# Report on

# War Driving Survey 2008

**Consolidated Report**

**Version 1.2**

Feb-2009

This report can be downloaded via URL

http://www.safewifi.hk/security.html

## *Organizers*

**Professional Information Security Association**

**(PISA)**

**專業資訊保安協會**

**http://www.pisa.org.hk**

**Hong Kong Wireless Technology Industry Association**

**(WTIA)**

**香港無線科技商會**

**http://www.hkwtia.org**

## *Sponsor*

**Office of the Telecommunications Authority**

**(OFTA)**

**電訊管理局**

**http://www.ofta.gov.hk**

## Copyright



## Disclaimer

This 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 report.

The points made here are kept concise for the purpose of presentation. If you require details of test and implementation please refer to other technical references.

## Photos


**War Driving in Hong Kong Island using Tram**

[From left]: CK Huen (PISA), Thomas Tseng (PISA), Alan Ho (PISA), Sang Young (PISA), Billy Yung (PISA), Kenny Chiu (WTIA), Ken Fong (WTIA)

**War Driving in New Territories using mini-bus**

[From left]: Alan Tam (PISA), Sang Young (PISA), Joseph Leung (WTIA), CK Huen (PISA), Kenny Chiu (WTIA), SC Leung (PISA)

## Photos

**War Driving in New Territories using mini-bus**

[From left]: Alan Tam (PISA), Alan Ho (PISA), Thomas Tsang (PISA), SC Leung (PISA), Joseph Leung (WTIA), Sang Young (PISA), CK Huen (PISA)


**War Driving in Kowloon using Bus**

[From left]: Michael Kan (WTIA), Ken Fong (WTIA), Warren Kwok (PISA), Nikita Leung, Jeff Lee (Y5Zone), Chan Chi Fong (FON), Sang Young (PISA), Jacky Cheng (WTIA), Jim Shek (PISA), Voker Lam (WTIA), Joseph Leung (WTIA), CK Huen (PISA), SC Leung (PISA), Alan Ho (PISA)

## Photos

**War Driving in Victoria Harbour**

Mr Y K Ha (OFTA) together with Ken Fong (WTIA), Joseph Leung (WTIA) and other participants


**War Driving in Victoria Harbour**

Participants before boarding

## Photos


**War Driving in Victoria Harbour**

Some of working staff and participants

**War Driving in Macau**

Hong Kong War Driving Team worked with the Macau Team for the 2nd Macau War Driving led by Geoffroy Thonon (2nd from the right)

## Photos


**War Driving in Macau**

The war driving team took a mini-bus to drive along bus route 6 & 15 that covered main districts in Macau including Coloane and Taipa Islands

## Terms used

| | |
|---|---|
| WLAN | Wireless Local Area Network. There are four popular standards now:<br>• 802.11a: using 5GHz, 54Mbps<br>• 802.11b: using 2.4GHz, 11Mbps<br>• 802.11g: using 2.4GHz, 54Mbps (most popular)<br>• 802.11n draft: using 2.4GHz or 5GHz, >100Mbps |
| War Driving | Collecting wireless LAN information including network name, signal strength, location by using a device capable of WLAN signal receiver and moving from one place to another. |
| GPS | GPS stands for Global Positioning System. It is a "constellation" of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The GPS is owned and operated by the U.S. Department of Defense but is available for general use around the world. |
| AP | Access Point. A device that serves as a communications "hub" for wireless clients |
| MAC | Media Access Control address. The physical address of a Wireless LAN card |
| SNR | Signal-to-Noise Ratio. A measurement of signal strength versus noise. |
| SSID | Service Set Identifier. The identifier name of each wireless LAN network |
| WEP | Wired Equivalent Privacy. An encryption protocol in using WLAN |
| WPA | Wireless Protected Access. An improved encryption protocol over WEP in using WLAN |
| WPA2 | 802.11i Standard on Wireless LAN security improvement |

## *Executive Summary*

In Nov and Dec 2008, **PISA** and **WTIA** jointly conducted the "War Driving 2008" field survey in Victoria Harbour, Hong Kong Island, New Territories and Kowloon. It is the **FIRST** organized and large-scaled wireless security survey to cover major areas in Hong Kong. The objective of this survey was to conduct a non-intrusive study on the status of Hong Kong WLAN security and arouse the public awareness in securing the use of WLAN so as to create a safe and sophisticated ubiquitous city.

