



# Report on

## Wireless LAN War Driving Survey 2015

### Hong Kong

Version 0.2  
September 2016

This report is produced for the event SafeWiFi 2015 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 2015 Hong Kong - Editorial Board

Dr. Ken FONG

### Acknowledgements

Name	Organization
Dr. Ken Fong - Convenor	WTIA
Mr. Roy Law – Convenor	WTIA
Mr Jason Pun	Chief Systems Manager (Digital Inclusion), Office of the Government Chief Information Officer
Mr. Eric Fan	PISA
Mr. Sang Young - Technical in charge	PISA / WTIA
Mr. Billy TSE	WTIA
Mr. Eric LEUNG	WTIA
Mr. Frankie WONG	PISA
Mr. Otto LEE	PISA
Mr. Jim Shek	PISA
Mr. Alan Ho	Valkyrie- X Security Research Group
Chan Chui Kwan	Advanced Diploma in Business Information Technology, HKU SPACE
Ng Po Yin	Advanced Diploma in Business Information Technology, HKU SPACE
Leung Ka Kiu	Advanced Diploma in Business Information Technology, HKU SPACE
Wong Ting Fung	Advanced Diploma in Business Information Technology, HKU SPACE

Photos



War Traming 2015@2015-12-06



War-driving 2015@2015-12-06

## 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 2015, the two associations **PISA** and **WTIA** jointly conducted the “War Driving 2015” 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 in year 2016. This survey is also part of the “SafeWiFi.hk” program. The objectives of this survey are to conduct a non-intrusive study on the status of Hong Kong WLAN security and arouse the public awareness in securing the use of Wi-Fi.

The field survey was conducted successfully with the help of volunteers engaged by two associations. The results were benchmarked against that of the previous studies conducted by PISA and WTIA since 2002 to plot the profile of Hong Kong Wi-Fi security development. The survey indicated that the adoption of secure WLAN keeps on increasing slightly.

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 Wi-Fi security strategies.

The Hong Kong WLAN Security Index is improved from 63 of 2014 to **71** of 2015.

## Introduction

In 2002, a team of **PISA** Wi-Fi investigators performed the city's first "War Driving" study on the Wireless LAN (a.k.a Wi-Fi) 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 primary scope of test was extended to:

- the whole tram way, covering the business corridor of the HK Island

In Dec 2015, **PISA** and **WTIA** conducted the 14th "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.

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
5. To observe if there is an interesting finding after collecting the information

*\* 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.

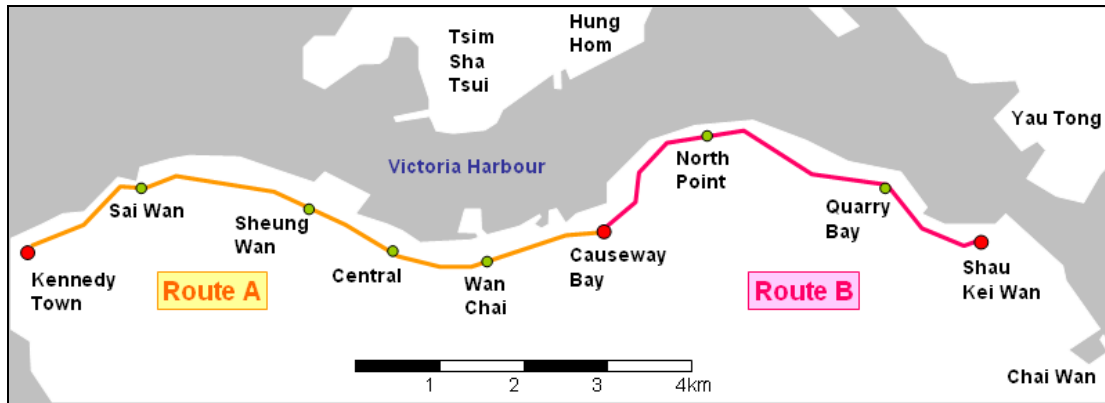
- Our objectives of the War Driving are to study the WLAN security status and compare it with the previous results, and to arouse the public awareness in WLAN security.
- We do not publicize the exact location and identity (e.g. SSID and MAC address) of any discovered AP. If such information appears 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:	
<b>Date:</b>	06 Dec, 2015 (Sunday)
<b>Time:</b>	10 am – 2 pm
<b>Equipments:</b>	<i>Hardware:</i> <ul style="list-style-type: none"><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></ul>
<b>Route:</b>	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 August 2016. 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 2015 Snapshots

Number of Access Points Captured	34,310
Access Points <b>without</b> using <b>Encryption</b>	5,772 (16.82%)
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>	2,399 (6.99%)

### 2015 Result Compared with Previous Years

The following table contains the result of whole tramway from year 2003 to year 2015.

