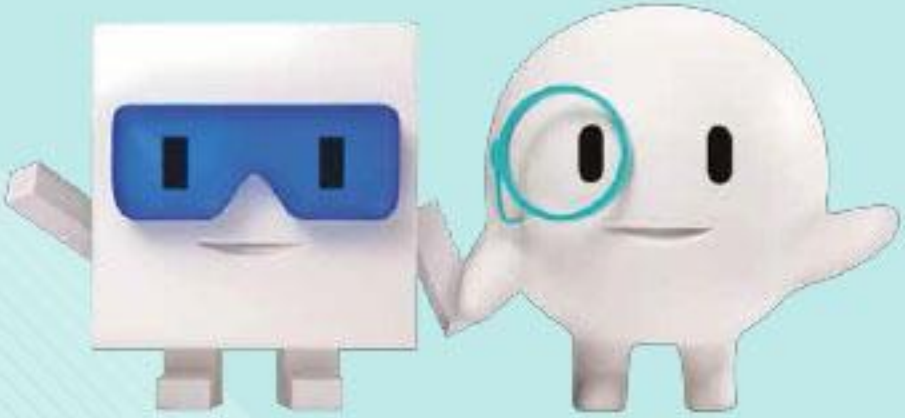
HKPC

Secure Network and Mobile Devices



All-round Productivity Partner
全方位企業伙伴

Agenda

- Introduction
- Wi-Fi Network
- Security Incident
- Security Measures
- Q & A

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)

香港電腦保安事故協調中心

- Established in **2001** and managed by HK Productivity Council.
- Cyber Threats Response and Defense Coordinator in Hong Kong.
- Member of the FIRST (Forum of Incident Response and Security Teams) and APCERT (Asia Pacific Computer Emergency Response Teams).
- Provide Internet users and Local Enterprises free of charge services.