With the funding support by Office of the Telecommunications Authority (OFTA), under the Public Awareness Campaign on WiFi Safety (SafeWiFi), this year's survey has the most comprehensive coverage capturing 30,457 unique Access Points (APs) during the 4-day assessment. Survey areas including not only tram routes like past years but also newly added areas like Kowloon, New Territories and Victoria Harbour.

Key findings from this survey – **we recommend adopting AES under WPA/WPA2 encryption mode**:

- 78% of APs are encryption enabled; this data has been being in increasing trend in the past few years
- Within the 78%, nearly 47% of APs are WEP configured. However, WEP can be easily hacked within 10 minutes and thus, is considered unsecured
- 24% of APs are WPA or WPA2 TKIP encrypted. They are more secure than WEP but has recently found loopholes which can also be hacked
- Only 7% of APs are WPA or WPA2 AES encrypted and are considered highly secured as of today's technology

From the survey, it is no doubt that people's awareness on WLAN security is growing year after year. However, hacking technology has also advanced quickly. Thus, **it is important for users to update their encryption methods regularly to avoid being hacked**.

As for the handling of SSID, 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). We also found that about 20% SSIDs are related to personal/company identity. We **suggest enabling the hidden SSID function and change SSID not to associate your identity/name** that can help reduce the chance of being hacked.

The study was carried out in a non-intrusive and responsible way. The information of individual vulnerable AP was not disclosed. In addition, details about a particular wireless LAN network were not shown. **PISA** and **WTIA** share a common vision in promoting the use of wireless network in a productive and secure manner. They call for the public awareness of the problem. They would follow up the findings with educational programs to promote the adoption of WLAN security strategies.

This report contains the consolidated figures from Hong Kong Island, Victoria Harbour, Kowloon and New Territories. Statistics from individual zone can be found in the respective reports. In addition, the Hong Kong War Driving Team worked with the Macau Team on 27 Sep 2008 for the 2nd Macau War Driving. In general, the Hong Kong and Macau results/figures are similar and are improving.

## *Introduction*

In 2002, a team of **PISA** wireless LAN security investigators performed the city's 1st "War Driving" study on the Wireless LAN Security Flaws in Hong Kong (mainly Hong Kong Island). It had aroused the public and corporation awareness to tighten their WLAN security loopholes. Since 2003, **PISA** and **WTIA** jointly conducted the annual "War Driving". The scope of test was extended to the whole tramway, covering the business corridor of the HK Island

In 2008, **PISA** and **WTIA** conducted the **FIRST** organized and large-scaled "War Driving" in Hong Kong. We collected the wireless LAN information using Vistumbler and WiFi Hopper. Information collected includes the number of Access Point, the percentage of Access Point with encryption and no encryption. In addition, we would like to investigate the usage of various encryption methods found in wireless LAN security.

## *Objectives of Study*

1. To study the current WLAN security status in Hong Kong
2. To study usage of encryption methods
3. To conduct a non-intrusive* information security study with responsible disclosure of information
4. To arouse the public awareness in WLAN security and follow up with education program

** The study involved neither sniffing of data nor jamming of network traffic. The tool used was mainly for discovery of wireless network broadcasted signals. No association with access point, no network connection was attempted during the war driving study. Please see Code of Ethics below.*

## *Code of Ethics*

The organizers, the reporter and all other participants agreed on the following points to the study to take care of the security and privacy issues.

- Our objective of the War Driving is to study the WLAN security status and compare it with the previous results, and to arouse the public awareness in WLAN security.
- We do not publicize the exact location and identity (e.g. SSID and MAC address) of any discovered AP. If such information appears in photos or other forms, such information will be fully masked.
- We do not connect to the IP network of any insecure AP to further explore their vulnerability.
- We do not interfere / jam any wireless traffic.
- We limit to the scope we state above only.

