Report on
Wireless LAN War Driving Survey 2009
Hong Kong

Version 0.1

Feb-2010

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.

Terms used

WLAN	Wireless Local Area Network. There are three 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, 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 Feb 2010, the two associations **PISA** and **WTIA** jointly selected two different types of estate in Hong Kong to compare the wireless LAN status. The objective of this survey was to figure out if any relationship between the type of estate to wireless LAN usage and security status.

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 Feb 2010, **PISA** and **WTIA** conducted the “War Driving” on two estates in Hong Kong. One is a private housing estate with 61 residential towers and a total of 12,698 apartment flats (Estate A). The other one is a old public housing estate with 9 residential buildings and a total of 3,129 apartment flats (Estate B).

We use notebook computer with built-in wireless LAN adapter and “War Driving” software – wifihopper or vistumbler to conduct this “War Driving” exercise. We take a walk in the public area of these estates to collect wireless LAN related information.

Objectives of Study

1. To compare the wireless LAN usage between two different type of estates.
2. To compare the usage of encryption methods between two different type of estates.

** 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.

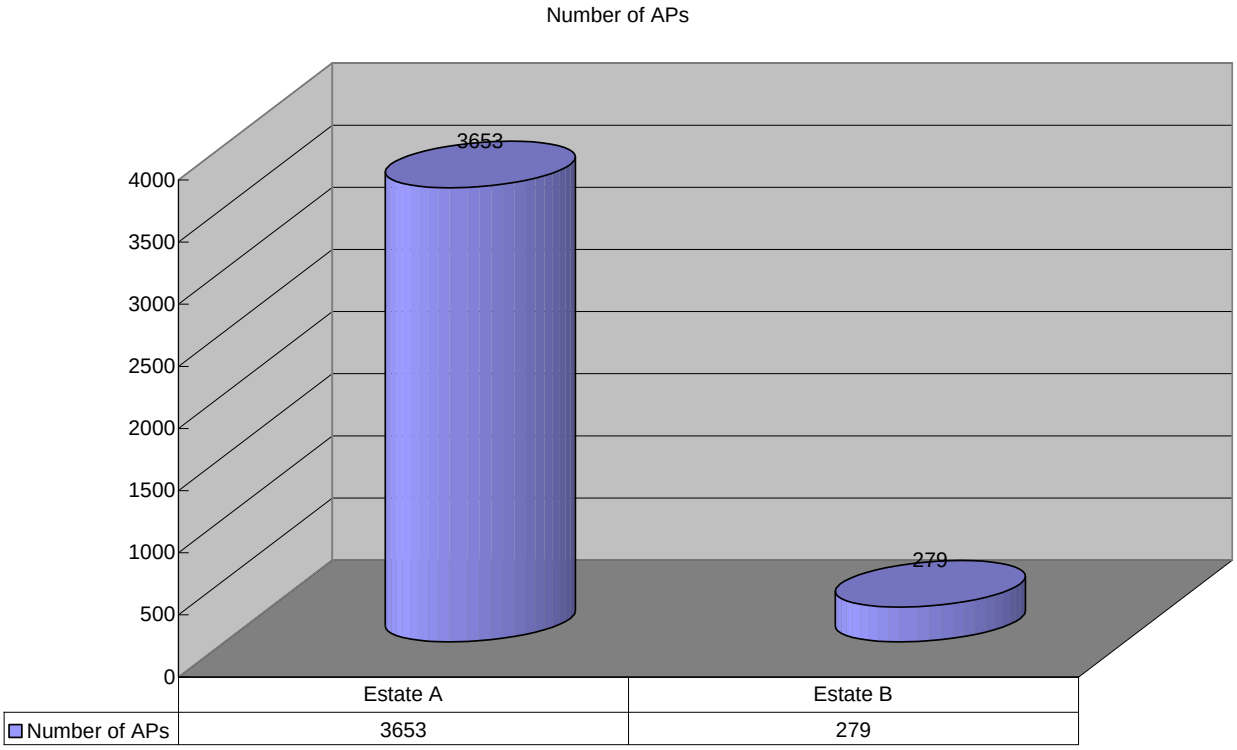
- Our objective of the War Driving is to study the WLAN security status and compare it with the previous results, and to arouse the public awareness in WLAN security.
- We do not publicize the exact location and identity (e.g. SSID and MAC address) of any discovered AP. If such information appears in 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.