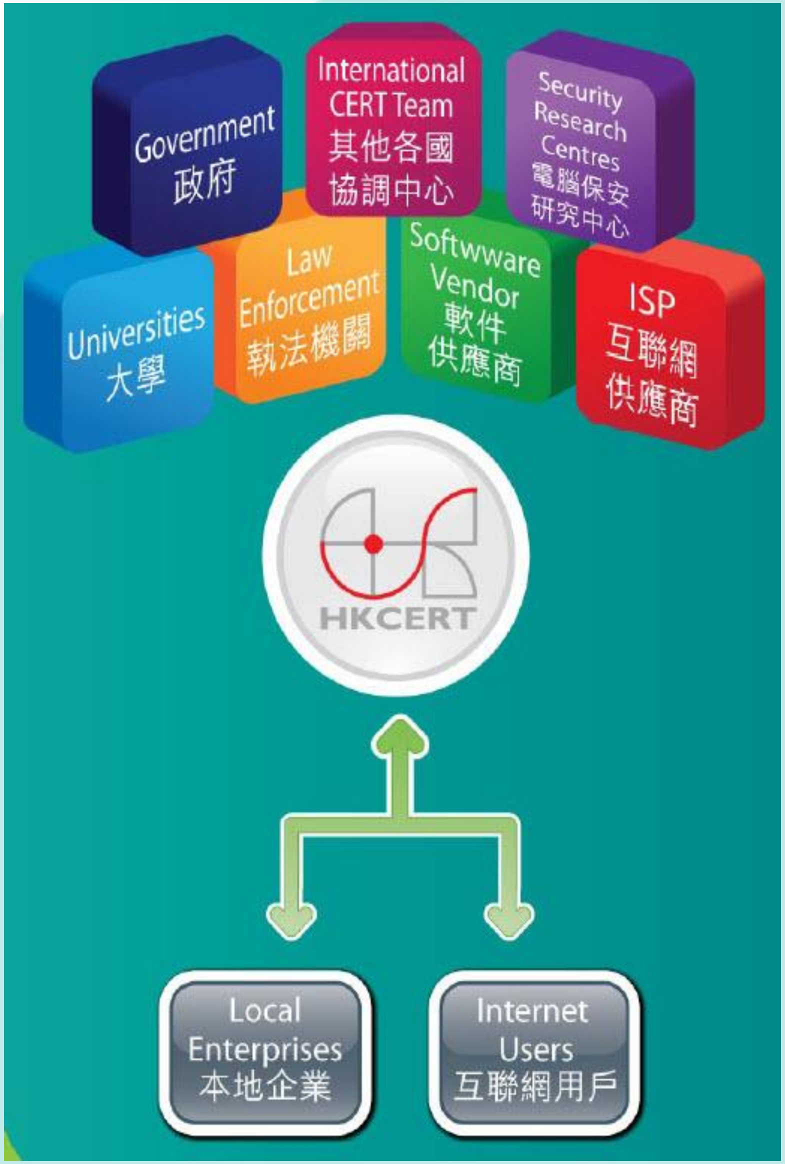
Services

- Incident Handling, Response and Coordination.
  - Incident Report and Response.
  - Proactive Discovery of Threats and Incidents.
  - Vulnerability Monitoring and Malware Detection and Analysis.

- Dissemination of Alerts, Warnings and Security related Information.
  - Security Alerts and Early Warnings.
  - Publications.
  - Monthly Newsletter.
  - Guidelines and Handbooks.

Services

- Security Awareness Building and Training.
  - Seminars and Briefing to the Public.
  - Conferences and Workshops.
- Coordination and Collaboration with Relevant Parties on Security Preventive Measures.
- Website & Free Mobile Apps (Apple iOS and Android).



