Report on

Wireless LAN War Driving Survey 2013

Hong Kong

Version 0.5

May 2014

This report is produced for the event SafeWiFi 2013 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

通訊事務管理局
COMMUNICATIONS
AUTHORITY

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

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.

Acknowledgements

Name	Organization
Mr. Alan HO - Convenor	PISA
Dr. Ken FONG - Convenor	WTIA
Mr. T.Y. CHAN	Acting Assistant Director (Regulatory), Office of the Communications Authority
Mr. Charles MOK	Legislative Councillor (I.T.), HKSAR
Mr. Eric FAN - Event Management	WTIA
Mr. Sang YOUNG - Technical in charge	PISA / WTIA
Mr. Andy HO	PISA
Mr. Billy TSE	WTIA
Mr. Danny HUNG	PISA
Mr. Eric LEUNG	WTIA
Mr. Frankie WONG	PISA
Mr. Jacky CHENG	WTIA
Mr. Joseph LEUNG	WTIA
Mr. Kevin LEUNG	PISA
Mr. Otto LEE	PISA
Mr. Plucky YAU	PISA
Mr. Roy LAW	WTIA
Mr. SC LEUNG	PISA
Mr. Terry CHAN	WTIA
Mr. Thomas TSANG	PISA
Mr. Voker LAM	WTIA

War Traming 2013@2013-12-22

War Flying@2013-05-11
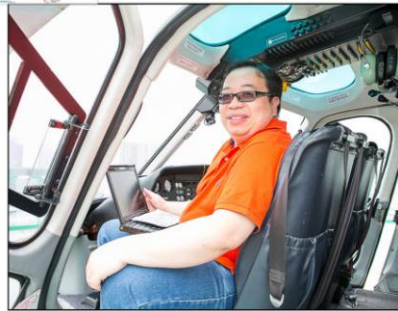
War Flying@2013-05-11

War Sailing@2014-03-26

Terms Used

WLAN	Wireless Local Area Network. There are five popular standards now: • 802.11a: using 5GHz, 54Mbps • 802.11b: using 2.4GHz, 11Mbps • 802.11g: using 2.4GHz, 54Mbps • 802.11n: using 2.4GHz or 5GHz, 300Mbps • 802.11ac: using 5GHz, 1.69Gbps
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 2013, 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 3 estates and War Sailing in year 2014. 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 very successful. 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, it is caused by a lot of Hotspots now by our observation to the collected data. The option of no encryption from Hotspots is a common configuration.

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 77 of 2012 to **75** of 2013.

Introduction

In 2002, a team of **PISA** Wi-Fi 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 2013, **PISA** and **WTIA** conducted the 12th "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 Sailing" in Victoria Harbour has been carried out to determine the characteristics at Sea.

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:	22 Dec, 2013 (Sunday)
Time:	10 am – 2 pm
Equipments:	*Hardware:* - Notebook computers - WLAN cards (internal and external) - Antennae (built-in and external +12dbi) - GPS - Android Tablet/Phone *Software:* - Vistumbler for Windows 7 and Vista Platforms (http://www.vistumbler.net) - WigleWifi Wardriving for Android OS (https://play.google.com/store/apps/details?id=net.wigle.wigleandroid)
Route:	Tramway from Kennedy Town to Shau Kei Wan
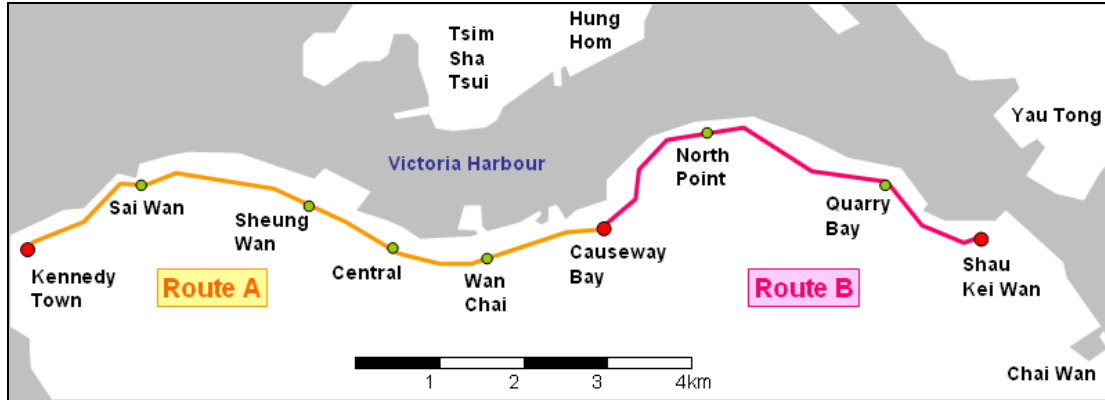
Estates War Driving

