software for wardriving is freely available on the Internet, notably, NetStumbler for Windows, Kismet or SWScanner for Linux, FreeBSD, NetBSD, OpenBSD, and DragonFly BSD, and KisMac for Macintosh. There are also homebrew wardriving applications for handheld game consoles that support Wi-fi, such as sniff_jazzbox for the Nintendo DS and Road Dog for the Sony PSP.

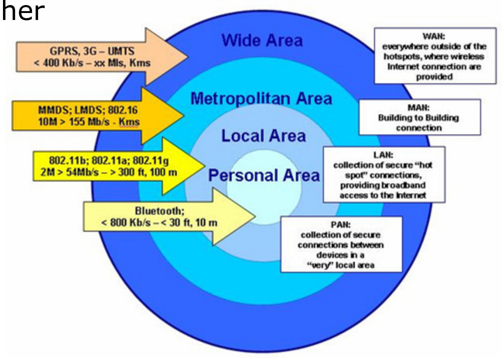
  - From Wikipedia, the free encyclopedia

Is this legal?

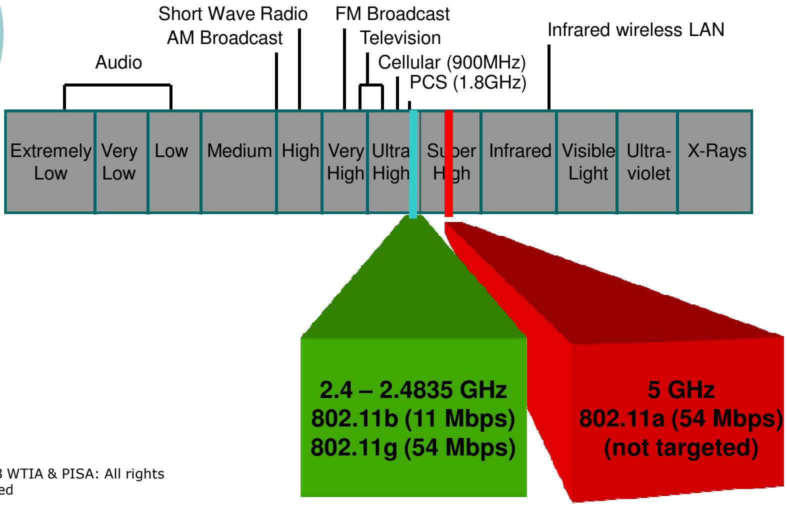
- there are always two sides
- Simply driving around a city searching for the existence of wireless networks in a non-intrusive way, with no ulterior motive cannot be illegal.
- However, if you are searching for a place to steal internet access, or commit computer crimes then the wardriving you performed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

Definition of War Driving (WD)

- WTIA and PISA Board and Neutral Definition: Collecting "**Wireless LAN**" information including network name, signal, location by using a device capable of WLAN signal receiver and moving from one place to another


GPRS, 3G – UMTS
< 400 Kb/s – xx Mls, Kms
MMDS; LMDS; 802.16
10M > 155 Mb/s - Kms
802.11b; 802.11a; 802.11g
2M > 54Mb/s – > 300 ft, 100 m
Bluetooth;
< 800 Kb/s – < 30 ft, 10 m
Wide Area
Metropolitan Area
Local Area
Personal Area
WAN:
everywhere outside of the hotspots, where wireless Internet connection are provided
MAN:
Building to Building connection
LAN:
collection of secure "hot spot" connections, providing broadband access to the Internet
PAN:
collection of secure connections between devices in a "very" local area

Our Focused in 2.4G License Free Spectrum



Short Wave Radio
AM Broadcast

FM Broadcast
Television

Cellular (900MHz)
PCS (1.8GHz)

Audio

Infrared wireless LAN

Extremely Low | Very Low | Low | Medium | High | Very High | Ultra High | Super High | Infrared | Visible Light | Ultra-violet | X-Rays

2.4 – 2.4835 GHz
802.11b (11 Mbps)
802.11g (54 Mbps)

5 GHz
802.11a (54 Mbps)
(not targeted)

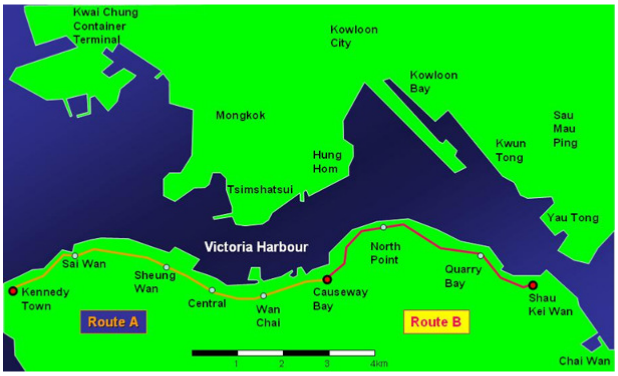
Our Code of Ethics in WD

- 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

War Tramming Route A & B

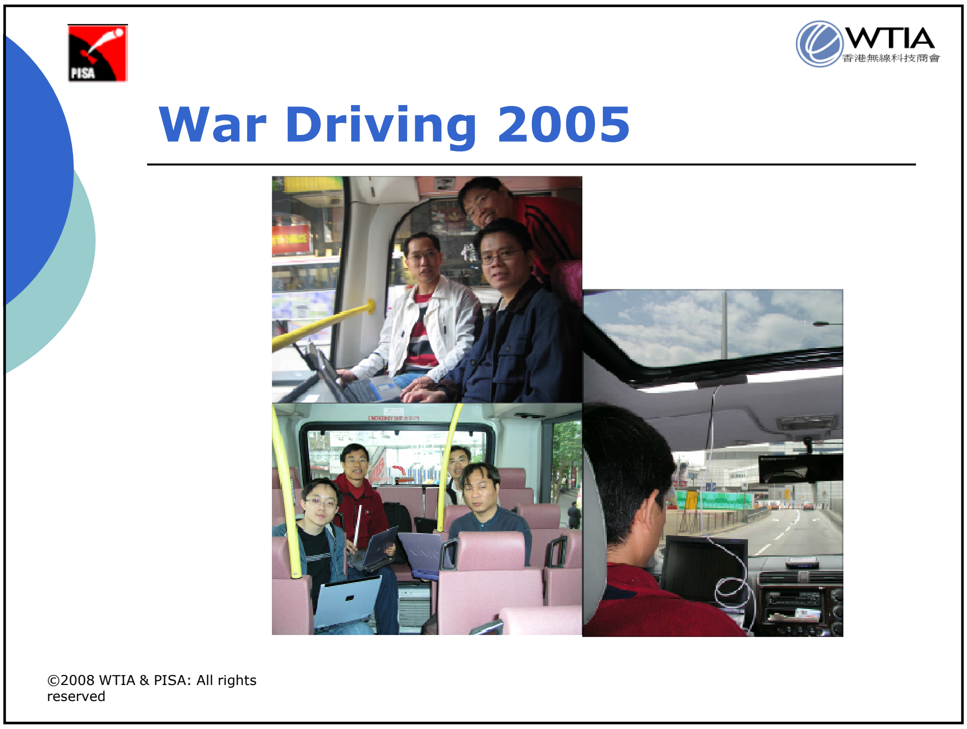


War Driving 2003

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

Hong Kong and Macau WiFi Security Survey (War Driving) 2007

A Tales of Two Cities :

