Report on

Wireless LAN War Driving Survey 2003 Hong Kong

Version 2.3

Nov-2003

This report can be downloaded via URL

http://www.pisa.org.hk/projects/wlan2003/wd2003.htm.

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

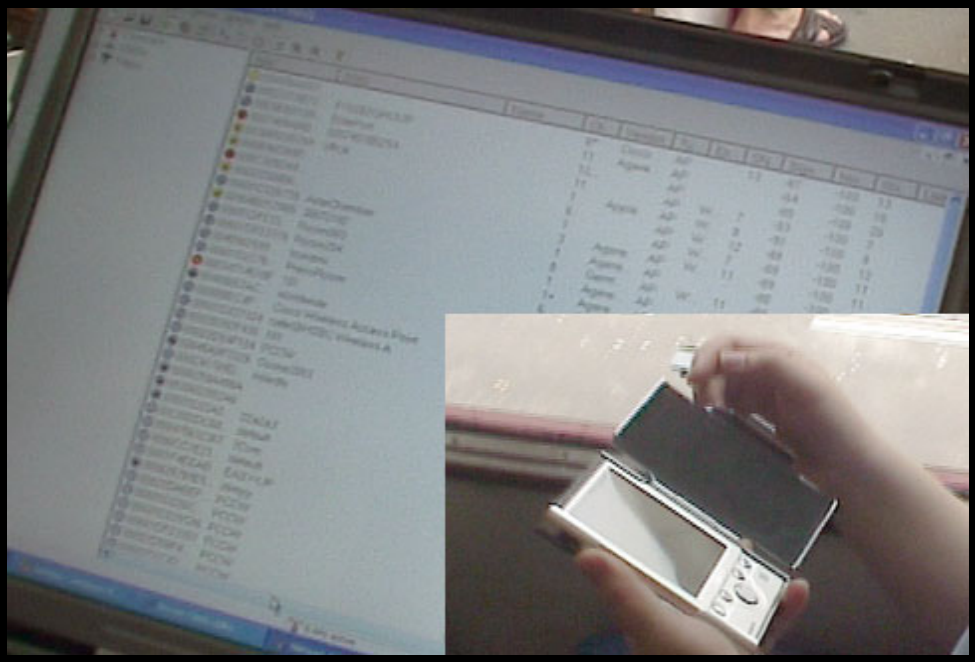
Briefing of the Code of Ethics at Pacific Place

[From left]: Sang(PISA), Jeff(e-Zone), SC(PISA), Dr. Lui & Artic (WTIA)

A +3dB antenna was used in Tramway War Driving.

[From left]: Jeff (e-Zone), Dr. Lui and Artic (WTIA), Jim (PISA)

Photos



War Driving is possible with simple equipment like a notebook computer or a PDA.

The team was comparing the findings of 2002 and 2003 at the Kennedy Town Tram Terminus

[From left]: Alan, Sang and Jim (PISA)

Photos

The War Driving Team with gears at the Victoria Peak (Peak-East point)

[Guys (& antenna) from left to right]: Clayton(+18dB), Ken(+14dB), Alan(+8dB), Jim & Sang

Discovering WLAN signal of Kowloon Peninsula with the +18dB antenna

(The tall building at the background was the International Financial Centre II)

Terms used

WLAN	Wireless Local Area Network. There are two popular standards now: • 802.11b: using 2.4GHz, 11Mbps (most popular) • 802.11g: using 2.4GHz, 54Mbps
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.

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 used wireless LAN

Executive Summary

In Oct 2003, the two associations **PISA** and **WTIA** jointly conducted the “War Driving 2003” field survey along the tramway of Hong Kong Island and from the Victoria Peak. 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 another study conducted by PISA in 2002 to plot the profile of Hong Kong WLAN security development. The survey indicated that the number of WLAN implementation had skyrocketed in the past year, and yet there was only a slight improvement in the adoption of security strategies. The number of discovered APs had notably increased by 153% while the percentage of improved security on the whole was only a few percents.

