



# Report on

## Wireless LAN War Driving Survey 2014

### Hong Kong

Version 0.3  
November 2015

This report is produced for the event SafeWiFi 2014 and 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



<http://www.ofca.gov.hk>



香港特別行政區政府  
政府資訊科技總監辦公室  
Office of the Government  
Chief Information Officer  
The Government of the HKSAR

<http://www.ogcio.gov.hk>

**Copyright**

PISA and WTIA owns the right to of using this material.

PISA and WTIA owns the copyright of this material. All rights reserved by PISA and WTIA.

A third party can use this material for non-commercial purpose, given that no change in the meaning or interpretation of the content is made and citations are made to PISA and WTIA.

**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 systems 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 the test and implementation, please refer to other technical references.

## Report on Wireless LAN War Driving Survey 2014 Hong Kong - Editorial Board

Dr. Ken FONG

### Acknowledgements

Name	Organization
Mr. Alan HO - Convenor	PISA
Dr. Ken FONG - Convenor	WTIA
Mr. Owen Wong	Chief Systems Manager, Office of the Government Chief Information Officer, HKSAR
Mr. Charles MOK	Legislative Councillor (I.T.), HKSAR
Mr. Eric FAN - Event Management	PISA / WTIA
Mr. Sang YOUNG - Technical in charge	PISA / WTIA
Mr. Andy HO	PISA
Mr. Billy TSE	WTIA
Mr. Eric LEUNG	WTIA
Mr. Frankie WONG	PISA
Mr. Otto LEE	PISA
Mr. Jacky Cheng	WTIA
Mr. Mike Lo	PISA
Mr. Calvin Yung	PISA
Chan Kwok Fai	IVE (Chai Wan)
Chau Chun Yip	IVE (Chai Wan)
Hang Ching Nam	IVE (Chai Wan)
Lam Tak Ho	IVE (Chai Wan)
Tai Ching Pong	IVE (Chai Wan)
Tung Ka Lok	IVE (Chai Wan)
Wong Wai Nam	IVE (Chai Wan)
Yuen Man Ho	IVE (Chai Wan)
Chan Ka Leong	IVE (Chai Wan)
Wong Ho Cheung	IVE (Chai Wan)

Photos



War Traming 2014@2014-12-21



War-driving (Victoria Peak) 2014@2015-6-27

## Terms Used

WLAN	Wireless Local Area Network. There are five popular standards now: <ul style="list-style-type: none"><li>• 802.11a: using 5GHz, 54Mbps</li><li>• 802.11b: using 2.4GHz, 11Mbps</li><li>• 802.11g: using 2.4GHz, 54Mbps</li><li>• 802.11n: using 2.4GHz or 5GHz, 300Mbps</li><li>• 802.11ac: using 5GHz, 1.69Gbps</li></ul>
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 communication "hub" for wireless clients. In SME or home, it is also referred as Wi-Fi 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.

WPS Wi-Fi Protected Setup. It is a standard for user to setup up a secure wireless home network without understanding the details of security settings in a wireless LAN environment.

## Executive Summary

In Dec 2014, the two associations **PISA** and **WTIA** jointly conducted the “War Driving 2013” field survey along the classic tramway of Hong Kong Island and War Flying. In addition, we carried out the war driving for three (3) estates and War Sailing in year 2015. This survey is also part of the “SafeWiFi.hk” program. The objective of this survey is 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 conducted successfully. The results were benchmarked against that of the previous studies conducted by PISA and WTIA since 2002 to plot the profile of Hong Kong WLAN security development. The survey indicated that the adoption of secure WLAN keeps on increasing slightly. Although the index is decreased, many Hotspots are installed now according to our observation to the collected data. It is common configuration of no encryption to Hotspot Wi-Fi access points.

The study was carried out in a non-intrusive and responsible way. It provides the abstracted view on the security status of WLANs in Hong Kong. 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.

The Hong Kong WLAN Security Index is decreased from 75 of 2013 to **63** of 2014.



