OFTA
電訊管理局

2nd JUCC Information Security Conference

Security in Mobile Computing

Mr Eric Lam

Assistant Director (Support)

Office of the Telecommunications Authority

20 May 2011

Outline

- Introduction
- Profile of Hong Kong Wireless Broadband Infrastructure
- Security Threats to Nomadic/Mobile Computing Devices
- Protecting Your Mobile Computing Devices
- Using WiFi Safely
- Public Awareness Programs – The SafeWiFi Campaign

  & the Hong Kong WLAN Safety Index
- Public WiFi Security Guidelines
- Way Forward

Introduction

- Mobile security was not an issue when there were few smartphones/tablets, and mobile data and WiFi services were not common

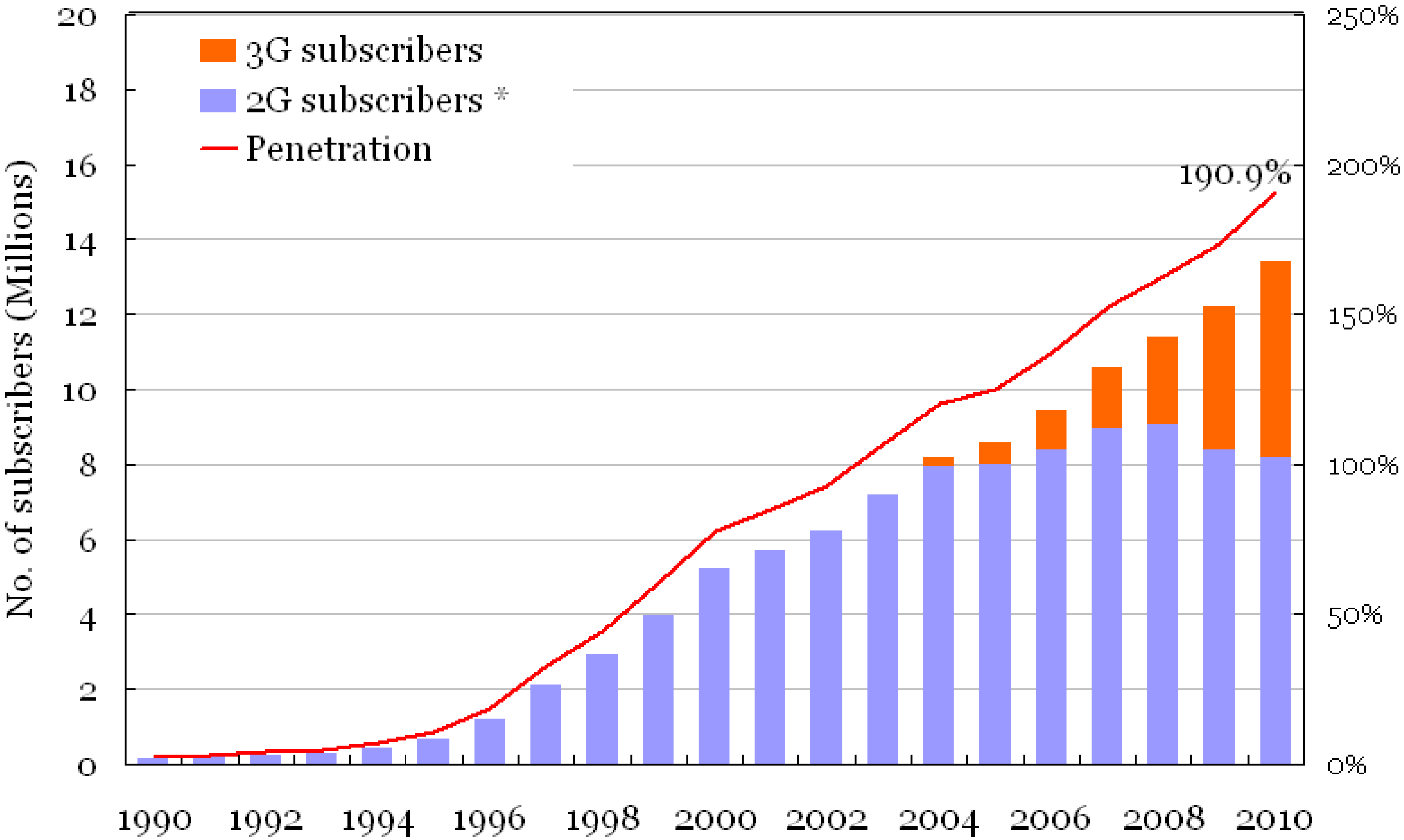
- The situation has changed significantly with the proliferation of smartphones, wider use of mobile data and WiFi services

