



*SafeWiFi Campaign 2010 (WiFi安全話咁易 2010)  
War-Sailing Event*

*Topic: Vulnerability of WiFi and Improvement on  
WiFi Security*

*by*

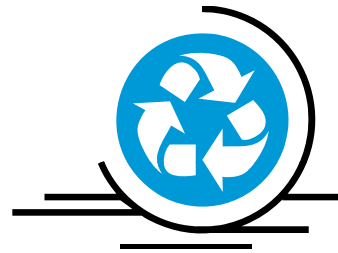
*Professional Information Security Association (PISA)  
專業資訊保安協會*

**Alan Ho**

20-Nov-2010

## Disclaimer

- The material and discussion in the demonstration is solely for promotion of security awareness and educational purposes. This material is NOT intended to be adopted in the course of attacking any computing system, nor does it encourage such act.
- PISA would warn that unauthorized access to computer system, damage of data and computer system are offences
- PISA takes no liability to any act of the user or damage caused in making use of the demonstration material

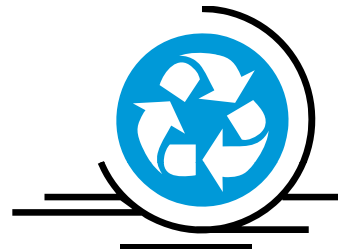


# Agenda



# Agenda


- Recent News
- Basics
- WLAN Network Survey
- Threats / Impact
- Tips and Recommendations
- Q & A



## About PISA



## About PISA

- Professional Information Security Association  
(專業資訊保安協會) – [www.pisa.org.hk](http://www.pisa.org.hk) 
- Established in 2001; not-for-profit organization
- Facilitate knowledge and information sharing among the PISA members
- Promote highest quality of technical & ethical standards and best-practices in information security
- Promote security awareness to the IT industry and general public in Hong Kong
- To be a de facto representative body of local information security professionals



# About PISA

## Journal



Study groups



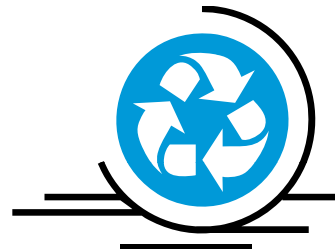
Sharing sessions, seminars, workshops



Comments to government & industry matters/policies



Media



## Recent News



# Recent News

## April/2010: Google Street View logs WiFi networks, Mac addresses



[Germany]

- Discovered that Google Street View captured Wi-Fi data during scanning

[Hong Kong]

- Google Street View car collected data in Hong Kong in early 2009
- 11/Mar/2010, Google Street View for Hong Kong/Macau were launched
- Jun/2010, HK Privacy Commissioner said that Google pledged deleting the data in question completely and will comply HK privacy law if future collection is needed

Reference:

- <http://online.wsj.com/article/BT-CO-20100608-704093.html>
- [http://www.theregister.co.uk/2010/04/22/google\\_streetview\\_logs\\_wlans/](http://www.theregister.co.uk/2010/04/22/google_streetview_logs_wlans/)
- <http://blogoscoped.com/forum/147935.html>
- [http://www.pcpd.org.hk/english/infocentre/press\\_20100517.html](http://www.pcpd.org.hk/english/infocentre/press_20100517.html)



## Recent News

### Jan/2007: Retailer TJX reports massive data breach

Credit, Debit data stolen (over 90 million card numbers stolen)



- Over 90 million credit and debit cards were stolen over a period of 18-months by hackers who managed to penetrate its network
- Hackers used a modified sniffer program to monitor and capture data from TJX's transaction systems. TJX was using the Wired Equivalent Privacy (WEP) encryption.
- Apr/2010: A five-year prison term for one of the criminals

Reference:

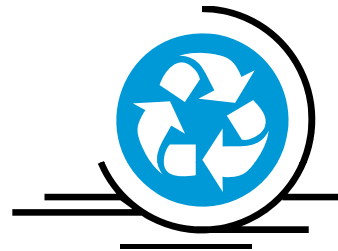
[http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_gci1254020,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1254020,00.html)

[http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_gci1249421\\_mem1,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1249421_mem1,00.html)

<http://www.infoworld.com/d/security-central/retailer-tjx-reports-massive-data-breach-953>