- Hong Kong: War Tramming
- Macau: Macau Tower, Bus Route 6, Bus Route 8

Objectives of WD2007

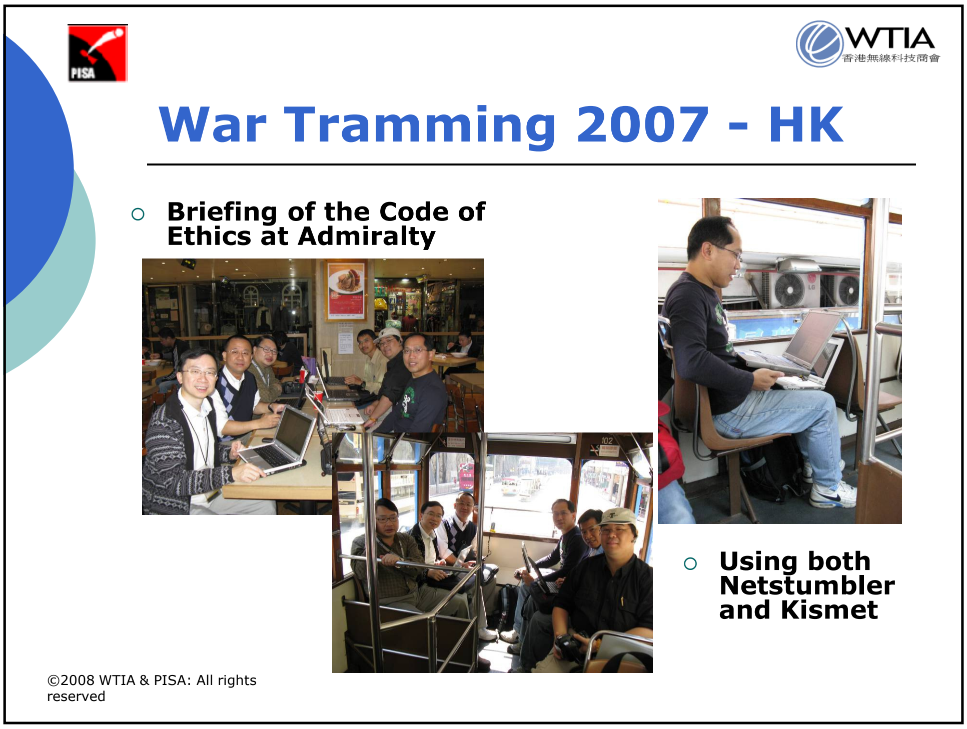
- To study the current WLAN security status of HK and Macau
- HK: to benchmark the result with previous figures from 2002 to 2006 in HK;
- Macau: As this is the first year of operation, the aim of the data collection this year is to form a base line of the environment in Macau. Later studies will then build on top of this; also benchmark the result with HK
- To conduct a non-intrusive WLAN security field study with responsible disclosure of information
- To study the feasibility of long distance war driving **(Macau)**
- To arouse public awareness in WLAN security in both HK and Macau

Part 1: The Hong Kong Side

Tramway War Driving 4 November 2007

Part 1: 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 targeted to benchmarks the results with that of the war driving study from year 2002 to 2006 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



War Tramming 2007 - HK

- Briefing of the Code of Ethics at Admiralty

- Using both Netstumbler and Kismet

War Tramming 2007 - HK

Date **Time**	4 November 2007 (Sunday) 10 a.m. to 1 p.m.
Equipment	Hardware: Notebook Computer with 802.11 a/b/g WLAN Cards and internal Omni-Directional Antenna; UMPC (Ultra Mobile PC); some with 5dB external antenna; GPS Software: Netstumbler; Kismet
Route	Route A Taking Tram from Queensway, Admiralty westwards to Kennedy Town Terminus, then return tram from Kennedy Town terminus to Sogo Department Store, Causeway Bay
	Route B Taking another tram from Causeway Bay to Shau Kei Wan terminus

Part 2: Macau War Driving

Macau + Bus Route 6 + Bus Route 8
15th September 2007

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

War Driving@Macau Tower

War Driving@Macau Tower

- Macau Tower has an altitude of 338m, offers a breathtaking birds-eye view over the Macau city .
- SkyWalk takes the teams to walk on the outer rim of the Tower with a height exposure of 233 metres above ground is very suitable for war driving
- Our objective is to study the feasibility of War Driving from a long distance

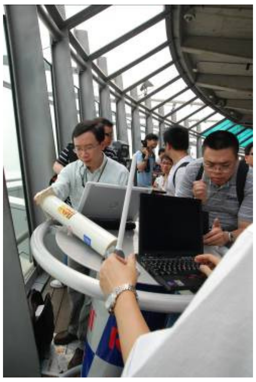
War Driving@Macau Tower

War Driving@Macau Tower

Date **Time**	15th September 2007 (Saturday) 10:45 a.m. to 12:30 p.m.
Equipment	Hardware: Notebook Computer with 802.11 a/b/g WLAN Cards and internal Omni-Directional Antenna; UMPC (Ultra Mobile PC); a +16dB directional antenna (approx. 1m long) with 30 degree angle sensitivity was used; GPS Software: Netstumbler; Kismet
Router	Skywalking on the outer rim of the Macau Tower with a height exposure of 233 metres above ground

War Driving@Macau Tower

- Discovering WLAN signal of Macau Island with the +16dB antenna

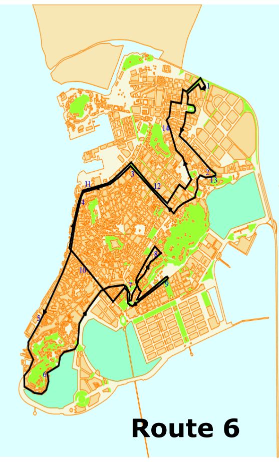


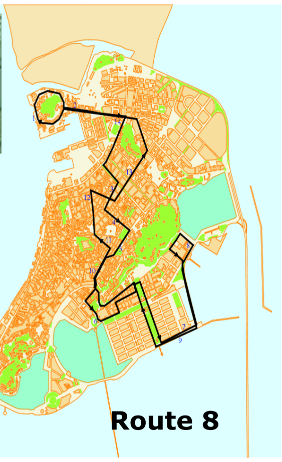
- Preparation work inside the Tower

War Driving:Bus Routes 6 & 8

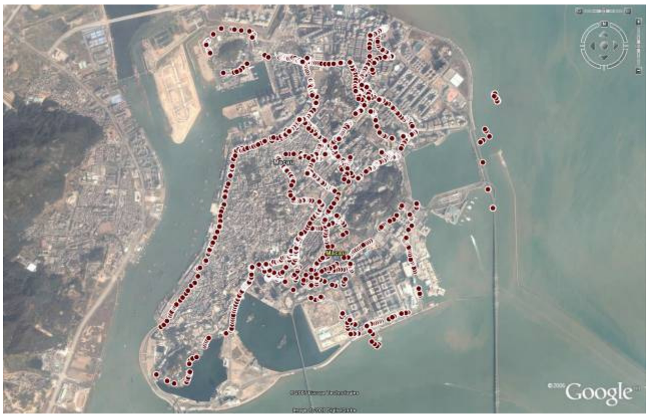
Date **Time**	15th September 2007 (Saturday) 12:30 p.m. to 4 p.m.
Equipment	Same as “Tramway War Driving” in HK
Router	Signal captured along two bus routes - Route 6 - Route 8