The result of the survey also proved that it was feasible to war drive from distances in the order of kilometres. With a high gain antenna, 257 APs was discovered at the Victoria Peak. Some of the discovered APs were from the far eastern edge of Hong Kong Island and Kowloon Peninsula. The possibility of war driving at such distance and height was out of the imagination of many people.

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.

In Oct 2003, **PISA** and **WTIA** jointly conducted the 2nd "War Driving" has been conducted to benchmark the improvement for the WLAN Security in Hong Kong. The scope of test has been 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

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 study the feasibility of long distance war driving and its impact to WLAN security
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 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 owner of the individual insecure APs. We publicize only consolidated figures.
- We do not connect to 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.

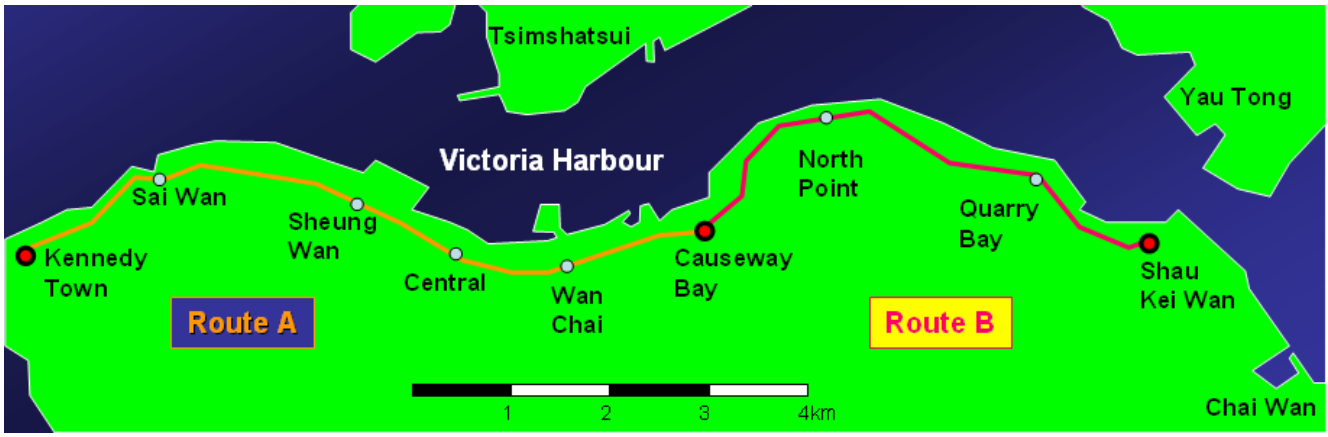
Methodology and Equipment

The War Driving was divided into 2 parts:

Part I: 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.
- By War Driving on a tram, we targeted to benchmark the results with that of the war driving study of year 2002 along the tramway from Kennedy Town to Causeway Bay (Route A).
- We also extended the route from Causeway Bay towards Shau Kei Wan, covering the whole tram way. This route is equivalent to the whole business corridor of Hong Kong Island. (Route B)

Date:	5-Oct-2003 (Sunday)
Time:	11 am -3 pm
Equipment:	*Hardware:* Notebook computers, WLAN cards and a +3dB omni-directional antenna (approximately 200mm long) *Software:* Netstumbler
Route:	• Route A: ○ Taking tram from Queensway, Admiralty westwards to Kennedy Town terminus, then return tram from Kennedy Town terminus to Sogo Department Store, Causeway Bay (this was the same route as in War Driving 2002) • Route B: ○ Taking another tram from Causeway Bay to Shau Kei Wan terminus



Part II: Victoria Peak War Driving

- The scenic Victoria Peak is a popular tourist spot. It has an altitude of 554m, overseeing the Hong Kong Island north coast and the whole Kowloon Peninsula. Round the peak is a path (the Lugard Road) with many scenic lookouts which are very suitable for war driving.
- By War Driving at the northern side of the Victoria Peak, we wanted to study the feasibility of War Driving from a long distance, e.g. the Kowloon Peninsula on the other side of the harbour.