Wi-Fi Network

© Luis Hernan

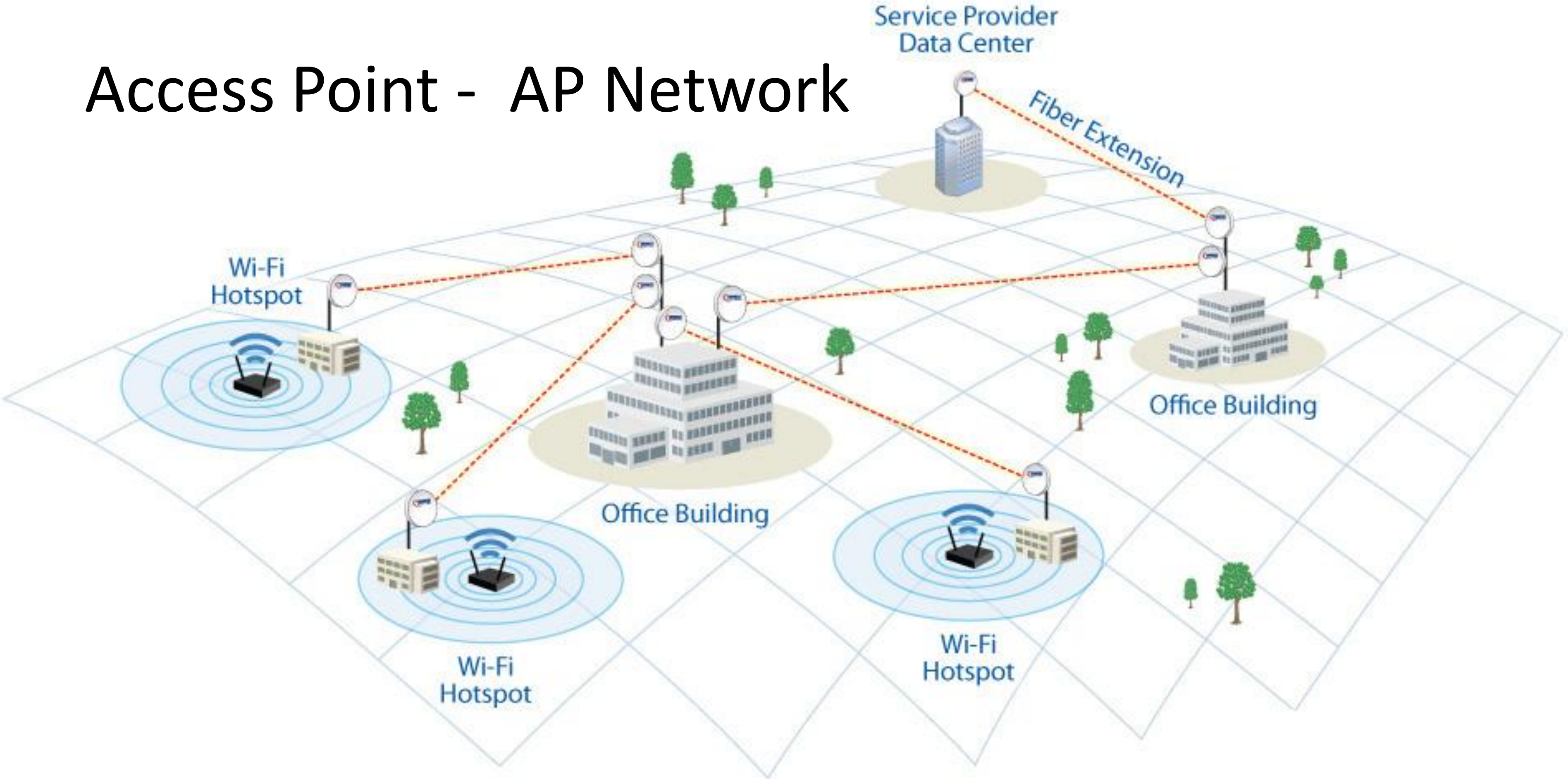
Wi-Fi Network

- 2.4GHZ, 5 GHZ
- IEEE 802.11/a/b/g/n/ac
- Data rate from 11 Mbps to 1 Gbps
- Coverage 35m - ~1km
- 4 billion Wi-Fi devices in use globally