Wireless Broadband Infrastructure

- **Mobile broadband by 5 operators**
  - HSDPA+: up to 42 Mbps
- **Broadband Wireless Access**
  - Three LTE networks, up to 100 Mbps
  - Service to be launched by end 2011
- **Public WiFi**
  - Over 9,000 Acess Points (APs) @ 5000 locations
- **Free GovWiFi**
  - covers 352 premises (will be further expanded to cover 40 additional locations by November 2013)

OFTA
電訊管理局

Mobile Date Service Penetration



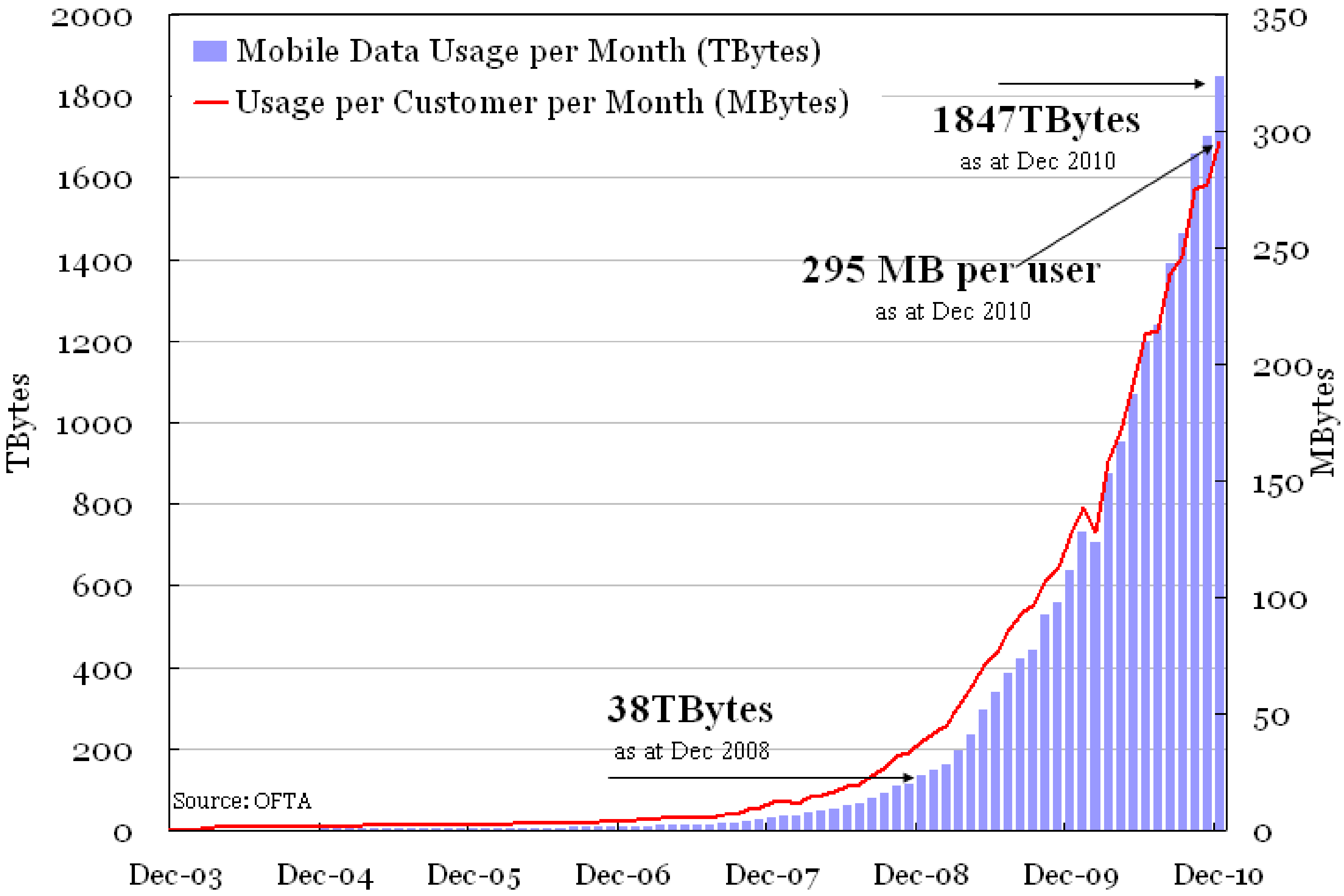
* The figures of 2G subscribers include those who subscribed 2G plan or using 2G prepaid card but occasionally use 3G services.