War Driving:Bus Routes 6 & 8

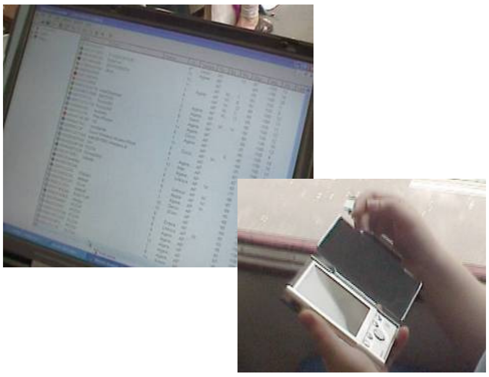

Route 6

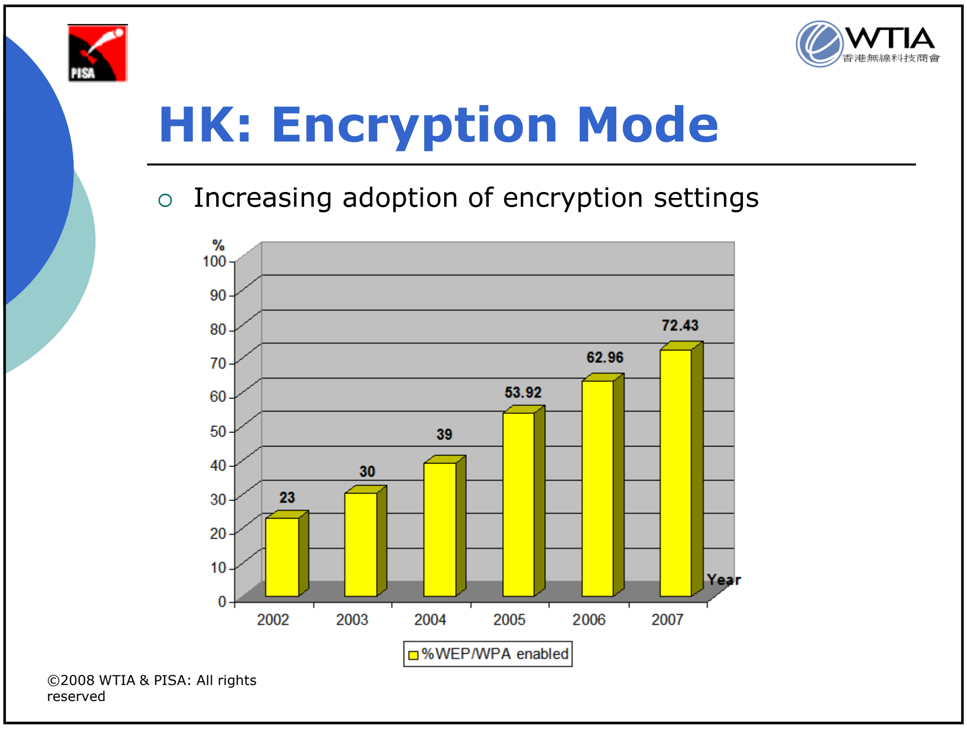

Route 8

War Driving:Bus Routes 6 & 8



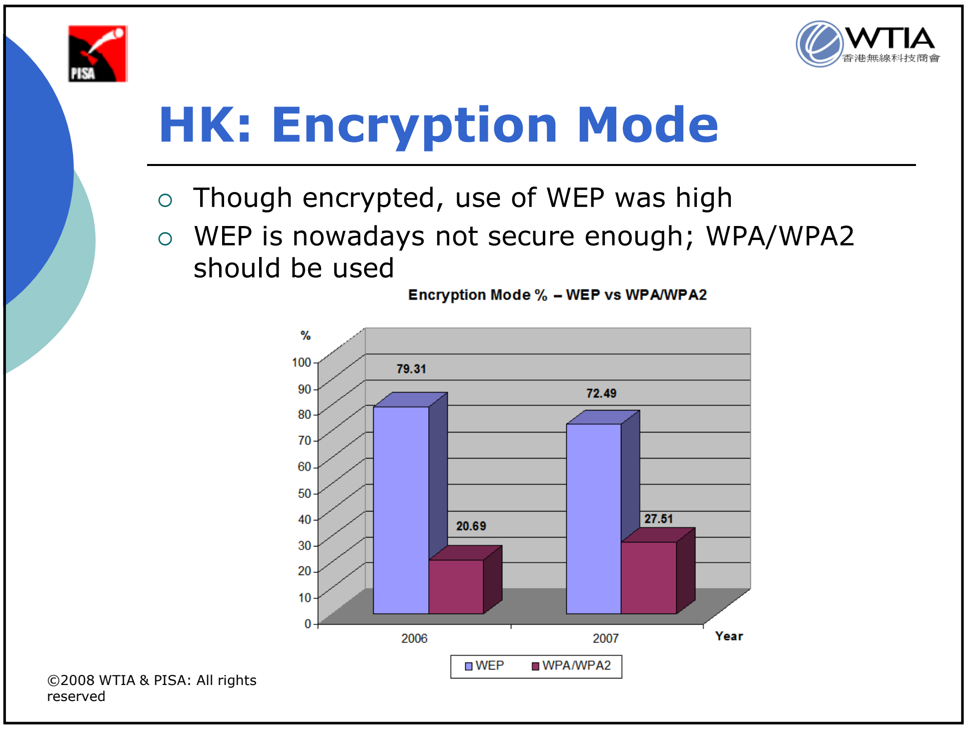
Summary of Finding





HK: Encryption Mode

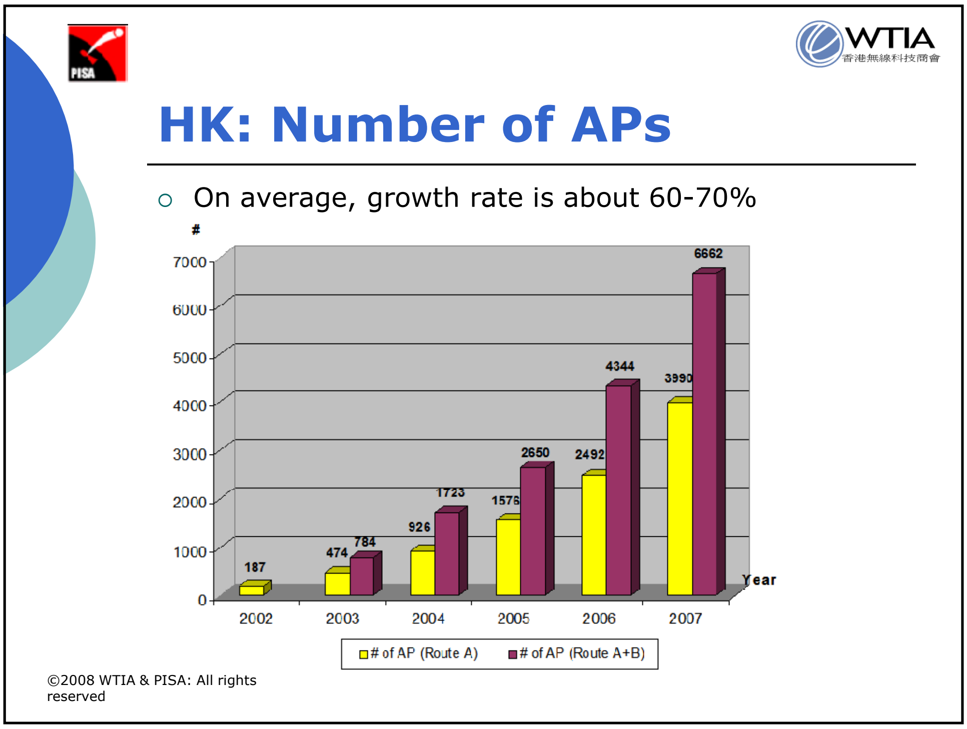
- Increasing adoption of encryption settings



