Report on

War Driving Survey 2009

Hong Kong

Consolidated Report

Version 1.0

Feb 2009

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

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.


WiFi
安全話咁揚
WTIA
e-zone
ISUZU


GIVE WAY
讓路
HKTDC

Terms used

WLAN	Wireless Local Area Network. There are four popular standards now: • 802.11a: using 5GHz, 54Mbps • 802.11b: using 2.4GHz, 11Mbps • 802.11g: using 2.4GHz, 54Mbps (most popular) • 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 2009, **PISA** and **WTIA** jointly conducted the "War Driving 2009" field survey in 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 58,224 unique Access Points (APs) during the 3 days assessment. Survey areas including not only tram routes like past years but also newly added areas like Kowloon and New Territories.

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

- 84% of APs are encryption enabled; this data has been being in increasing trend in the past few years;
- 43% of APs are WEP configured. However, WEP can be easily hacked within 10 minutes and thus, is considered unsecured;
- 40% of APs are WPA or WPA2 TKIP encrypted. This is getting close to using WEP this year. They are more secure than WEP but has recently found loopholes which can also be hacked;
- Only 6% 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. It is also noted that the number of WEP and WPA/WPA2 is very close this year. This shows that WLAN users is adopting a more secure WLAN configurations. However, the percentage of adopting the most secure one – WPA/WPA2 AES encryption method is low. It may show that WLAN users lack of knowledge on security configuration in wireless LAN environment. In general, hacking technology has also advanced very quickly. Thus, it is important for users to update their encryption methods regularly to avoid 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, 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 12 Sep 2009 for the 3rd Macau War Driving.

Introduction

In 2002, a team of **PISA** wireless LAN security investigators performed the city's first "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 and 2009, **PISA** and **WTIA** conducted the 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 2009 was held in Hong Kong Island, New Territories and Kowloon in 3 different days. We conducted the War Driving with the following software:

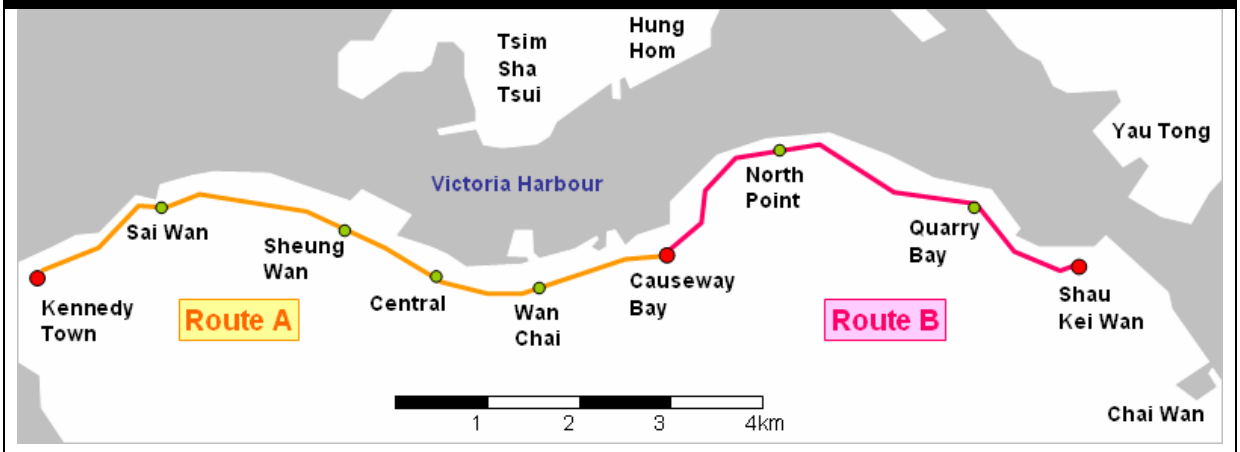
- Commercial software – WiFi Hopper was selected. Although it is commercial software, the evaluation mode is more than enough to perform war driving. It works in XP and Vista.
- Open source software – Vistumbler was another one used in this War Driving. It makes use of Microsoft Vista's netsh command for collecting WLAN information. The drawback is working in Vista only. It works in Vista and Windows 7.
- 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:	29-Nov-2009 (Sunday)	13-Dec-2009 (Sunday)	27-Dec-2009 (Sunday)
Time:	10:00am – 1:00pm	10:00am - 2:00pm	9:30am - 1:30pm
Equipment:	*Hardware:* Notebook computers, WLAN cards, antennae and GPS *Software:* Vistumbler (http://vistumbler.sourceforge.net) WiFi Hopper (http://www.wifihopper.com)		
Transportation:	Tram	Rental Mini-bus	Rental Bus
Route:	Admiralty ↓ Kennedy Town ↓ Sheng Wan ↓ Admiralty ↓ Wai Chai ↓ Causeway Bay ↓ North Point ↓ Quarry Bay ↓ Shau Kei Wan	Tsuen Wan ↓ Sha Tin ↓ Tai Po ↓ Fanling ↓ Sheung Shui ↓ Yuen Long ↓ Tin Shui Wai ↓ Tuen Mun ↓ Tsing Yi ↓ Kwai Fong	Tsim Sha Tsui ↓ Nathan Road ↓ Sham Shui Po ↓ Lai Chi Kwok ↓ Boundary Street ↓ Kowloon Bay ↓ Kwun Tong ↓ Junk Bay ↓ Kwun Tong Bypass ↓ Chanthan Road N. ↓

