Report on

Wireless LAN War Driving Survey 2011

Hong Kong

Version 1.2

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 Communications Authority

(OFCA)

通訊事務管理辦公室

http://www.ofca.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 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.

Photos

黃道益
活絡油
十靈丹
重量級配方
WONG TO YICK
WiFi 安全話咁易 2011
www.SafeWiFi.hk

Unrivalled Distinction
eservation: 8202-3377
大眾財務
PUBLIC FINANCE
押

Est. 1904
Established
28
WiFi 安全話咁易
www.SafeWiFi.hk

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 • 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 communication “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.
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 2011, the two associations **PISA** and **WTIA** jointly conducted the "War Driving 2011" field survey along the classic tramway of Hong Kong Island and 3 estates. 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 & 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 2011, **PISA** and **WTIA** conducted the 10th "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 WLAN 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 was 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.

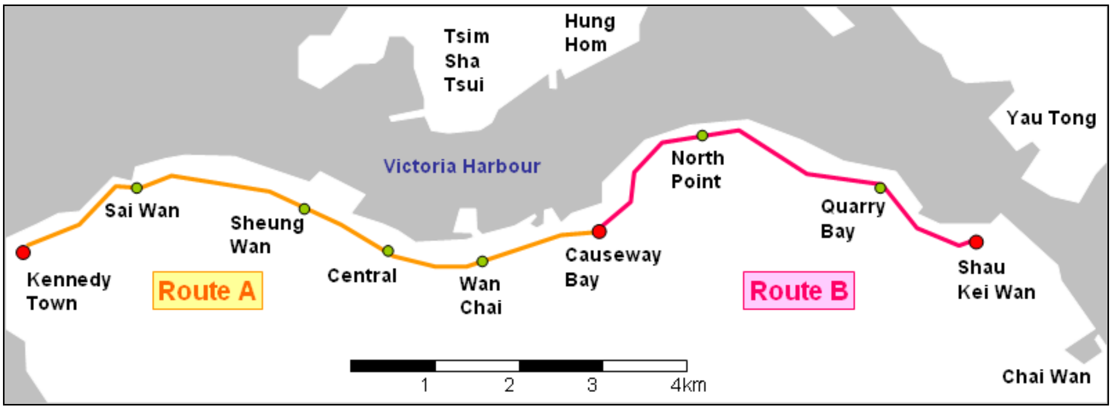
- Our objectives of the War Driving are to study the WLAN security status and compare it with the previous results, and to arouse the public awareness in WLAN security.
- We do not publicize the exact location and identity (e.g. SSID and MAC address) of any discovered AP. If such information appears 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:	18 Dec, 2010 (Sunday)
Time:	10 am – 2 pm
Equipments:	*Hardware:* • Notebook computers • WLAN cards (internal and external) • Antennae (built-in and external +12dbi) • GPS *Software:* • Vistumbler for Windows 7 and Vista Platforms (http://www.vistumbler.net) • WiFi Hopper for Vista Platforms (http://www.wifihopper.com)
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. 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

Findings and Analysis - Tramway

Tramway War Driving 2011 Snapshots

Number of Access Points Captured	16,618
Access Points without using Encryption	2,013 (12.12%)
Access Points without securing the SSID *(include default SSID, SSID same as trailing hexadecimal of AP's MAC address, hotspots etc)*	1,510 (9.09%)
Access Points using 802.11b	282 (1.7%)

2011 Result Compared with Previous Years

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

2003 Oct 5	2004 Nov 28	2005 Dec 4	2006 Oct 15	2007 Nov 4	2008 Nov 9	2009 Nov 26	2010 Dec 5	2011 Dec 18
Sunny	Sunny	Sunny	Occasional Raining	Sunny	Trace Raining	Sunny	Sunny	Fine & Dry
				Number of Access Points				
784	1,723	2,650	4,344	6,662	7,388	15,753	16,462	16,618
				No Encryption				
70%	61%	46.08%	37.04%	27.57%	19.26%	15.50%	13.64%	12.12%
				Insecure SSIDs				
43%	46%	42.98%	44.01%	30.29%	20.41%	11.57%	13.70%	9.09%

Highlights

1. The number of detectable deployment along the tramway, comparing with last year, slightly increases by 0.95%. It seems that it reached our detection capacity.
2. The percentage of APs with encryption turned on improves by 1.52%. It is, again, slightly improved.
3. The percentage of APs with SSID secured improves by 4.61%. It is better than last year.