## Introduction

In 2002, a team of **PISA** Wi-Fi investigators performed the city's first "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 2014, **PISA** and **WTIA** conducted the 13th "War Driving" again to benchmark the improvement for the WLAN Security in Hong Kong. In addition, we conducted the "War Driving" at 3 types of estate in order to understand the security situation with respect to the characteristics of estates. And also, the "War Driving" in the Peak.

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

## Objectives of this 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 the 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 Wi-Fi security and follow up with education programs

*\* The study involved **neither sniffing of data nor jamming of network traffic**. The tool used was mainly for the discovery of wireless network broadcasted signals. No association with access points and no network connection were attempted during the war driving study and no data user data was captured. Every participant agreed and endorsed the Code of Ethics which is documented in the next section.*

## Code of Ethics

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

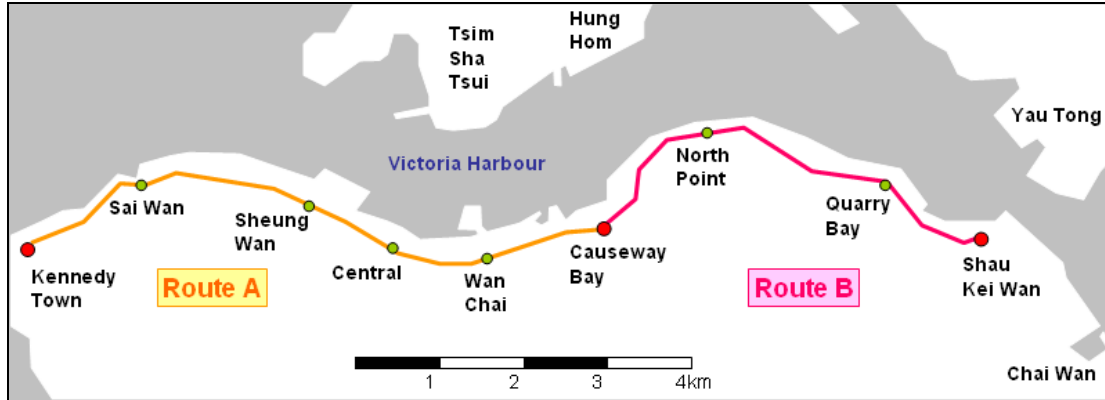
- Our objectives of the War Driving are to study the WLAN security status and compare it with the previous results, and to arouse the public awareness in WLAN security.
- We do not publicize the exact location and identity (e.g. SSID and MAC address) of any discovered AP. If such information appears in photos or other forms, it will be fully masked.
- We do not connect to the IP network of any insecure AP to further exploit its vulnerabilities.
- We do not interfere / jam any wireless traffic.
- We do not capture or collect any WLAN traffic payloads or data.
- 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 a 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 conducted since year 2003 along the tramway from Kennedy Town to Shau Kei Wan. This route was equivalent to the whole business corridor of the Hong Kong Island

Details:	
Date:	21 Dec, 2013 (Sunday)
Time:	10 am – 2 pm
Equipments:	<i>Hardware:</i> <ul style="list-style-type: none"><li>• Notebook computers</li><li>• WLAN cards (internal and external)</li><li>• Antennae (built-in and external +12dbi)</li><li>• GPS</li><li>• Android Tablet/Phone</li></ul> <i>Software:</i> <ul style="list-style-type: none"><li>• WigleWifi Wardriving for Android OS (<a href="https://play.google.com/store/apps/details?id=net.wigle.wigleandroid">https://play.google.com/store/apps/details?id=net.wigle.wigleandroid</a>)</li><li>• Vistumbler for Windows 7 and Vista Platforms (<a href="http://www.vistumbler.net">http://www.vistumbler.net</a>)</li></ul>
Route:	Tramway from Kennedy Town to Shau Kei Wan



### Estates War Driving

This year, PISA and WTIA conducted the “War Driving” on three (3) estates in Hong Kong in March of 2014. The objective of this exercise is to identify if any significant deviation of encryption usage by comparing to the exercise we did by using Tram.