This year, PISA and WTIA conducted the "War Driving" on three (3) estates in Hong Kong within the March of 2013. 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	- Private Housing Estate 61 Residential Towers - Total 12,698 apartment flats - Completion since 1977 - Middle-class population
Estate B	- Home Ownership Scheme 12 Residential Blocks - Total 4,200 apartment flats - Completion since 1993
Estate C	- Public Housing Estate 9 Residential Buildings - Total 3,129 apartment flats - Completion since 1963

War Flying

On 11 May 2013, we conducted the second WLAN Security Survey from Air by using the

Helicopter. 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. This part of Access Points cannot be recognized by using Tram and Walking in the Estates.

With the limitation of flying time of half an hour, we try to cover the area including Hong Kong Island, Kowloon and New Territories business and residential building. The flying cruise is as shown below:
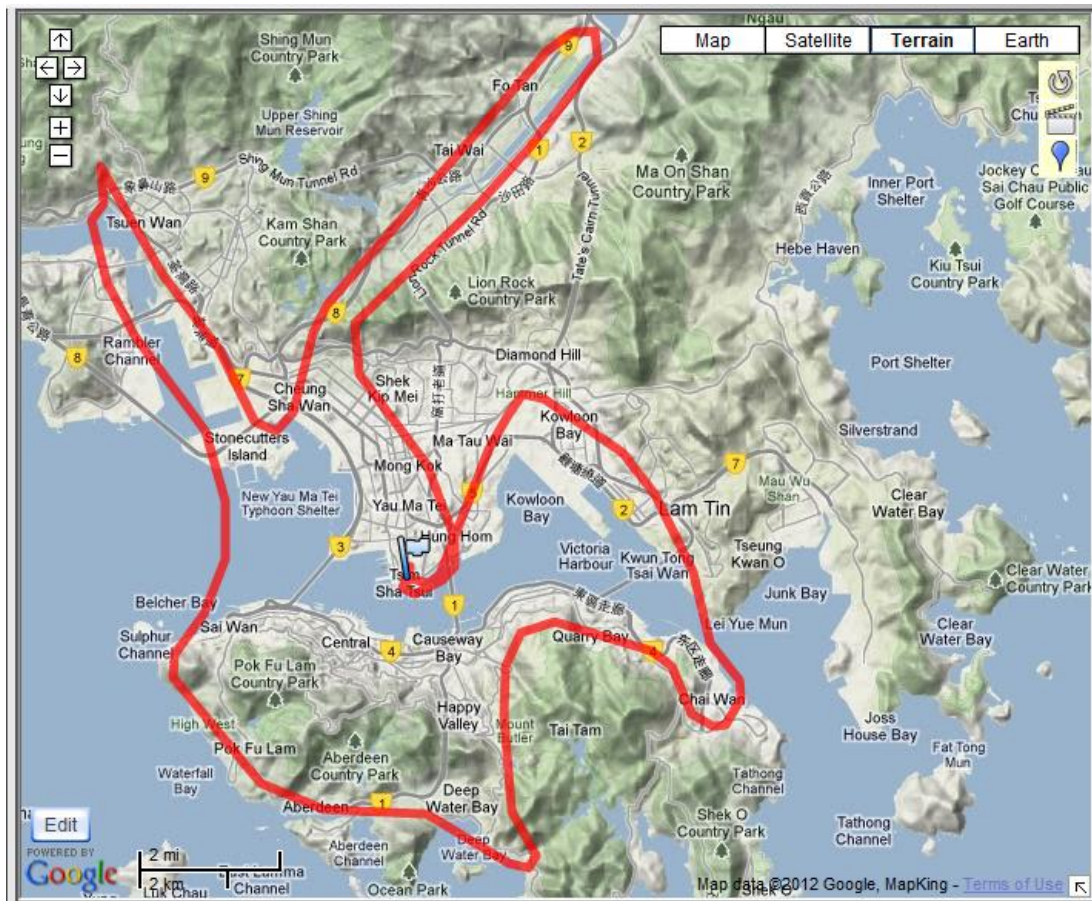
War Sailing