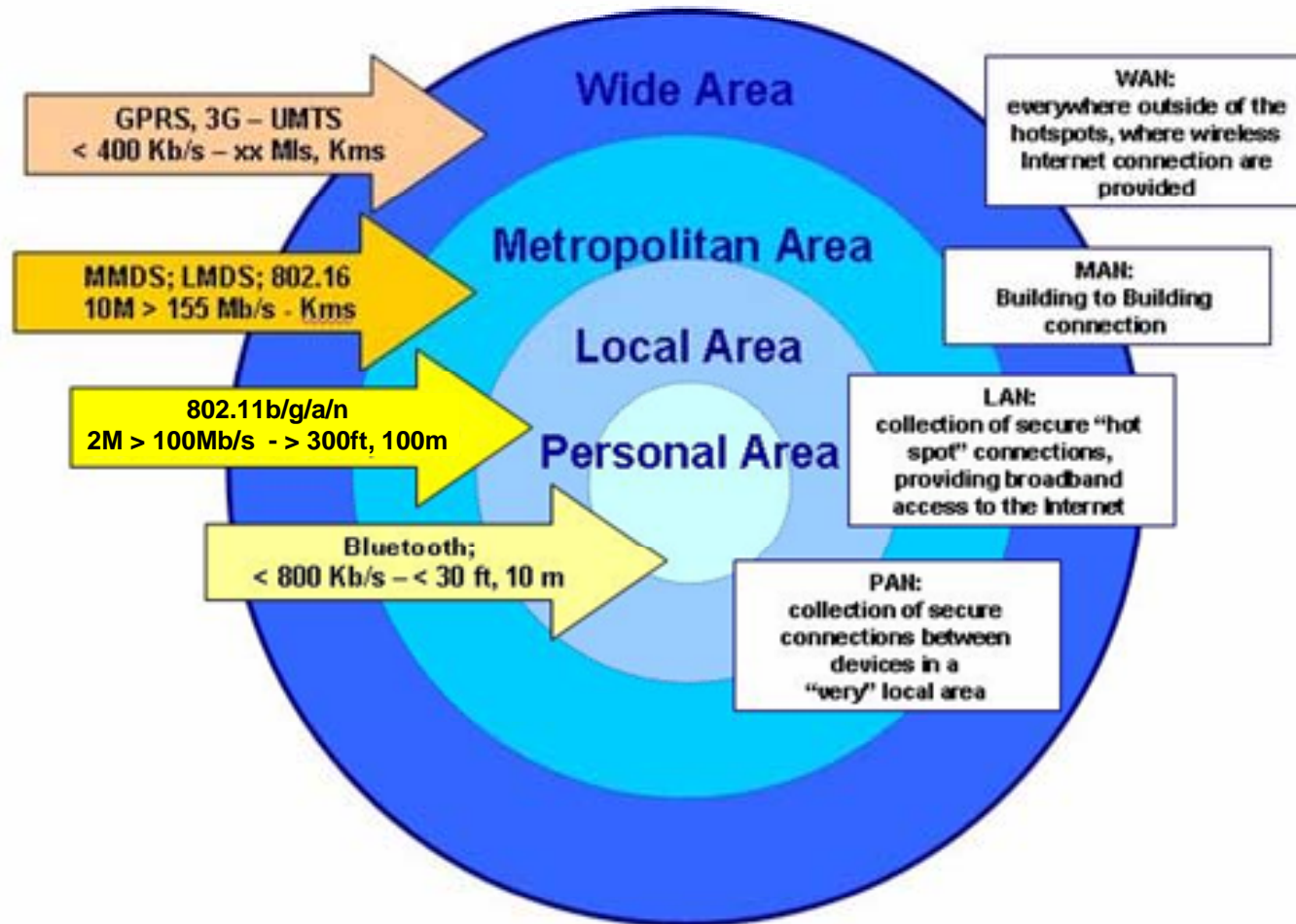
<http://www.secpoint.com/fiveyear-sentence-tjxcoconspirator.html>

[http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_gci1360065\\_mem1,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1360065_mem1,00.html)

