Report on

Wireless LAN War Driving Survey 2005-06

Hong Kong

Version 1.0

May-2006

Organizers

Professional Information Security Association

(PISA)

專業資訊保安協會

Hong Kong Wireless Technology Industry Association

(WTIA)

香港無線科技商會

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.

Photos

[4/Dec/2005] War-tramming using 5dBi omni-directional antenna

[From left]: Ken Fong (WTIA), Sang Yong (PISA) and Alan Ho (PISA)

[4/Dec/2005] War-tramming using 8dBi omni-directional antenna

[From left]: Clayton Check (WTIA) and Alan Tam (PISA)

Photos

[4/Dec/2005] War-tramming survey finished at Shau Kei Wan

[From left]: Alan Tam (PISA), Clayton Check (WTIA), Alan Ho (PISA), Ken Fong (WTIA) and Sang Young (PISA)

[26/Feb/2006] The War Driving Team gathered at Tsim Sha Tsui Bus Terminal before the survey. We split into 2 teams for the survey.

[Back row from left]: Ken Fong, S.C. Leung, Jim Shek, James Chan, Alan Ho and Anthony Lai
[Front row from left]: Wallace Wong, Sang Young, Vincent Lee, Stanley Lin and Eddy Yuen

Photos

[26/Feb/2006] Bus trip from Tsim Sha Tsui to Cheung Sha Wan

We found that built-in WLAN device of a newer Centrino notebook PC could detect even more WLAN APs than a usual PCMCIA WLAN card with a 5dBi external antenna.

[26/Feb/2006] Bus trip from Tsim Sha Tsui to Cheung Sha Wan

Though a bus is moving faster than a tram, the number of APs detected in this trip was not bad. There were about 2300 APs found in this trip.

Photos

[26/Feb/2006] The team took off at Cheung Sha Wan Bus Terminal and was waiting for a return bus back to Tsim Sha Tsui

[From left]: Alan Ho, Sang Young, Eddy Yuen, Stanley Lin, Anthony Lai and Vincent Lee

[26/Feb/2006] Another team took a bus from Tsim Sha Tsui to Whampoa

[Back row from left]: S.C. Leung and Jim Shek

[Front row from left]: Wallace Wong and James Chan

Photos

[26/Feb/2006] The team took off at Whampoa Bus Terminal and was waiting for a return bus back to Tsim Sha Tsui.

[26/Feb/2006] The team returned back to Tsim Sha Tsui

Photos

[26/Feb/2006] The team got on a car and continued some more survey

[26/Feb/2006] Put the antenna on the top of the car for better detection of WLAN APs

Terms used

WLAN	Wireless Local Area Network. 802.11a/b/g are more 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, 108Mbps • "Pre-N": A Pre-N wireless router uses two transmitters and three receivers to double the speed of existing 802.11 devices to 108 Mbps. Pre-N products let customers boost speed before 802.11n devices are available.
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. Third generation GPS devices is capable of acquiring satellite signals even in challenging situation e.g. between tall buildings. Compared to the previous generation, power consumption is reduced, higher sensitivity & fast signal acquisition and higher accuracy.

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	IEEE 802.11i is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. WPA implemented a subset of 802.11i and full implementation of 802.11i is called WPA2. The 802.11i architecture include: 802.1X for authentication, Robust Security Network (RSN) for keeping track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication. Another important element of the authentication process is the four-way handshake.

Executive Summary

In Dec 2005, the two associations **PISA** and **WTIA** jointly conducted the "War Driving 2005" field survey along the classic tramway of Hong Kong Island and in Feb 2006 on bus/car in some areas in Kowloon. It was our **4th round** of the annual war-driving survey since 2002. The objective of the survey was 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 three previous studies conducted by PISA in 2002, and by PISA & WTIA in 2003 & 2004 to plot the profile of Hong Kong WLAN security development. The survey indicated that the number of WLAN implementation had skyrocketed in the past three or four years, and yet there was some improvement in the adoption of security strategies.