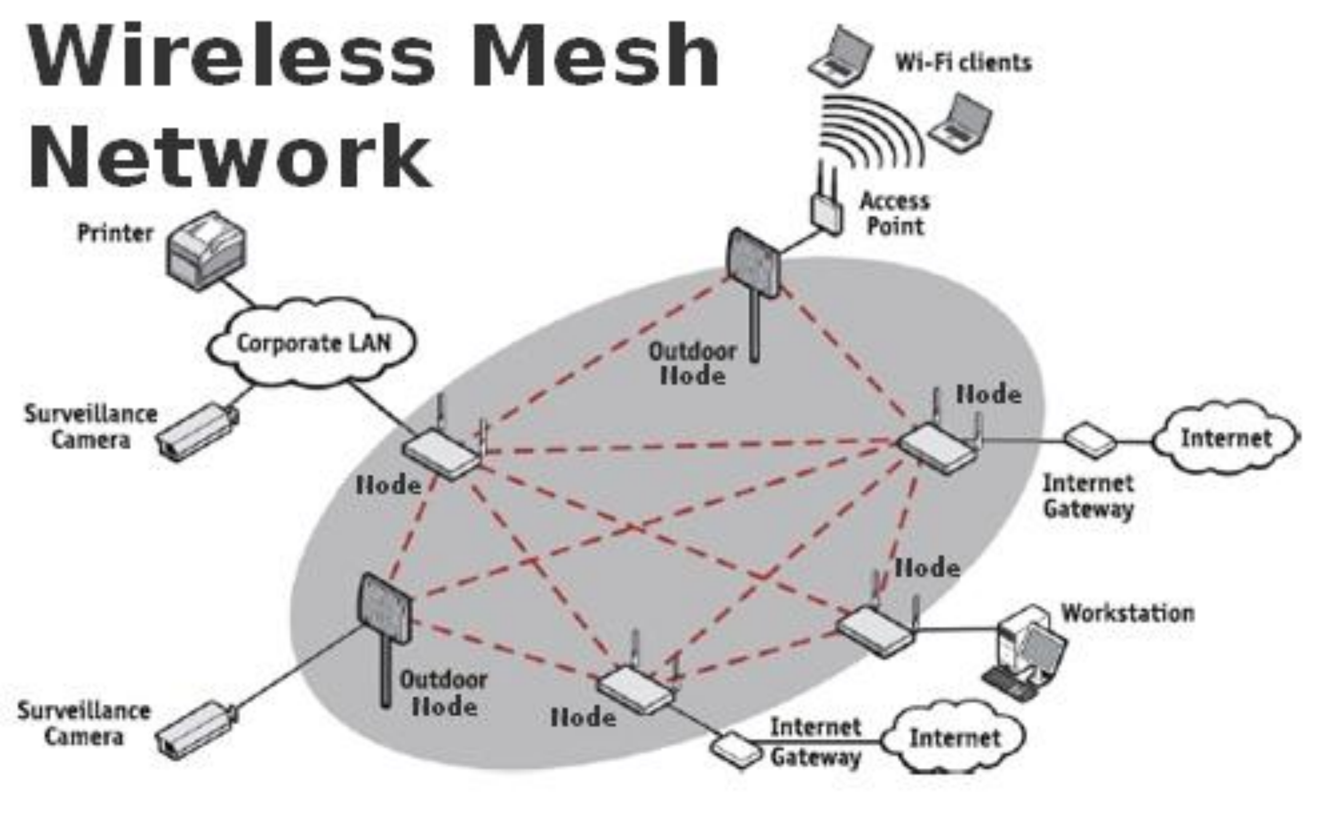
- The Evolution of Wireless – ‘Wi-Fi’ (Infographic) http://prafulla.net/interesting-contents/world-interesting-contents/the-evolution-of-wireless-infographic/