Source: OFTA

OFTA

電訊管理局

Mobile Date Traffic Growth



1847TBytes
as at Dec 2010

295 MB per user
as at Dec 2010

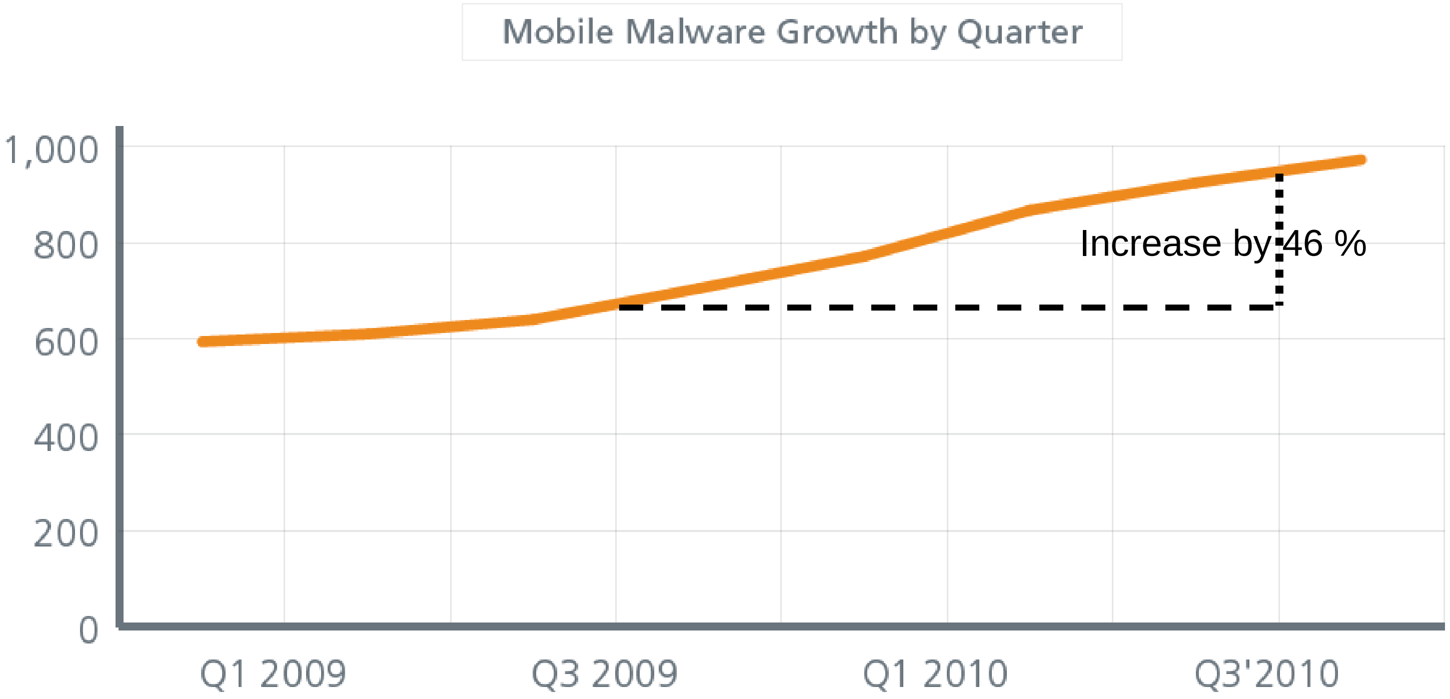
38TBytes
as at Dec 2008

Source: OFTA

OFTA
電訊管理局

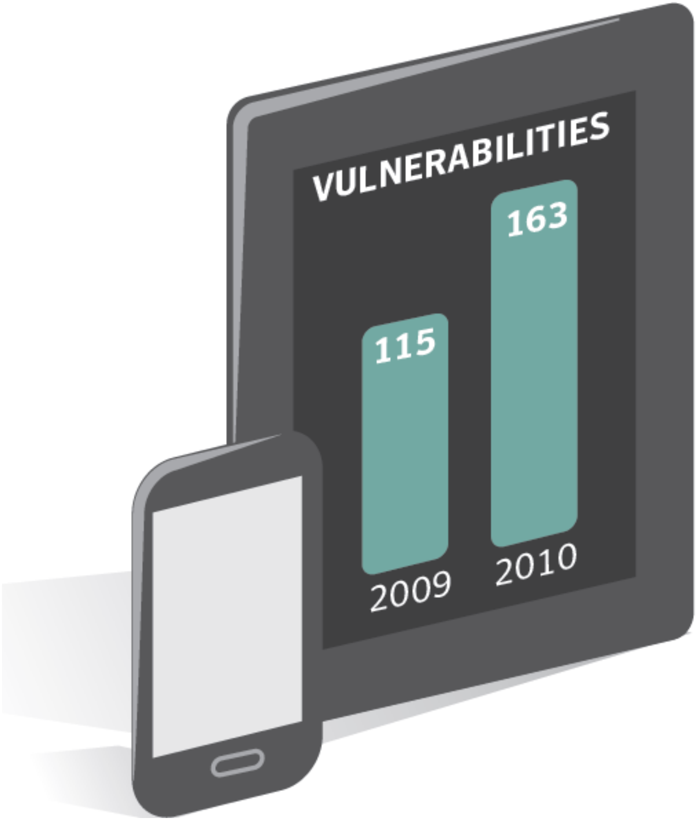
Source : OFTA

Mobile Threat Increase



Source : McAfee Threats Report: Fourth Quarter 2010

Mobile OS Vulnerabilities



Source : Symantec Internet Security Threat Report - Trends for 2010

Avoid Mobile Malware - Dos

- Install Anti-Virus software for mobile devices
- Install latest patches