## *Methodology and Equipment*

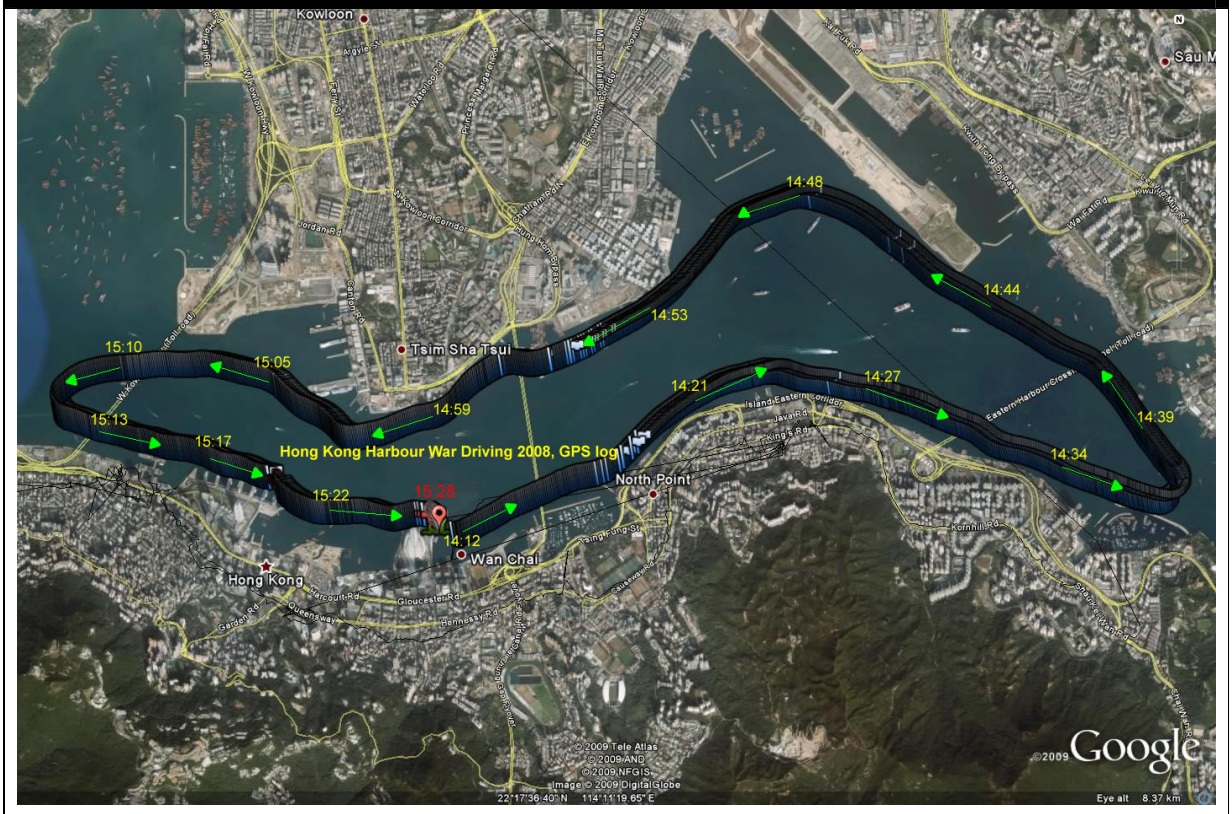
The War Driving 2008 was held in Victoria Harbour, Hong Kong Island, New Territories and Kowloon in 4 different days. We conducted the War Driving with the following software:

- Commercial software – WiFi Hopper was selected. Although it is commercial software, the evaluation mode is more than enough to perform war driving.
- Open source software – Vistumbler was another one used in this War Driving. It makes use of Microsoft Vista's netsh command for collecting WLAN information. The drawback is working in Vista only.
- WiFi Hopper and Vistumbler allows us to distinguish the details of encryption mode an Access Point was configured. We can obtain the portion of WEP, WPA or WPA2 Personal and Enterprise. What's more, the encryption algorithm either (TKIP/RC4 or CCMP/AES) can be shown.

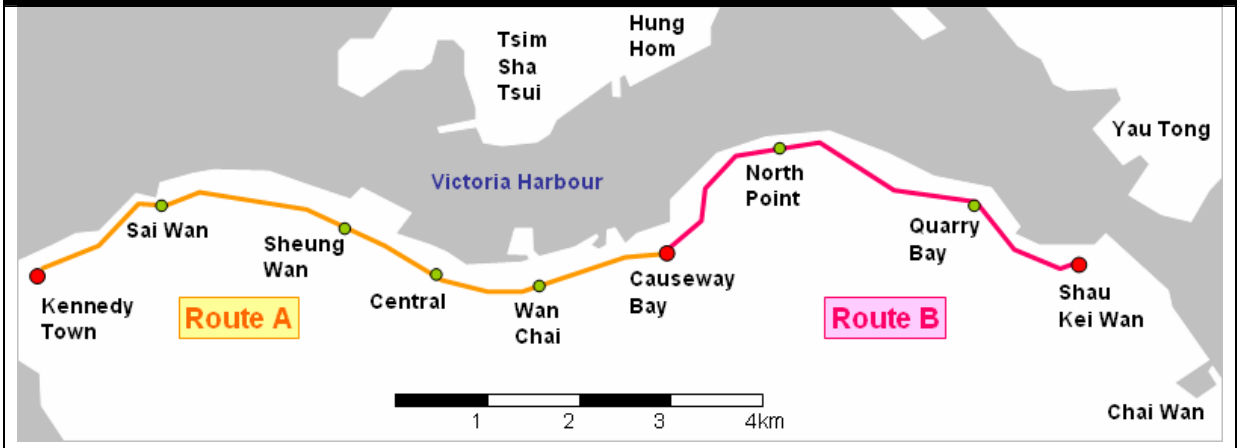
**Below are the details of date and route:**

