# Report on

# Wireless LAN War Driving Survey 2010

# Hong Kong

Version 1.0

Feb 2011

This report can be downloaded from:

http://www.safewifi.hk

---

**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

**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


2010 War Traming Team: about to get in the tram (from left to right):
Michael Kan, Eric Lo, Gretel Chan, Jacky Cheng, Voker Lam, Ken Fong, Sang Young, Lawrence Li, Alan Ho, WS LAM

Standard War Driving Equipment: Notebook, Antenna, and GPS device


Another GPS device


Team members working on the software configuration (left to right): Voker Lam, Jacky Cheng, WS LAM and Alan Ho

Standing (left to Right): Ken Fong, Eric Leung, Sang Young and Voker Lam
Sitting (Left to Rigth): WS LAM, Alan Ho, Jacky Cheng, Lawrence Li, Gretel Chan, Eric Lo and Michael Kan


Finished War Traming 2010 Exercise (Left to Right): Eric Lo, Eric Leung, Sang Young, Lawrence Li, Ken Fong, Voker Lam, Jacky Cheng, *Driver*, Gretel Chan, Alan Ho, *Staff from Tram Company*, and WS LAM

## 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<br>• 802.11n: using 2.4 or 5GHz, 300Mbps |
| War Driving | Collecting wireless LAN information including network name, signal strength, location, and security settings 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. In SME or home, it is also referred as WLAN router. |
| 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. It is also referred as network name. |
| WEP | Wired Equivalent Privacy. An encryption protocol in using WLAN. |
| WPA | Wireless Protected Access. An improved encryption protocol over WEP in using WLAN. |
| WPA2 | IEEE 802.11i Standard on Wireless LAN security improvement. |

| | |
|---|---|
| TKIP | Temporal Key Integrity Protocol. An encryption protocol in using WPA. |
| AES-CCMP | Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. An encryption protocol in using WPA2. |

## Executive Summary

In Dec 2010, the two associations **PISA** and **WTIA** jointly conducted the “War Driving 2010” field survey along the classic tramway of Hong Kong Island. This suvery is also part of the “SafeWiFi.hk” program. 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.

The field survey was very successful. The results were benchmarked against that of the previous studies conducted by PISA & WTIA since 2002 to plot the profile of Hong Kong WLAN security development. The survey indicated that the number of WLAN implementation keeps on increasing, and yet there was some improvement in the adoption of security strategies.

The study was carried out in a non-intrusive and responsible way. The information of individual vulnerable AP was not disclosed.

**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.

## Introduction

In 2002, a team of **PISA** investigators performed the city's 1st "War Driving" study on the Wireless LAN Security Flaws in Hong Kong. It had aroused the public and corporations 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 tram way, covering the business corridor of the HK Island

In Dec 2010, **PISA** and **WTIA** conducted the 9th "War Driving" again to benchmark the improvement for the WLAN Security in Hong Kong.

Since 2008, "Wireless LAN War Driving Survey" becomes part of the program of "SafeWiFi.hk". More information about the "SafeWiFi.hk" program can be found in http://www.safewifi.hk.

## Objectives of Study

1. To study the current WLAN security status of Hong Kong and to benchmark the result with that of the previous year
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.

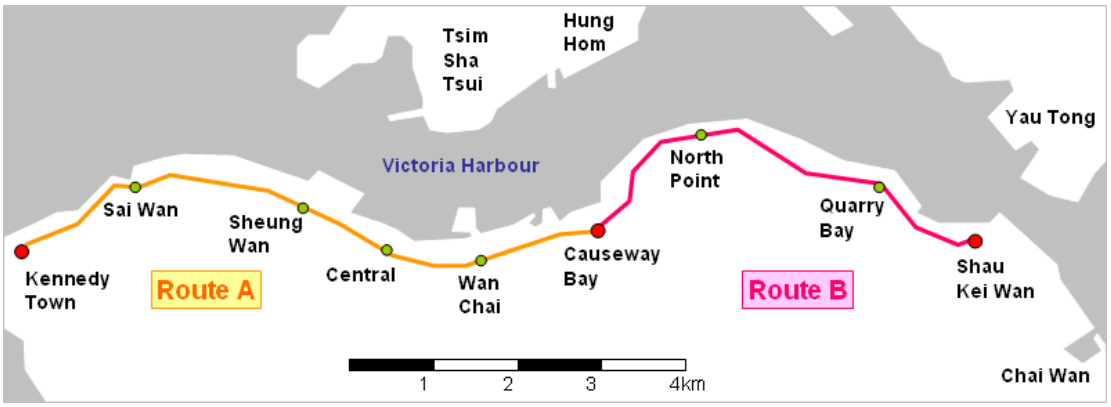
- Our objective of the War Driving is to study the WLAN security status and compare it with the previous results, and to arouse the public awareness in WLAN security.
- We do not publicize the exact location and identity (e.g. SSID and MAC address) of any discovered AP. If such information appears in 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 do not capture or collect any WLAN traffic payloads.
- We limit to the scope we state above only.