Encryption Usages

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

WEP, WPA and WPA2 Usage Distribution

	2008	2009	2010	2011
Encryption Type	%	%	%	%

	2008	2009	2010	2011
No Encryption	22.86	15.50	13.64	12.12
WEP	43.18	45.01	34.05	24.66
WPA Personal using TKIP	13.53	11.65	13.53	11.98
WPA Personal using AES	1.02	0.91	1.94	2.05
WPA Enterprise using TKIP	11.76	7.31	5.92	5.72
WPA Enterprise using AES	0.03	0.02	0.02	0.01
WPA2 Personal using TKIP	3.26	10.90	7.39	10.06
WPA2 Personal using AES	3.31	5.10	19.21	29.4
WPA2 Enterprise using TKIP	0.62	3.07	0.92	1.73
WPA2 Enterprise using AES	0.43	0.53	3.38	2.27
Total:	**100**	**100**	**100**	**100**

The usages of WEP, WPA, and WPA2 are 35.05%, 21.41% and 30.09% in year 2010 while the usages of these are 24.66%, 19.76% and 43.46% in year 2011. Although the total encryption usage is slightly improved by 1.53% only, nearly 10% are shifting to more secure methods – WPA and WPA2. It is consistent with the previous year of improvements. As a result, we have 10% usage improvement in adopting more secure methods – WPA and WPA2.

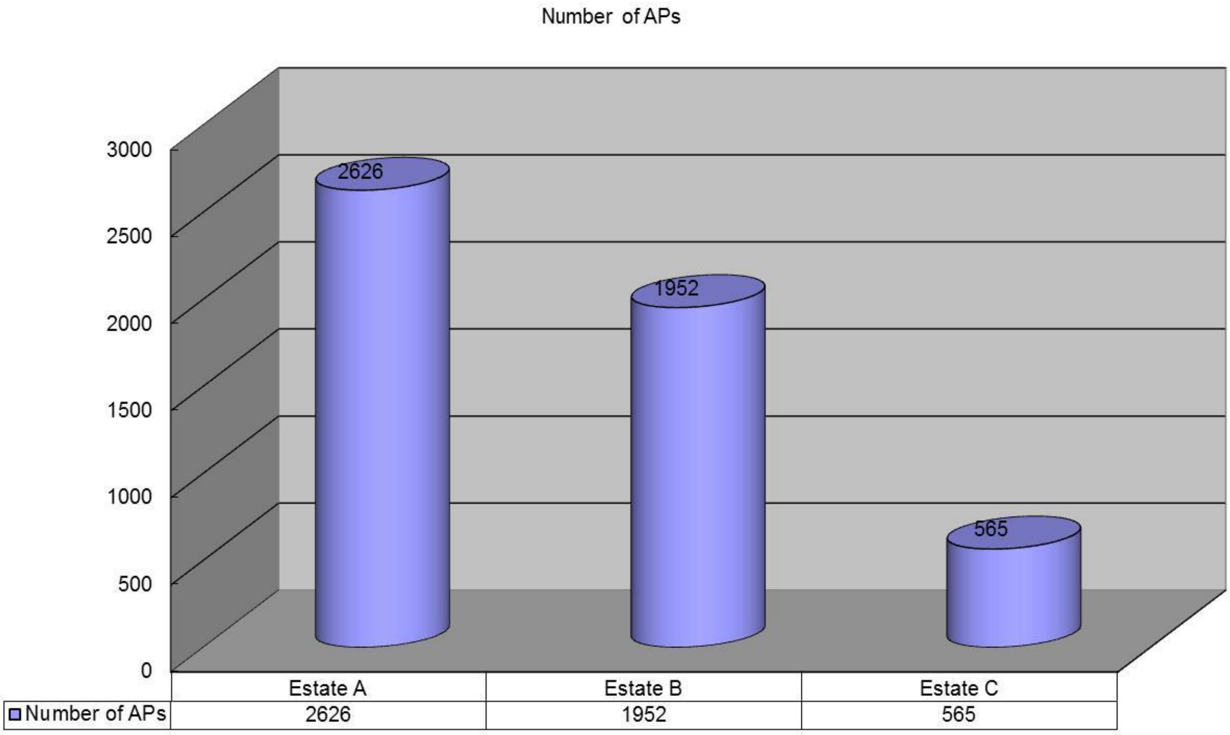
TKIP and AES Distribution

	2008	2009	2010	2011
Encryption Type	%	%	%	%
No Encryption	22.86	15.50	13.64	12.12
WEP	43.18	45.01	34.05	24.66
WPA/WPA2 using TKIP	29.17	32.93	27.76	29.49
WPA/WPA2 using AES	4.79	6.56	24.55	33.74
Total:	**100**	**100**	**100**	**100**