The demographic information of these estates is as follow:

Type	Demographic Information
Estate A	<ul style="list-style-type: none"> <li>• Private Housing Estate</li> <li>• 61 Residential Towers</li> <li>• Total 12,698 apartment flats</li> <li>• Completion since 1977</li> <li>• Middle-class population</li> </ul>
Estate B	<ul style="list-style-type: none"> <li>• Home Ownership Scheme</li> <li>• 12 Residential Blocks</li> <li>• Total 4,200 apartment flats</li> <li>• Completion since 1993</li> </ul>
Estate C	<ul style="list-style-type: none"> <li>• Public Housing Estate</li> <li>• 9 Residential Buildings</li> <li>• Total 3,129 apartment flats</li> <li>• Completion since 1963</li> </ul>

## Findings and Analysis - Tramway

### Tramway War Driving 2014 Snapshots

Number of Access Points Captured	24,977
Access Points <b>without</b> using <b>Encryption</b>	5,809 (23.26%)
Access Points <b>without securing</b> the <b>SSID</b> <i>(include default SSID, SSID same as trailing hexadecimal of AP's MAC address, hotspots etc)</i>	5,217 (20.89%)

### 2014 Result Compared with Previous Years

The following table contains the result of whole tramway from year 2003 to year 2013.

Date of Test	Weather Condition	Number of Total Access Points	% of No Encryption	% of Insecure SSIDs
21 Dec 2014	Sunny	24,977	23.26% ↓	20.89% ↓
22 Dec 2013	Sunny	28,478	15.31% ↓	11.38% ↓
2 Dec 2012	Cloudy with a few rain patches	39,074	11.26% ↑	5.73% ↑
18 Dec 2011	Fine & Dry	16,618	12.12% ↑	9.09% ↑
5 Dec 2010	Sunny	16,462	13.64% ↑	13.40% ↓
26 Nov 2009	Sunny	15,753	15.50% ↑	11.57% ↑
9 Nov 2008	Trace Raining	7,388	19.26% ↑	20.41% ↑
4 Nov 2007	Sunny	6,662	27.50% ↑	30.29% ↑
15 Oct 2006	Occasional Raining	4,344	37.04% ↑	44.01% ↓
4 Dec 2005	Sunny	2,650	46.08% ↑	12.98% ↑
28 Nov 2004	Sunny	1,723	61.00% ↑	46.00% ↓
5 Oct 2003	Sunny	784	70.00%	43.00%

#### Legend

↑: Improved from security point of view

↓: Unsatisfied from security point of view

## Highlights

1. The number of detectable deployment along the tramway, comparing with last year, decreased by **12.29%**. The main reason is that we mainly relied on the Android Tablet and the overall processing power was decreased.
2. The percentage of APs with encryption turned on decreased by **7.95%**.
3. The percentage of APs with SSID secured decreased by **9.51%**.
4. From point 2 and 3, the overall security is worse than previous year. One of observation is that there are many hotspots from service provider. It causes the number of insecure SSID and non-encrypted APs increasing. It is estimated that there around 28.5% of detected Access Points are hotspot.

## Encryption Usages

The figures below cover the encryption usages break down comparing with last few years. Before 2008, we use Netstumbler as the war-driving tool which cannot distinguish between WEP, WPA and WPA2. Therefore, the comparison is starting from year 2008.

### WEP, WPA and WPA2 Usage Distribution

	2008	2009	2010	2011	2012	2013	2014
<b>Encryption Type</b>	%	%	%	%	%	%	%
No Encryption	22.86	15.50	13.64	12.12	11.26	15.31	23.26
WEP	43.18	45.01	34.05	24.66	15.47	13.27	5.75
WPA Personal using TKIP	13.53	11.65	13.53	11.98	15.43	9.62	20.67
WPA Personal using AES	1.02	0.91	1.94	2.05	3.66	2.96	9.27
WPA Enterprise using TKIP	11.76	7.31	5.92	5.72	1.14	0.64	3.13
WPA Enterprise using AES	0.03	0.02	0.02	0.01	0.1	0.04	0.31
WPA2 Personal using TKIP	3.26	10.90	7.39	10.06	1.81	1.76	4.18
WPA2 Personal using AES	3.31	5.10	19.21	29.4	41.7	47.33	27.02
WPA2 Enterprise using TKIP	0.62	3.07	0.92	1.73	0.01	0.01	0.12