Date:	12-Oct-2003 (Sunday)
Time:	11 am -3 pm
Equipment:	Same as "Tramway War Driving", except that a +18dB directional antenna (approximately 1m long) with 15° beam angle sensitivity was used
Route:	• Signals captured at two checkpoints of the Victoria Peak. ○ Point 1: Peak-West ○ Point 2: Peak-East (near Peak Tram station)

Two Checkpoints on the Victoria Peak

Point <1> Peak-West Point <2> Peak-East (near Peak Tram Station)

Summary of Findings

Part I: Tramway War Driving

1. Number of Access Points Captured

Locations	Number of unique Access Points captured
Route A: Tramway, from Kennedy Town to Causeway Bay	**474**
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	**784**

2. Overall the implementation of 802.11g in Hong Kong is below 10%.

More 802.11g implementation is found in the eastern part of Hong Kong.

Route A: Tramway, from Kennedy Town to Causeway Bay	2.6%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	9.1%

3. The use of WEP is around 30%

Route A: Tramway, from Kennedy Town to Causeway Bay	31.1%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	28.2%

4. The proportion of AP without securing SSID (include default SSID, well-known SSID and SSID same as trailing hexadecimal of AP's MAC address)

Route A: Tramway, from Kennedy Town to Causeway Bay	35.8%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	52.4%

Note: there were 10 hotspots which used well-known SSID.

5. Used Channels

- The most common channels are 1, 6 and 11.
- There are a few (six) 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

6. How is the result compared with War Driving 2002?

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
Date	7-Jul-2002	5-Oct-2003
Day	Sunday morning	
Weather	occasional light shower	sunny
Route	Kennedy Town - Causeway Bay	
No. of AP	187	474
% of WEP disabled	77%	69%
% of insecure SSID	51%	39%

(1) The number of detectable deployment along the tramway has increased by 153%.

(2) The percentage of APs with WEP turned on has improved by 8%.

(3) The percentage of APs with SSID secured has improved by 12%.

Conclusion:

- We can see a great leap in the use of WLAN whereas the **improvement in security is only a small step.**
- **The percentage of AP with WEP disabled still amounted to near 70%**
- Many APs broadcasted the SSID into the air. **Many APs were still using the factory setting of SSID**. The unchanged SSID could further 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.

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

	2003 Overall
Date	5-Oct-03
Route	Kennedy Town - Shau Kei Wan
No. of AP	784
% of WEP disabled	70%
% of insecure SSID	43%

Part II: Victoria Peak War Driving

7. Peak War-Driving with a stronger antenna was possible

- The +18dB 15° beam angle antenna was panned to different angles to maximize signals received. It was specifically orientated to target at points in Hong Kong Island north (Central and Wan Chai), Kowloon Peninsula, far away point in the west (Kwai Chung Container Terminal) and the east (Shau Kei Wan).
- The Peak War Driving was able to capture a great number of APs. This was comparable to Tramway War Driving with +3dB antenna.
- The APs captured in Peak-West is a superset of that of Peak-East.