Date of Test	Weather Condition	Number of Total Access Points	% of No Encryption	% of Insecure SSIDs
6 Dec 2015	Cloudy	34,310	16.82% <span style="color: green;">↑</span>	6.99% <span style="color: green;">↑</span>
21 Dec 2014	Sunny	24,977	23.26% <span style="color: red;">↓</span>	20.89% <span style="color: red;">↓</span>
22 Dec 2013	Sunny	28,478	15.31% <span style="color: red;">↓</span>	11.38% <span style="color: red;">↓</span>
2 Dec 2012	Cloudy with a few rain patches	39,074	11.26% <span style="color: green;">↑</span>	5.73% <span style="color: green;">↑</span>
18 Dec 2011	Fine & Dry	16,618	12.12% <span style="color: green;">↑</span>	9.09% <span style="color: green;">↑</span>
5 Dec 2010	Sunny	16,462	13.64% <span style="color: green;">↑</span>	13.40% <span style="color: red;">↓</span>
26 Nov 2009	Sunny	15,753	15.50% <span style="color: green;">↑</span>	11.57% <span style="color: green;">↑</span>
9 Nov 2008	Trace Raining	7,388	19.26% <span style="color: green;">↑</span>	20.41% <span style="color: green;">↑</span>
4 Nov 2007	Sunny	6,662	27.50% <span style="color: green;">↑</span>	30.29% <span style="color: green;">↑</span>
15 Oct 2006	Occasional Raining	4,344	37.04% <span style="color: green;">↑</span>	44.01% <span style="color: red;">↓</span>
4 Dec 2005	Sunny	2,650	46.08% <span style="color: green;">↑</span>	12.98% <span style="color: green;">↑</span>
28 Nov 2004	Sunny	1,723	61.00% <span style="color: green;">↑</span>	46.00% <span style="color: red;">↓</span>
5 Oct 2003	Sunny	784	70.00%	43.00%

Legend

↑: Improved from security point of view, compare with previous year

↓: Unsatisfied from security point of view, compare with previous year

### Highlights

1. The number of detectable deployment along the tramway, comparing with last year, improved by **37.37%**. The primary reason is that the Android Tablet is more powerful than those one used in year 2015.
2. The percentage of APs with encryption turned on improved by **6.44%**.
3. The percentage of APs with SSID secured improved by **13.9%**.
4. From point 2 and 3, the overall security is better than previous year.

### 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 with the introduction of new tools Vistumbler. Since 2014, the WigleWiFi for Android is used.

#### WEP, WPA and WPA2 Usage (expressed in %) Distribution

Year	No Encryption	WEP	WPA	WPA2
2015	16.82	5.84	33.81	43.53
2014	23.26	5.75	33.38	37.61
2013	15.31	13.27	13.26	58.16
2012	11.26	15.47	20.33	52.94
2011	12.12	24.66	19.76	43.46
2010	13.64	34.05	21.41	30.9
2009	15.50	45.01	19.89	19.6
2008	22.86	43.18	26.34	7.62

The usages of WEP, WPA, and WPA2 are 5.75%, 33.38% and 37.61% in year 2014 while the usages of these are **5.84%**, **33.81%** and **43.53%** in year 2015. The usage of WPA is still maintaining in high percentage. It could be the phenomena of routers were replaced and the suggested encryption of new routers is configured to automatic mode. It means supporting both WPA and WPA2 simultaneously.

TKIP and AES Usage (expressed in %) Distribution

Year	No Encryption	WEP	TKIP	AES
2015	16.82	5.84	26.79	50.55
2014	23.26	5.75	28.10	42.89
2013	15.31	13.27	12.03	59.39
2012	11.26	15.47	18.39	54.88
2011	12.12	24.66	29.49	33.73
2010	13.64	34.05	27.76	24.55
2009	15.50	45.01	32.93	6.56
2008	22.86	43.18	29.17	4.79

From another point of view, the adoption of more secure encryption methods (i.e. AES) increases from 42.89% to 50.55%.