	2008	2009	2010	2011	2012	2013	2014
WPA2 Enterprise using AES	0.43	0.53	3.38	2.27	9.42	9.06	6.29
<b>Total:</b>	<b>100</b>	<b>100</b>	<b>100</b>	<b>100</b>	<b>100</b>	<b>100</b>	<b>100</b>

The usages of WEP, WPA, and WPA2 are 13.27%, 13.26% and 58.16% in year 2013 while the usages of these are 5.75%, 33.38% and 37.61% in year 2014. Although the overall use of encryption is decreased this year, the use of WEP is dropping significantly while the WPA is increasing. It could be the phenomena of home routers were replaced. The suggested encryption of new routers is configured to automatic mode. It means supporting both WPA and WPA2 simultaneously. This is the reason of the decrease of WEP and increase of WPA mode.

#### TKIP and AES Distribution

	2008	2009	2010	2011	2012	2013	2014
<b>Encryption Type</b>	<b>%</b>	<b>%</b>	<b>%</b>	<b>%</b>	<b>%</b>	<b>%</b>	<b>%</b>
No Encryption	22.86	15.50	13.64	12.12	11.26	15.31	23.26
WEP	43.18	45.01	34.05	24.66	15.47	13.27	5.75
WPA/WPA2 using TKIP	29.17	32.93	27.76	29.49	18.39	12.03	28.10
WPA/WPA2 using AES	4.79	6.56	24.55	33.74	54.88	59.39	42.89
<b>Total:</b>	<b>100</b>	<b>100</b>	<b>100</b>	<b>100</b>	<b>100</b>	<b>100</b>	<b>100</b>

From another point of view, the adoption of more secure encryption methods (i.e. AES) increases from 59.39% to 42.89%.

#### WPS Usage

Wi-Fi Protected Setup (WPS) is a computing standard that attempts to allow easy establishment of a secure wireless home network. A major security flaw was revealed in December 2011 that affects wireless routers with the WPS feature. In this year, we also aim to indentify the potential risk of WPS by also discovering the amount of WPS turn-on on the discovered AP.

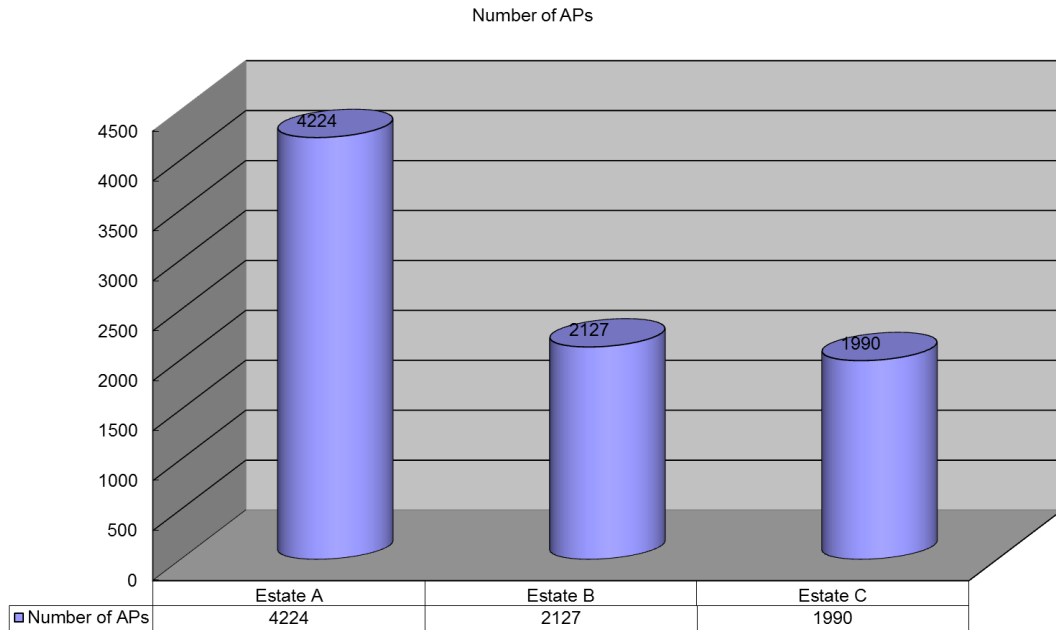
	2012	2013	2014
<b>WPS Usage</b>	39.82%	34.67%	34.08%