The overall percentage of AP with encryption has already exceeded 50% both in the tramway survey (53.92%) in Hong Kong Island and the bus/car survey (55.89%) in Kowloon. Although the encryption rate exceeded 50%, it is only one area of improvement in WLAN security that is not sufficient. We have concerns on the SSID security. We found that the use of factory default SSID (39%) or personal-identity-associable SSID (10% individual and 10% organisation) is quite high. The use of non-broadcast SSID is rather low (only 4%). There should be room of improvement of the SSID area.

As compared to last year, the number of discovered APs in the tramway had notably **increased by** 53.8**%** (though the rate of increase was flattened as compared to last year's 120%) as well as the percentage of adoption of encryption setting has **improved** 15%.

As the 802.11g market is getting matured and more products are available, we found a **sharp increase of adoption of 802.11g AP from 14.16% last year to 66.42% this year.**

Since we want to know the situation in Kowloon, we conducted a WLAN survey this time in Kowloon. We found that the **overall results (tram in Hong Kong Island vs bus/car in Kowloon) are similar in terms of encryption rate, 802.11g adoption and the use of factory default SSIDs**.

We did some analysis of the SSID names that we collected in the Kowloon survey. We found that there are **still quite high percentage (39%) of APs are with factory default SSIDs**. This may mean the administrators of the APs may not change other default settings (e.g. administrator password). There were also **many SSIDs that associate or may associate with the identity of person, family or the organization** (10% of organization name, 10% of individual name, some are even using the web/ftp site name or email address name, etc.). Where possible, this should be avoided as attackers/hackers can locate you and your organizations easily.

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

We have been doing WLAN war-driving surveys since 2002. The one held in Dec 2005 & Feb 2006 was our 4th round war-driving survey. Below is an introduction of the past WLAN war-driving surveys.

Annual War Driving	Description
1st War Driving	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
2nd War Driving	In Oct 2003, **PISA** and **WTIA** jointly conducted the 2nd "War Driving". The scope of test was extended to • the whole tram way, covering the business corridor of the HK Island • lookouts at the Victoria Peak, covering far-away signal of the HK Island north and the Kowloon Peninsula, at an bird-eye view
3rd War Driving	In Nov 2004 & Jan 2005, **PISA** and **WTIA** conducted the 3rd "War Driving" again to benchmark the improvement for the WLAN Security in Hong Kong. Some new ideas of the 2004 war driving include: • the whole tramway, covering the business corridor of the HK Island • touring on boat in the Victoria Harbour, covering the both side of HK Island and Kowloon at the sea level • making a real-life connection to an authorized access point in the middle of Victoria Harbour • using GPS in locating position and mapping of path
4th War Driving	In Dec 2005 & Feb 2006, **PISA** and **WTIA** conducted the 4th "War Driving" again to benchmark the improvement for the WLAN Security in Hong Kong. Highlights of the 2005 war driving include: • the whole tramway, covering the business corridor of the HK Island • riding on bus/car in some areas of Kowloon

.

Objectives of 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 conduct a non-intrusive***** information security study with responsible disclosure of information
3. 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 and the reporter 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 masked.
- We do not connect to the IP network of any insecure AP to further explore their vulnerabilities.
- We do not interfere / jam any wireless traffic.
- We limit to the scope we state above only.

