Report on

Wireless LAN War Driving Survey for Estates 2010

Hong Kong

Version 1.0

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 Telecommunications Authority

(OFTA)

電訊管理局

http://www.ofta.gov.hk

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 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 communications “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.

Executive Summary

In Dec 2010, the two associations **PISA** and **WTIA** jointly selected three 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.

As an usual practice, this study was carried out in a non-intrusive and responsible way. No personal information, sensitive information and payloads were collected during the data collection stage. The information of individual vulnerable wireless LAN 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.

In this year's study, we can identify that trend of adopting more secure encryption technologies is increasing although the percentage of usage is not satisfied.

Introduction

In Dec 2010, PISA and WTIA conducted the “War Driving” on three estates in Hong Kong. The demographic information of these three estates are as follows:

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 • An aging population

We use notebook computer with built-in wireless LAN adapter, antenna and “War Driving” software – 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 among these estates with respect to the type of estates.
2. To compare the usage of encryption methods among these two different type of estates.
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 program

** 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.*

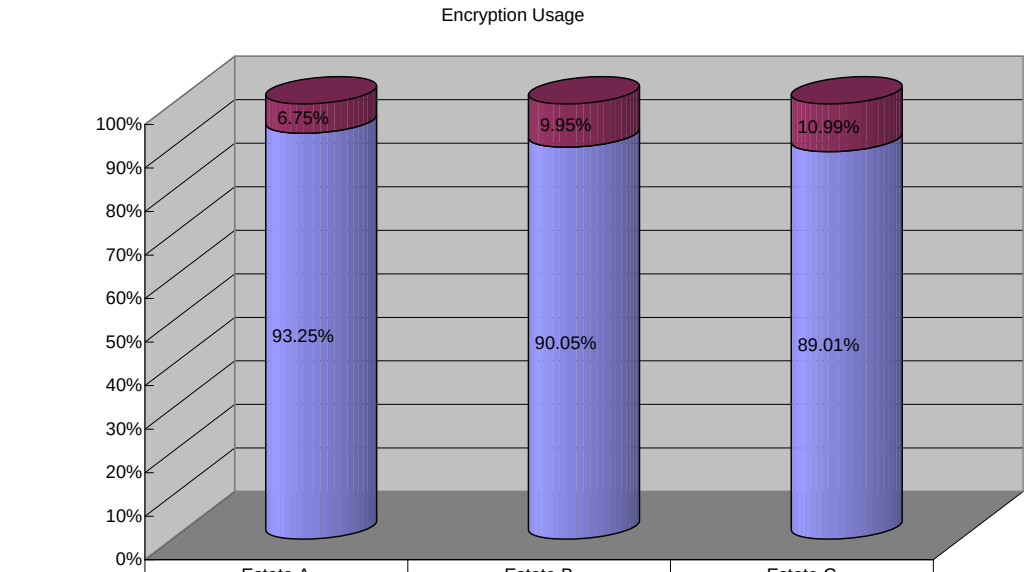
Code of Ethics

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 do not capture or collect any WLAN traffic payloads.
- We limit to the scope we state above only.