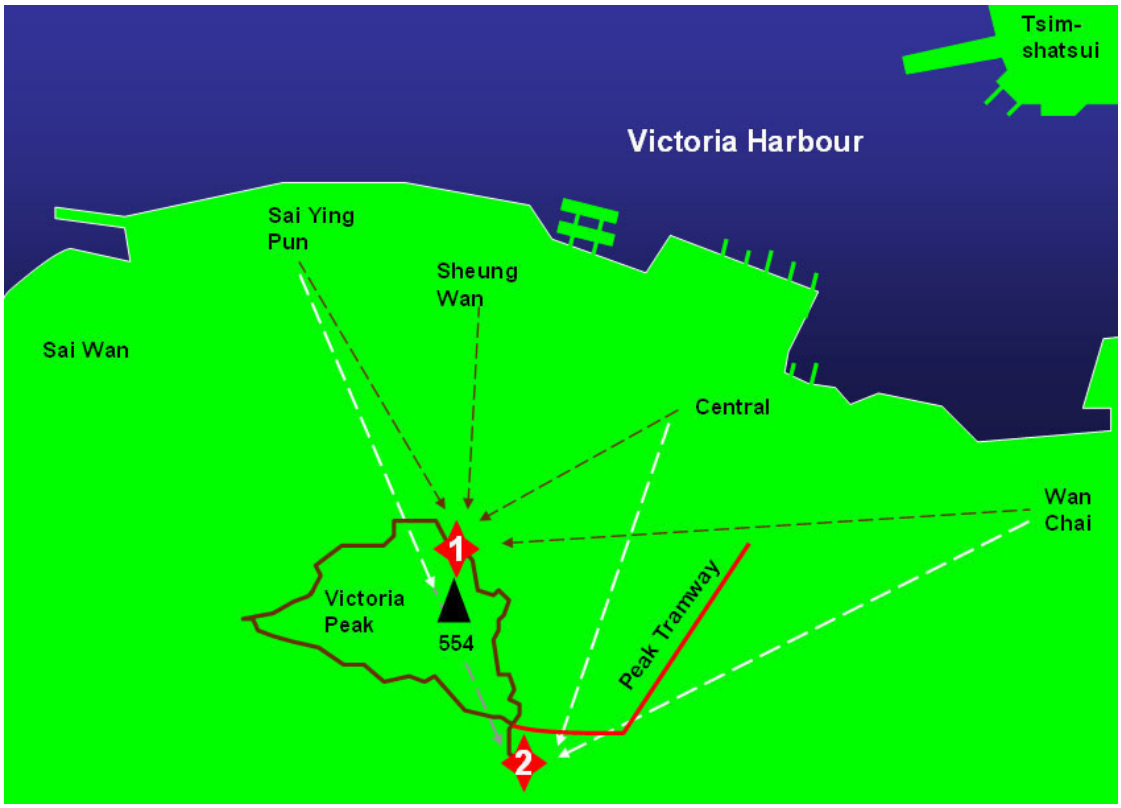
Locations in Victoria Peak	Number of unique Access Points captured
Peak-West	**257**
Peak-East	**120** (subset of Peak-West)

- The statistics of the security attributes of APs discovered at Peak-West (i.e. including all APs discovered at Peak-East) is shown below.

Peak-West AP Statistics	Percentage
Overall the implementation of 802.11g	4.7%
AP with WEP turned off	71.2%
AP without securing SSID	46.3%

8. Critical point to succeed in the Peak War-Driving

- The 257 APs captured at Peak-West include all 120 APs captured from Peak-East. Naturally one point is much more successful than the other. Why?
- What are the differences of the 2 points?