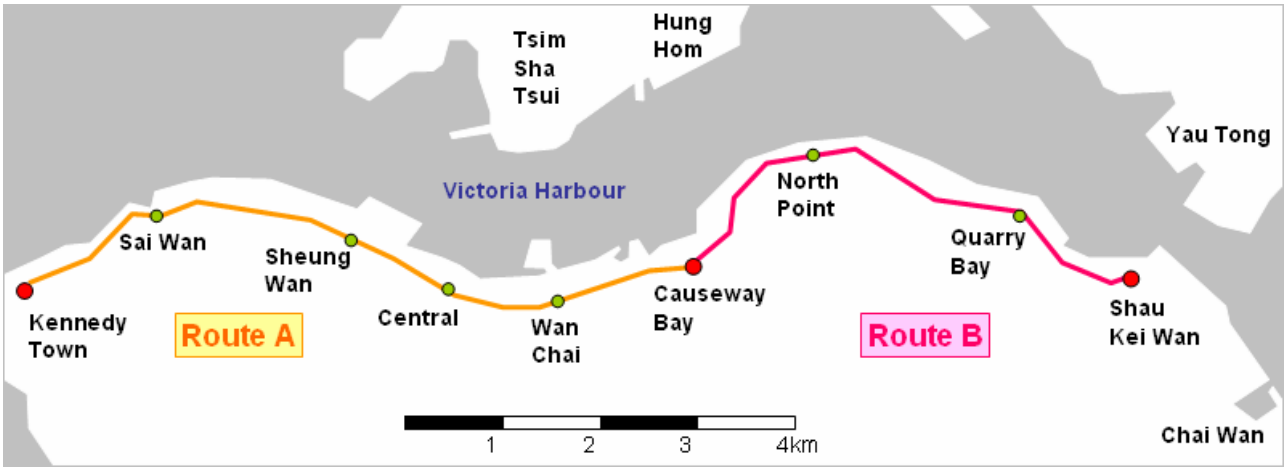
Methodology and Equipment

The War Driving was divided into 2 parts: ***War Tramming*** and ***War Driving on Bus/Car***.

Part I: War Tramming (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 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 of year 2002, 2003 and 2004 along the tramway from Kennedy Town to Causeway Bay (Route A).
- We also benchmarked the results with that of the war driving study of year 2003 and 2004 along the tramway from Kennedy Town to Shau Kei Wan. This route was equivalent to the whole business corridor of Hong Kong Island. (Route B).

Date:	4-Dec-2005 (Sunday)
Time:	10 am -1 pm
Equipment:	*Hardware:* Notebook computers, WLAN cards & some with a +5dB omni-directional antenna *Software:* Netstumbler *(Netstumber results of antennae of +5dB or below were used as a control to compare with previous years' results)*
Route:	• Route A: o Taking a tram from Queensway, Admiralty westwards to Kennedy Town terminus, then a return tram from Kennedy Town terminus to Sogo Department Store, Causeway Bay (this was the same route as in War Driving 2002, 2003 and 2004) • Route B: o Taking another tram from Causeway Bay to Shau Kei Wan terminus (this was the same route as in War Driving 2003 and 2004)



Part II: War Driving on Bus/Car (in Kowloon)

- In the past years, we conducted WLAN surveys in Hong Kong or in the sea. How about the situation in Kowloon? Would the statistics similar to the results of tramway? This curiosity drove us to conduct a survey in Kowloon this time.
- We chose bus since it is comparatively the slowest public transport in Kowloon. The routes we chosen covered Tsim Sha Tsui, Yau Ma Tei, Mong Kok, Sham Shui Po, Cheung Sha Wan and Hung Hom that are representatives of both commercial and residential areas in Kowloon. The survey on car was an add-on to the bus survey.

Date:	26-Feb-2006 (Sunday)
Time:	10 am -12:30 pm
Equipment:	Different antenna were used - + 8dB omni-directional antenna - + 5dB omni-directional antenna - null antenna Other equipment - GPS device (serial/USB) for recording longitude/latitude information

Findings and Analysis

Part I: War-Tramming (Tramway War Driving)

Note: the war tramming statistics (NetStumbler) below was generated by the consolidated log from war drivers with antenna having a gain of +5dB or below.

1. Number of Access Points Captured

Locations	Number of unique Access Points captured
Route A: Tramway, from Kennedy Town to Causeway Bay	1576
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	2650

2. Overall the implementation of 802.11g in Hong Kong is around 66%.

Route A: Tramway, from Kennedy Town to Causeway Bay	68.15%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	66.42%

3. WEP/WPA Encryption is disabled for around 46% of APs

Route A: Tramway, from Kennedy Town to Causeway Bay	45.56%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	46.08%

4. The proportion of AP with factory default SSID [1]

Route A: Tramway, from Kennedy Town to Causeway Bay	39.47%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	42.98%

5. Used Channels

- The most common channels are 1, 6 and 11 (82.60% of total).
- There are a few (19) APs using channels beyond 11, captured along the tramway.