HK: Encryption Mode

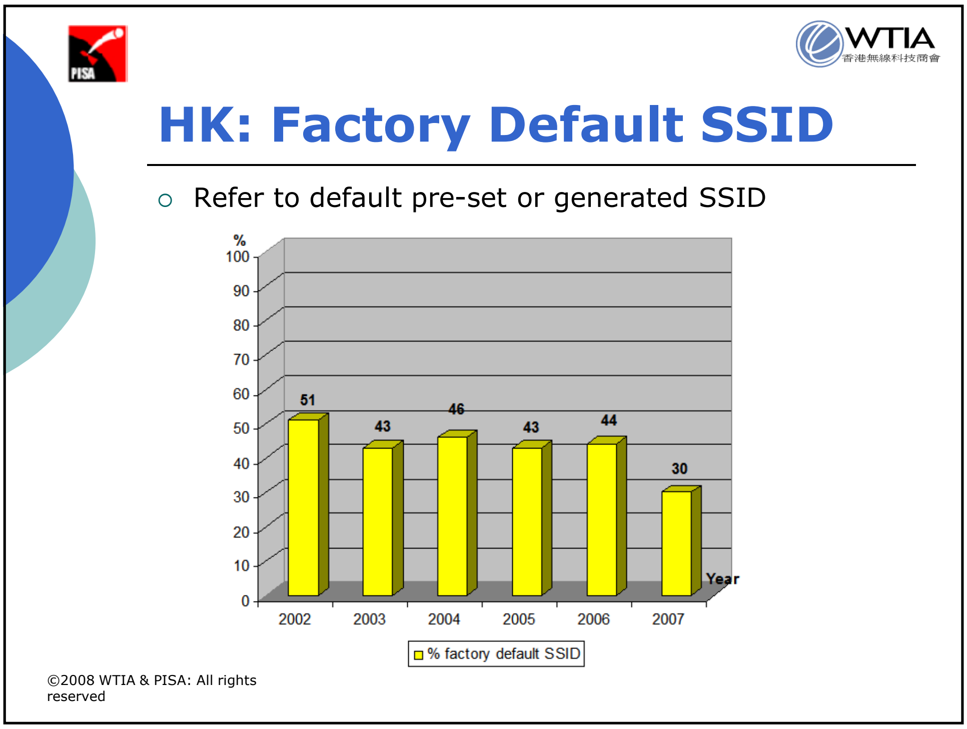
- Though encrypted, use of WEP was high
- WEP is nowadays not secure enough; WPA/WPA2 should be used

Encryption Mode % – WEP vs WPA/WPA2



HK: Number of APs

- On average, growth rate is about 60-70%



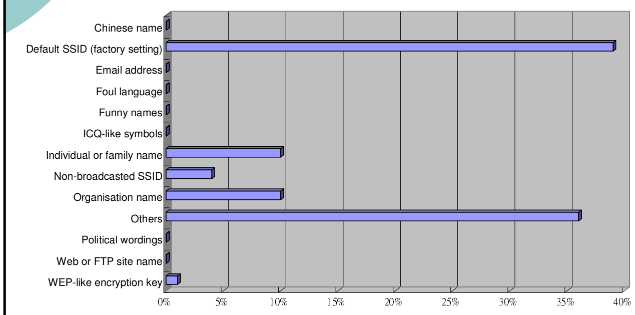
HK: Factory Default SSID

- Refer to default pre-set or generated SSID

HK: Factory Default SSID

- In 2005's SSID analysis, about 20% SSID were associated with individual/family name or organisation name.
- Using factory default SSID may mean you have not change the other default settings including the administration password
- Recommend to change to be not easily identifiable.

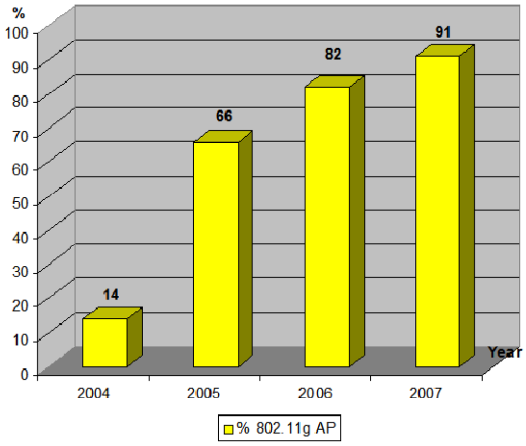
High-Level Analysis of SSID

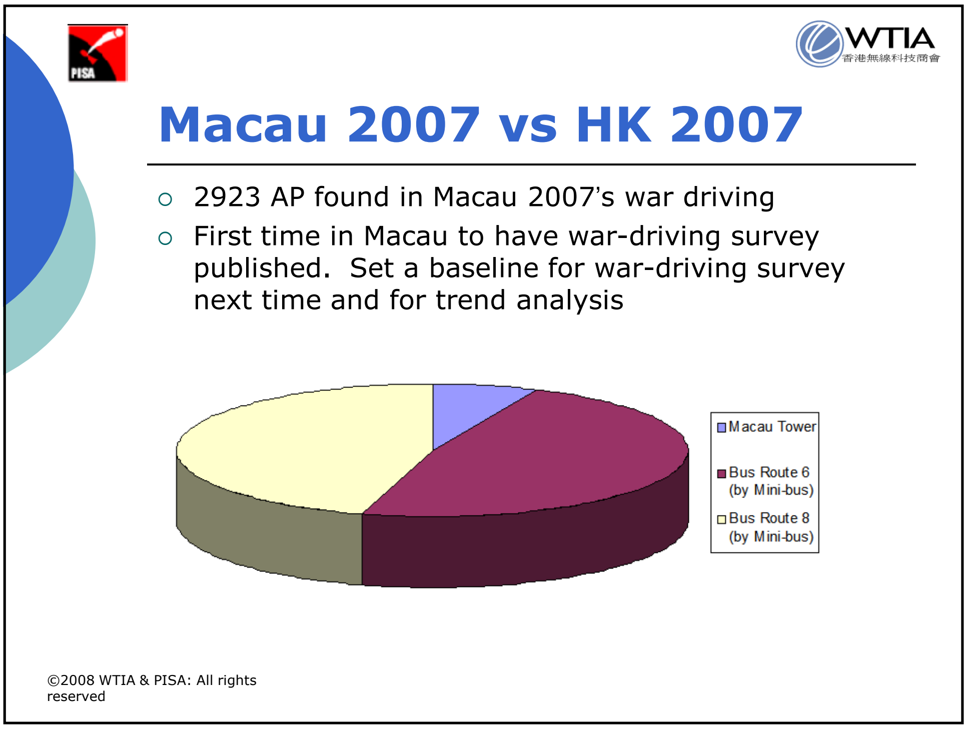


Category	Percentage
Chinese name	0.01%
Default SSID (factory setting)	39%
Email address	0.01%
Foul language	0.01%
Funny names	0.01%
ICQ-like symbols	0.01%
Individual or family name	10%
Non-broadcasted SSID	4%
Organisation name	10%
Others	36%
Political wordings	0.01%
Web or FTP site name	0.01%
WEP-like encryption key	1%