Background information of the Estates

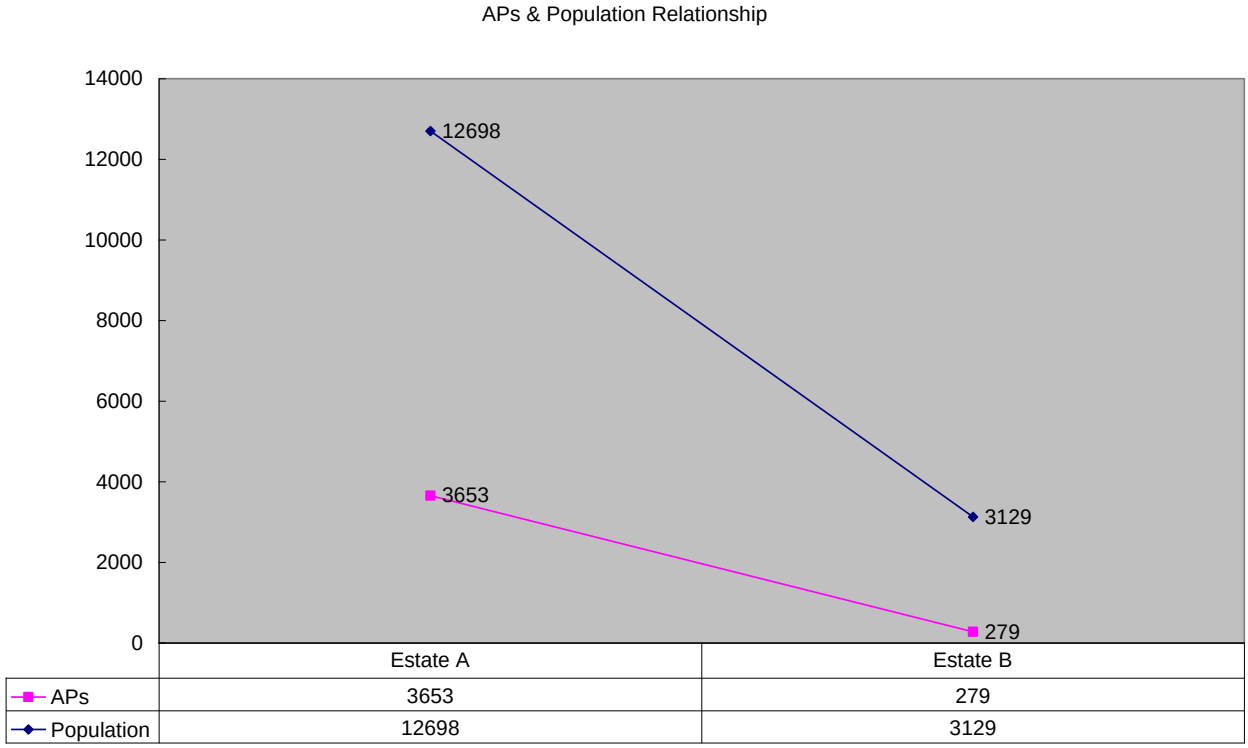
Estate A	Information	Estate B
Private Housing Estate	Type	Public Rental Housing Estate
Since 1977	Year	Since 1963
61	Number of Apartment Buildings	9
12,698	Apartment Flats	3,129
Middle-class population	Features	An aging population