Note:
- Some APs are ETSI channel models supporting channels 1-13.
- In some countries only channels 1 – 11 are allowed whereas while channel 14 is approved in Japan. See unofficial reference:
http://dqd.com/~mayoff/notes/ap500/Help/terms/frequency_channel.html

[1] Including factory default SSID, SSID with vendor-specific string, SSID same as trailing hexadecimal of AP's MAC address

6. How are the results compared with War Driving of past years?

In order to make a comparison, we followed the same route of the War Driving 2002 from Kennedy Town to Causeway Bay in Route A of the journey and record the result. A table for comparison is drawn:

	2002	2003	2004	2005
Date	07-Jul-02	05-Oct-03	28-Nov-04	04-Dec-05
Day	Sunday morning			
Weather	occasional light shower	sunny	sunny	sunny
Route	Kennedy Town - Causeway Bay			
No. of AP	187	474	926	1576
% of WEP/WPA disabled	77%	69%	60%	46%
% of factory default SSID	51%	39%	44%	39%
% of 802.11g AP			8.32%	68.15%

(1) The number of detectable deployment along the tramway, comparing with last year, has increased by 70%.

(2) The percentage of APs with WEP/WPA turned on has improved by 14%.

(3) The percentage of APs with factory default SSID has decreased by 5%.

(4) Adoption 802.11g AP has sharply increased from 8.32% to 68.15%

- If we look at the whole tramway, we can still arrive at the similar conclusion.

	2003 Overall	2004 Overall	2005 Overall
Date	05-Oct-03	28-Nov-04	04-Dec-05
Day	Sunday morning		
Weather	Sunny		
Route	Kennedy Town - Shau Kei Wan		
No. of AP	784	1723	2650
% of WEP/WPA disabled	70%	61%	46%
% of factory default SSID	43%	46%	43%
% of 802.11g AP		14.16%	66.42%

(1) The number of detectable deployment along the tramway, comparing with last year, has increased by 53.8%.

(2) The percentage of APs with WEP/WPA turned on has improved by 15%.

(3) The percentage of APs with factory default SSID has decreased by 3%.

(4) Adoption 802.11g AP has sharply increased from 14.16% to 66.42%

Part II: War Driving on Bus/Car (in Kowloon)

Note 1: In War Driving on Bus/Car, we used several different antennae. We consolidated the readings from different war drivers into one single log. Duplicated records are trimmed.

Note 2: Unless otherwise specified, the statistics was generated by the consolidated log from different antenna.

1. Number of Access Points Captured

Location	Number of unique Access Points captured
Some areas in Kowloon, namely, Tsim Sha Tsui, Yau Ma Tei, Mong Kok, Sham Shui Po, Cheung Sha Wan and Hung Hom.	**4999**

2. Implementation of 802.11g, WEP/WPA and SSID configuration

AP Statistics	Percentage
Overall the implementation of 802.11g	3334 (66.69%)
AP with WEP/WPA disabled	2205 (44.11%)
AP with factory default SSID [2]	1954 (39.09%)

When comparing with war tramming results along Kennedy Town to Causeway Bay, the percentage of 802.11g implementation, WEP/WPA disabled and the use of factory default SSIDs were similar.

Note that the readings of war tramming and war driving on bus/car were taking with antennae with different sensitivity. The comparison by absolute number thus has no statistical value. However, the comparison by the percentage, on the other hand, could be meaningful.