- Enable personal firewall
- Scan mobile devices for malware periodically
- Exercise care when downloading apps
- Apply firmware updates for smartphones

Avoid Mobile Malware – Don’ts

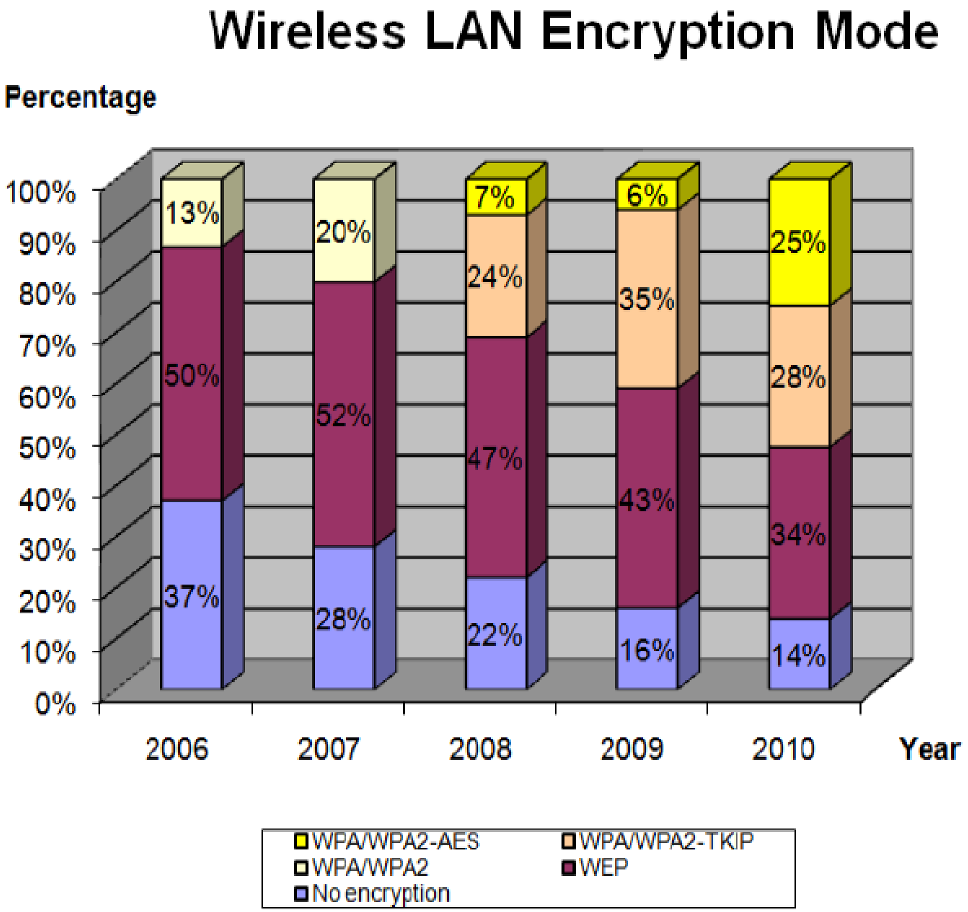
- Don’t use Bluetooth when not needed
- Don’t open MMS and SMS from unidentified sources
- Don’t execute files attached with email
- Don’t break smartphone OS (jailbreak)
- Don’t download apps from untrusted sources
- Don’t use modified or hacked software

2010 Data on WiFi Encryption

How safe are AP in HK?