Comparison

1. Number of Unique AP captured

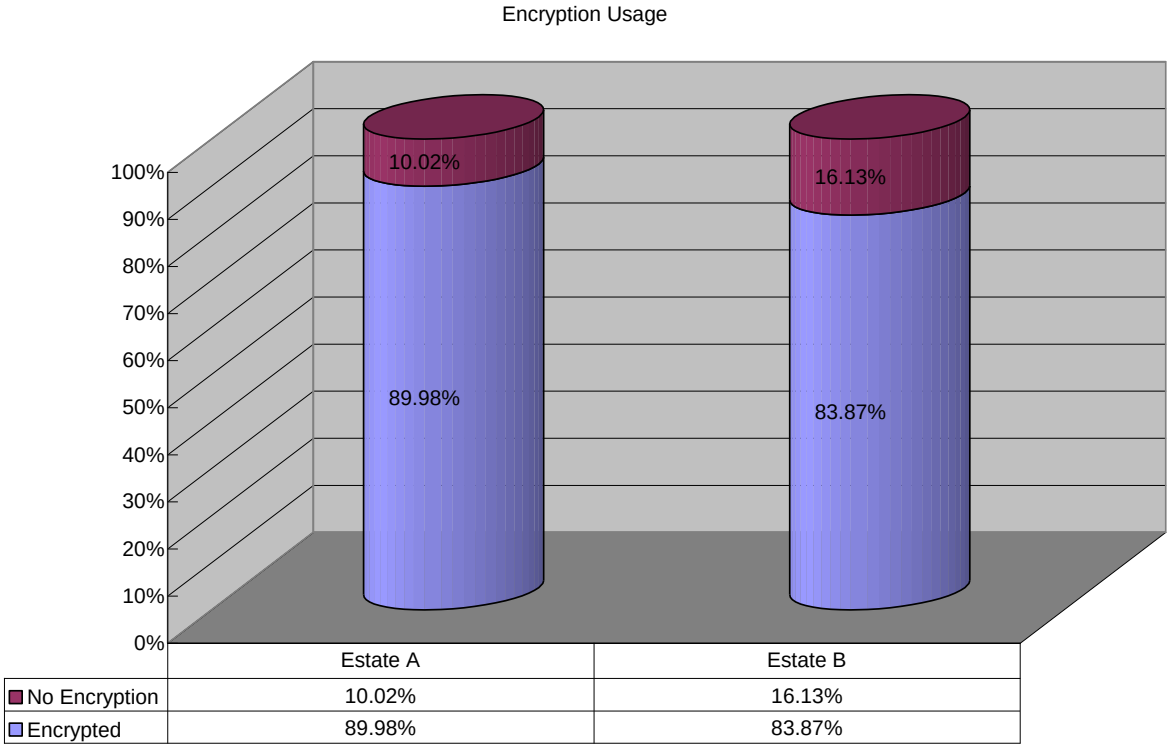


2. The Relationship between population and number of discovered Access Points



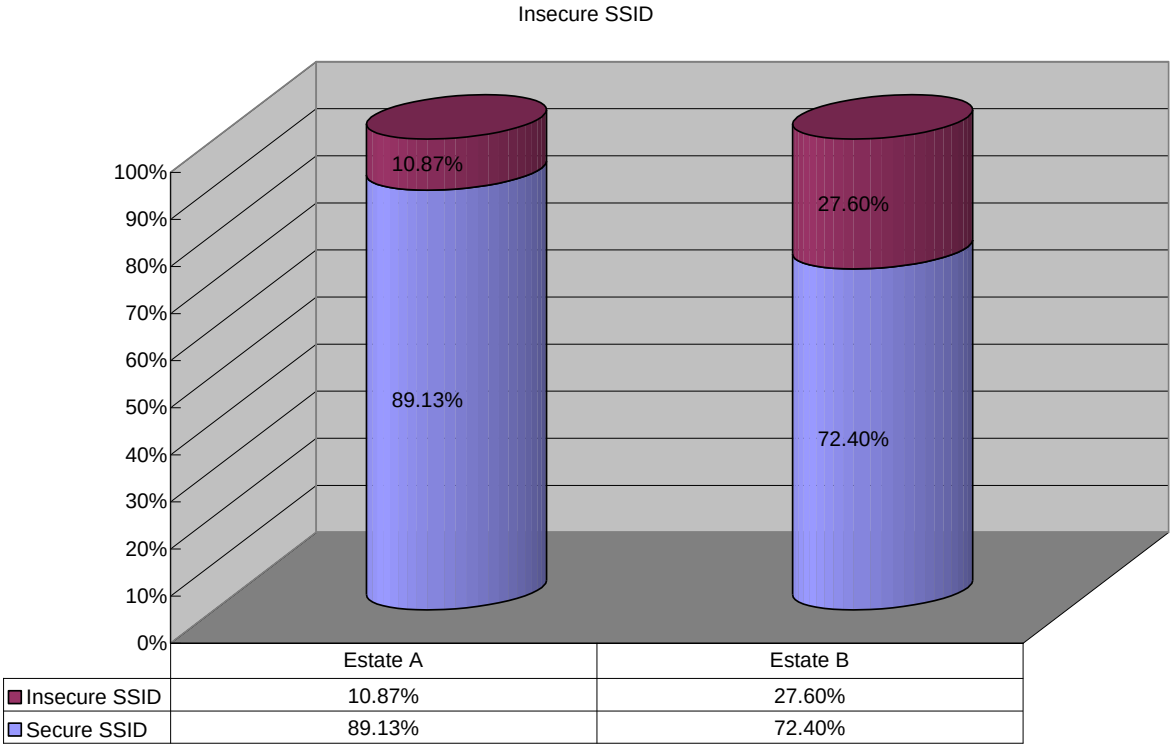
	Estate A	Estate B
APs	3653	279
Population	12698	3129