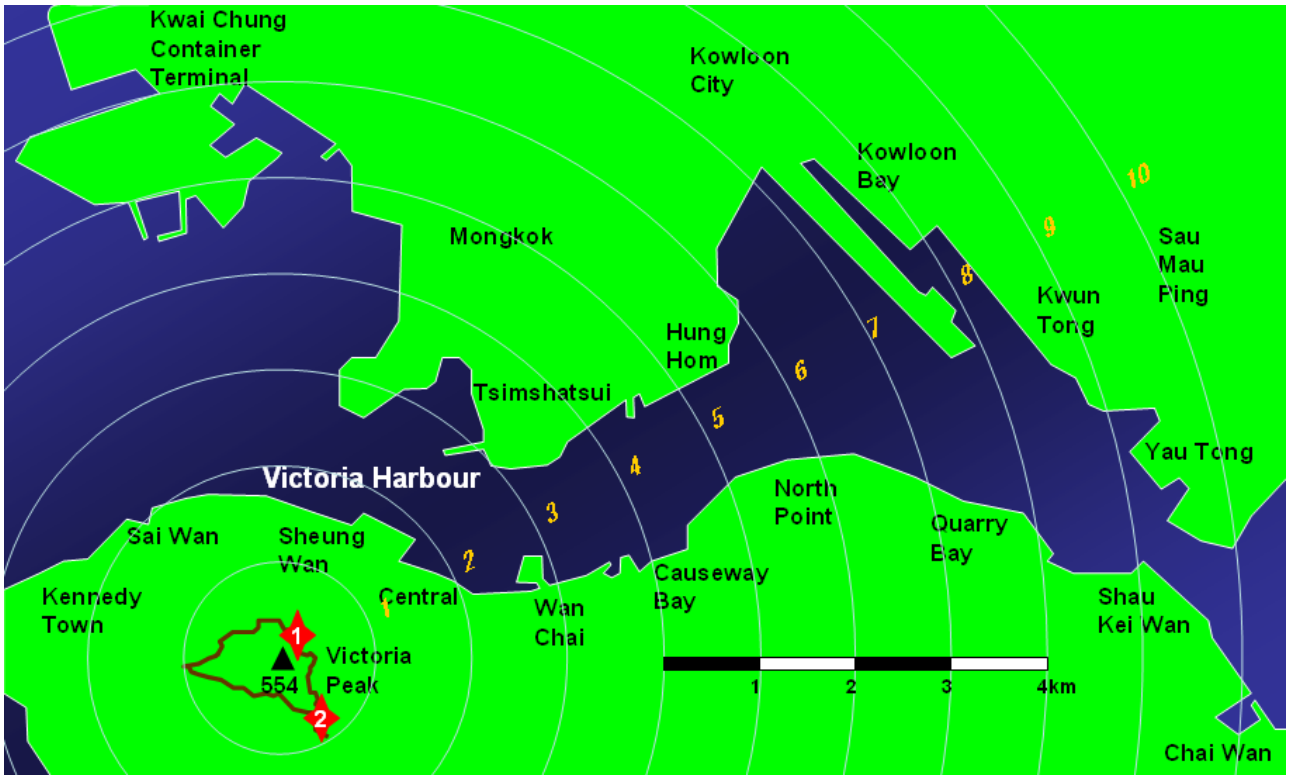
- Firstly, for far away APs, the geographically difference in terms of distance and direction of the two points (Peak-East and Peak-West) are insignificant.
- Peak-West (Point <1>) has a better position for both western and eastern because it is on the convex spur. It is in the line of sight of even eastern part of island including Hopewell centre. It is however, not in line of sight to some Wan Chai areas near the slope.
- Peak-East (Point <2>) is in the concave valley and mostly blocked to the western Hong Kong like Sai Ying Pun. It however, has a better sight to Wan Chai areas near the slope.

Conclusion:

1) **Line-of-sight** is a critical factor in WLAN signal transmission (this is also well-known in theory).
2) Since the 2 points at peak has insignificant difference in terms of distance and direction to far away APs, we cannot draw a conclusion on importance of distance compared with direction.
3) From our experiment, **the antennae orientation and its beam angle** are critical to reception and coverage. They must be carefully tuned. This has an implication on both performance and security.

9. How far can WLAN signal be transmitted and received?

Below is a map showing the horizontal distance of various points from the Victoria Peak. The equi-distant lines (circles) are separated by 1 km.



We can calculate the line-of-sight distance of the points from the Victoria Peak by simple mathematics.