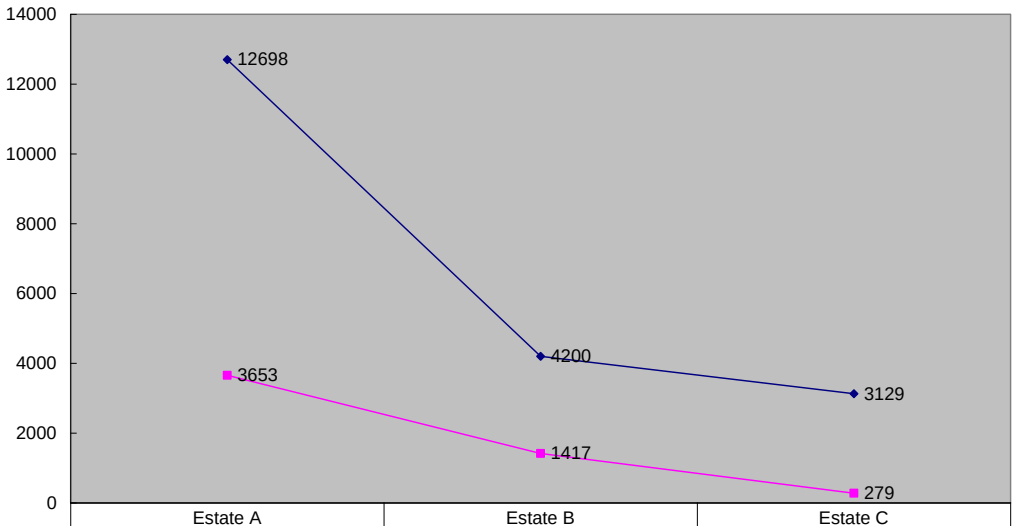
Comparison

1. Number of Unique AP Captured



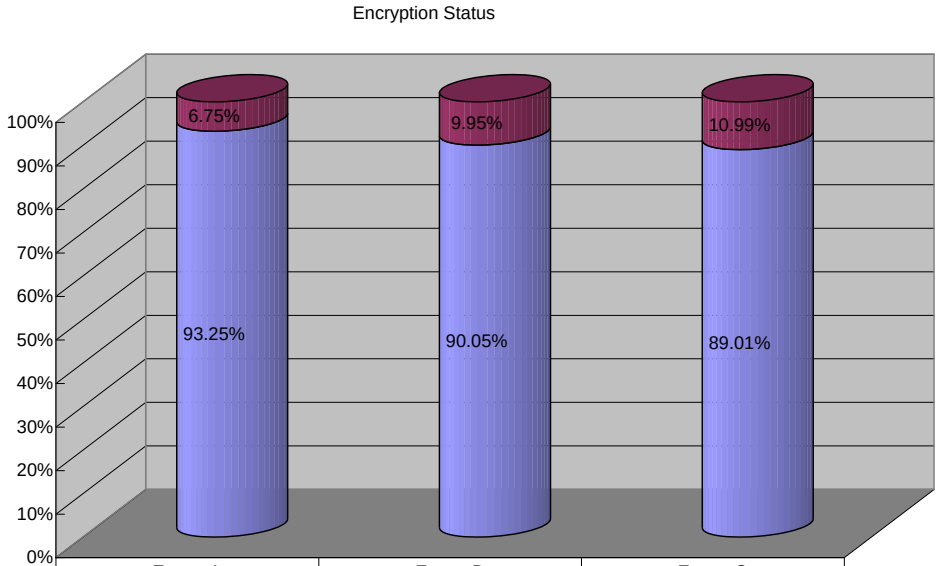
	Estate A	Estate B	Estate C
No Encryption	6.75%	9.95%	10.99%
Encrypted	93.25%	90.05%	89.01%

2. Relationship between population and number of discovered Access Points



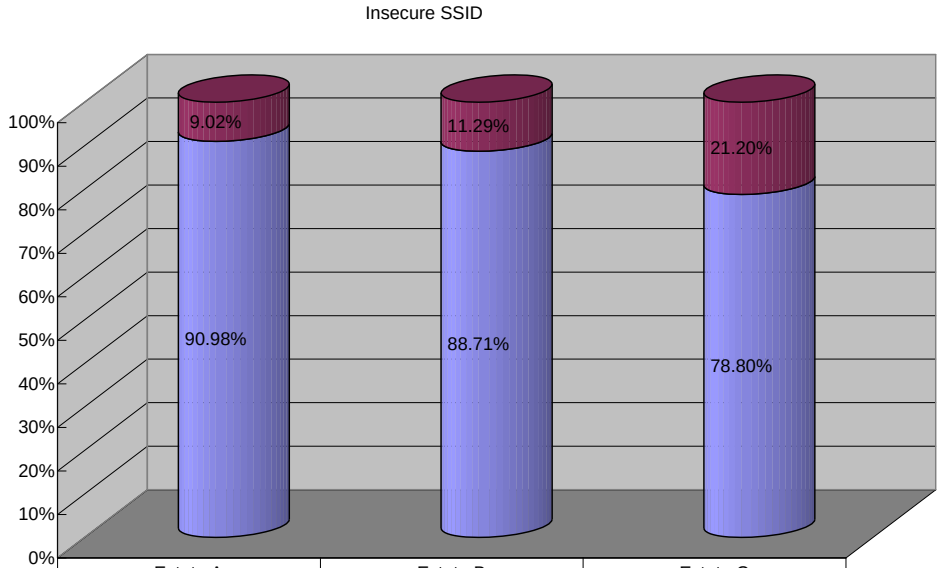
	Estate A	Estate B	Estate C
APs	3653	1417	279
Population	12698	4200	3129