HK: Adoption of 802.11g

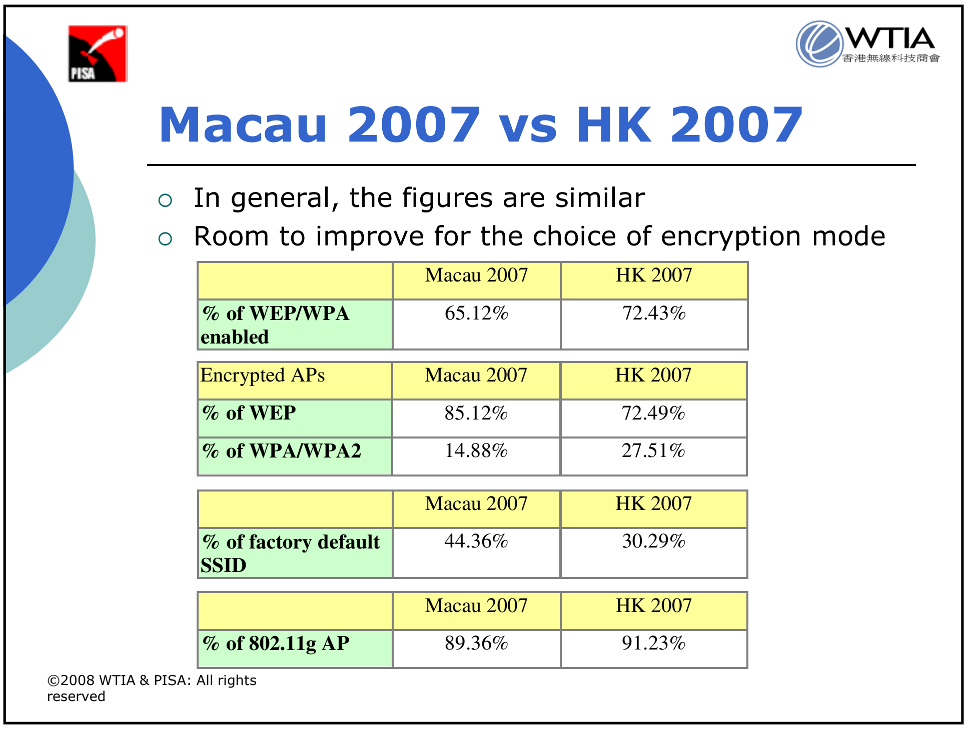
- Over 90% are 802.11g AP





Macau 2007 vs HK 2007

- 2923 AP found in Macau 2007’s war driving
- First time in Macau to have war-driving survey published. Set a baseline for war-driving survey next time and for trend analysis



Macau 2007 vs HK 2007

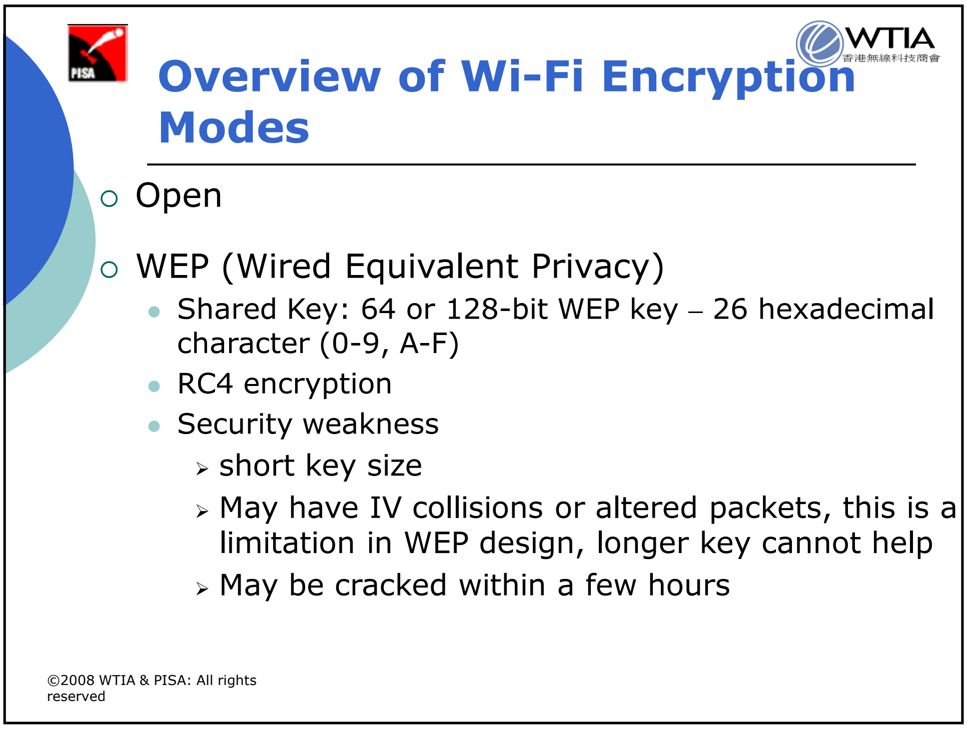
- In general, the figures are similar
- Room to improve for the choice of encryption mode

	Macau 2007	HK 2007
% of WEP/WPA enabled	65.12%	72.43%

Encrypted APs	Macau 2007	HK 2007
% of WEP	85.12%	72.49%
% of WPA/WPA2	14.88%	27.51%

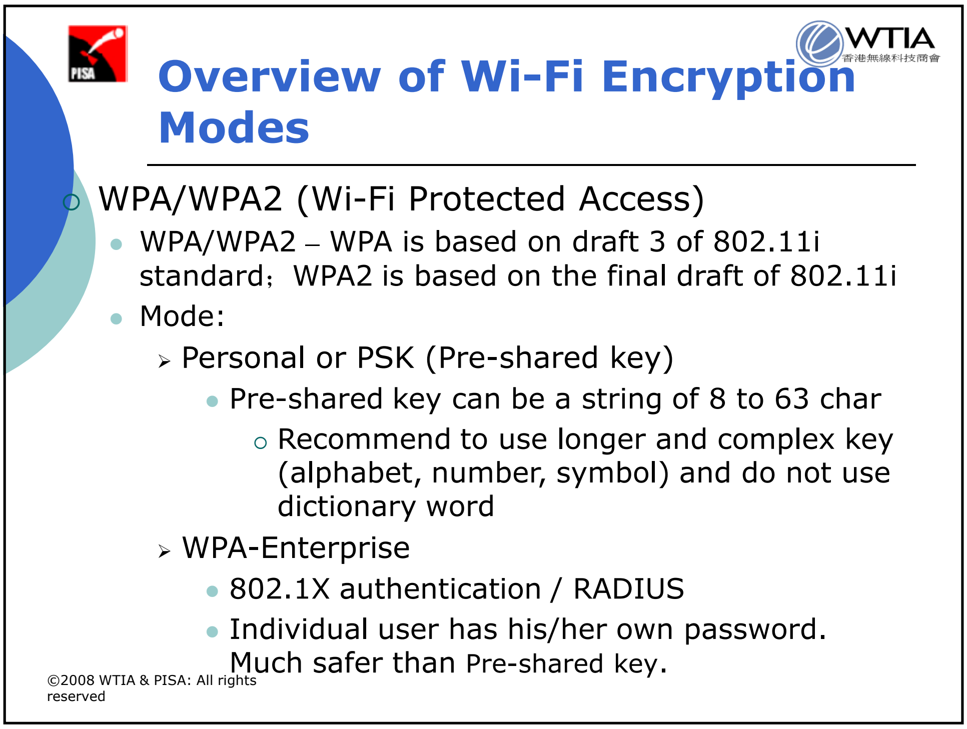
	Macau 2007	HK 2007
% of factory default SSID	44.36%	30.29%