On 26 Mar 2014, we conducted the "War Sailing" by using Harbour Tour service from The "Star" Ferry Company. The coverage area is shown in the following map.

Tramway War Driving 2013 Snapshots

Number of Access Points Captured	28,478
Access Points without using Encryption	4,360 (15.31%)
Access Points without securing the SSID *(include default SSID, SSID same as trailing hexadecimal of AP's MAC address, hotspots etc)*	3,241 (11.38%)
Access Points using 802.11b	81 (0.28%)

2013 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
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 27.2%. The main reason is that we decreased the number of machines and the overall processing power was decreased.
2. The percentage of APs with encryption turned on decreased by 4.05%.
3. The percentage of APs with SSID secured decreased by 5.65%.
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.

Encryption Usages

Vistumbler allow us to run the War Driving under Vista and Windows 7 computers. The figures below cover the encryption usages break down comparing with last few years.

WEP, WPA and WPA2 Usage Distribution

	2008	**2009**	**2010**	**2011**	**2012**	**2013**
Encryption Type	%	%	%	%	%	%
No Encryption	22.86	15.50	13.64	12.12	11.26	15.31
WEP	43.18	45.01	34.05	24.66	15.47	13.27
WPA Personal using TKIP	13.53	11.65	13.53	11.98	15.43	9.62
WPA Personal using AES	1.02	0.91	1.94	2.05	3.66	2.96
WPA Enterprise using TKIP	11.76	7.31	5.92	5.72	1.14	0.64
WPA Enterprise using AES	0.03	0.02	0.02	0.01	0.1	0.04
WPA2 Personal using TKIP	3.26	10.90	7.39	10.06	1.81	1.76
WPA2 Personal using AES	3.31	5.10	19.21	29.4	41.7	47.33
WPA2 Enterprise using TKIP	0.62	3.07	0.92	1.73	0.01	0.01
WPA2 Enterprise	0.43	0.53	3.38	2.27	9.42	9.06

	2008	2009	2010	2011	2012	2013
using AES						
Total:	100	100	100	100	100	100

The usages of WEP, WPA, and WPA2 are 15.47%, 20.33% and 52.94% in year 2012 while the usages of these are 13.27%, 13.26% and 58.16% in year 2013. Although the overall use of encryption is decreased this year, the secure methods – WPA and WPA2 is closed to last year.