3. Encryption Status



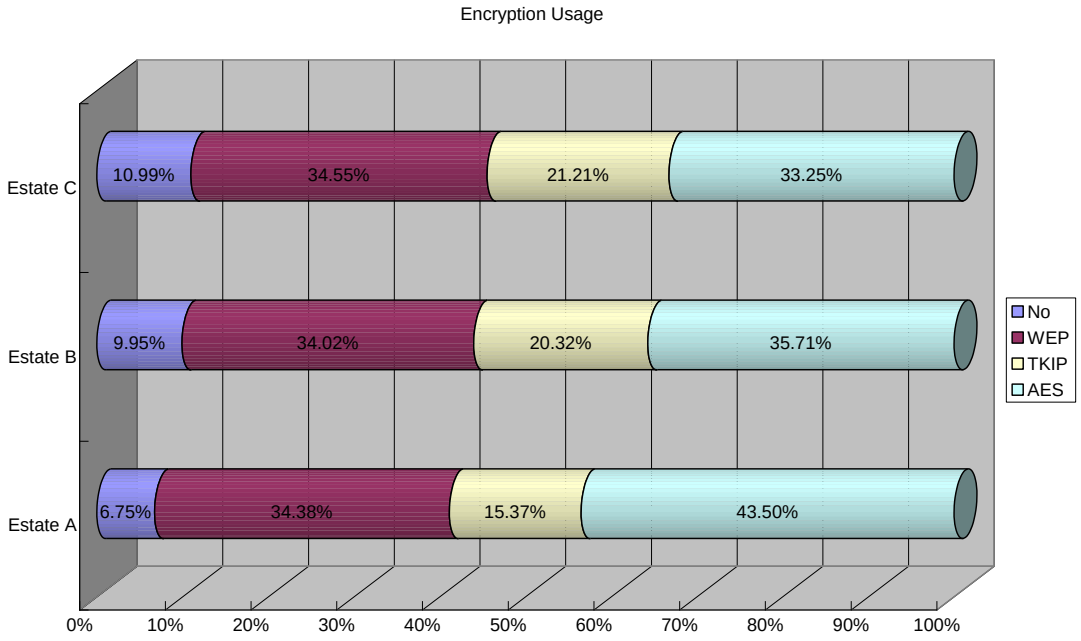
	Estate A	Estate B	Estate C
No Encryption	6.75%	9.95%	10.99%
Encrypted	93.25%	90.05%	89.01%

4. Insecure SSID



	Estate A	Estate B	Estate C
Insecure SSID	9.02%	11.29%	21.20%
Secure SSID	90.98%	88.71%	78.80%

5. Encryption Usage



Estate A
Estate C 16.13% 10.99% Improved by 5.14%

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 other population.
- From encryption distribution point of view, middle-class population leads the use of more secure encryption protocol than others estates.

- The percentage of protecting their SSID is performed better in middle-class population than other populations.
- It was identified that the figures in every area is similar in Home Ownership Scheme and Public Housing Estate.
- Middle-class population leads in the WLAN security implementation.

** The End **