Wi-Fi Network

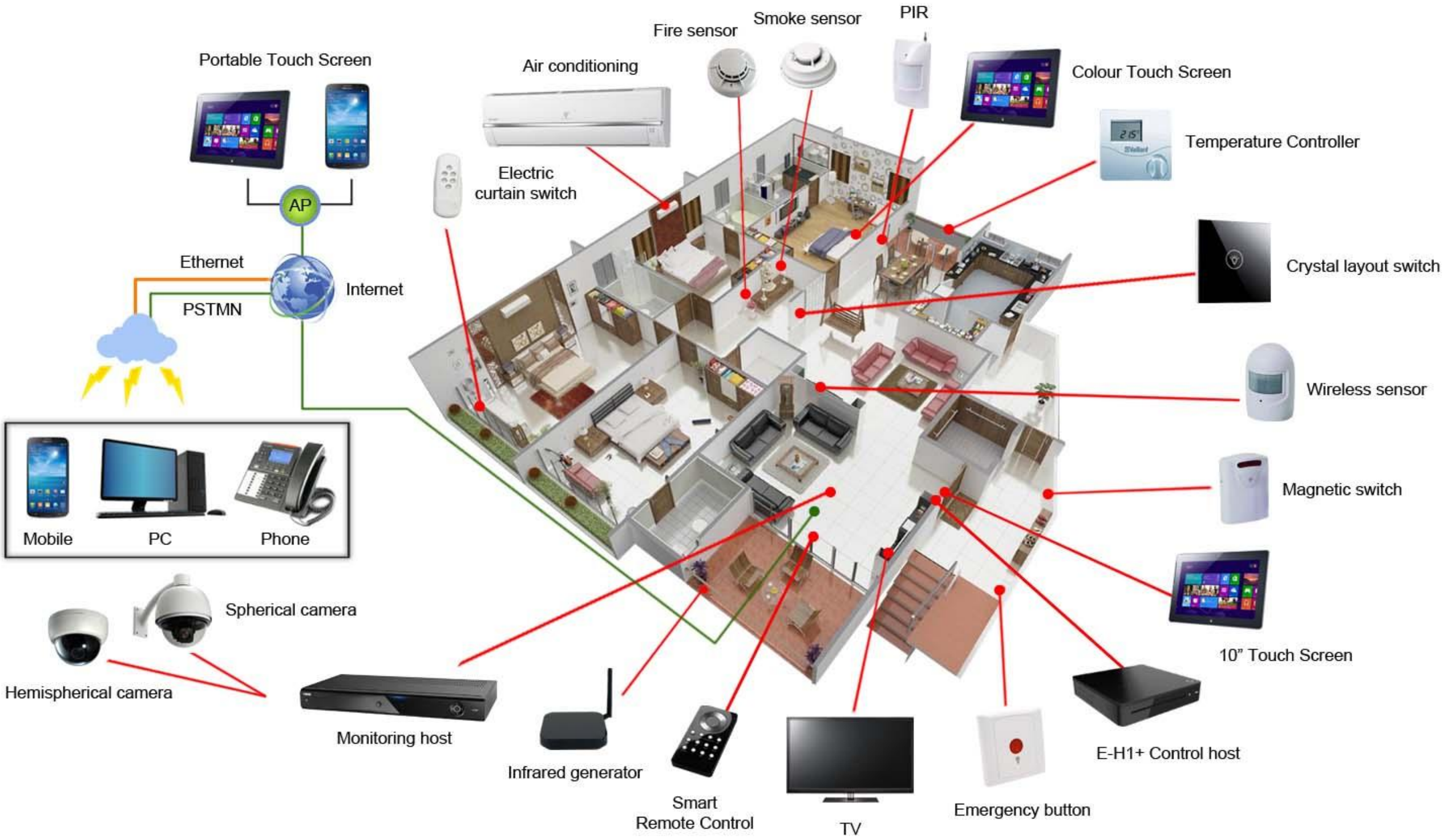
Access Point - AP Network



Wi-Fi Network



Use of Wi-Fi Network

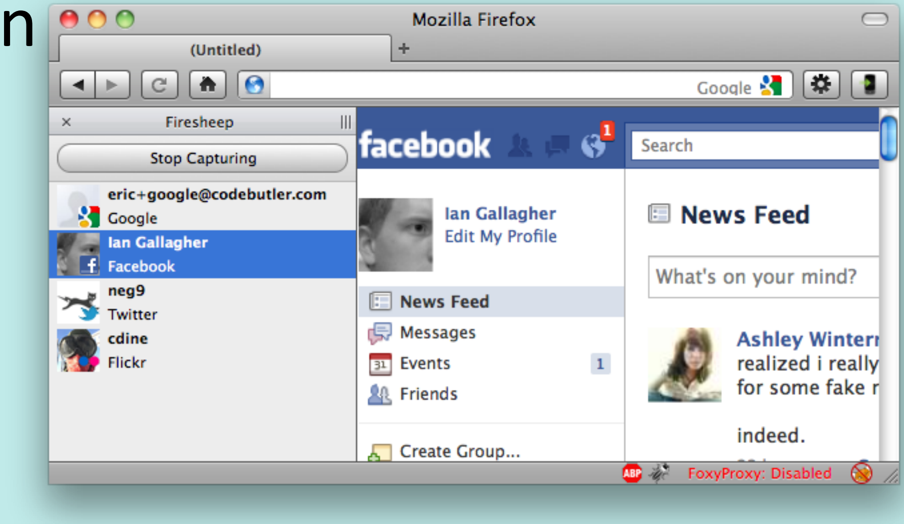


HKPC

HKCERT

Security Incident

- Firesheep (2010)
- Firefox add-on
- Capture social networking website user credentials on open wireless network.
- Blacksheep – protect against Firesheep
- Use https connection


Mozilla Firefox

(Untitled)

Google

Firesheep

Stop Capturing

eric+google@codebutler.com
Google

Ian Gallagher
Facebook

neg9
Twitter

cdine
Flickr

facebook

Search

Ian Gallagher
Edit My Profile

News Feed

What's on your mind?