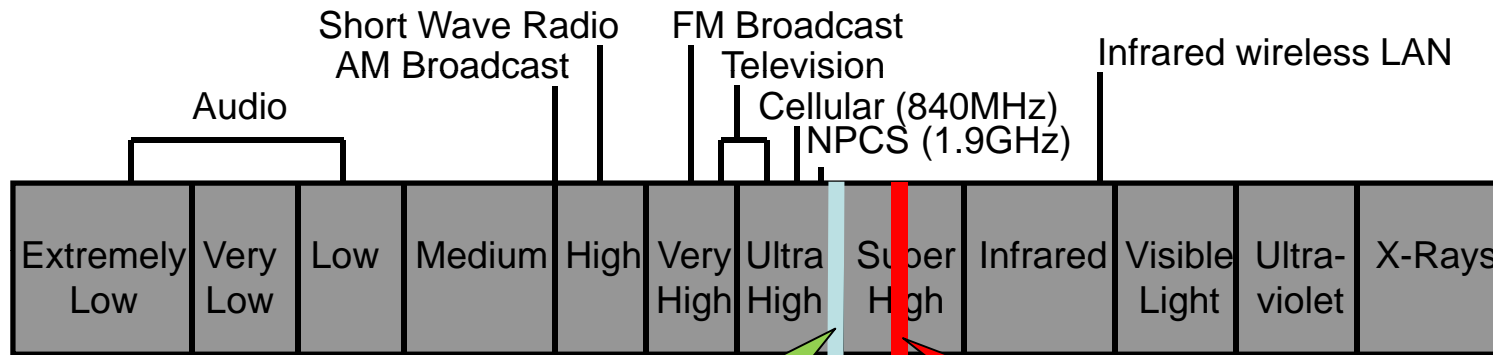


# Basics

# Types of Wireless Networks

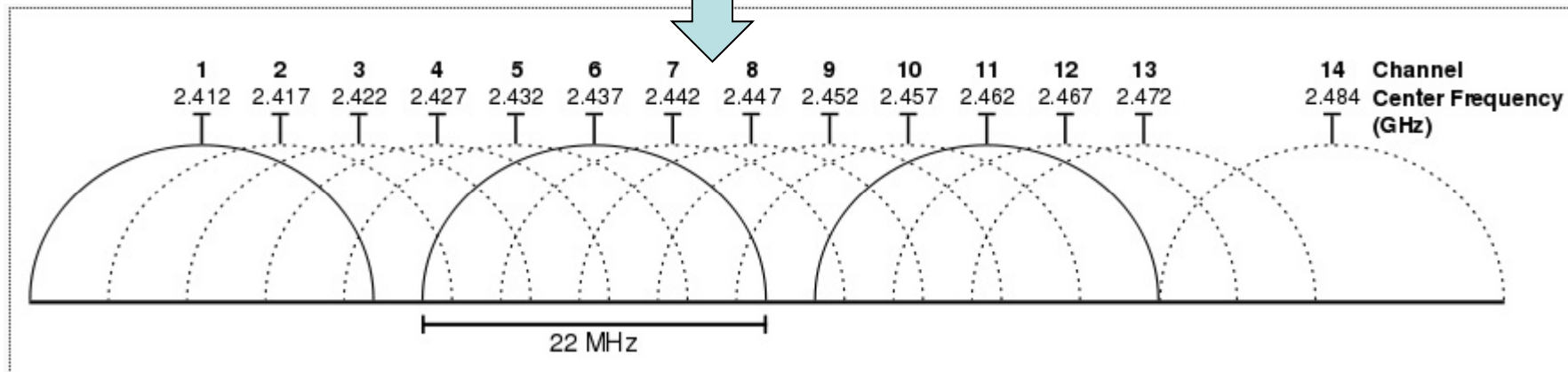


# Wireless Spectrum



**2.4GHz**  
**802.11b/g/n**

**5GHz**  
**802.11a/n**



Graphical representation of Wi-Fi channels in 2.4 GHz band  
(Source: [http://en.wikipedia.org/wiki/List\\_of\\_WLAN\\_channels](http://en.wikipedia.org/wiki/List_of_WLAN_channels))

# 802.11 Network

Protocol	Maximum throughput	Normal throughput in practice	Wireless spectrum	Channels in Hong Kong
802.11b	11Mbps	4Mbps	2.4GHz	1-13
802.11g	54Mbps	20Mbps	2.4GHz	1-13
802.11a	54Mbps	20Mbps	5GHz	36-64
802.11n	450Mbps to 600Mbps	100Mbps+ to 125Mbps+	2.4GHz or 5GHz	1-13, 36-64

Wi-Fi is often used as a synonym for IEEE 802.11 technology -- a trademark of the Wi-Fi Alliance to certify WLAN devices based on the IEEE 802.11 standards