Although the overall percentage of APs with WEP/WPA disabled is 44.11% as a whole, we found a interesting finding that the percentage of WEP/WPA disabled was much higher (about 65%) during the initial part of the bus trip from Tsim Sha Tsui to Mong Kok. The figures were dropping as we moved

[2] In the above table, "AP with factory default SSID" refers to factory default settings like:
- SSID that uses the ASCII characters of the station's hexadecimal MAC address;
- SSID that uses the ASCII characters of the station's hexadecimal MAC address subtracted by 1;
- SSID that uses a vendor-specific string concatenated with the ASCII characters of part of the station's hexadecimal MAC address;
- SSID that uses a vendor-specific string or generic string like “any” or “default”;

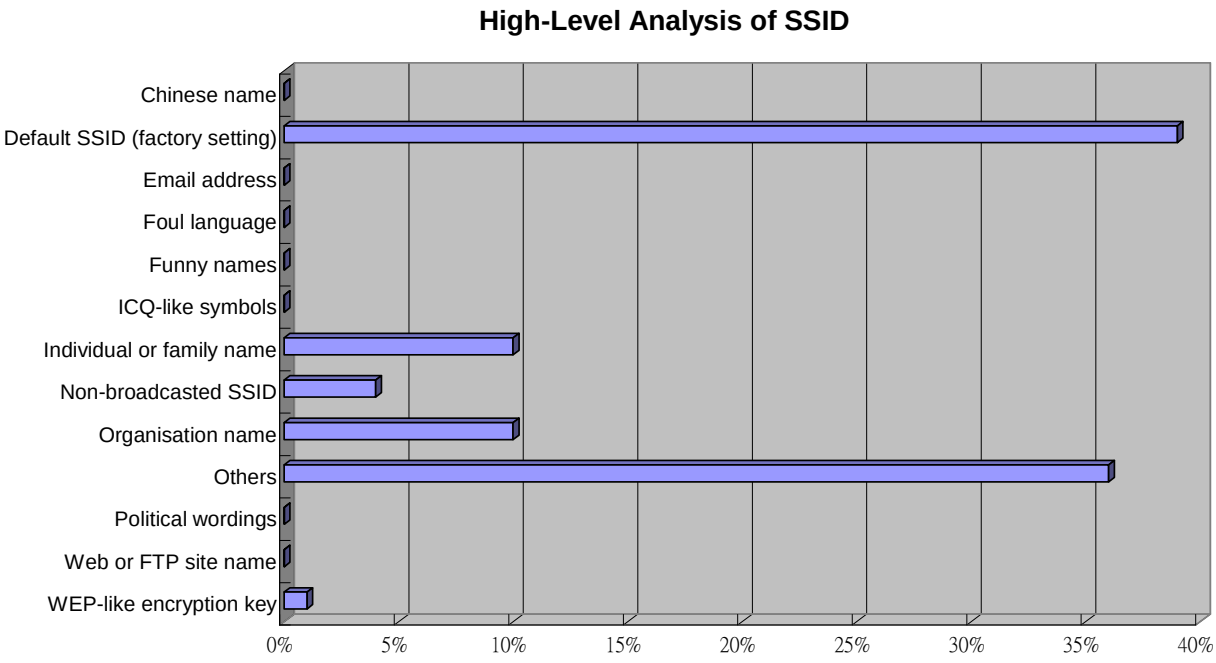
on the bus trip to Cheung Sha Wan. We briefly checked the log files and we believe this phenomenon may be because of relatively more hotspots, hotels, shopping malls, etc. in Tsim Sha Tsui to Mong Kok.

Other Findings

SSID analysis and statistics

We have performed some high level analysis of the 4999 SSID collected during the war-driving on bus/car. Below is a summary of the statistics.

Category	Percentage
Chinese name	0.01%
Default SSID (factory setting)	39%
Email address	0.01%
Foul language	0.01%
Funny names	0.01%
ICQ-like symbols	0.01%
Individual or family name	10%
Non-broadcasted SSID	4%
Organisation name	10%
Others	36%
Political wordings	0.01%
Web or FTP site name	0.01%
WEP-like encryption key	1%



From the above findings, it exhibits around 39% among total number of detected wireless Access Points (abbrev. APs) are configured with default SSIDs (or SSID of factory setting). For every brand new Access

Points, particular manufacturer will assign a default SSID to its product. It may be the manufacturer's name, MAC address or simply marked as "default", etc. In fact, the SSID is configurable but is not mandatory to be changed. Using a default SSID may mean that the administrator of the AP might not change the default settings including the default administrator password. They might be targets of hackers.