News Feed
Messages
Events 1
Friends

Create Group...

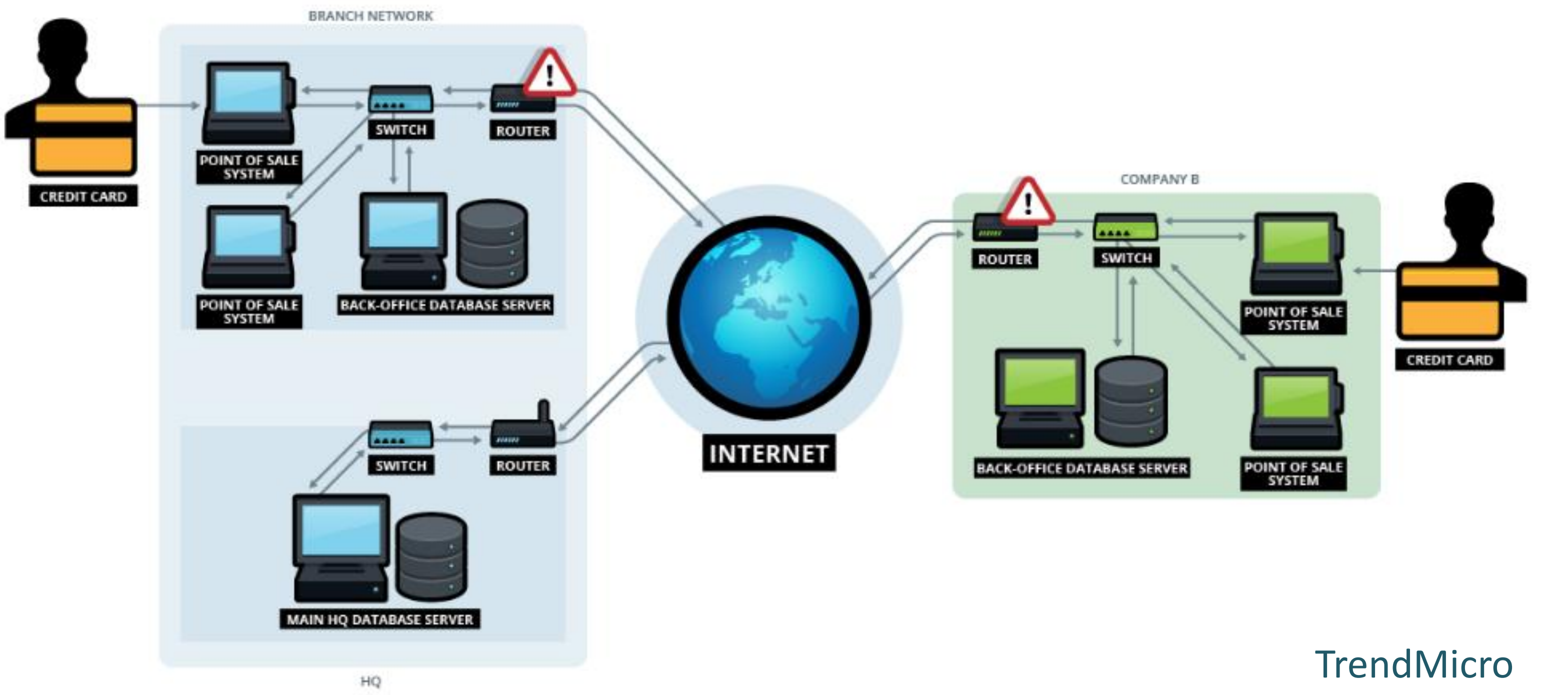
Ashley Winterr
realized i really
for some fake r

indeed.