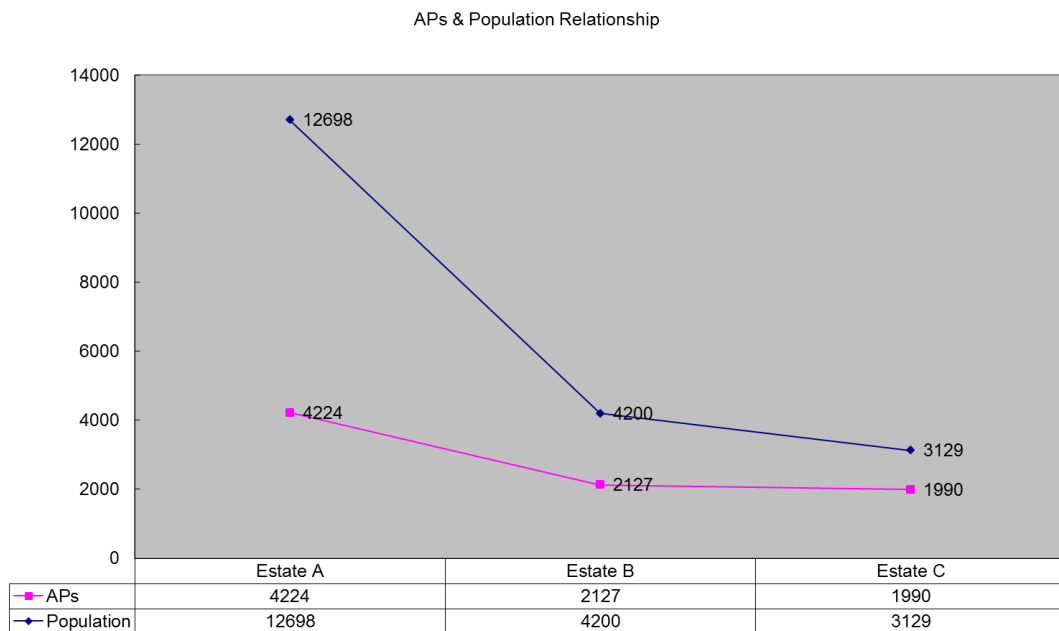
It is observed that there is slightly improved in the adoption of disable WPS feature.