During our war driving, we discovered there were about 10% of SSIDs with organization and company names. Some of them define their SSIDs with their web domain address. When we search a SSID "XYZ" from Google with the query "XYZ Hong Kong", it displays their web site. SSIDs with organization/company names include shops, manufacturers, trading companies, hotspots, schools or churches. Where possible, we do not recommend setting SSID with the organization name. Hackers can easily identify the APs of the company and may launch attack (e.g. DDoS) or intrude to the internal network of the company. The outcome could be disastrous if confidential business or client information were stolen or exposed.

From our analysis, there was about 1% of detected APs putting their generated Wired Equivalent Privacy (WEP) key as their SSIDs. WEP is a scheme to secure wireless networks (WiFi). If the WEP key is exposed, anyone can go into the network without extra effort.

For the remaining detected APs, they may be personal name, email address, flat number, family name, symbol and other meaningless strings. It is also our first time to detect an AP with SSID in Chinese characters. In addition, some are configured with "Foul" language and politics-related statements. We do not recommend setting SSID that could uncover one's identity (e.g. XX Family, a person's name, flat number, email address, etc). Your neighbours or someone who know you may identify you and your network maybe hacked via social engineering attacks/techniques. We strongly recommend rectifying it immediately.

Disabling the broadcasting of the SSID is a more secured security setting. However, the percentage of non-broadcasted SSID (i.e. empty SSID) we found is not high (only about 4%).

For recommendations, we recommend not to use SSID names that can associate with your or your organization's identity. For a more safety measure, broadcasting function is better to disable and connections are restricted to approved MAC addresses in order to reduce the risk of unauthorized access. Enable encryption and if possible, use WPA/WPA2 instead of WEP (WEP is not secure nowadays). For a better network infrastructure practice, sensitive internal network and wireless network should be segregated. If connections are required, another layer of authentication including VPN or One-Time Password could be considered. Regular wireless site surveying and log review is recommended to detect any rogue Access Points and unauthorized connections.

Early adopters of “pre-N” APs

During our 4th round war driving in Dec/2005 and Feb/2006, we found some “pre-N” APs. They are examples of early adopters of the pre-version of 802.11n technology.

In March 2006, the IEEE unanimously approved a draft version of 802.11n that is expected to become the next generation standard for wireless networks. The standard provides for increased range and speeds as compared to current 802.11g standards. Draft 802.11n will also have backward compatibility with current 802.11b and g products.

802.11n will support bandwidth greater than 100 Mbps. 802.11n will work by utilizing multiple wireless antennas in tandem (or "MIMO" (Multiple Input, Multiple Output)) to transmit and receive data.

Some manufacturers offer "pre-N" wireless equipment. A Pre-N wireless router uses two transmitters and three receivers to double the speed of existing 802.11 devices to 108 Mbps. Pre-N products let customers boost speed before 802.11n devices are available.

Conclusion

Part I: War Tramming

- We still see a drastic growth of the number of WLAN AP (increased by 53.8% as compared to last year) but the growth rate was not as sharp as last year.
- For the adoption of encryption in WLAN AP, we find out that the adoption rate was exceeded 50% (i.e. both in the tramway survey (53.92%) in Hong Kong Island and the bus/car survey (55.89%) in Kowloon)**. Although the encryption rate exceeded 50%, it is only one area of improvement in WLAN security that is not sufficient. We have concerns on the SSID security. We found that wide use of factory default SSID.**
- Most APs broadcasted the SSID into the air. **Many APs were still using the factory setting of SSID**. The unchanged SSID may imply that the owners of the APs might not have even changed other default settings like administrative password. A hacker can try to associate to the AP without much difficulty.

Part II: War Driving on Bus/Car (in Kowloon)

- When comparing with war tramming along Kennedy Town to Causeway Bay, the percentage of 802.11g implementation, WEP/WPA disabled and the use of factory default SSIDs were similar.
- Although bus is moving faster than tram, we found that we can detect many APs and we think it is another good choice of public transport for locations that do not have tramway.

* * * The End * * *