- 14 % no encryption
- 34 % WEP
- i.e. 48 % AP

HIGHLY INSECURE



Source : Hong Kong Wireless Technology Industry Association

WiFi Security - Dos

- Use WPA/WPA2 encryption
- Change the default SSID
- Change the default administrative password;
- Update firmware of AP to remove vulnerabilities
- Use secure web interface (HTTPS) for AP management
- Activate MAC address filter

WiFi Security - Don’ts

- Don’t use WEP AP
- Don’t use dictionary word as password
- Don’t broadcast SSID
- Don’t place AP near a window
- Don’t use DHCP - manual assignment is more secure than automatic assignment

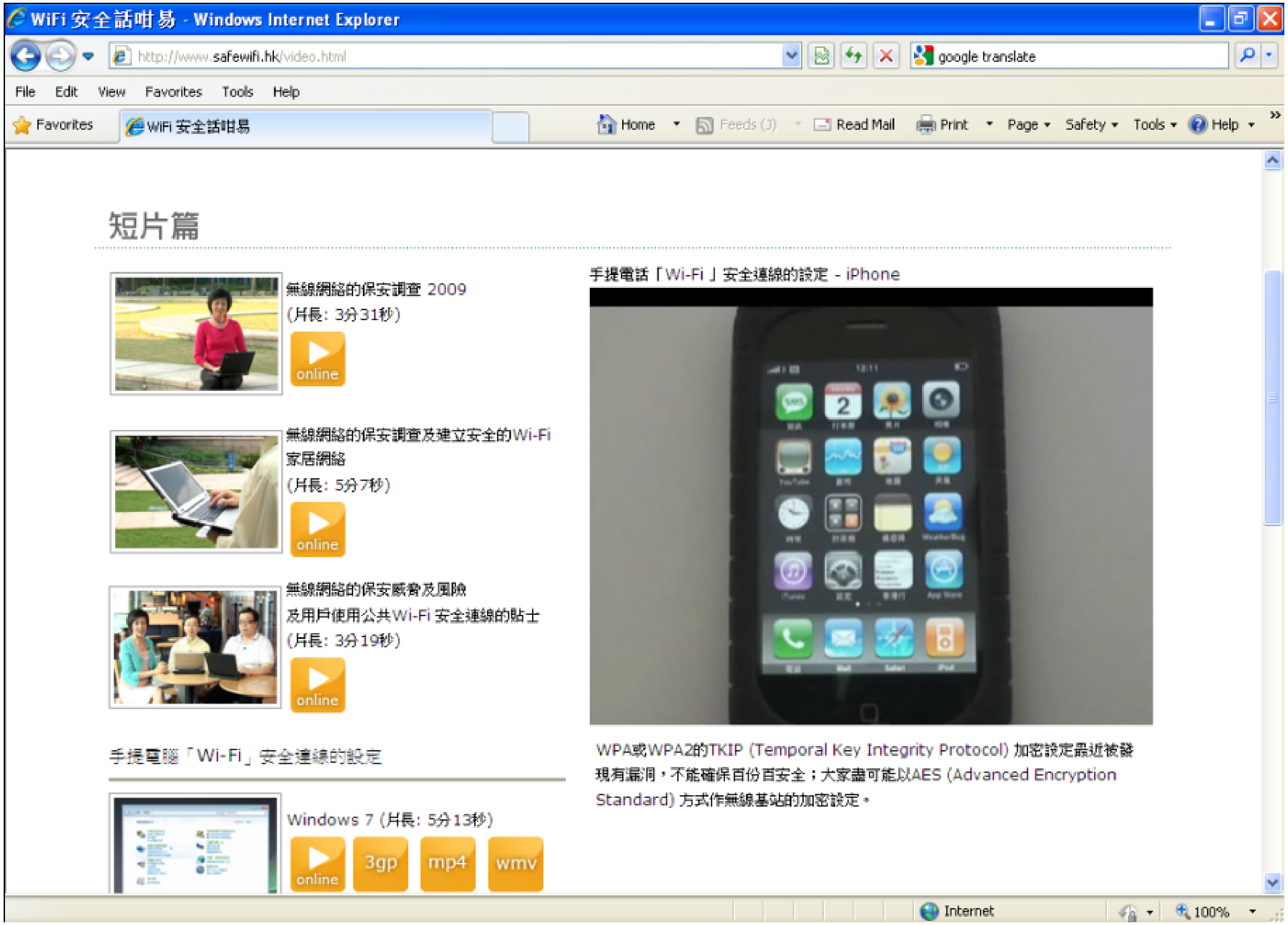
Public Awareness Program – the SafeWiFi Campaign