From another point of view, the adoption of more secure encryption methods (i.e. AES) increases from 24.55% to 33.74%. There is some improvement in adopting more secure encryption methods.

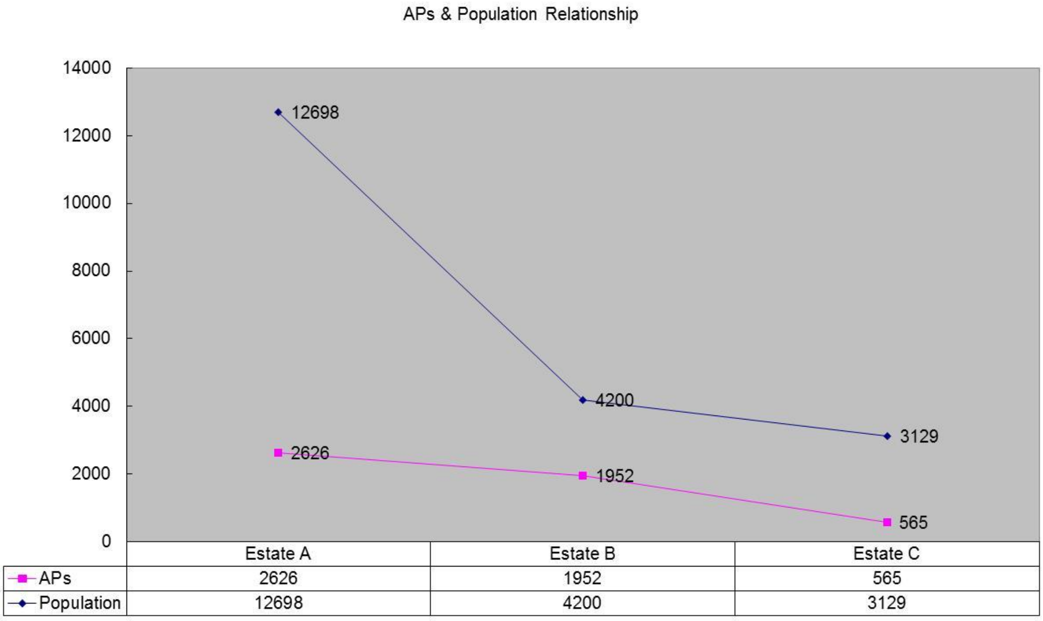
Findings and Analysis - Estates

1. Number of Unique AP Captured



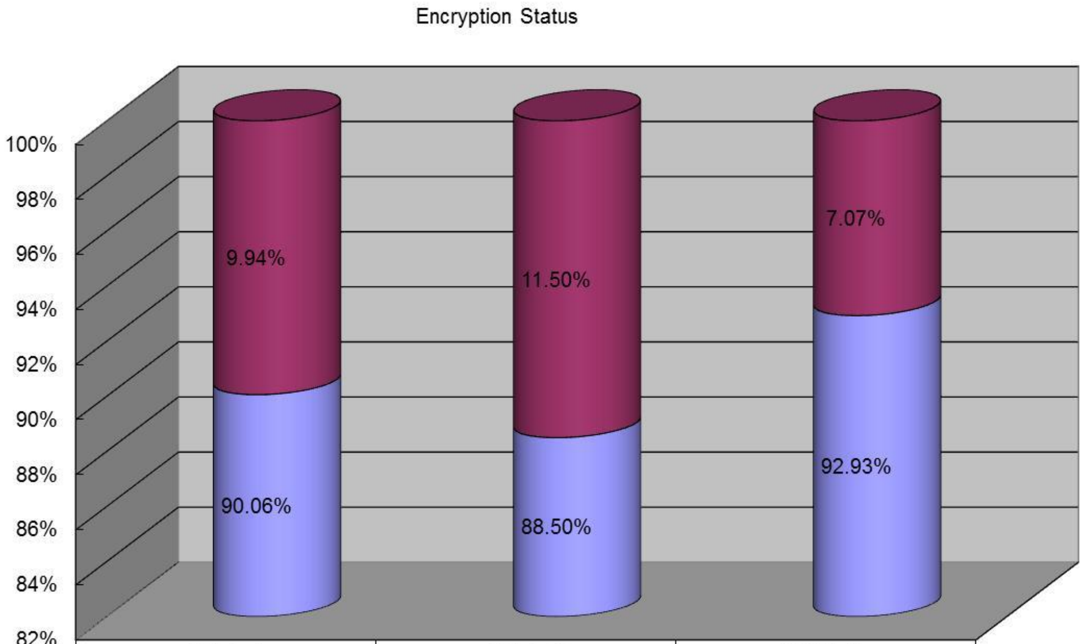
	Estate A	Estate B	Estate C
□ Number of APs	2626	1952	565