	Horiz dist (km) H	Vert dist (km) = ht. of Peak V	Line-of-sight dist (km) SQRT ($H^2 + V^2$)
Peak-West to City Hall	2.0	0.55	2.08
Peak-East to City Hall	2.2	0.55	2.27
Peak-West to HKCEC	3.2	0.55	3.25
Peak-East to HKCEC	3.0	0.55	3.05
Peak-West to TST	3.6	0.55	3.64
Peak-East to TST	3.9	0.55	3.94
Peak-West to Kwai Chung Container	6.3	0.55	6.32
Peak-East to Kwai Chung Container	7.2	0.55	7.22
Peak-West to Shau Kei Wan	8.7	0.55	8.72
Peak-East to Shau Kei Wan	9.2	0.55	9.22
Peak-West to Sau Mou Ping	10.4	0.55	10.41
Peak-East to Sau Mou Ping	10.5	0.55	10.51

- We could receive AP signals from nearby points in the Hong Kong Island, by pointing the antenna at the target, say, around **City Hall in Central** or around **HKCEC in Wan Chai**. These targets were 2km to 3.3km away.

- We could receive AP signals from the **Kowloon Peninsula** (estimated 10-20 APs). They might come from TST, Mongkok or even Kwai Chung Container Terminal. These targets were 3.6km to 7.2km away.

- We could also receive signals from nine of the APs we captured **along the tramway from Kennedy Town to Shau Kei Wan** in the previous week. We had carefully verified their SSID and MAC address. The SNR of the signals of the nine APs is tabled below. (Remark: at the peak we are using a +18dB antennae while along the tramway we used a +3dB antenna.) We can see that AP5 is probably located near **Shau Kei Wan** which was measured to be about 9km from the Peak.

	Signal-to-Noise Ratio (dB)		
AP (anonymous)	**Peak West** (+18dB antenna)	**Tram - Kennedy Town to Causeway Bay** (+3dB antenna)	**Tram - Causeway Bay to Shau Kei Wan** (+3dB antenna)
AP1	17	9	
AP2	10	12	
AP3	10	20	
AP4	9	17	
AP5	**6**	**5**	**16**
AP6	5	15	
AP7	5	2	
AP8	2	7	
AP9	-1	11	

- We could also receive signals in Peak-West from an AP whose name signified its location in **Sau Mou Ping** which is 10.5 km away. Although we ***cannot*** verify its location, it is possible that an AP with a suitable antenna can transmit signals over 10km, given the orientation of the antennae of the transmitting and receiving ends matching well. (In open space, WLAN signal can transmit up to 20km with very high gain antenna.)

Conclusion:

- With a sensitive antenna which was correctly oriented, **it was possible to receive WLAN signals from about 10km in the line-of-sight. War Driving from a long distance is totally feasible and even from high up in the mountain.**
- We thus **should not take for granted that WLAN is secured from hacker out-of-sight!**

10. How strong was the received WLAN signal at the Peak?

- The high gain antenna was proved to be very useful in improving the sensitivity of reception. It was verified by taking it off and observed the drop in SNR of the received signals from the APs.

- The Signal Strength Distribution Analysis (using SNR) is plotted below:

	Peak-East (+18dB ant)		Peak-West (+18dB ant)		Tram-Kennedy Town (+3dB ant)		Tram- Shau Kei Wan (+3dB ant)	
	%age	# of APs	%age	# of APs	%age	# of APs	%age	# of APs
Total		**120**		**257**		**474**		**321**
below 10dB	62.5%	75	61.9%	159	36.3%	172	39.6%	127
10-19 dB	32.5%	39	32.7%	84	49.4%	234	48.3%	155
20-29 dB	**5.0%**	**6**	**5.4%**	**14**	12.9%	61	11.2%	36
30-39 dB	0.0%	0	0.0%	0	1.3%	6	0.6%	2
40 dB or above	0.0%	0	0.0%	0	0.2%	1	0.3%	1

- **At the Peak, we are still able to achieve a SNR of near 30dB for a few APs we captured! (best was 28dB).**

Conclusion:

- **With an even better antenna, we might be able to have a strong enough signal to connect to! Hacking from a distance is totally possible, provided equipment is available. So every effort should be taken to secure the wireless LAN network.**

* * * The End * * *