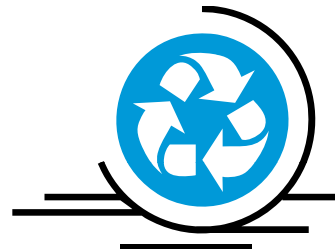


Reference:

- IEEE 802.11 -- [http://en.wikipedia.org/wiki/IEEE\\_802.11#cite\\_note-CNAF-10](http://en.wikipedia.org/wiki/IEEE_802.11#cite_note-CNAF-10)
- WLAN channels -- [http://en.wikipedia.org/wiki/List\\_of\\_WLAN\\_channels](http://en.wikipedia.org/wiki/List_of_WLAN_channels)
- WLAN channels (Hong Kong) -- <http://support.apple.com/kb/SP20>
- 802.11n -- <http://www.itworld.com/mobile-amp-wireless/100710/getting-most-80211n>

# Characteristics of 802.11 Network

- No physical wiring → high mobility
- No network border
  - First-line of protection: **network encryption**
- Network performance subjects to physical environment
  - Wall, iron bar (windows), interference by other wireless network, etc



# 802.11/Wi-Fi Network Survey





# War Driving

- War Driving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle using a Wi-Fi-equipped computer, such as a laptop or a PDA
- Tools
  - Software
    - Vistumbler (<http://www.vistumbler.net/downloads.html>)
    - Wifi-Hopper (<http://wifihopper.com/download.html>)
  - Hardware
    - Notebook PC or PDA with a WLAN adaptor
    - GPS (optional)
    - External antenna (optional)



# War Driving

Vistumbler v10 Beta 10 - By Andrew Calcutt - 01/06/2010 - (2010-06-21 10-26-23.mdb)

File Edit Options View Settings Interface Extra Help \*Support Vistumbler\*

Stop Use GPS Active APs: 14 / 31 Latitude: N 0000.0000  
Actual loop time: 1002 ms Longitude: E 0000.0000

Graph1 Graph2

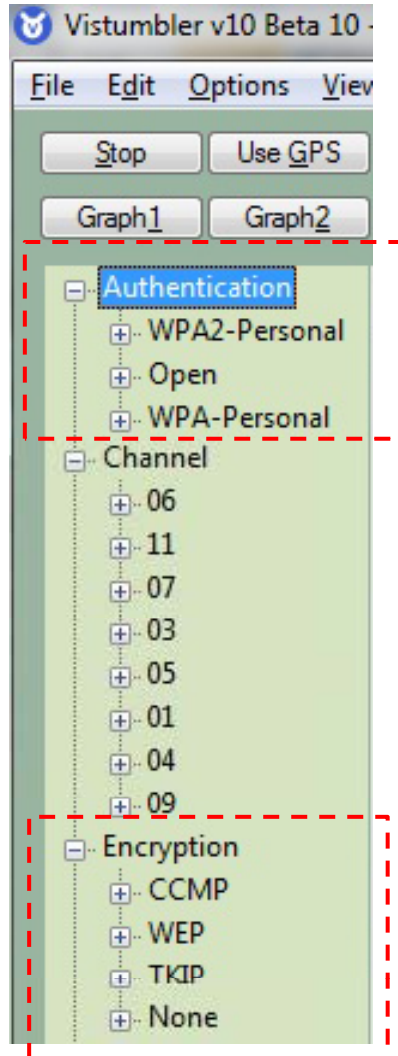
#	Active	Mac Address	SSID	Signal	Channel	Authentication	Encryption	Network Type	Latitude	Longitude	Manufacturer
3	Dead	00:0E:2E:BB		0%	11	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	Edimax Technol...
3	Dead	00:13:10:41		0%	6	WPA2-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys, LLC
2	Dead	00:27:19:CB		0%	6	Open	None	Infrastructure	N 0.0000000	E 0.0000000	TP-LINK TECHN...
2	Dead	00:25:C4:0B		0%	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Ruckus Wireless
2	Dead	00:23:CD:17		0%	9	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	TP-LINK TECHN...
2	Active	00:25:9C:48		30%	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys, LLC
2	Dead	00:E0:FC:4C		0%	11	WPA2-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	HUAWEI TECHN...
2	Dead	00:15:EB:4E		0%	3	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	ZTE CORPORATI...
2	Active	00:0D:0B:14		23%	11	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	Buffalo Inc.
2	Dead	00:B0:0C:02		0%	6	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	Unknown
2	Dead	D8:5D:4C:A		0%	9	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	TP-LINK Techno...
2	Dead	00:15:EB:60		0%	4	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	ZTE CORPORATI...
1	Dead	00:1C:F0:7E		0%	6	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	D-Link Corporati...
1	Dead	00:25:9C:62		0%	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys, LLC
1	Active	00:14:BF:F2		40%	5	WPA2-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys LLC
1	Active	00:16:01:F4		36%	3	WPA2-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Buffalo Inc.
1	Dead	00:23:CD:C		0%	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	TP-LINK TECHN...
1	Dead	00:25:86:56		0%	6	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	TP-LINK Techno...
1	Dead	00:22:6B:82		0%	6	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys, LLC
1	Active	00:13:10:B7		35%	7	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys, LLC
1	Active	00:22:93:44		25%	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	ZTE Corporation
1	Dead	00:90:CC:EA		0%	11	WPA2-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Planex Commun...
9	Active	00:11:6B:1F		43%	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Digital Data Co...
8	Active	00:1C:10:C0		45%	11	WPA2-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys, LLC
7	Active	00:23:69:14		93%	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys, LLC
6	Active	00:1C:DF:05		43%	6	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	Belkin Internatio...
5	Active	00:23:F8:22		51%	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	ZyXEL Communi...
4	Active	00:13:46:71		28%	6	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	D-Link Corporati...