| Date: | Oct 25, 2008 (Saturday) | 9-Nov-2008 (Sunday) | Nov 23, 2008 (Sunday) | Dec 7, 2008 (Sunday) |
|---|---|---|---|---|
| Time: | 12:45pm - 3:30pm | 10:00am – 1:00pm | 10:00am - 2:00pm | 2:00pm - 6:00pm |
| Equipment: | *Hardware:*<br>Notebook computers, WLAN cards, antennae and GPS<br>*Software:*<br>Vistumbler (http://vistumbler.sourceforge.net)<br>WiFi Hopper (http://www.wifihopper.com) | | | |
| Transportation: | Rental Ferry | Tram | Rental Mini-bus | Rental Bus |
| Route: | Around Victoria Harbour from Wan Chai and back to Wan Chai | Admiralty<br>↓<br>Kennedy Town<br>↓<br>Sheng Wan<br>↓<br>Admiralty<br>↓<br>Wai Chai<br>↓<br>Causeway Bay<br>↓<br>North Point<br>↓<br>Quarry Bay<br>↓<br>Shau Kei Wan | Tsuen Wan<br>↓<br>Sha Tin<br>↓<br>Tai Po<br>↓<br>Fanling<br>↓<br>Sheung Shui<br>↓<br>Yuen Long<br>↓<br>Tin Shui Wai<br>↓<br>Tuen Mun<br>↓<br>Tsing Yi<br>↓<br>Kwai Fong | Tsim Sha Tsui<br>↓<br>Nathan Road<br>↓<br>Sham Shui Po<br>↓<br>Lai Chi Kwok<br>↓<br>Boundary Street<br>↓<br>Kowloon Bay<br>↓<br>Kwun Tong<br>↓<br>Junk Bay<br>↓<br>Kwun Tong Bypass<br>↓<br>Chanthan Road N.<br>↓<br>Tsim Sha Tsui |

Below is the route of War Driving 2008 on Ferry around Victoria Harbour:



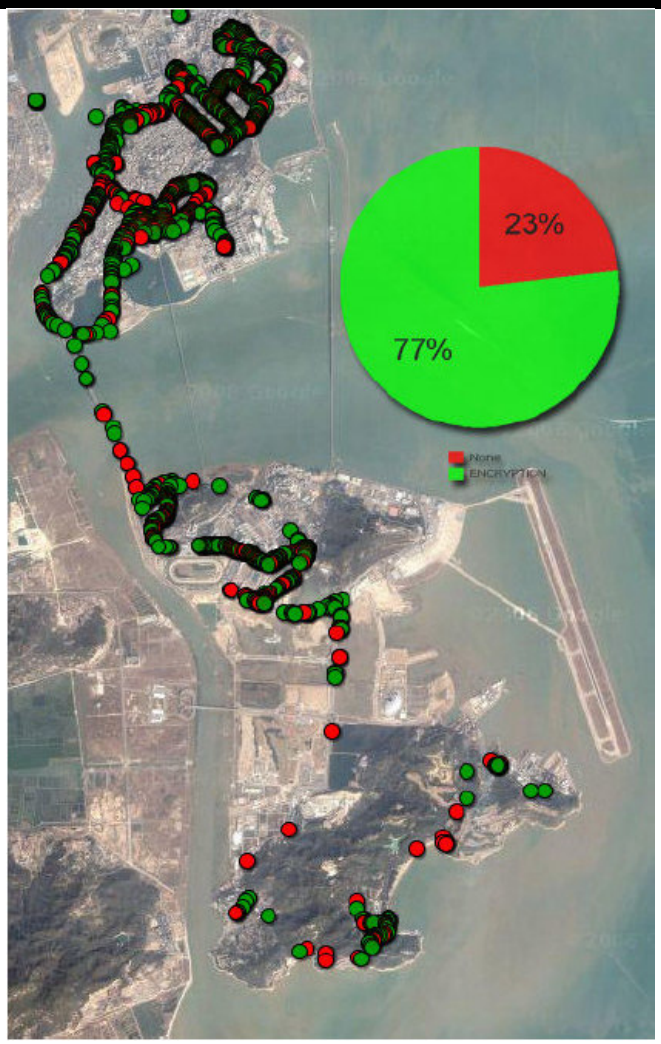

Below is the route of War Driving 2008 on Tram at Hong Kong Island:



Below is the route of War Driving 2008 on mini-bus at New Territories:


Below is the route of War Driving 2008 on Bus at Kowloon.