- Sponsored by OFTA since 2008 to promote WiFi Security Awareness
- Major activities
  - A thematic portal for WiFi Security
  - Annual War Driving Exercise
  - Public Seminars

Thematic website (www.safewifi.hk)

- Security tips
- Videos on secure WiFi settings for iPhone, Android, BlackBerry, Windows, Mobile Windows, MAC and Linux
- Archives of war driving reports
- Events and activities

Thematic website (www.safewifi.hk)


WiFi 安全話咁易 - Windows Internet Explorer
http://www.safewifi.hk/video.html
google translate
File Edit View Favorites Tools Help
Favorites
WiFi 安全話咁易
Home
Feeds (J)
Read Mail
Print
Page
Safety
Tools
Help
Internet
100%

短片篇

無線網絡的保安調查 2009
(片長: 3分31秒)
online

無線網絡的保安調查及建立安全的Wi-Fi 家居網絡
(片長: 5分7秒)
online

無線網絡的保安威脅及風險
及用戶使用公共Wi-Fi 安全連線的貼士
(片長: 3分19秒)
online

手提電腦「Wi-Fi」安全連線的設定

Windows 7 (片長: 5分13秒)
online 3gp mp4 wmv

手提電話「Wi-Fi」安全連線的設定 - iPhone

WPA或WPA2的TKIP (Temporal Key Integrity Protocol) 加密設定最近被發現有漏洞，不能確保百份百安全；大家盡可能以AES (Advanced Encryption Standard) 方式作無線基站的加密設定。

OFTA
電訊管理局

War Driving

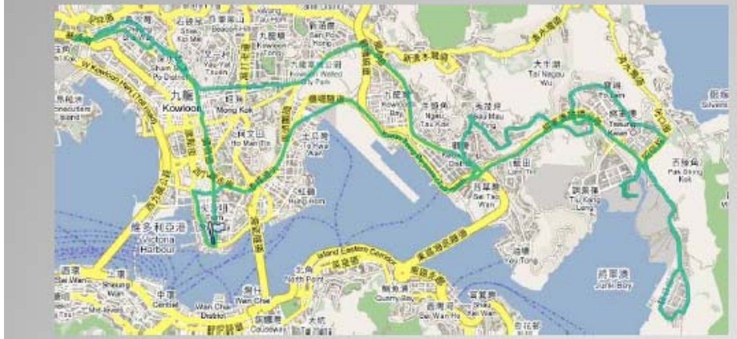
Objectives

- **Study the status of WiFi Security**
- **Benchmark the annual results**
- **Study the use of encryption models in APs**
- **Arouse public awareness on WiFi Security**

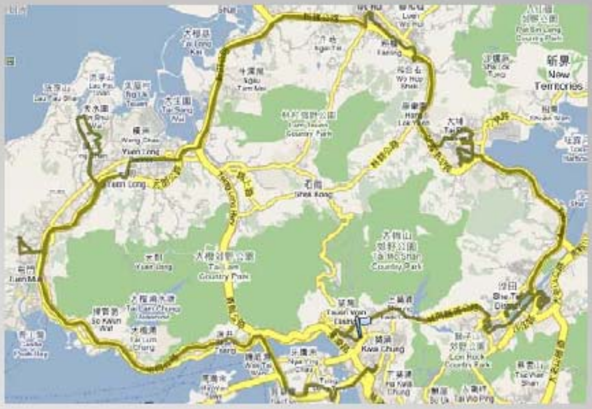
Code of ethics for War Driving

- Survey conducted in a non-intrusive manner
- Do not publish locations and SSID of APs
- Do not connect to insecure APs
- Do not interfere with wireless traffic
- Do not capture WiFi payloads
- Data will be destroyed after report published