TKIP and AES Distribution

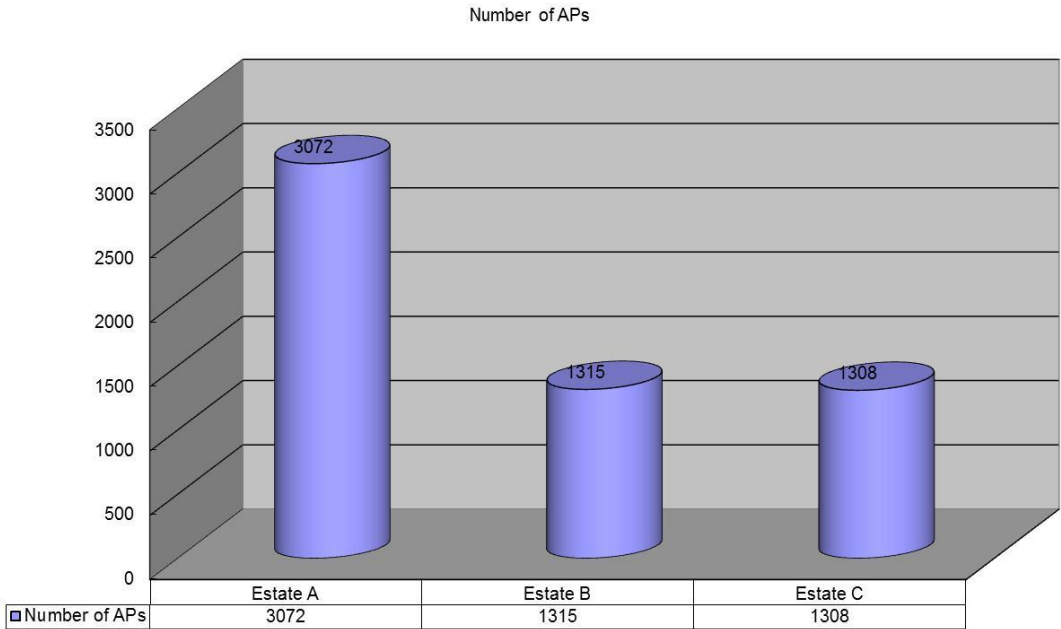|	2008	2009	2010	2011	2012	2013
Encryption Type	%	%	%	%	%	%
No Encryption	22.86	15.50	13.64	12.12	11.26	15.31
WEP	43.18	45.01	34.05	24.66	15.47	13.27
WPA/WPA2 using TKIP	29.17	32.93	27.76	29.49	18.39	12.03
WPA/WPA2 using AES	4.79	6.56	24.55	33.74	54.88	59.39
Total:	100	100	100	100	100	100

From another point of view, the adoption of more secure encryption methods (i.e. AES) increases from 54.88% to 59.39%. Although the overall use of encryption is decreased, the more preferred encryption – AES is improved by 4.51%.
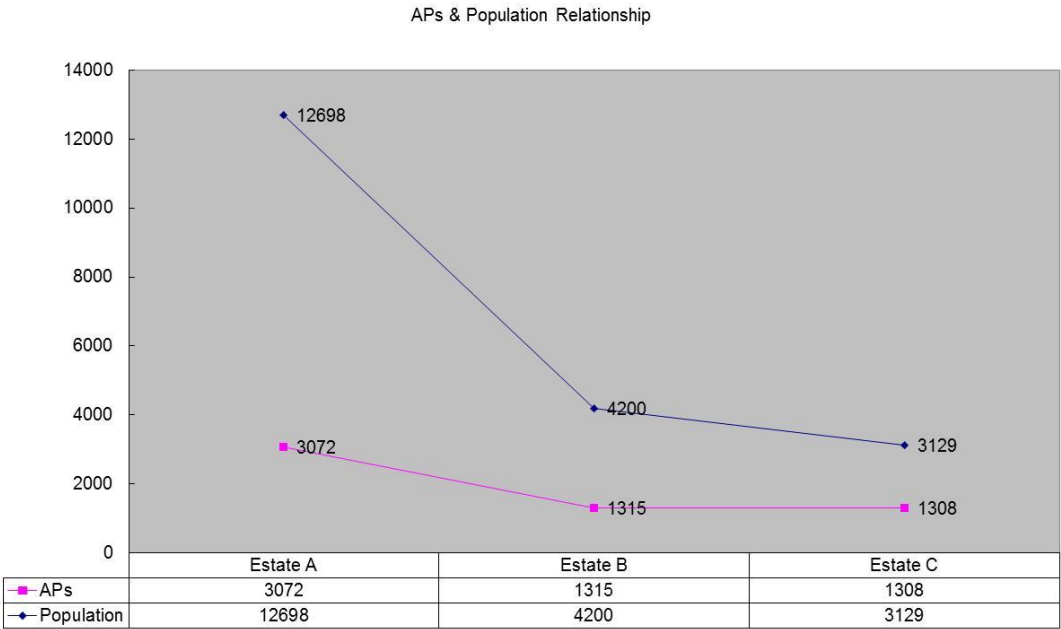
WPS Usage (Experimental)

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.   However, Vistumbler cannot determine if the target Access Point enabling WPS or not. Therefore, we try to test the WPS features for the target Access Point by using "WigleWifi Wardriving for Android OS". **The percentage of enabling WPS of total Access Points is 34.67%** for year 2013. By comparing the last year's figure - 39.82%. There is an improvement of **5.15%**.