3. Encryption Usage



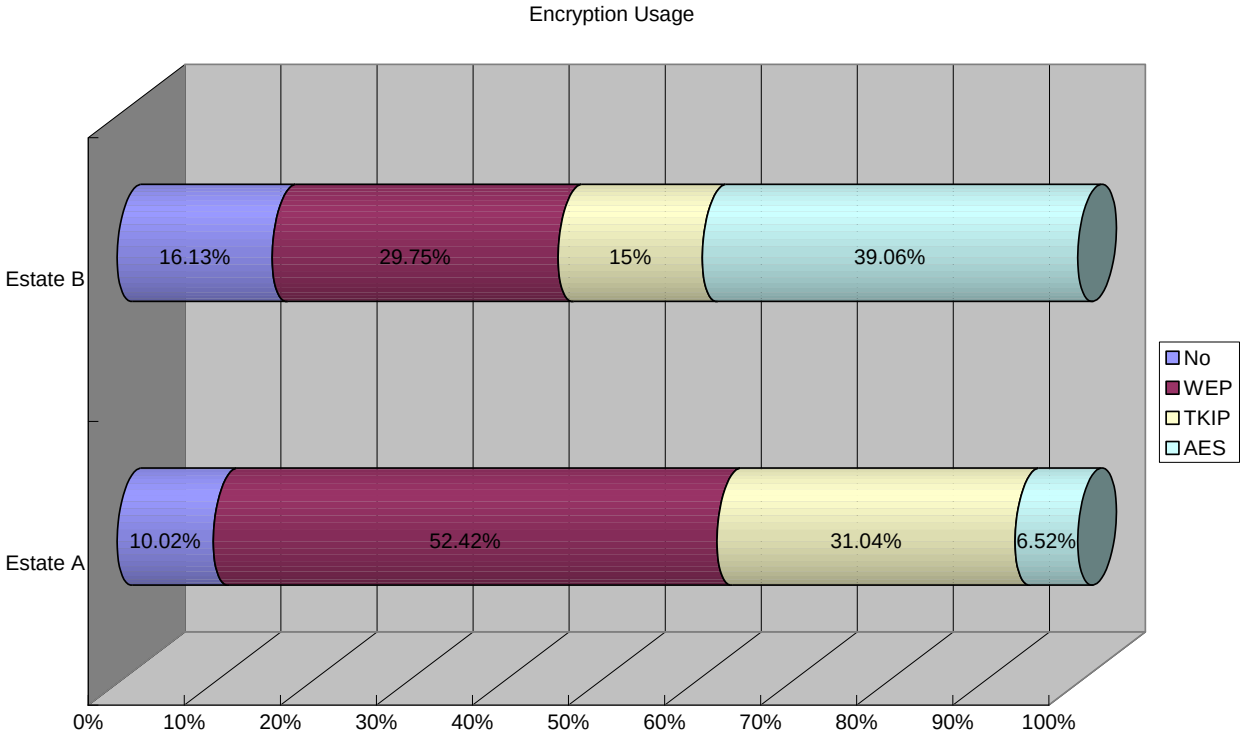
	Estate A	Estate B
No Encryption	10.02%	16.13%
Encrypted	89.98%	83.87%