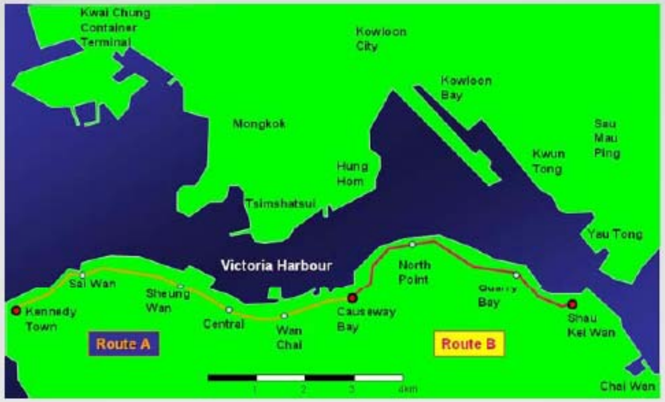
Route Maps of War Driving



Kowloon



New Territories



Hong Kong Island

HK WiFi Security Index

- Developed jointly by HKWTIA and PISA
- A single index for the easy interpretation of the WiFi Security Trend of Hong Kong
- Help to compare data collected in different War Driving surveys and to quantify the “improvements” or “deterioration” in information security measures

Elements of HK WiFi Security Index

The index is composed of three elements:

- **Public Awareness (20%) -**

  Percentage of APs using encryption

- **Best Practice (20%) -**

  Percentage of APs using non-default SSID

- **Technology Merit (60%) –**

  Security score of WiFi technologies

  (according to the security level – see Next Slide)

Metrics of Technology Merits

Criticality of vulnerability	Score	Description
L1	100	No vulnerability found in the technology
L2	80	Found a vulnerability in theory (concept)
L3	60	A proof of concept verified the vulnerability exploitable
L4	50	Exploit is found conducted by skilful personnel but source code not widely distributed
L5	30	Source code of exploit is published to public
L6	20	Handy tool is available for script kiddies to use
L7	0	No encryption