1. Number of Unique AP Captured

Number of APs

	Estate A	Estate B	Estate C
Number of APs	3072	1315	1308

2. Relationship between population and number of discovered Access Points

APs & Population Relationship

	Estate A	Estate B	Estate C
APs	3072	1315	1308
Population	12698	4200	3129

3. Encryption Status

Encryption Status

	Estate A	Estate B	Estate C
No Encryption	7.55%	5.78%	11.09%
Encrypted	92.45%	94.22%	88.91%

4. Encryption Usage

Encryption Usage

Estate C: No 11.09%, WEP 12.61%, TKIP 18.27%, AES 58.03%

Estate B: No 5.78%, WEP 9.66%, TKIP 35.21%, AES 49.35%

Estate A: No 7.55%, WEP 8.79%, TKIP 33.59%, AES 50.07%
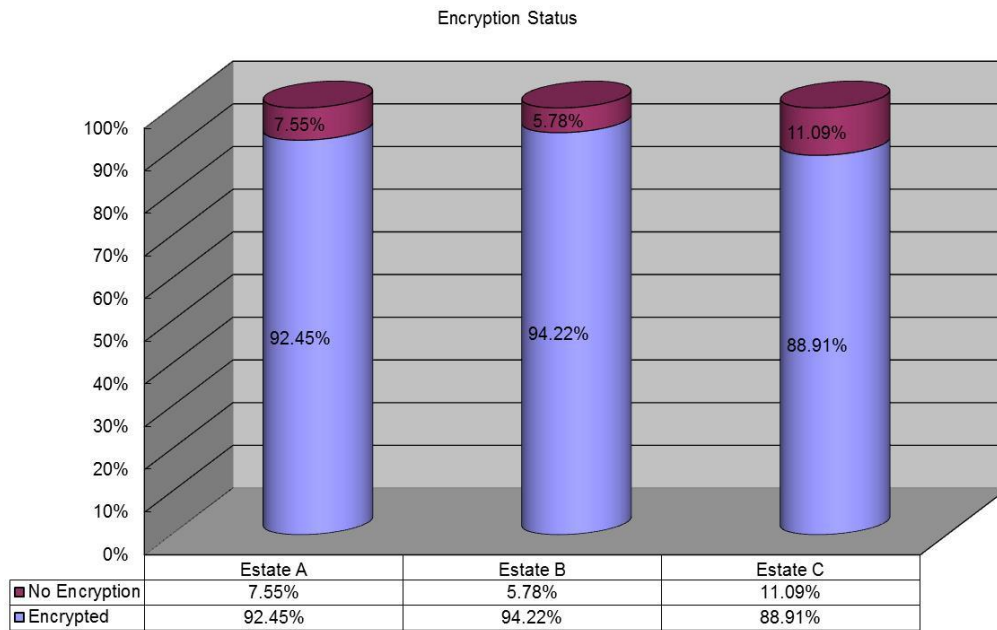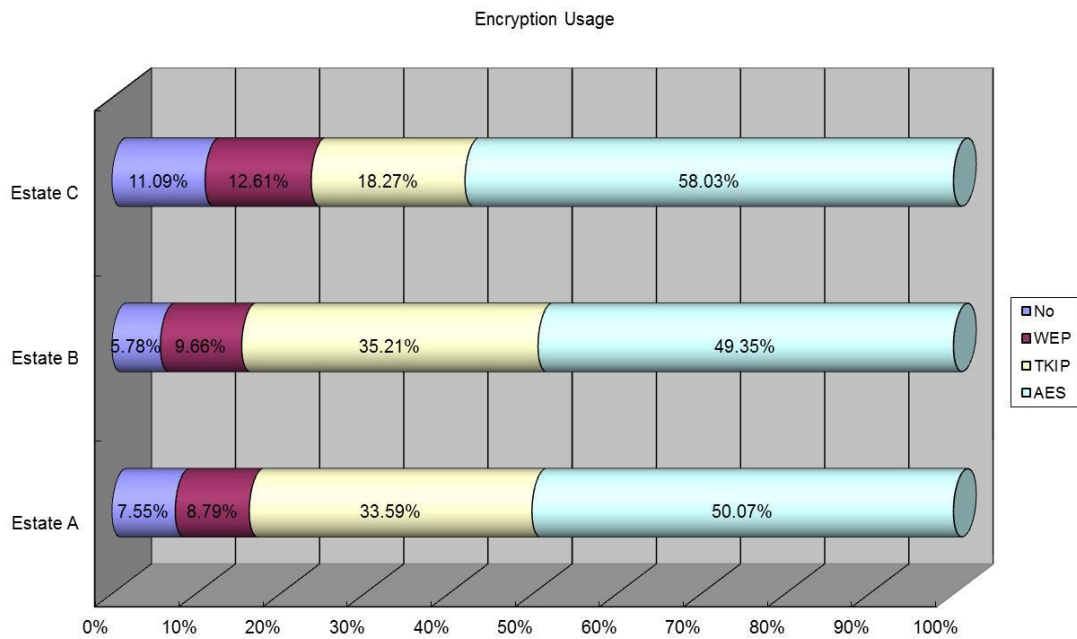
5. Comparison with Previous Years