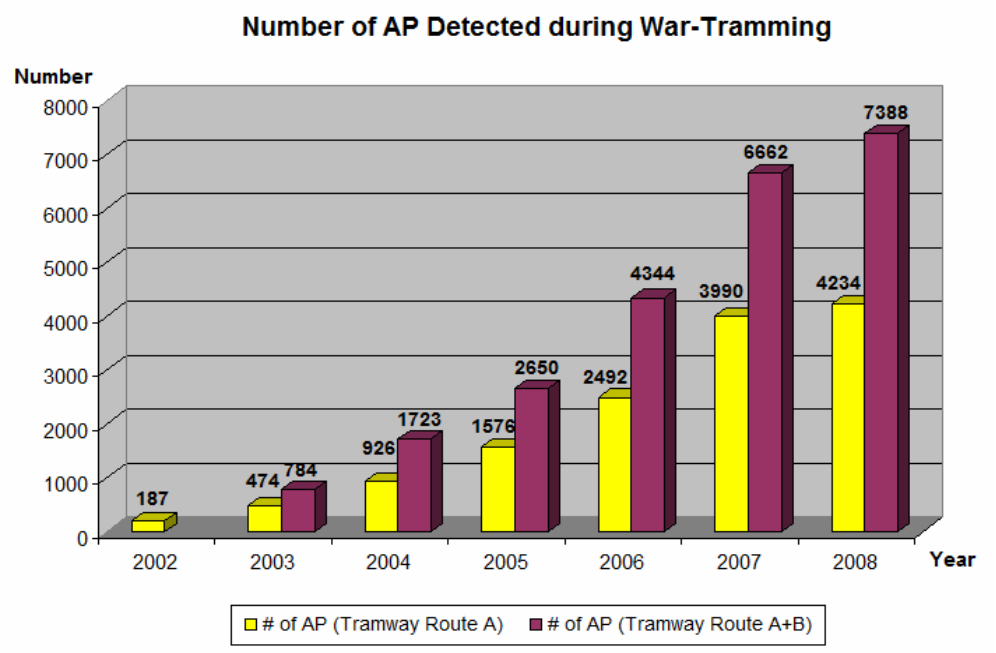
Hong Kong & Macau War Driving Teams conducted the 2nd Macau War Driving on 27 Sep 2008



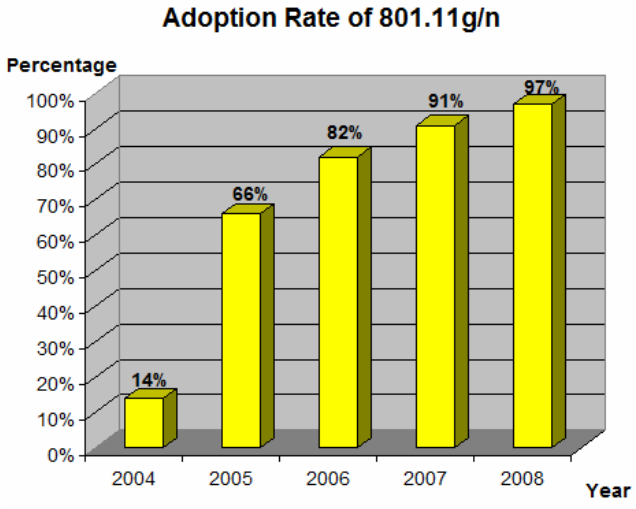
## *Findings and Analysis*

### 1. Number of Unique Access Points Captured: 30457

Among the 30457 APs, 7388 APs were collected from the tramway. Comparing to our previous years' tramway results, the number of AP detected is on a growing trend, however, the growing rate was flattening.