**Unauthorized access to computer system, damage of data and computer system are offences**



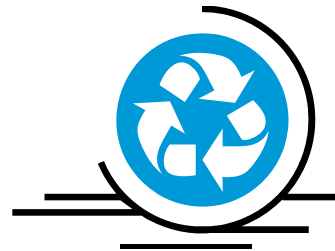
# War Driving



Authentication	Encryption
Open	WEP
WPA-Personal	TKIP
Open	None
WPA2-Personal	CCMP
WPA2-Personal	CCMP
WPA2-Personal	CCMP
WPA-Personal	TKIP
Open	WEP
Open	WEP
Open	WEP
WPA2-Personal	CCMP
Open	WEP
Open	WEP
WPA2-Personal	CCMP
WPA-Personal	TKIP
WPA-Personal	TKIP

Callouts from the table:

- WEP (points to the first row)
- None (points to the third row)
- WPA2-AES (points to the fifth row)
- WPA-TKIP (points to the seventh row)



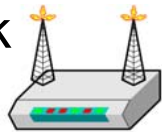
## Threats and Impacts

## Threats / Impacts

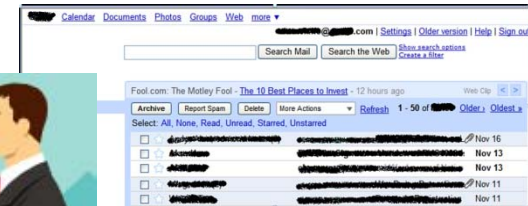
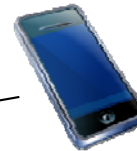
- Network bandwidth sharing → slower performance
- Commit crime or launch attack
  - Hackers may hack your computer(s) in the your network
    - Commit crimes
    - Perform attack to other networks (botnet / zombie computers)
- Potential data loss / leakage of sensitive information
  - Hacker may hack your computer(s) in the your network
    - Steal sensitive information on the computer(s) or in the network
  - If network encryption is “none” or “WEP”, hackers can possibly capture unencrypted sensitive information transmitted in the network (e.g. email) or even replayed your browser sessions e.g. email session (via sidejacking)

# Sidejacking Attack

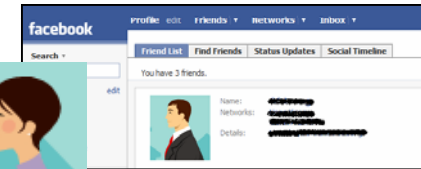
Open ~~lock~~ or WEP ~~lock~~  
enabled wireless  
network