WPS Usage

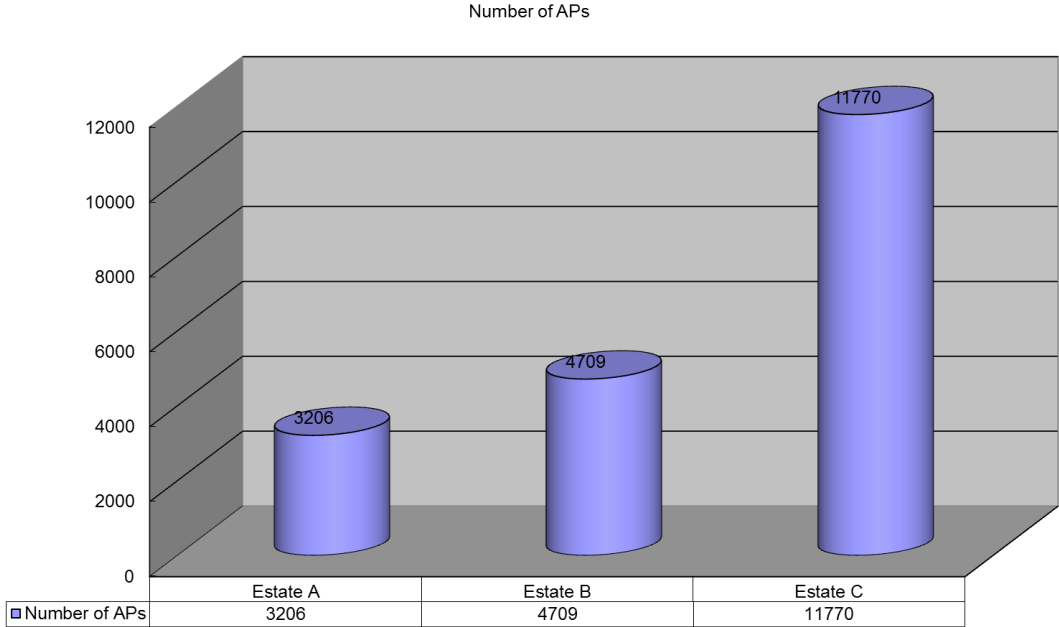
Wi-Fi Protected Setup (WPS) is a computing standard that attempts to allow easy establishment of a secure wireless home network. A major security flaw was revealed in December 2011 that affects wireless routers with the WPS feature. In this year, we also aim to indentify the potential risk of WPS by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

	2012	2013	2014	2015
<b>WPS Usage</b>	39.82%	34.67%	34.08%	28.82%

It is observed that there is some improvement in the adoption of disable WPS feature.