FoxyProxy: Disabled

Security Incident

- Attack Point of Sales (POS) system via wireless network.



TrendMicro

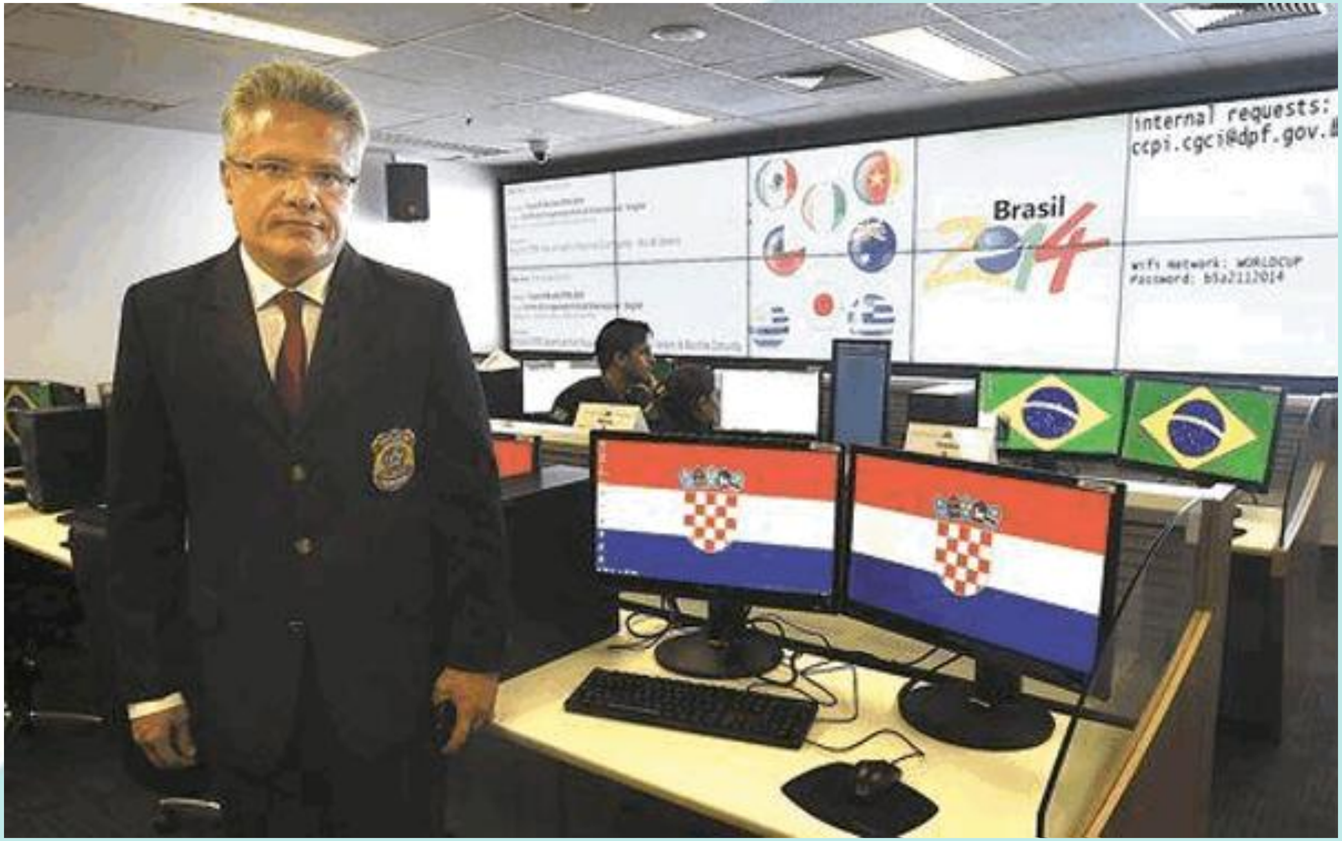
Security Incident

- Hacker make use of vulnerable wireless access point to launch DDoS attack.
- Improper configuration
  - Telnet port 23 opened.
  - Default user id and password.
- Wireless AP, TV Box, Broadband Router, Mobile devices, etc.