	Macau 2007	HK 2007
% of 802.11g AP	89.36%	91.23%



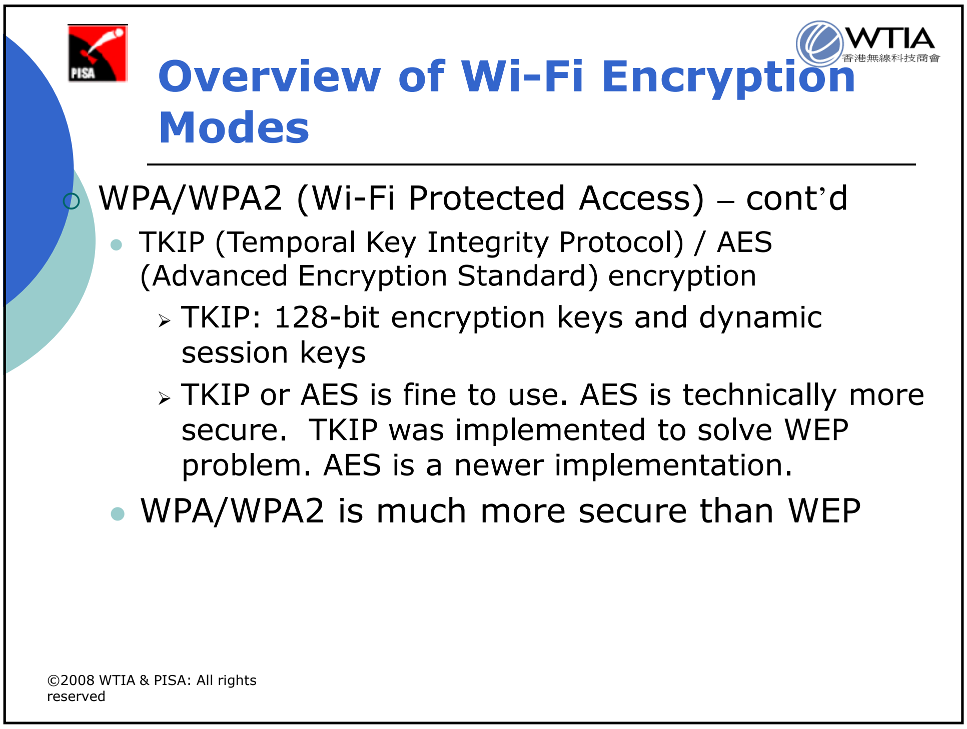
Overview of Wi-Fi Encryption Modes

- 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



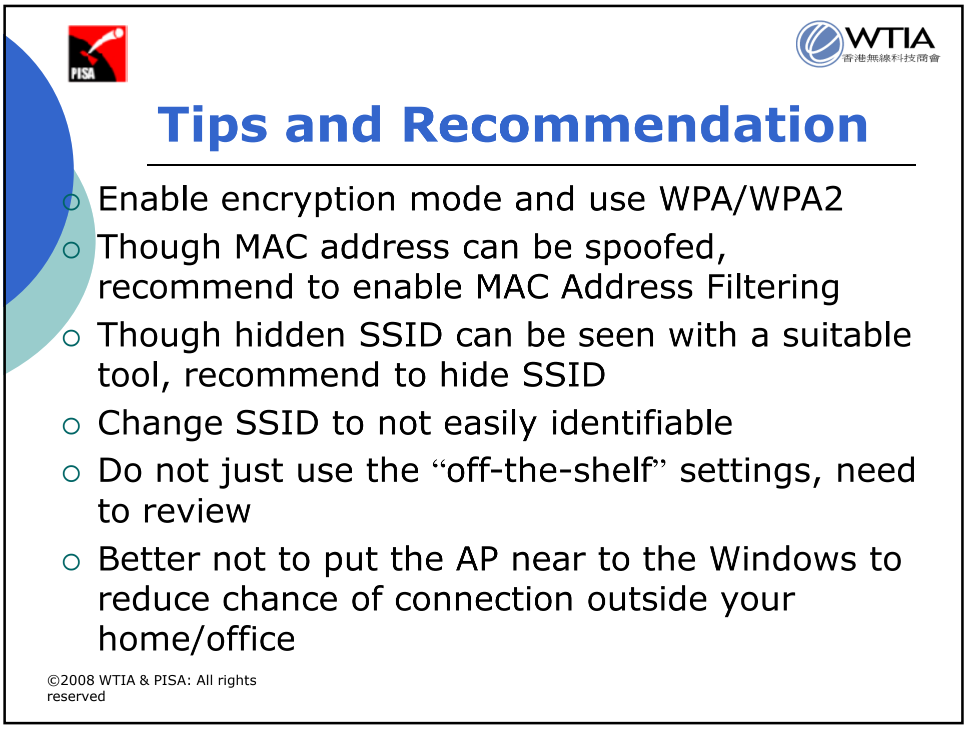
Overview of Wi-Fi Encryption Modes

- 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 to use 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.