# Findings and Analysis - Estates

## 1. Number of Unique AP Captured

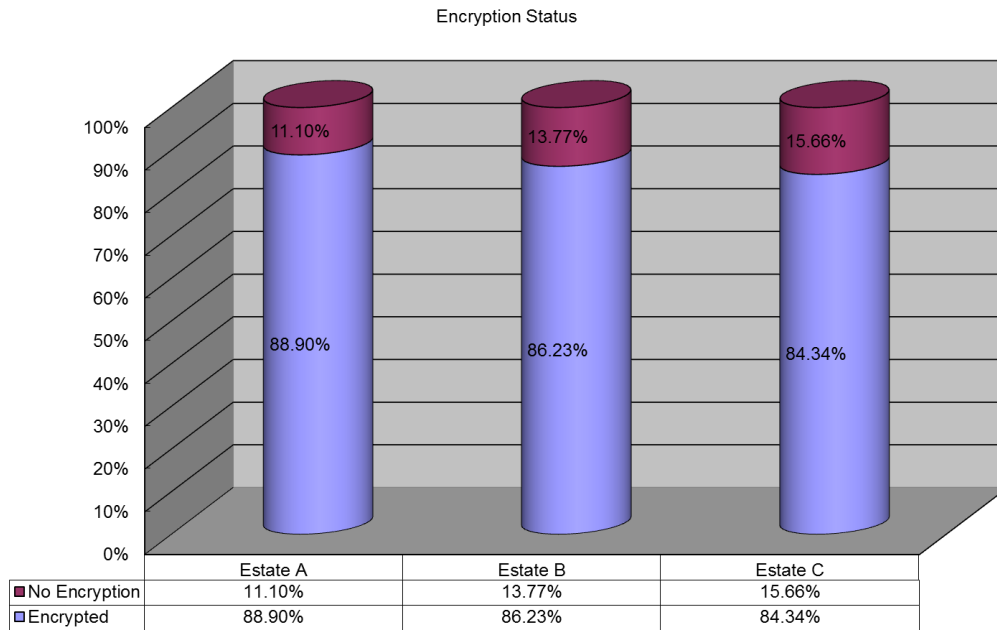


## 2. Relationship between population and number of discovered Access Points

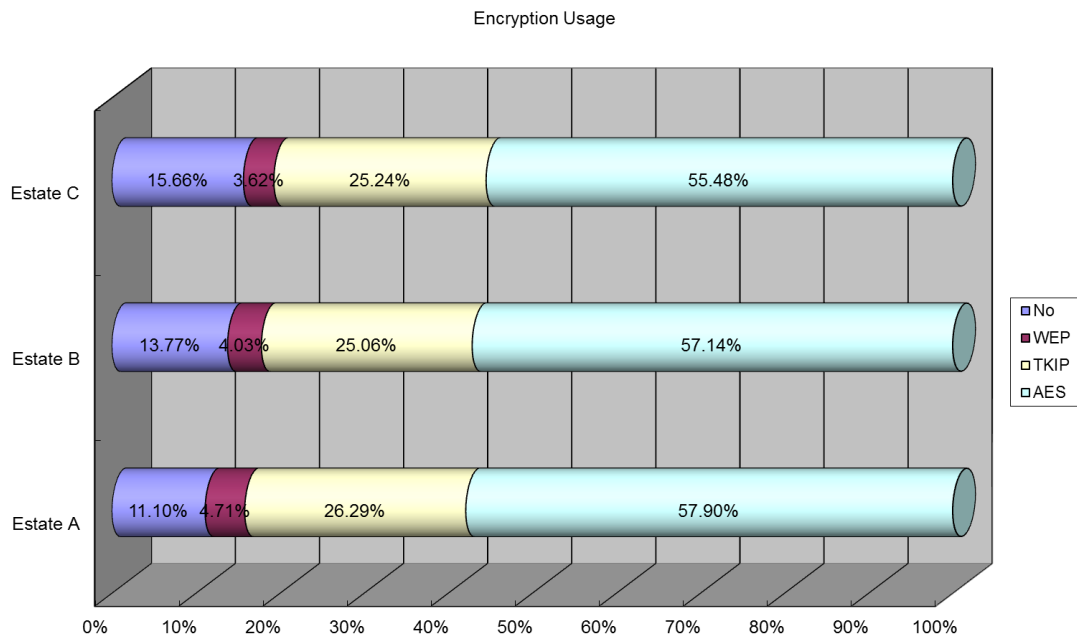




### 3. Encryption Status



### 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	2015	Remarks
Estate A	3261	2626	3364	3072	4224	3206	Nil
Estate B	1417	1952	2838	1315	2127	4709	Nil
Estate C	382	565	1057	1308	1990	11770	Nil

### 5.2 Encryption Status (No Encryption)

	2010	2011	2012	2013	2014	2015	Remarks
Estate A	6.75%	9.94%	7.22%	7.55%	9.99%	11.10%	🔴
Estate B	9.95%	7.07%	4.90%	5.78%	3.29%	13.77%	🔴
Estate C	10.99%	11.50%	5.77%	11.09%	13.02%	15.66%	🔴

### 5.3 Encryption Usage

	2010	2011	2012	2013	2014	2015	Remarks
<b>Estate A</b>							
No	6.75%	9.94%	7.22%	7.55%	9.99%	11.10%	Security Degraded 📉
WEP	34.38%	24.89%	16.56%	8.79%	5.28%	4.71%	Security Improved 📈
TKIP	15.37%	15.87%	13.91%	33.59%	30.66%	26.29%	Security Improved 📈
AES	43.5%	49.30%	62.31%	50.07%	54.07%	57.90%	Security Improved 📈
<b>Estate B</b>							
No	9.95%	7.07%	4.90%	5.78%	3.29%	13.77%	Security Degraded 📉
WEP	34.02%	26.54%	21.21%	9.66%	4.51%	4.03%	Security Improved 📈
TKIP	20.32%	17.73%	17.94%	35.21%	35.40%	25.06%	Security Improved 📈
AES	35.71%	48.66%	55.95%	49.35%	56.80%	57.14%	Security Improved 📈
<b>Estate C</b>							
No	10.99%	11.50%	5.77%	11.09%	13.02%	15.66%	Security Degraded 📉
WEP	34.55%	20.01%	18.92%	12.61%	7.49%	3.62%	Security Improved 📈

<b>TKIP</b>	21.21%	16.80%	21.00%	18.27%	30.60%	25.24%	Security Improved 
<b>AES</b>	33.25%	51.69%	54.31%	58.03%	48.89%	55.48%	Security Improved 

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 2015.