2. Relationship between population and number of discovered Access Points



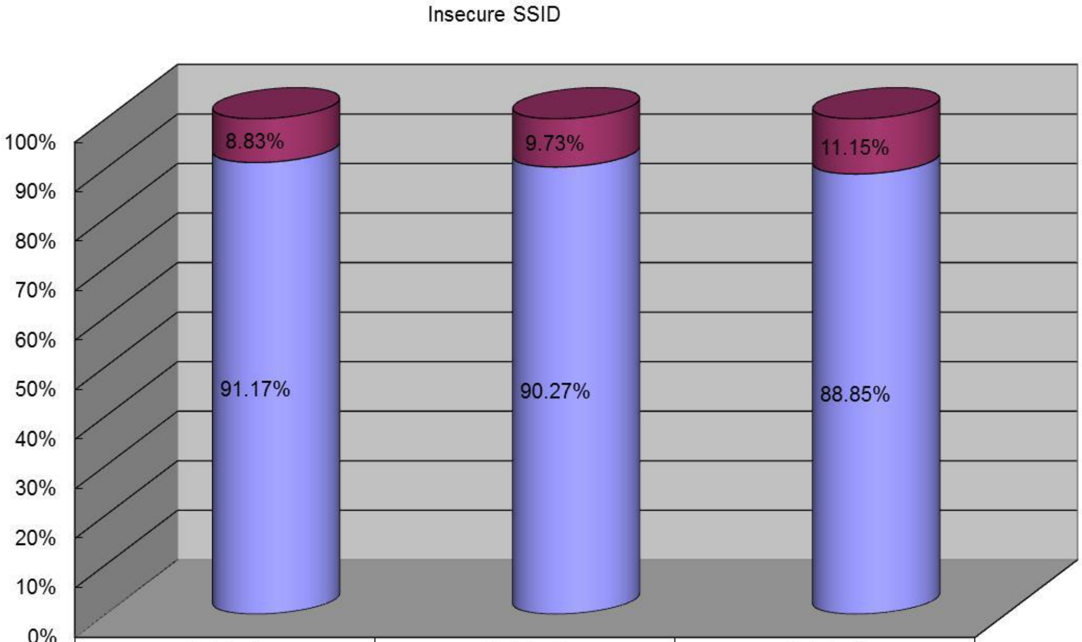
	Estate A	Estate B	Estate C
APs	2626	1952	565
Population	12698	4200	3129