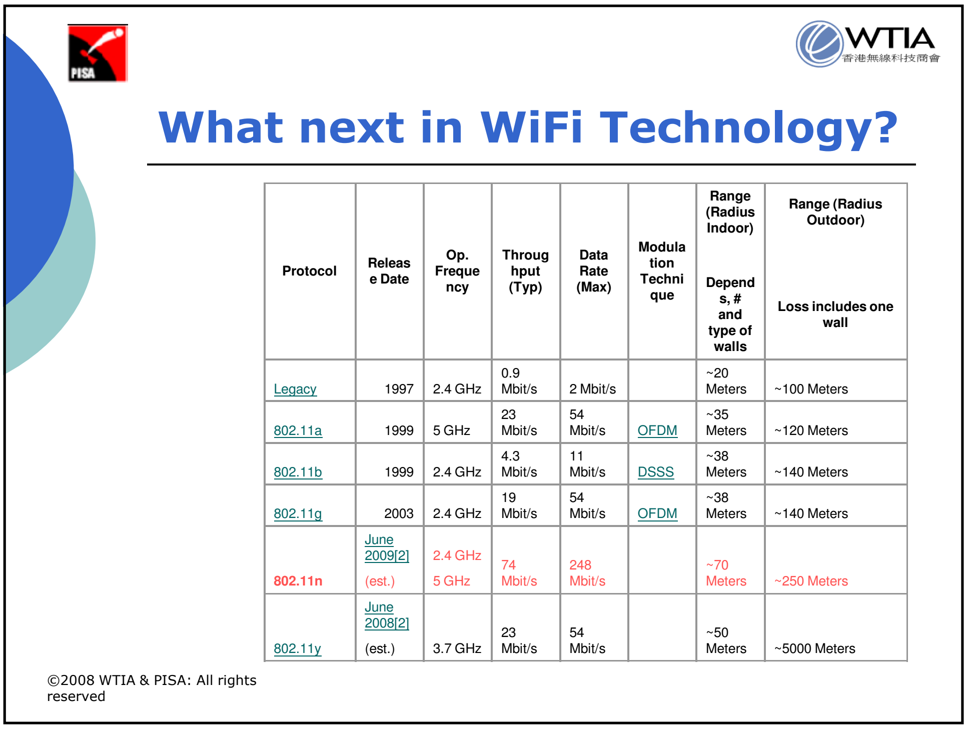
Overview of Wi-Fi Encryption Modes

- WPA/WPA2 (Wi-Fi Protected Access) – cont'd
  - TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) encryption
    - TKIP: 128-bit encryption keys and dynamic session keys
    - TKIP or AES is fine to use. AES is technically more secure. TKIP was implemented to solve WEP problem. AES is a newer implementation.
  - WPA/WPA2 is much more secure than WEP



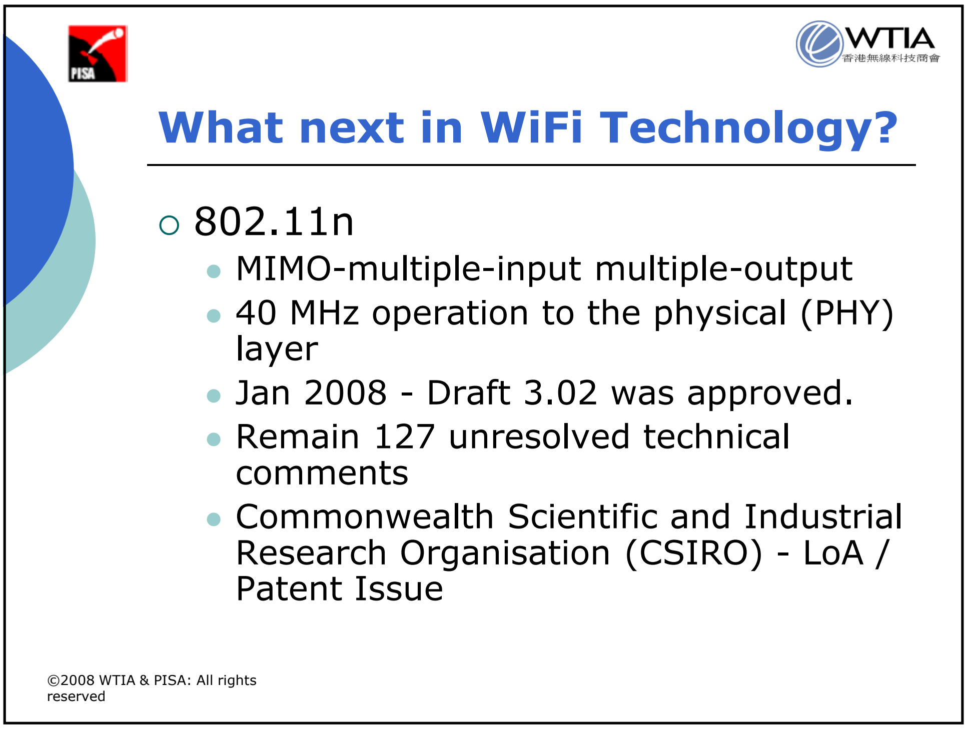
Tips and Recommendation

- Enable encryption mode and use WPA/WPA2
- 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



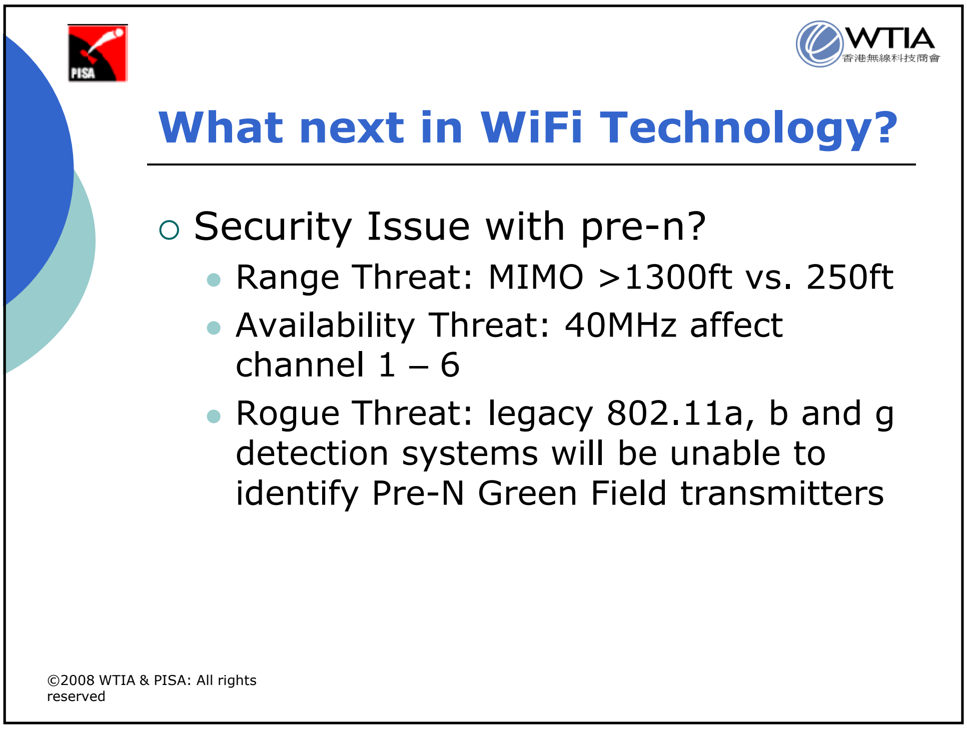
What next in WiFi Technology?

Protocol	Release Date	Op. Frequency	Throughput (Typ)	Data Rate (Max)	Modulation Technique	Range (Radius Indoor) Depends, # and type of walls	Range (Radius Outdoor) Loss includes one wall
Legacy	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s		~20 Meters	~100 Meters
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	~35 Meters	~120 Meters
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	~38 Meters	~140 Meters
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	OFDM	~38 Meters	~140 Meters
802.11n	June 2009[2] (est.)	2.4 GHz 5 GHz	74 Mbit/s	248 Mbit/s		~70 Meters	~250 Meters
802.11y	June 2008[2] (est.)	3.7 GHz	23 Mbit/s	54 Mbit/s		~50 Meters	~5000 Meters