			Tsim Sha Tsui

Below is the route of War Driving 2009 on Tram at Hong Kong Island:



Below is the route of War Driving 2009 on mini-bus at New Territories:

Below is the route of War Driving 2009 on Bus at Kowloon.

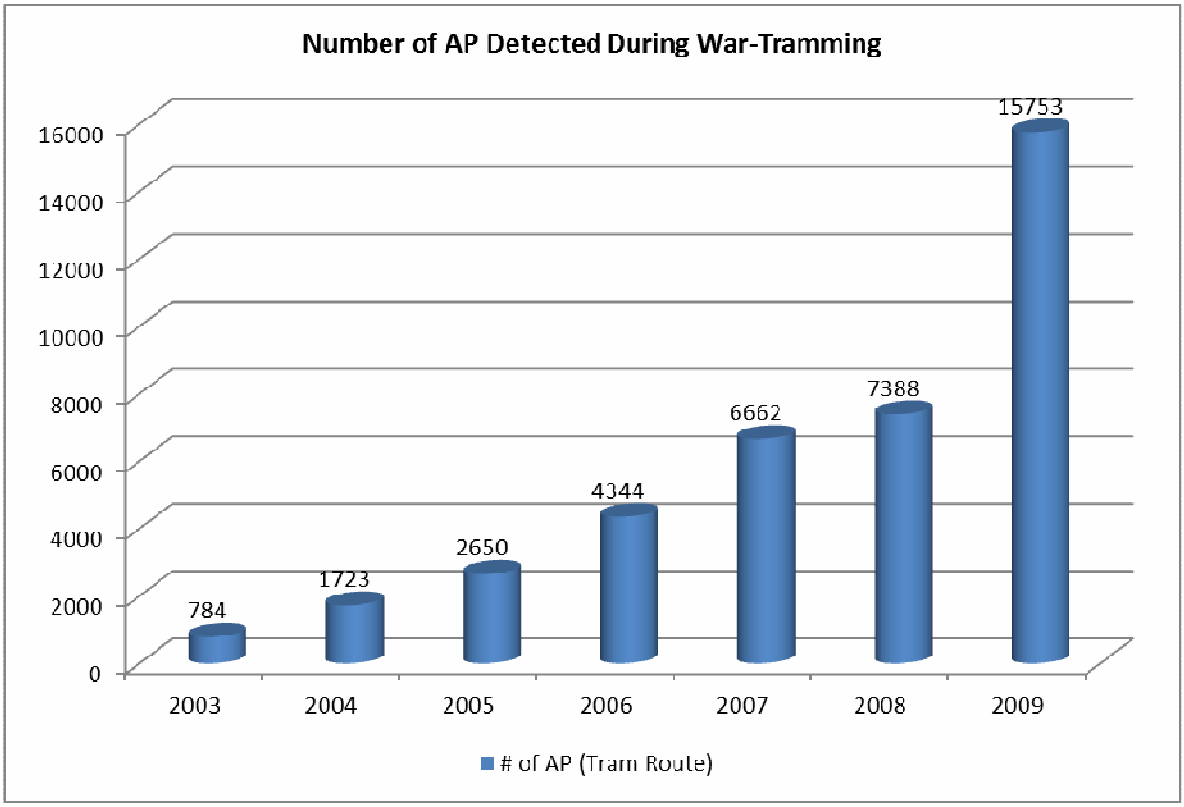
Findings and Analysis

1. Number of Unique Access Points Captured: 58,224

Comparing the baseline of tramway, the number of AP detected is on a growing trend. However, a significant grow has been recorded in this year. It is because we have made some changes on the equipments with the battery life of a notebook computer getting longer. The changes include:

- Using faster machines
- Tuning on wireless LAN card's performance in battery mode
- Tuning on the CPU performance in battery mode

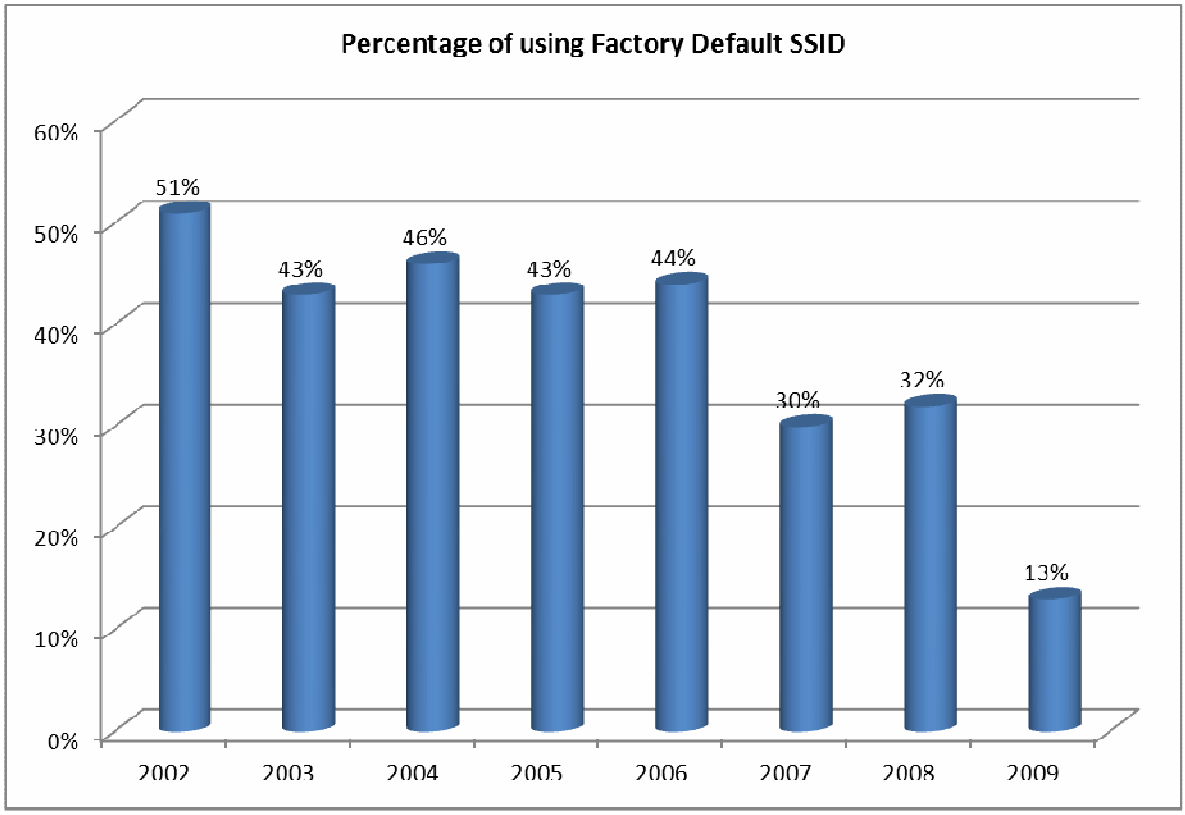
The draw back of above tunings is the result of the highest battery consumption.



2. SSID Settings

	2008	2009
SSID Settings		
Proportion of Default SSID	31.51%	13.47%
Proportion of Hidden SSID	8.26%	13.49%
Proportion of Well-known Hotspot SSID	9.45%	6.41%
Proportion of other SSID setting	50.78%	66.63%
Total:	**100%**	**100%**

As for the handling of SSID, about 14% of users have not changed the default SSID and this may mean other system settings are also not changed (including the administrator password). The overall SSID settings are much better computer with last year. Although this is much better by comparing with last year's status, we still suggest enabling the hidden SSID function and change SSID not to associate your identity/name that can help reduce the chance of being hacked.