3. Encryption Status



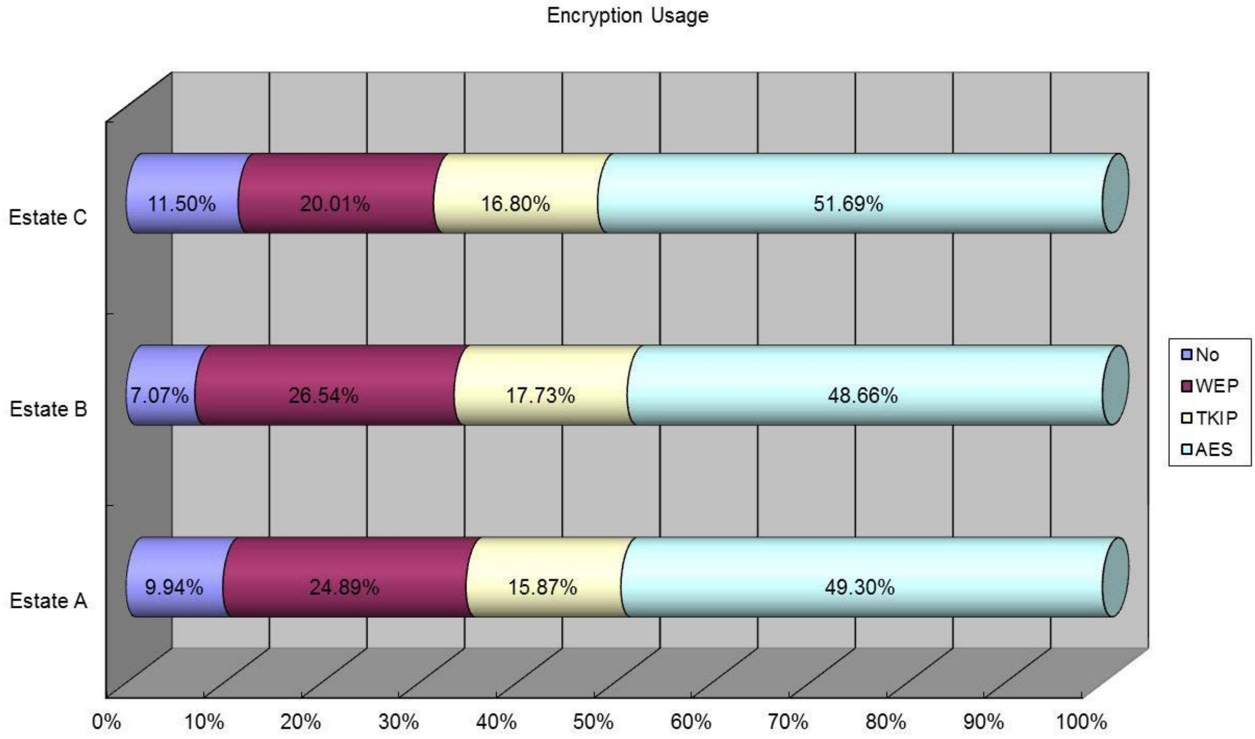
	Estate A	Estate B	Estate C
🟪 No Encryption	9.94%	11.50%	7.07%
🟦 Encrypted	90.06%	88.50%	92.93%

4. Insecure SSID



	Estate A	Estate B	Estate C
🟪 Insecure SSID	8.83%	9.73%	11.15%
🟦 Secure SSID	91.17%	90.27%	88.85%

5. Encryption Usage



6. Comparison Between 2010 and 2011

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

6.1 Number of Unique Access Points Captured

	2010	2011	Remarks
Estate A	3,261	2626	Decrease 19.47%
Estate B	1,417	1952	Increase 37.76%
Estate C	382	565	Increase 47.91%

6.2 Encryption Status (No Encryption)

	2010	2011	Remarks
Estate A	6.75%	9.94%	Degraded by 3.27%
Estate B	9.95%	7.07%	Improved by 2.88%

Estate C	10.99%	11.50%	Degraded by 0.51%

The overall encryption is improved in Estate B only while degrading by around 3% in both Estate A and C. However, this figure may be affected by the number of hotspots in these estates. Most Wi-Fi hotspots provide no encryption by default.

6.3 Insecure SSID

	2010	**2011**	**Remarks**
Estate A	9.02%	8.83%	Improved by 0.19%
Estate B	11.29%	9.73%	Improved by 1.56%
Estate C	21.2%	11.15%	Improved by 10.05%

Improvements exist in three estates. It shows that people will change the SSID to avoid other users' mis-connections. There is an significant improvement in Estate C.