## Findings and Analysis - Estates

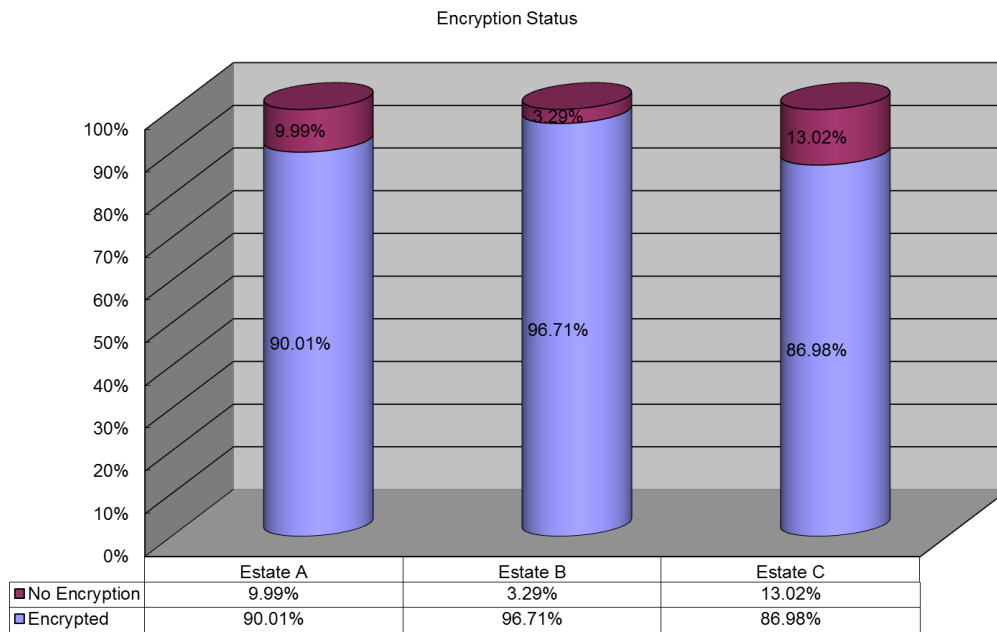
### 1. Number of Unique AP Captured



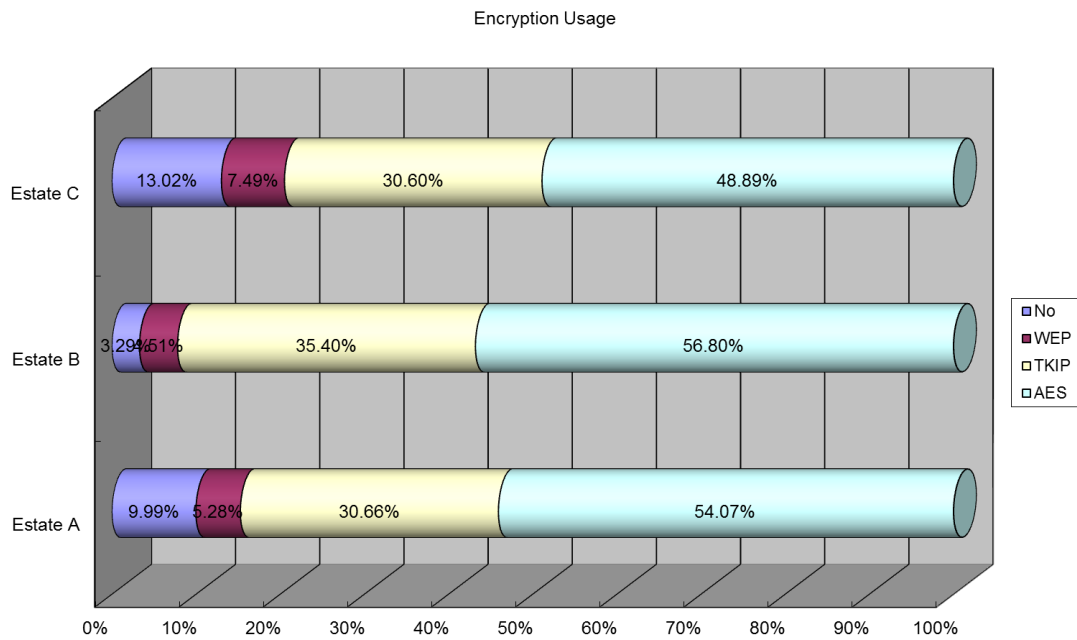
### 2. Relationship between population and number of discovered Access Points



### 3. Encryption Status



### 4. Encryption Usage



## 5. Comparison with Previous Years

We did a similar exercise since year 2010. Below is the comparison in areas including the Number of Access Points, Encryption Status, and Encryption Usage.

### 5.1 Number of Unique Access Points Captured




	2010	2011	2012	2013	2014	Remarks
Estate A	3,261	2626	3364	3072	4224	
Estate B	1,417	1952	2838	1315	2127	
Estate C	382	565	1057	1308	1990	

### 5.2 Encryption Status (No Encryption)

	2010	2011	2012	2013	2014	Remarks
Estate A	6.75%	9.94%	7.22%	7.55%	9.99%	2.44% more with no encryption 🚩
Estate B	9.95%	7.07%	4.90%	5.78%	3.29%	Improved
Estate C	10.99%	11.50%	5.77%	11.09%	13.02%	1.93% more with no encryption 🚩