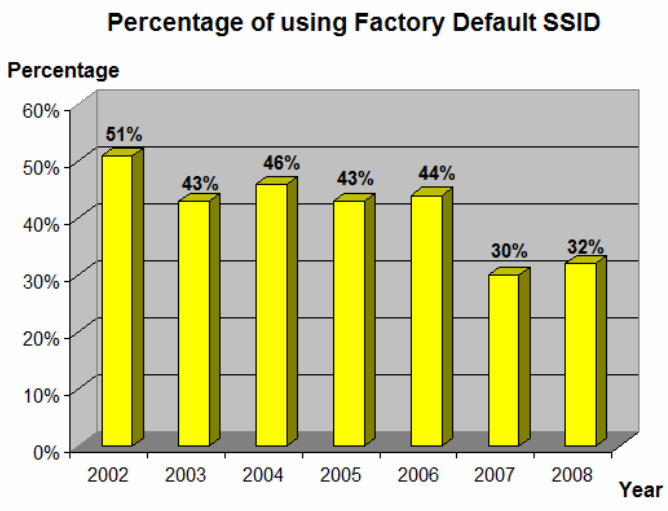

### 2. Overall the implementation of 802.11g or 802.11n in Hong Kong: 97.08%

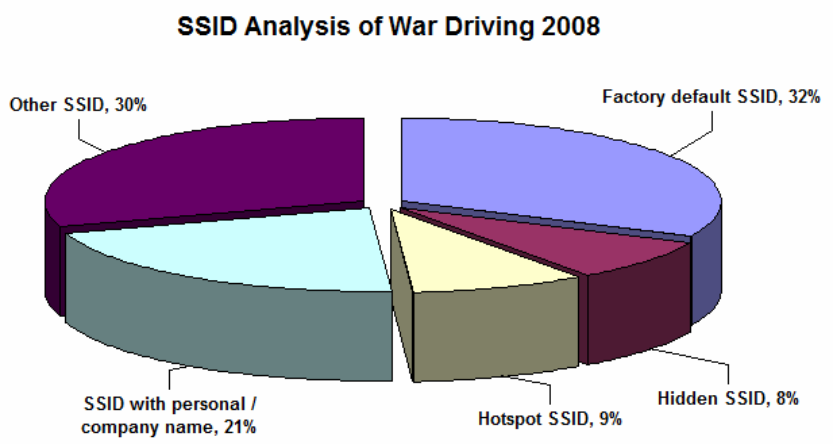


## 3. SSID Settings

| SSID Settings | Proportion |
|---|---|
| Proportion of Default SSID | 31.51% |
| Proportion of Hidden SSID | 8.26% |
| Proportion of Well-known Hotspot SSID | 9.45% |
| Proportion of SSID setting related to personal/company identity | 21.43% |
| Proportion of other SSID setting | 29.35% |
| **Total:** | **100%** |

As for the handling of SSID, 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). We also found that about 20% SSIDs are related to personal/company identity. We suggest enabling the hidden SSID function and change SSID not to associate your identity/name that can help reduce the chance of being hacked.