### Findings and Analysis - Field Experiment at Crowded Location

SSID of the Honey Spot	Free WiFi
Demographic Information	<ul style="list-style-type: none"> <li>- Public Space that freely accessible by locals and tourists</li> <li>- Estimated area: 5,724.71 m<sup>2</sup></li> </ul>
Time of the test	16:18 – 17:03
Recorded broadcast probe request	9,691
No. of unique client associated with the Honey Spot	4

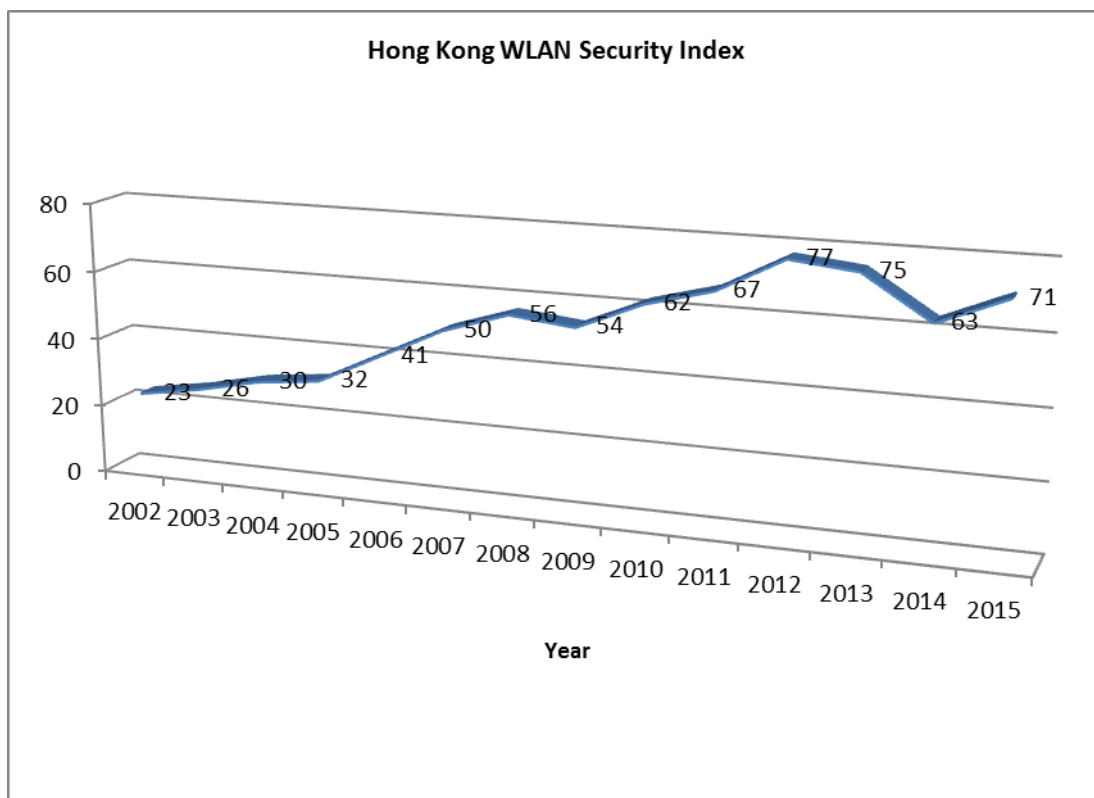
When performing the field experiment at the selected location, the unencrypted WiFi signal was broadcasted publicly with SSID “Free WiFi”. During the experiment, we have recorded 9,691 broadcast probe request in total. There were 4 unique clients connected to this Honey Spot. The results were satisfactory.

## 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 year 2002 to 2015:



The index is increased in year 2015, we are looking forward to seeing the improvement in next year.

## Conclusion

### Tramway War Driving

- This year, data collected from Wigle using Android Phone/Tablet
- The use of WEP maintains at around 6%, similar to last year. We shall keep on observing it if this figure is going to saturate.
- **The percentage of Access Points with encryption enabled is around 83 percentages, a slight increase.**
- Large portion of APs are open in year 2015, due to the large number of AP Hotspots which provide no encryption.
- **The percentage of AP with WPS enabled is dropping from 34.08 to 28.82 percentages.** There is known security vulnerability in WPS. It has some 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 77%**. 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, **26.76%** of WLANs are using TKIP although the figure decreased.
- WEP is dropping significantly while TKIP is increasing drastically since 2014. 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 increased **from 42.89% to 50.55%**. Improvement is indicated but it is not the best in our 14 year's study.

### Estate War Driving

- Number of discovered APs should directly relate to the number of population in the past, but there is a strange behavior in Estate 3. We shall observe again in the next year.
- 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 30 percentages.** There is known

security vulnerability in WPS. It has improvement but it still shows that large **WLANs are subjected to this attack** in this area.

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

- The Hong Kong WLAN Security Index of 2015 is 71 while the index of 2014 is 63. The index figure is going up again.

#### **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