6.4 Encryption Usage

	2010	**2011**	**Remarks**
Estate A			
No	6.75%	9.94%	Security Degraded ↓
WEP	34.38%	24.89%	Security Improved ↑
TKIP	15.37%	15.87%	Security Degraded ↓
AES	43.5%	49.30%	Security Improved ↑
Estate B			
No	9.95%	7.07%	Security Improved ↑
WEP	34.02%	26.54%	Security Improved ↑
TKIP	20.32%	17.73%	Security Improved ↑
AES	35.71%	48.66%	Security Improved ↑
Estate C			
No	10.99%	11.50%	Security Degraded ↓
WEP	34.55%	20.01%	Security Improved ↑
TKIP	21.21%	16.80%	Security Improved ↑
AES	33.25%	51.69%	Security Improved ↑

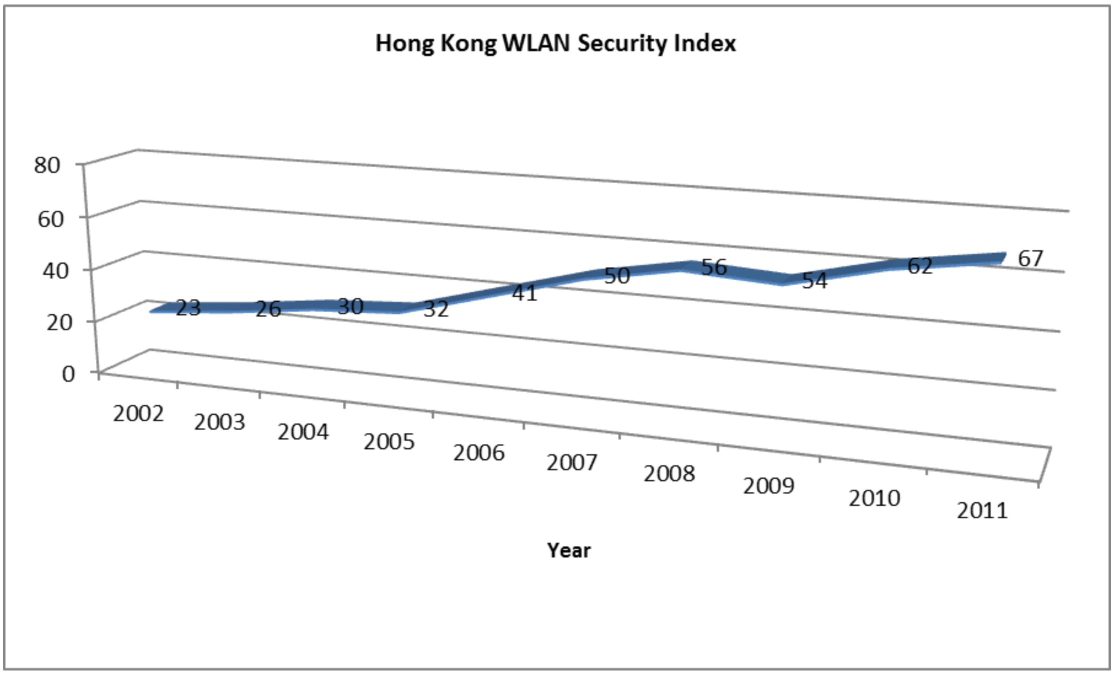
In terms of encryption, the AES would be the best choice at this moment. The use of AES in these estates is nearly 50% of the total APs. It shows that there is a trend of improvements in the adoption of secure Wi-Fi networks.

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 2011.



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 88 percentages.**
- For the default SSID issue, around 90% of default SSID is changed. However, **only 17.15%** (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 1.7%.

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, 24.66% 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 out for more than 6 years**.
- The adoption of WPA/WPA2 is improved **over 60%**. 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, 29.49% of WLANs are using TKIP. It drops by 1.73% comparing with year 2010.
- The adoption of more secure encryption methods – AES is increased from 24.55% to 33.73%.
- Although the adoption of encryption wireless LAN traffic is slightly increased, more WLANs are configured with more secure methods.

Estate War Driving

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

Hong Kong WLAN Security Index

- The Hong Kong WLAN Security Index of 2011 is 67 while the index of 2010 is 62. It shows some improvements in WLAN security implementation are found in Hong Kong.

Participants

Name	Organization
Alan Ho / Convenor	PISA
Andy Wong	WTIA
Eric Fan	WTIA
Eric Leung	WTIA
Gretal Chan	WTIA
James Lam	HKET
Jim Shek	PISA
Joseph Leung	WTIA
Ken Fong / Convenor	WTIA
Leo Sin	PISA
Mike Lo	PISA
Pak-yick Wong	WTIA
Sang Young	PISA/WTIA
SC Leung	PISA
Voker Lam	WTIA
Warren Kwok	PISA
WS LAM	PISA