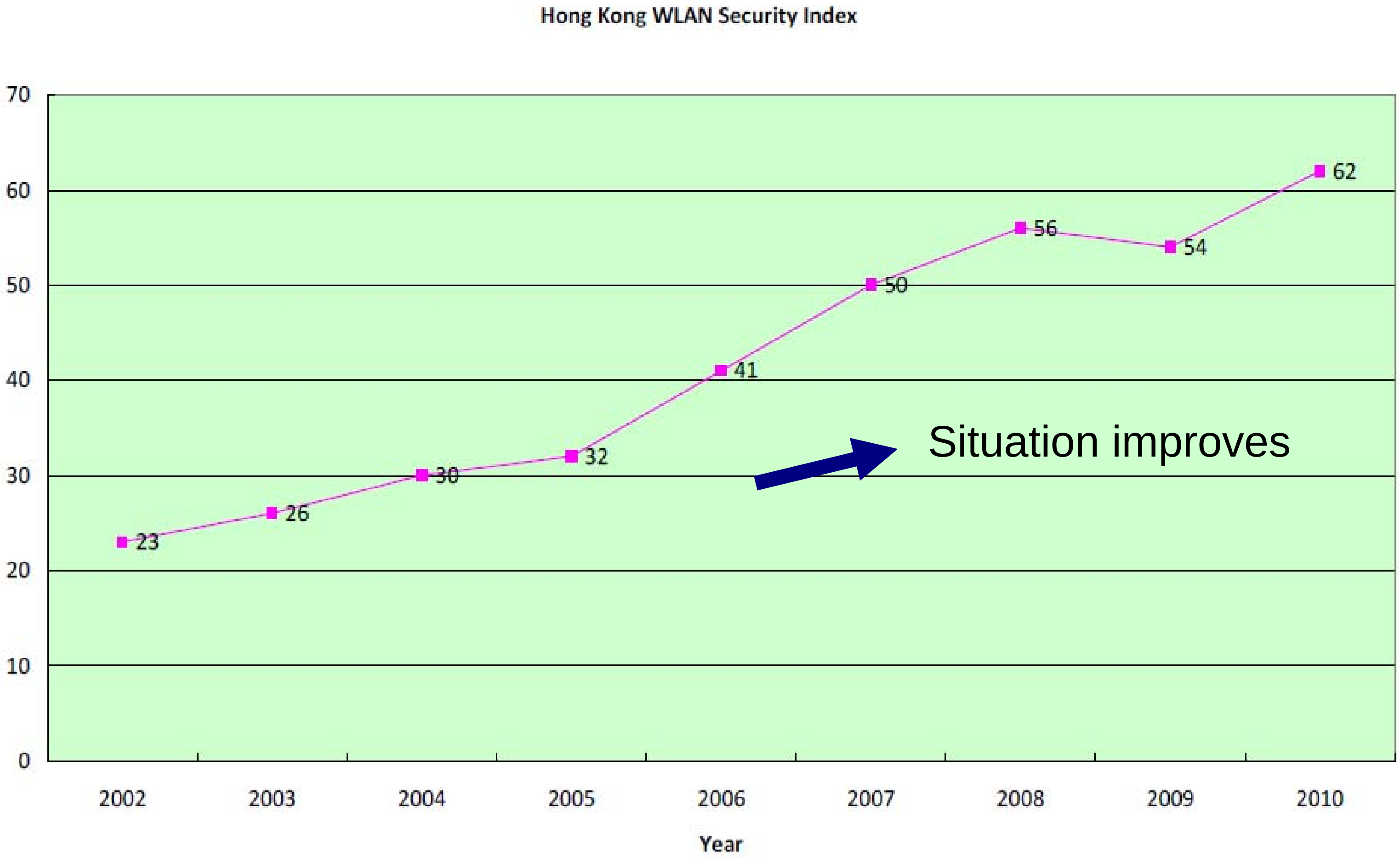
2009 HK WiFi Security Index

Parameters	*2009 (%)*	*Weight*
Encryption applied	85	20
No default SSID	88	20
WEP, L6	45	20 x 0.6
WPA/WPA2 – TKIP; (L4)	33	50 x 0.6
WPA/WPA2 – AES (L1)	7	100 x 0.6

The HKWSI for 2009 is ***54*** based on the calculation below:

[20 x 0.85] + [20 x 0.88] + 0.6 [0.45 x 20 + 0.33 x 50 +0.07x100]

HKWSI 2002 - 2010



Situation improves

Public WiFi Security Guidelines (1)

- **An industry working group on public Wi-Fi security was set up in mid 2007**
- **WiFi Security Work GROUP Members**
  - Office of the Telecommunications Authority (OFTA)
  - Office of the Government Chief Information Officer (OGCIO)
  - Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)
  - Fixed Carrier Licensees providing public WiFi service
  - Class licensees for the provision of public WiFi service
  - Relevant professional organizations

Public WiFi Security Guidelines (2)

- **“Guidelines on the Security Aspects for the Design, Implementation, Management and Operation of Public Wi-Fi Service” first published in October 2007**

- **Key Components of the Guidelines**
  - Practical security measures for public Wi-Fi service with particular emphasis on the air interface
  - User best practice in using public Wi-Fi services
  - Reporting requirement in relation to severe security violations

Public WiFi Security Guidelines (3)

- **Security Measures**
  - **Management Measures**
    - Implement appropriate security policies and business contingency plan
    - Perform security risk assessment and independent security audit
    - Establish in-house procedures on incident response and remedy (with regular update).
  - **Operational Measures**
    - Ensure effective security measures are in place to support the daily operation, e.g. SSID and administrative passwords and IP address range are properly configured and firmware for APs is up-to-date.

Public WiFi Security Guidelines (4)

- **Basic Technical Measures**
  - Employ strong encryption
  - Keep record of the login identity
  - Prohibit peer-to-peer attack
  - separate Wi-Fi network from other public service provisions

- **Advanced Technical Measures**
  - Implement secure authentication methodology,

    secure air interface encryption and firewall
  - Deploy anti-virus and anti-spyware systems, intrusion detection and/or intrusion prevention systems and wireless IPS

Public WiFi Security Guidelines (4)

- **User Best Practices**
  - Operators should inform and advise their customers from time to time about the risks associated with the public Wi-Fi service
  - Operators are also encouraged to make reference to “Tips on Wireless Security for End-users” at the Government’s one-stop information security portal (www.infosec.gov.hk)

- **Incident Reporting**
  - Operators concerned are required to report to OFTA whenever a severe security violation that meets certain triggering criteria occurs, following the procedures stipulated in the guideline document

- **The Guidelines can be downloaded from OFTA’s website at**

  http://www.ofta.gov.hk/en/report-paper-guide/guidance-notes/gn_200817.pdf

OFTA
電訊管理局

Way Forward

The Government will

- Continue to promote public awareness by mounting own education programs or sponsoring programs conducted by industry/professional institutions
- Review regularly the information security guidelines and update them to meet with new developments

IT Experts should

- help to pass the message about information security to users in their organisation
- include security considerations into their IT system design and implementation

~ Thank You ~

My email : ads@ofta.gov.hk

OFTA’s website : http://www.ofta.gov.hk