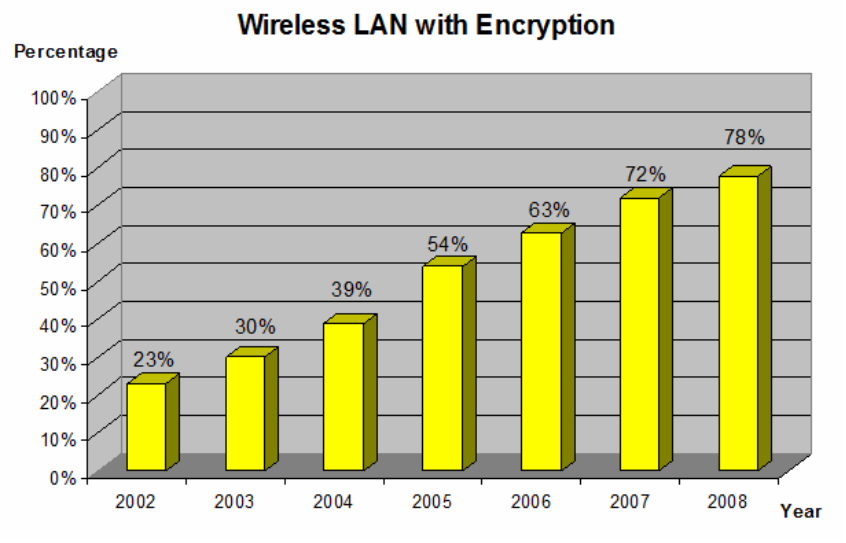
## 4. Encryption Settings

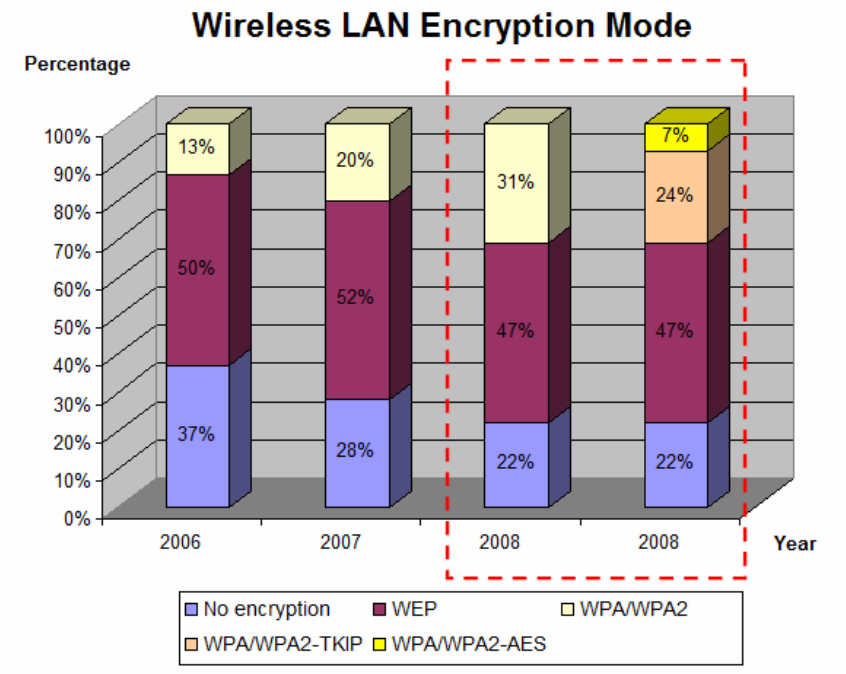
5.

| Encryption Settings | Proportion |
|---|---|
| No Encryption | 22.35% |
| WEP | 46.48% |
| WPA | 23.61% |
| WPA Personal using TKIP | 14.42% |
| WPA Personal using AES | 2.15% |
| WPA Enterprise using TKIP | 6.97% |
| WPA Enterprise using AES | 0.04% |
| WPA Unclassified | 0.03% |
| WPA2 | 7.56% |
| WPA2 Personal using TKIP | 2.53% |
| WPA2 Personal using AES | 4.62% |
| WPA2 Enterprise using TKIP | 0.16% |
| WPA2 Enterprise using AES | 0.24% |
| WPA2 Unclassified | 0.01% |
| **Total:** | **100%** |

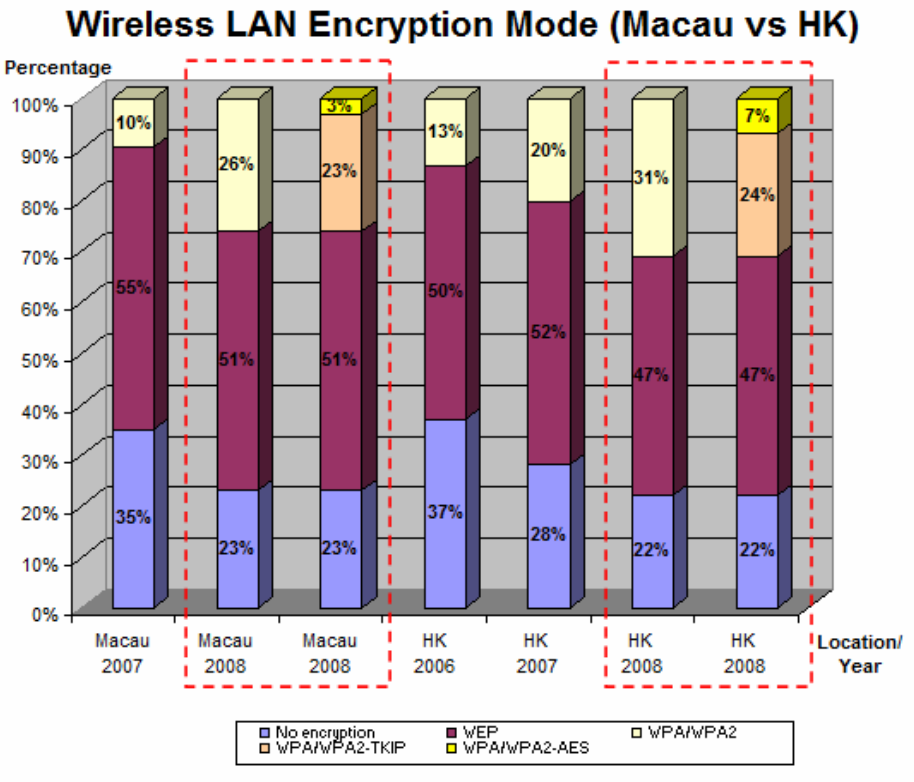
The usage of WEP, WPA, and WPA2 are 46.48%, 23.61% and 7.56% respectively. There are two common encryption methods in the implementation of WPA and WPA2. They are TKIP/RC4 and the CCMP mode of AES. The TKIP/RC4 is modification of WEP to mitigate the weakness found in WEP. However, in a recent study, it is discovered that a weakness in TKIP of WPA or WPA2. Attackers can decrypt the content under certain conditions. This weakness is not happened in AES. In our study, we found that only 7.05% is using the most secure method – AES.