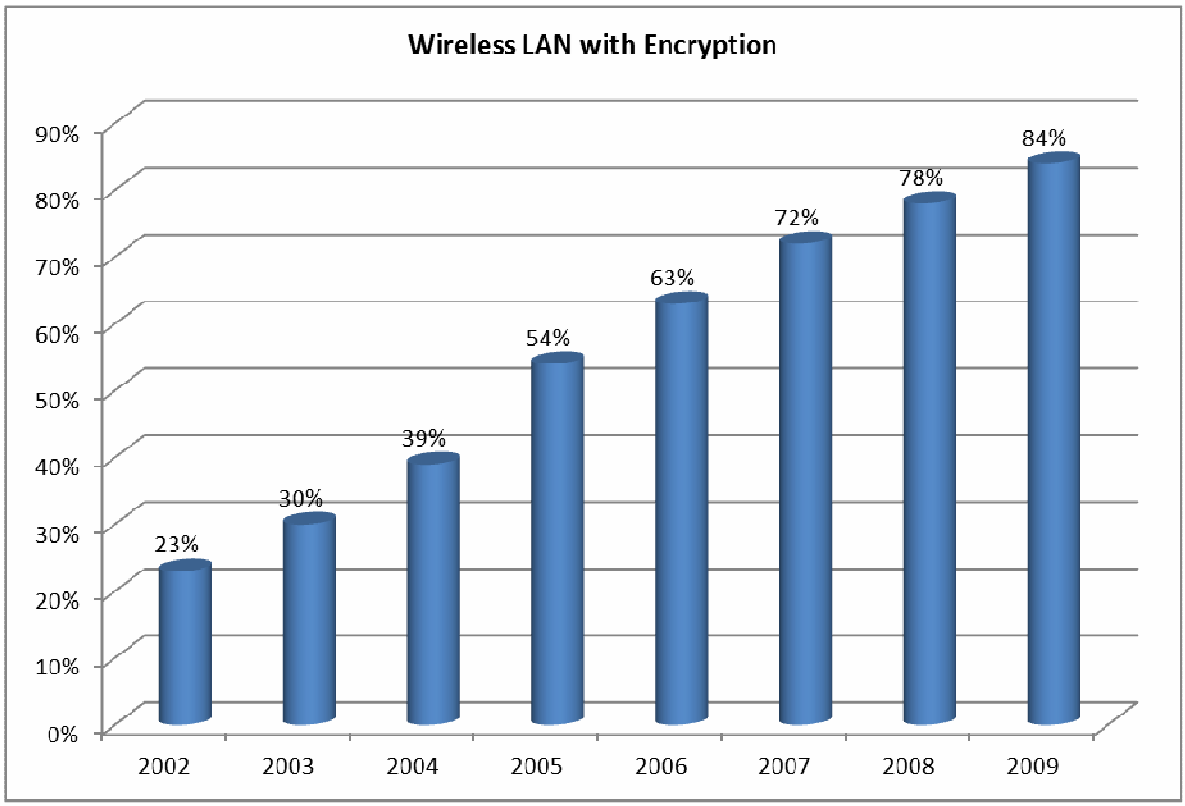


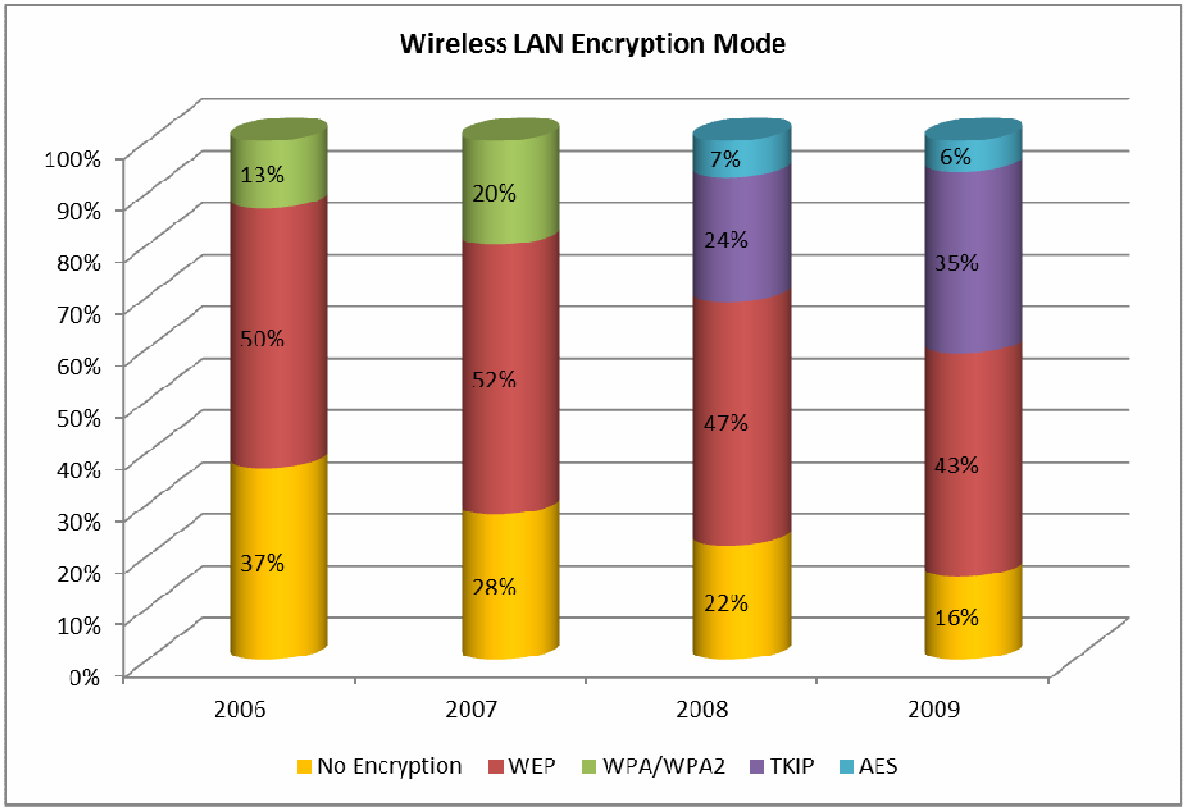
3. Encryption Settings

	2008	2009
Encryption Settings		
No Encryption	**22.35%**	**16.42%**
WEP	**46.48%**	**43.18%**
WPA	**23.61%**	**20.82%**
WPA Personal using TKIP	14.45%	10.80%
WPA Personal using AES	2.15%	1.12%
WPA Enterprise using TKIP	6.97%	8.89%
WPA Enterprise using AES	0.04%	0.00%
WPA2	**7.56%**	**19.58%**
WPA2 Personal using TKIP	2.54%	11.63%
WPA2 Personal using AES	4.62%	4.66%
WPA2 Enterprise using TKIP	0.16%	3.06%
WPA2 Enterprise using AES	0.24%	0.23%
Total:	**100%**	**100%**

By observation above, it can be seen that the WPA2's adoption is higher. 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 6% is using the most secure method – AES. This figure is dropped.

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 6% WLAN is adopting this highly secured encryption mode).





Conclusion

Hong Kong War Driving 2009

- Recommend adopting AES under the WPA/WPA2 encryption mode
    - The percentage of AP with encryption enabled was 85% and was improving as compared to previous years.
    - 43% 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 34.08% of discovered Access Points using this encryption in WPA or WPA2.
    - Only 6% of total discovered Access Points are using the most secure encryption method – CCMP/AES.
- As for the handling of SSID, about 14% of users have not changed the default SSID and this may mean other system settings are also not changed (including the administrator password). 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.

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
Charles Mok	Member	Professional Information Security Association
Eric Leung	Member	Hong Kong Wireless Technology Industry Association
Eric Lo	Member	Hong Kong Wireless Technology Industry Association
Frank Chow	Member	Professional Information Security Association
Jacky Tsoi	Member	Professional Information Security Association
Jim Shek	Member	Professional Information Security Association
Joseph Leung	Member	Hong Kong Wireless Technology Industry Association
Lawrence	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
Warren Kwok	Member	Professional Information Security Association
WS Lam	Member	Professional Information Security Association

* * * The End * * *