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	Remarks
Estate A	3,261	2626	3364	3072	Decrease 8.68% *
Estate B	1,417	1952	2838	1315	Decrease 53.66% *
Estate C	382	565	1057	1308	Increase 23.75%

* the war-driving device has been changed to android tablet

5.2 Encryption Status (No Encryption)

	2010	2011	2012	2013	Remarks
Estate A	6.75%	9.94%	7.22%	7.55%	0.33% more with no encryption 👎
Estate B	9.95%	7.07%	4.90%	5.78%	0.88% more with no encryption 👎
Estate C	10.99%	11.50%	5.77%	11.09%	5.32% more with no encryption 👎

There number of Access Points with no encryption is increased this year due to the fact that the number of Hotspots increased. This is in-sync with all the estates we checked.

5.3 Encryption Usage

	2010	2011	2012	2013	Remarks
Estate A					
No	6.75%	9.94%	7.22%	7.55%	Security Degraded ⬇
WEP	34.38%	24.89%	16.56%	8.79%	Security Improved ⬆
TKIP	15.37%	15.87%	13.91%	33.59%	No preferred setting, Security Degraded ⬇
AES	43.5%	49.30%	62.31%	50.07%	Security Improved ⬆
Estate B					
No	9.95%	7.07%	4.90%	5.78%	Security Degraded ⬇
WEP	34.02%	26.54%	21.21%	9.66%	Security Improved ⬆
TKIP	20.32%	17.73%	17.94%	35.21%	No preferred setting, Security Degraded ⬇
AES	35.71%	48.66%	55.95%	49.35%	Security Improved ⬆
Estate C					

No	10.99%	11.50%	5.77%	11.09%	Security Degraded ⬇
WEP	34.55%	20.01%	18.92%	12.61%	Security Improved ⬆
TKIP	21.21%	16.80%	21.00%	18.27%	Security Improved ⬆
AES	33.25%	51.69%	54.31%	58.03%	Security Improved ⬆

In terms of encryption, the AES would be the best choice at this moment. The use of AES in these estates is over 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 2013.

War Flying using Helicopter

Year	2012	2013	
Number of AP Captured	5,493	6,526	
% of No Encryption	16.69%	11.28%	Security Improved
Encryption Usage			
No	16.69%	11.28%	Security Improved
WEP	20.99%	15.74%	Security Improved
TKIP	12.34%	17.79%	No preferred settings, security degraded
AES	49.98%	55.19%	Security Improved

In terms of encryption, the AES would be the best choice at this moment. The use of AES is nearly 50% of the total APs. It is consistence with the figures of Tramway and Estates. The overall security is improved in year 2013.