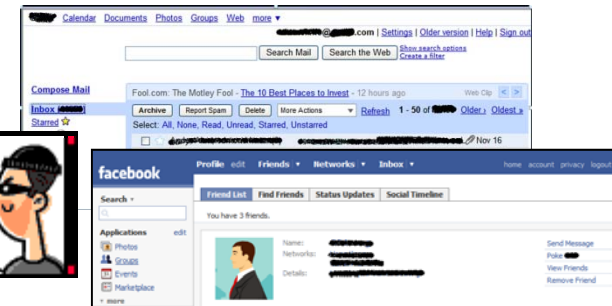
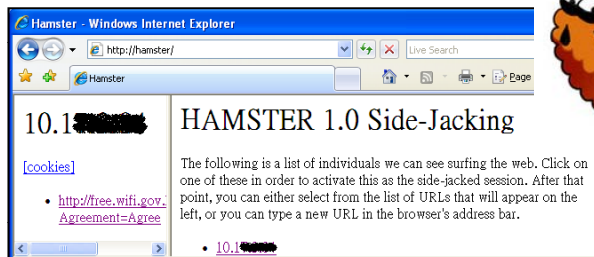
cookies, URL



cookies, URL



sidejack



Enter to victim's browser sessions

# WEP key cracking



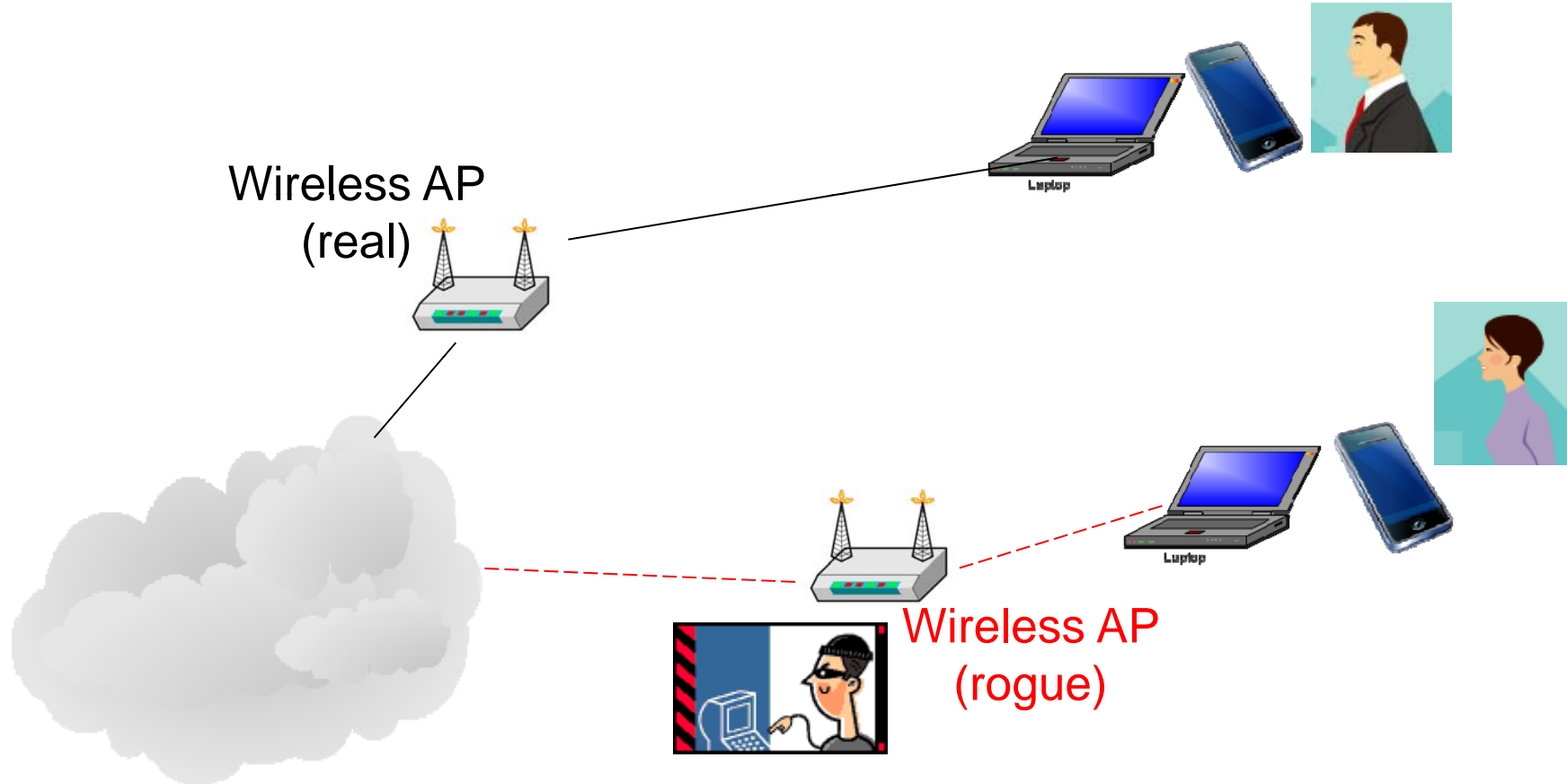
- 蹭網卡 (cost about \$150)  
【漢語拼音】：cèng ;  
廣東話：【發蝨蹭】
- Automatically crack WEP key in a few minutes