### 5.3 Encryption Usage

	2010	2011	2012	2013	2014	Remarks
<b>Estate A</b>						
No	6.75%	9.94%	7.22%	7.55%	9.99%	Security Degraded 🚩
WEP	34.38%	24.89%	16.56%	8.79%	5.28%	Security Improved 🟢
TKIP	15.37%	15.87%	13.91%	33.59%	30.66%	Security Improved 🟢
AES	43.5%	49.30%	62.31%	50.07%	54.07%	Security Improved 🟢
<b>Estate B</b>						
No	9.95%	7.07%	4.90%	5.78%	3.29%	Security Improved 🟢
WEP	34.02%	26.54%	21.21%	9.66%	4.51%	Security Improved 🟢
TKIP	20.32%	17.73%	17.94%	35.21%	35.40%	No preferred setting, Security Degraded 🚩
AES	35.71%	48.66%	55.95%	49.35%	56.80%	Security Improved 🟢
<b>Estate C</b>						
No	10.99%	11.50%	5.77%	11.09%	13.02%	Security Degraded 🚩

<b>WEP</b>	34.55%	20.01%	18.92%	12.61%	7.49%	Security Improved 
<b>TKIP</b>	21.21%	16.80%	21.00%	18.27%	30.60%	Security Degraded 
<b>AES</b>	33.25%	51.69%	54.31%	58.03%	48.89%	Security Degraded 

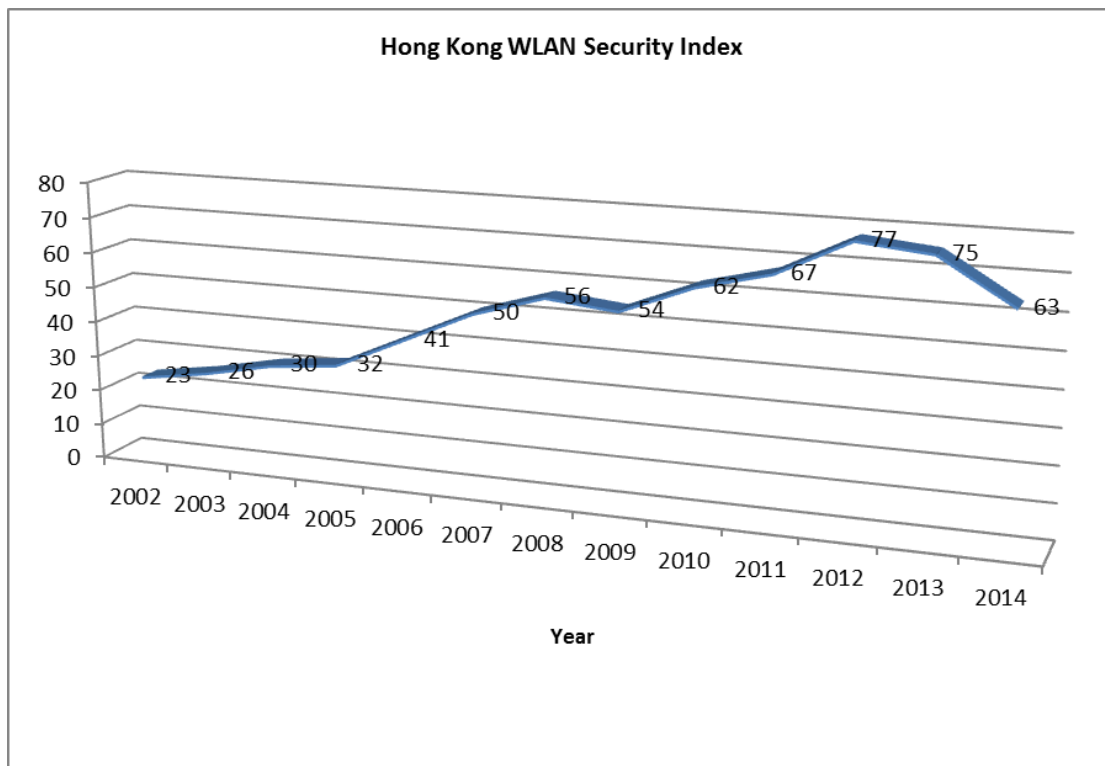
In terms of encryption, the AES would be the best choice at this moment. The use of AES in these estates is closed to 50% of the total APs. In addition, the use of WEP is dropping. It shows that the adoption of secure Wi-Fi networks, particular by home users, are improving in year 2014.