## Methodology and Equipment

**Tramway War Driving**

- Tram is only available in a handful of cities around the world and tram riding is a popular activity of tourists in Hong Kong
- 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 of the road.
- By War Driving on a tram, we targeted to benchmark the results with that of the war driving study of since year 2003 along the tramway from Kennedy Town to Shau Kei Wan. This route was equivalent to the whole business corridor of Hong Kong Island.

| **Details:** | |
|---|---|
| Date: | 5 Dec, 2010 (Sunday) |
| Time: | 10 am – 2 pm |
| Equipments: | *Hardware:*<br>• Notebook computers<br>• WLAN cards (internal and external)<br>• Antennae (built-in and external +12dbi)<br>• GPS<br>*Software:*<br>• Vistumbler for Windows 7 and Vista Platforms (http://www.vistumbler.net)<br>• WiFi Hopper for Vista Platforms (http://www.wifihopper.com) |
| Route: | Tramway from Kennedy Town to Shau Kei Wan |


Tsim
Sha
Tsui
Hung
Hom
Yau Tong
Victoria Harbour
North
Point
Quarry
Bay
Sai Wan
Sheung
Wan
Causeway
Bay
Kennedy
Town
Route A
Central
Wan
Chai
Route B
Shau
Kei Wan
1
2
3
4km
Chai Wan

## Findings and Analysis

**Tramway War Driving 2010**

| | |
|---|---|
| Number of Access Points Captured | 16,462 |
| Access Points without using Encryption | 2,246 (13.64%) |
| Access Points without securing the SSID<br>*(include default SSID, SSID same as trailing hexadecimal of AP's MAC address, hotspots etc)* | 2,255 (13.70%) |
| Access Points using 802.11b | 169 (1.03%) |

**2010 Result Compared with Previous Years**

The following table contains the result of whole tramway from year 2003 to year 2010.

| 2003<br>Oct 5 | 2004<br>Nov 28 | 2005<br>Dec 4 | 2006<br>Oct 15 | 2007<br>Nov 4 | 2008<br>Nov 9 | 2009<br>Nov 26 | 2010<br>Dec 5 |
|---|---|---|---|---|---|---|---|
| Sunny | Sunny | Sunny | Occasional Raining | Sunny | Trace Raining | Sunny | Sunny |
| *Number of Access Points* | | | | | | | |
| 784 | 1,723 | 2,650 | 4,344 | 6,662 | 7,388 | 15,753 | 16,462 |
| *No Encryption* | | | | | | | |
| 70% | 61% | 46.08% | 37.04% | 27.57% | 19.26% | 15.50% | 13.64% |
| *Insecure SSIDs* | | | | | | | |
| 43% | 46% | 42.98% | 44.01% | 30.29% | 20.41% | 11.57% | 13.70% |

**Highlights**

1. The number of detectable deployment along the tramway, comparing with last year, has slightly increased by 4.5%.
2. The percentage of APs with encryption turned on has improved by 1.85%.
3. The percentage of APs with SSID secured has improved by 2.12%.

**Encryption Usages**

Vistumbler and Wifihopper allow us to run the War Driving under Vista environment. The figures below covered the encryption usages break down comparing with last few years.

WEP, WPA and WPA2 Usage Distribution

| | 2008 | 2009 | 2010 |
|---|---|---|---|
| **Encryption Type** | % | % | % |
| No Encryption | 22.86 | 15.50 | 13.64 |

| | | | |
|---|---|---|---|
| WEP | 43.18 | 45.01 | 34.05 |
| WPA Personal using TKIP | 13.53 | 11.65 | 13.53 |
| WPA Personal using AES | 1.02 | 0.91 | 1.94 |
| WPA Enterprise using TKIP | 11.76 | 7.31 | 5.92 |
| WPA Enterprise using AES | 0.03 | 0.02 | 0.02 |
| WPA2 Personal using TKIP | 3.26 | 10.90 | 7.39 |
| WPA2 Personal using AES | 3.31 | 5.10 | 19.21 |
| WPA2 Enterprise using TKIP | 0.62 | 3.07 | 0.92 |
| WPA2 Enterprise using AES | 0.43 | 0.53 | 3.38 |
| **Total:** | **100** | **100** | **100** |

The usages of WEP, WPA, and WPA2 are 45.01%, 19.89% and 19.60% in year 2009 while the usages of these are 35.05%, 21.41% and 30.09% in year 2010. Although the total encryption usage is slightly improved by 1.85% only, nearly 10% are shifting to more secure methods – WPA and WPA2.