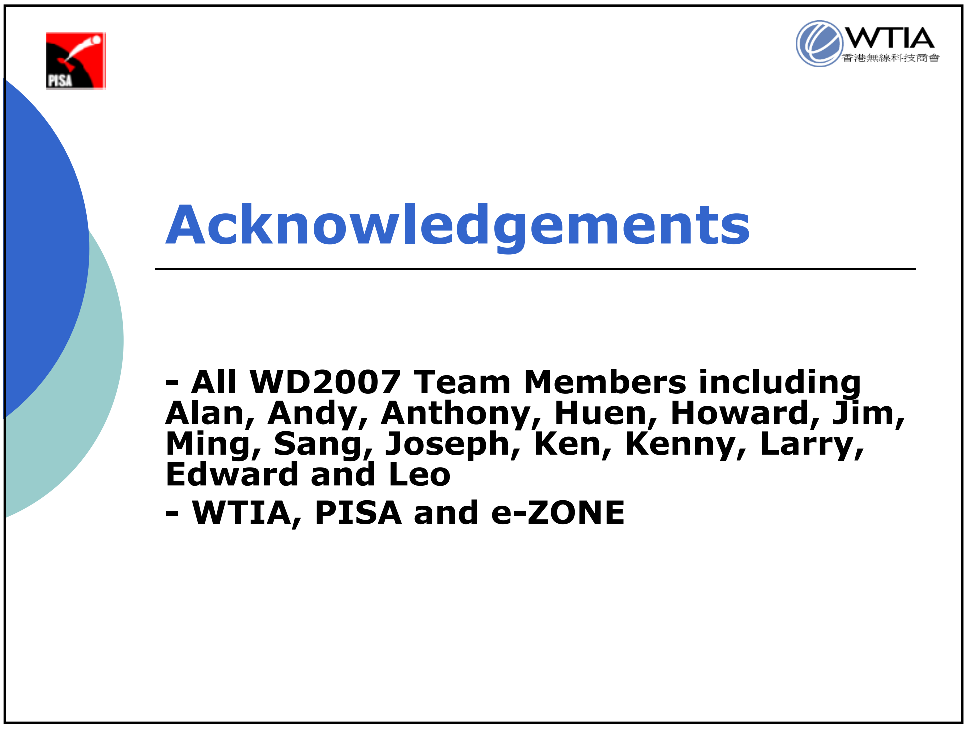
What next in WiFi Technology?

- 802.11n
  - MIMO-multiple-input multiple-output
  - 40 MHz operation to the physical (PHY) layer
  - Jan 2008 - Draft 3.02 was approved.
  - Remain 127 unresolved technical comments
  - Commonwealth Scientific and Industrial Research Organisation (CSIRO) - LoA / Patent Issue



What next in WiFi Technology?

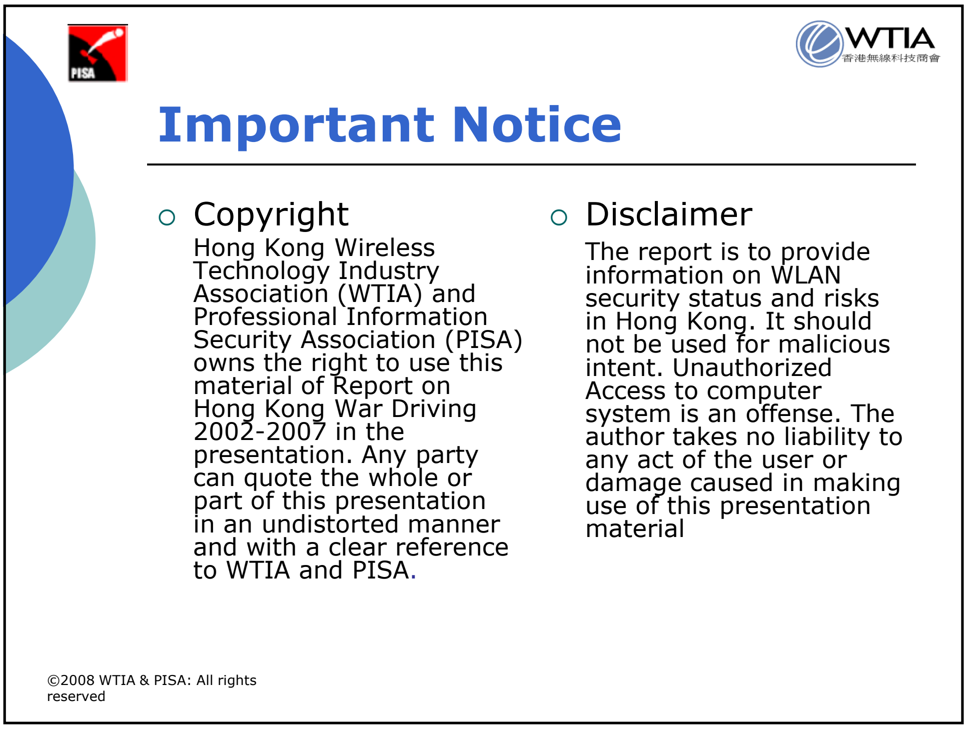
- Security Issue with pre-n?
  - Range Threat: MIMO >1300ft vs. 250ft
  - Availability Threat: 40MHz affect channel 1 – 6
  - Rogue Threat: legacy 802.11a, b and g detection systems will be unable to identify Pre-N Green Field transmitters



Acknowledgements

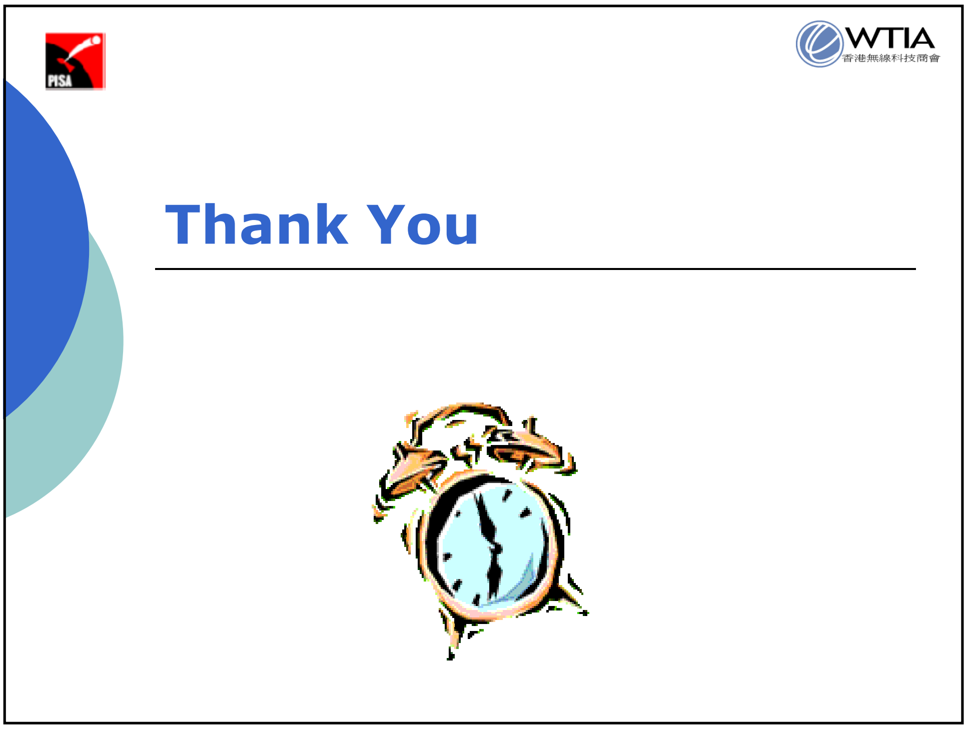
- All WD2007 Team Members including Alan, Andy, Anthony, Huen, Howard, Jim, Ming, Sang, Joseph, Ken, Kenny, Larry, Edward and Leo

- WTIA, PISA and e-ZONE



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 2002-2007 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