4. Insecure SSID



	Estate A	Estate B
Insecure SSID	10.87%	27.60%
Secure SSID	89.13%	72.40%

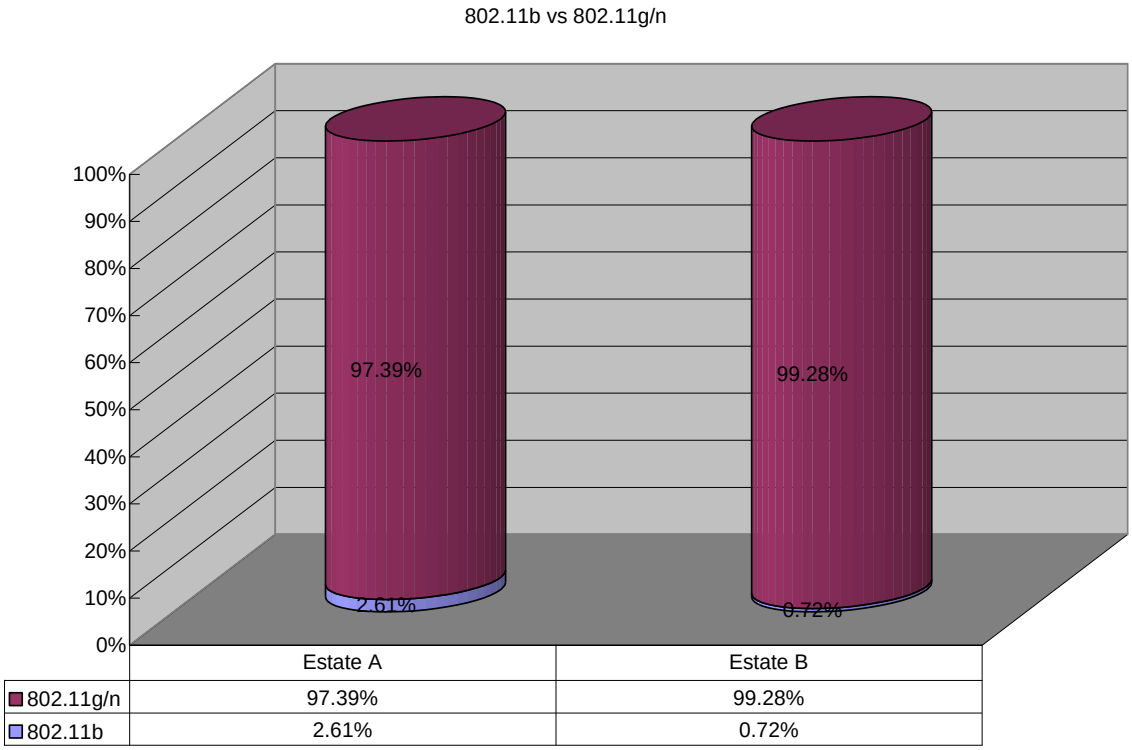
5. Encryption Usage



Details of Encryption Usage:

Estate A	Encryption Analysis	Estate B
10.02%	No Encryption	16.13%
52.42%	WEP	29.75%
10.92%	WPA-PSK-TKIP	9.68%
1.51%	WPA-PSK-AES	6.45%
11.33%	WPA2-PSK-TKIP	1.08%
4.87%	WPA2-PSK-AES	24.37%
7.75%	WPA-Enterprise-TKIP	4.3%
0%	WPA-Enterprise-AES	0%
1.04%	WPA2-Enterprise-TKIP	0%
0.14%	WPA2-Enterprise-AES	8.24%

6. 802.11b vs 802.11g/n



	Estate A	Estate B
802.11g/n	97.39%	99.28%
802.11b	2.61%	0.72%

Conclusion

- The more the population, the more the discovered Access Points. It could also relate to the aging of population. The younger the population, the more the discovered Access Points.
- The percentage of using encryption is performed better in middle-class population than aging population.
- Although the percentage of using encryption is smaller in the aging population, the percentage of using more secure one is more.
- Almost all of the APs discovered in the aging population are using latest wireless LAN technologies. It can be considered that the adoption of wireless LAN is later in the aging population than the middle-class population.
- The percentage of protecting their SSID is performed better in middle-class population than aging population.

* * * The End * * *