Reference:

<http://forum.vlshk.com/view.php?id=47>

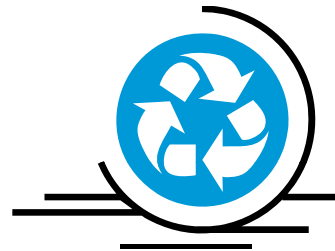
1

# Man-in-the-Middle Attack



Acting as a proxy to intercept/view the content transmitting through the network





## Tips & Recommendations

# Tips and Recommendations

- Secure the WLAN network using WPA/WPA2-AES under personal mode or WPA/WPA2 enterprise mode

Encryption	Level of security	Remark
None	Insecure	•No encryption at all
WEP	Insecure	<ul style="list-style-type: none"> <li>•Shared password/key</li> <li>•WEP key can be cracked in a few minutes</li> <li>•Cracking tools are widely available</li> <li>•Due to old design, security cannot be improved with a longer WEP key</li> </ul>
WPA/WPA2 Personal TKIP	Comparatively still safe but recommend to use AES security mode	<ul style="list-style-type: none"> <li>•Shared password/key</li> <li>•TKIP is theoretically can be cracked</li> <li>•Tools are emerging but not widely used</li> <li>•Recommend to use shorter Key Renewal time if AES option is not available</li> </ul>
WPA/WPA2 Personal AES	Secure	<ul style="list-style-type: none"> <li>•Shared password/key</li> <li>•No threat discovered at the moment</li> </ul>
WPA/WPA2 Enterprise AES	Secure	<ul style="list-style-type: none"> <li>•Individual user ID &amp; password with a backend authentication server (802.1X authentication / RADIUS)</li> <li>•No threat discovered at the moment</li> </ul>



## Tips and Recommendation

- Though MAC address can be spoofed, recommend to enable MAC Address Filtering
- Though hidden SSID can be seen with a suitable tool, recommend to hide SSID
- Change SSID to not easily identifiable
- Do not just use the “off-the-shelf” settings, need to review
- Better not to put the AP near to the Windows to reduce chance of connection outside your home/office
- For additional security, place WLAN AP outside the Intranet and then connect to Intranet via VPN, etc.

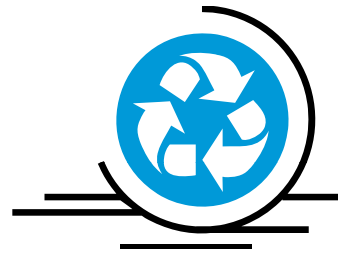
# Tips and Recommendation

- Hotspot
  - Use secured channels to handle sensitive data (e.g. email, social network, online transactions)
    - Some hotspot service provider(s) provide both secured and unencrypted channels
    - HK government Wi-Fi – both secured and unencrypted channels are available. (Secured channel: “freegovwifi-e” using WPA encryption)
  - Beware of rogue access points – be aware of any strange behaviours/response during the connections (remark: some enterprise wireless network systems can detect rogue access points)
  - Use VPN in case secured channel is not available
- May consider using 3G HSDPA thumb key (i.e. not using 802.11/Wi-Fi network) to handle sensitive data

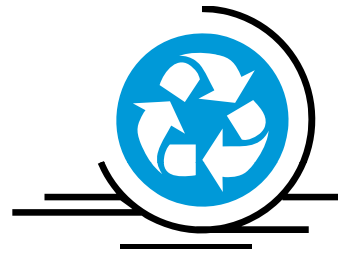


# Contact PISA

- Contact  
Alan Ho : [alan.ho@pisa.org.hk](mailto:alan.ho@pisa.org.hk)
- Website  
– <http://www.pisa.org.hk>



## Q & A



**Thank You**