War Sailing with The Star Ferry

| Number of AP Captured	3,107
Encryption Usage	
No	26.49%
WEP	7.31%
TKIP	9.69%
AES	56.51%

When performing War Sailing, we are far away from the Access Points which are installed along the Victoria Harbour. Therefore, we found a lot of Access Points that are installed by service providers (known as Hotspots. From the raw data, there are 44.03% of the discovered Access Points are Hotspots. Hotspot providers provide mixing authentication and encryption supports to users. This includes "No Encryption" configuration. Therefore, over 25% of the discovered Access Points provides no encryptions.

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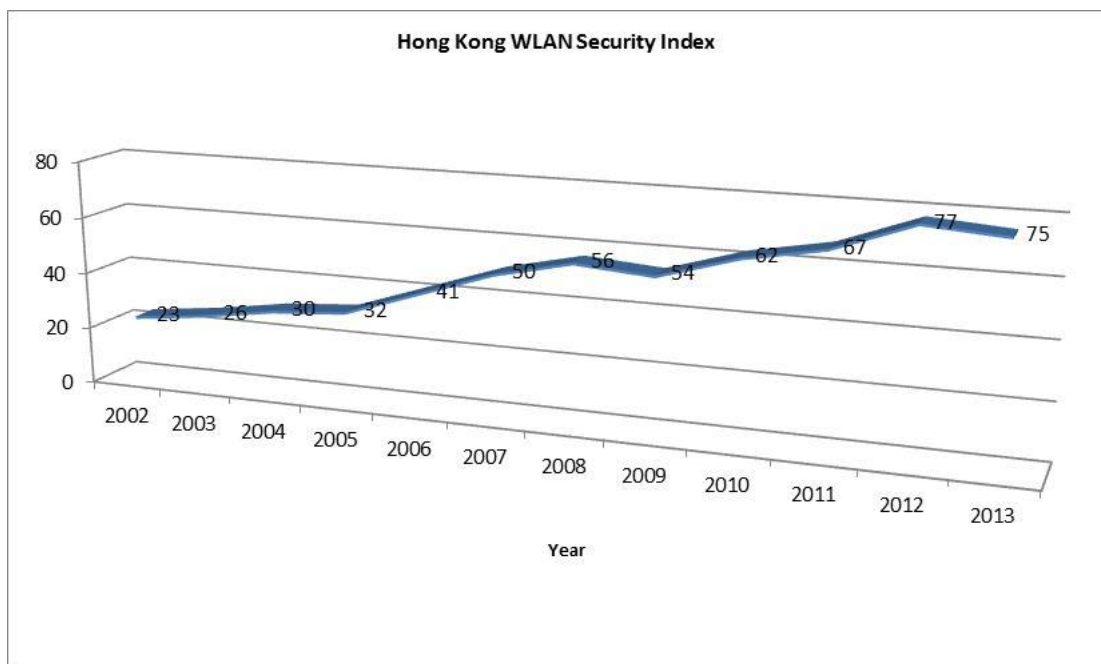
The index is dropped slightly in year 2013 due to the fact that more of "no encryption" access points discovered. Most of the contribution to "no encryption" is from Hotspot service provider.

Tramway War Driving

- 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.**
- For the default SSID issue, around 89% of default SSID is changed. Moreover, there are over **26%** of SSIDs **are hidden**. Hidden SSID is considered as first line defense of a WLAN.
- **The percentage of AP with WPS enabled is around 36 percentages**. There is known security vulnerability in WPS. It has **5%** 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, 13.27% of WLANs are still using WEP. Although there is a large percentage improvement, **we are still not satisfied with this figure as the latest technologies are outdated for more than 8 years**.
- 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, 12.03% of WLANs are using TKIP. It drops by 6.36% comparing with year 2012. Improvement was kept on in this year.
- The adoption of more secure encryption methods – AES is increased from 54.88% to 59.39%. Although the overall use of encryption is dropped, the adoption of AES increased by 4.51%. **It shows that Access Points with the most secure encryption methods** is **keeping on increasing**.

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.
- The adoption of most secure encryption method is aligned with the survey using Tram and Helicopter.

War Flying & War Sailing

- The percentage of using AES encryption is nearly 50% which is aligned with the other

survey methods.

Additional Sample Check on WPS in other area

- **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 2013 is 75 while the index of 2012 is 77. The index is dropped slightly due to the fact that more of "no encryption" access points discovered.

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 15% 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.