## 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), for analyzing data collected in War Driving surveys over the years.

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

PISA and WTIA maintain this Index to keep tracking on the implementation status in WLAN security in Hong Kong. Below is the graph representing the index from 2002 to 2014:



The index is dropped slightly in year 2013 due to the fact that more of “no encryption” access points discovered. Most of the contribution to “no encryption” is from Hotspot service provider.

## Analysis without the inclusion of public Hotspot

As most of public hotspot provides the non-encryption to Wi-Fi, we observed that there is about 28.5% of the collected Access Points are classified as Hotspot. In this section, we try to analysis the security status if public hotspots are excluded. The result is as follow:

- Number of Access Points: 17,866
- Number of Access Points with WPS enabled: 47.65%
- Access Points without Encryption: 8.74%
- Access Points with Encryption: 91.26% and the breakdown on the use of encryption technologies are:
  - WEP: 7.61%
  - TKIP: 34.65%
  - AES: 49%

By using this set of figure, using the AES is the favor to private Wi-Fi. Another observation is that many Access Points configured with WPS enable which is not a best practice for a secure Wi-Fi setting.

## Conclusion

### Tramway War Driving

- This year, data collected from Wigle using Android Phone/Tablet
- The use of WEP dropped significantly, from ~13% to ~6% this year. We can see a leap in the use of encryptions whereas the overall improvement in security is improved.
- **The percentage of Access Points with encryption enabled is around 85 percentages.**
- Large portion of APs are open in year 2014, due to the large number of AP Hotspots which provide no encryption. There are around 28.5% of discovered Access Points are Public hotspot which provides no encryption option for user.
- **The percentage of AP with WPS enabled is around 34.08 percentages.** There is known security vulnerability in WPS. It has **1.92%** improvement by comparing to last year. However, it still shows that around **most of WLANs are subjected to this attack.**

### Encryption Usages

- In recent year, WEP cracking methods are enhanced. It allows an intruder to penetrate to a WLAN using WEP cracking within 10 minutes of time. In our study, only around **6% of WLANs are still using WEP.**
- The adoption of WPA/WPA2 is improved **over 70%**. It shows the adoption of more secure encryption methods is increasing.
- In year 2008, there is a way to crack WPA using TKIP as an encryption algorithm. In our study, **28.10%** of WLANs are using TKIP.
- WEP is dropping significantly while TKIP is increasing drastically. It may be due to the case that the old Access Points were replaced but configured with **automatic selection of TKIP and CCMP (AES)**. We suggest enforcing the use of CCMP (AES) only.
- The adoption of more secure encryption methods – AES is decreased **from 59.39% to 42.89%.**

### Estate War Driving

- Number of discovered APs is directly related to the number of population.
- The percentage of using AES encryption is over 50% this year in our sampled three estates.

### WPS Usage

- **The percentage of AP with WPS enabled is around 35 percentages.** There is known security vulnerability in WPS. It has improvement but it still shows that large number of

**WLANs are subjected to this attack** in this area.

#### **Hong Kong WLAN Security Index**

- The Hong Kong WLAN Security Index of 2014 is 63 while the index of 2013 is 75. The index is dropped due to the facts that
  - large number of AP Hotspots which provide no encryption option to user.
  - percentage of TKIP is increasing.

#### **Overall Observation**

- The percentage of “no encryption” is increasing this year. It seems to be that the security adoption in Wi-Fi networks is worse than last year. However, when we investigate the raw data in details, we found that over 28.5% of Access Points are from Hotspot service providers in War Driving. Hotspot providers provide mixing authentication and encryption supports to users. This includes “No Encryption” configuration.
- If the hotspot Access Points are excluded, there is a slightly improvement. Only 8.74% of Wi-Fi networks are configured with no encryption. However, there are 47.65% of Wi-Fi networks are configured with WPS enable.