Statistics show that the use of encryption settings is increasing. Though adoption of encryption settings is increasing, the use of WEP was still high. WEP is nowadays not secure. For WPA/WPA2-TKIP, loopholes were found in recent study and can be hacked. Hence, more secure WPA/WPA2-AES should be used (currently, only 7% WLAN is adopting this highly secured encryption mode).



Comparing the adoption of encryption mode statistics between Hong Kong and Macau, the results and trends are similar.




## *Conclusion*

### Hong Kong War Driving 2008

- Recommend adopting AES under the WPA/WPA2 encryption mode
    - The percentage of AP with encryption enabled was 78% and was improving as compared to previous years.
    - 48% of discovered Access Points were configured with WEP. However, WEP is considered as insecure encryption method. The fastest cracking time of WEP is below 10 minutes.
    - TKIP is considered not secure due to recent discovered weakness. In this year's study, there were 24.08% of discovered Access Points using this encryption in WPA or WPA2.
    - Only 7.05% of total discovered Access Points are using the most secure encryption method – CCMP/AES.
- As for the handling of SSID, 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). We also found that about 20% SSIDs are related to personal/company identity. We suggest enabling the hidden SSID function and change SSID not to associate your identity/name that can help reduce the chance of being hacked.

## *Detailed figures of each zone*

The combined figures of this report are consolidated from the reports of Hong Kong Island, Victoria Harbour, Kowloon and New Territories. These reports can be downloaded from http://www.safewifi.hk/security.html.:

| War Driving at | Report name |
|---|---|
| Hong Kong Island | Report on Wireless LAN War Driving Survey 2008 – Part I :Hong Kong Island<br>wd2008-HKI.pdf |
| Victoria Harbour | Report on Wireless LAN War Driving Survey 2008 – Part II: Victoria Harbour<br>wd2008-Harbour.pdf |
| Kowloon | Report on Wireless LAN War Driving Survey 2008 – Part III: Kowloon<br>wd2008-Kowloon.pdf |
| New Territories | Report on Wireless LAN War Driving Survey 2008 – Part IV: New Territories<br>wd2008-NT.pdf |

## *War Driving Participants*

**Last but not the least, thanks to the contribution of the war driving team to make the Hong Kong War Driving 2008 successful!**

| Name | Title | Organization |
|---|---|---|
| Alan Ho | Convener | Professional Information Security Association |
| Ken Fong | Convener | Hong Kong Wireless Technology Industry Association |
| Alan Tam | Member | Professional Information Security Association |
| Billy Yung | Member | Professional Information Security Association |
| CK Huen | Member | Professional Information Security Association |
| Eric Leung | Member | Hong Kong Wireless Technology Industry Association |
| Howard Lau | Member | Professional Information Security Association |
| Jacky Cheng | Member | Hong Kong Wireless Technology Industry Association |
| Jim Shek | Member | Professional Information Security Association |
| Joseph Leung | Member | Hong Kong Wireless Technology Industry Association |
| Kenny Chiu | Member | Hong Kong Wireless Technology Industry Association |
| Michael Kan | Member | Hong Kong Wireless Technology Industry Association |
| Sang Young | Member | Professional Information Security Association |
| SC Leung | Member | Professional Information Security Association |
| Thomas Tseng | Member | Professional Information Security Association |
| Voker Lam | Member | Hong Kong Wireless Technology Industry Association |
| Warren Kwok | Member | Professional Information Security Association |

* * * The End * * *