TKIP and AES Distribution

| | 2008 | 2009 | 2010 |
|---|---|---|---|
| **Encryption Type** | % | % | % |
| No Encryption | 22.86 | 15.50 | 13.64 |
| WEP | 43.18 | 45.01 | 34.05 |
| WPA/WPA2 using TKIP | 29.17 | 32.93 | 27.76 |
| WPA/WPA2 using AES | 4.79 | 6.56 | 24.55 |
| **Total:** | **100** | **100** | **100** |

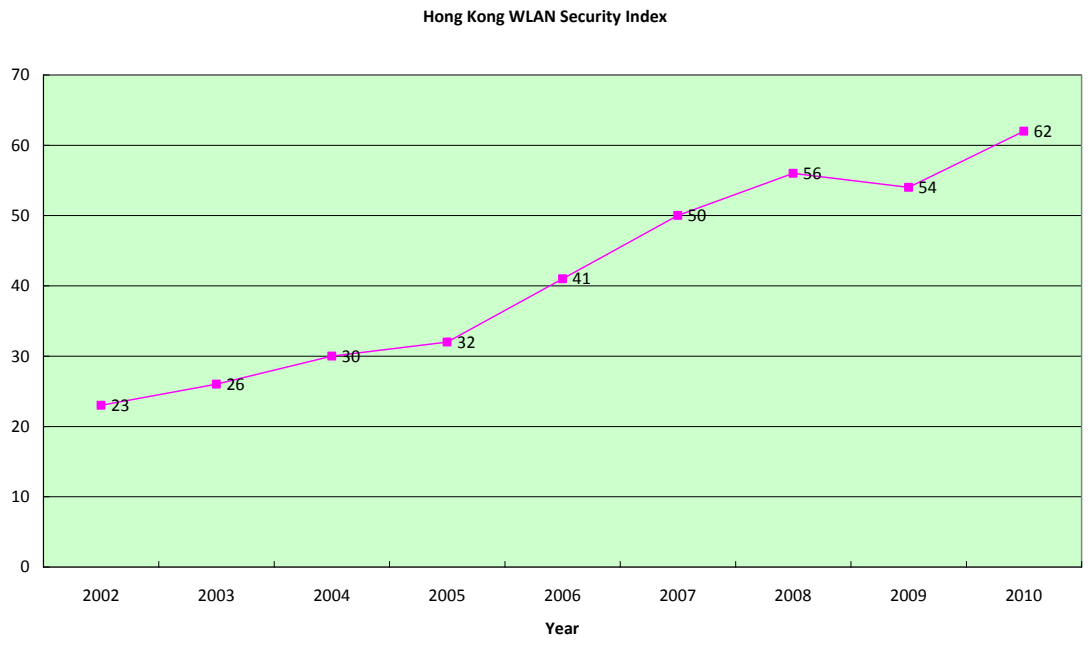
From another point of view, the adoption of more secure encryption methods (i.e. AES) increased from 6.56% to 24.55%. There is significant improvement in adopting more secure encryption method.

## Hong Kong WLAN Security Index [香港無線網絡安全指數]

The Hong Kong WLAN Security 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.

This index takes into account the factors of overall public awareness of encryption applied in Hong Kong, the best practice in securing the WLAN infrastructure and the technologies adopted. Every year, we will review the weighting to these three factors by referring if any vulnerabilities discovered.

PISA and WTIA maintains this Index to keep track on the implementation status in WLAN security in Hong Kong. Below is the graph representing the index from 2002 to 2010.



## Conclusion

**Tramway War Driving**

- We can see a leap in the use of encryptions whereas the overall improvement in security is improved.
- **The percentage of AP with encryption enabled is around 86 percentages.**
- For the default SSID issue, around 80% of default SSID was changed. However, **only 16.95%** (which is slightly improved from previous year) of total **SSIDs are hidden**. Hidden SSID is considered as first line defense of a WLAN.
- The use of 802.11b device which may not support sophisticated encryption technologies is dropped to 1.03%.

**Encryption Usages**

- In recent year, WEP cracking methods were enhanced. It allows an intruder to penetrate to a WLAN using WEP cracking within 10 minutes of time. In our study, 34.05% of WLANs are still using WEP. Although there is a large percentage improvement, **we still not satisfy with this figure due to the latest technologies are out for more than 5 years**.
- The adoption of WPA/WPA2 is improved **over 50%**. It shows the adoption of more secure encryption method is increasing.
- In year 2008, there is a way to crack WPA using TKIP as encryption algorithm. In our study, 27.76% of WLANs are using TKIP. It shows the improvement of 5.17% comparing with year 2009.
- The adoption of more secure encryption methods – AES is increased from 6.56% to 24.55%.
- Although the adoption of encryption wireless LAN traffic is slightly increased, more WLANs are configured with more secure methods.

**Hong Kong WLAN Security Index**

- The Hong Kong WLAN Security Index of 2010 is 62 while the index of 2009 is 54. It shows some improvement in WLAN security implementation in Hong Kong.

** The End **