Protect Your Home Network Devices from Joining the Botnet Army

https://www.hkcert.org/my_url/en/blog/14123001

What's wrong?


internal requests:
ccpi.cgci@dpf.gov.b
Brasil 2014
wifi network: WORLDCUP
Password: b5a2112014

Security Measures

Network Design

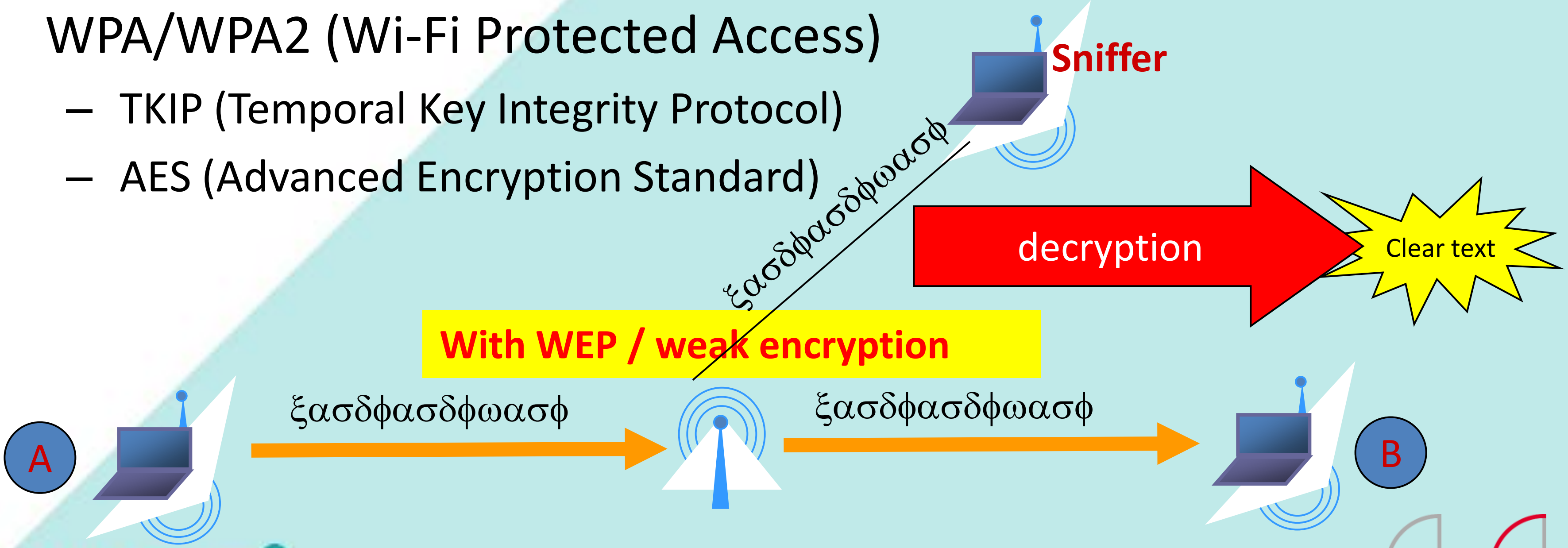
- Account Management
- Device Management
- Network Segmentation
- Access Control
- Audit Trail

Account Management

- Authentication
  - User authentication system
  - Landing page (Captive Portal)
  - WPA/WPA2 enterprise (authorization server required)
  - Password Control (Default setting)
  - Use encryption

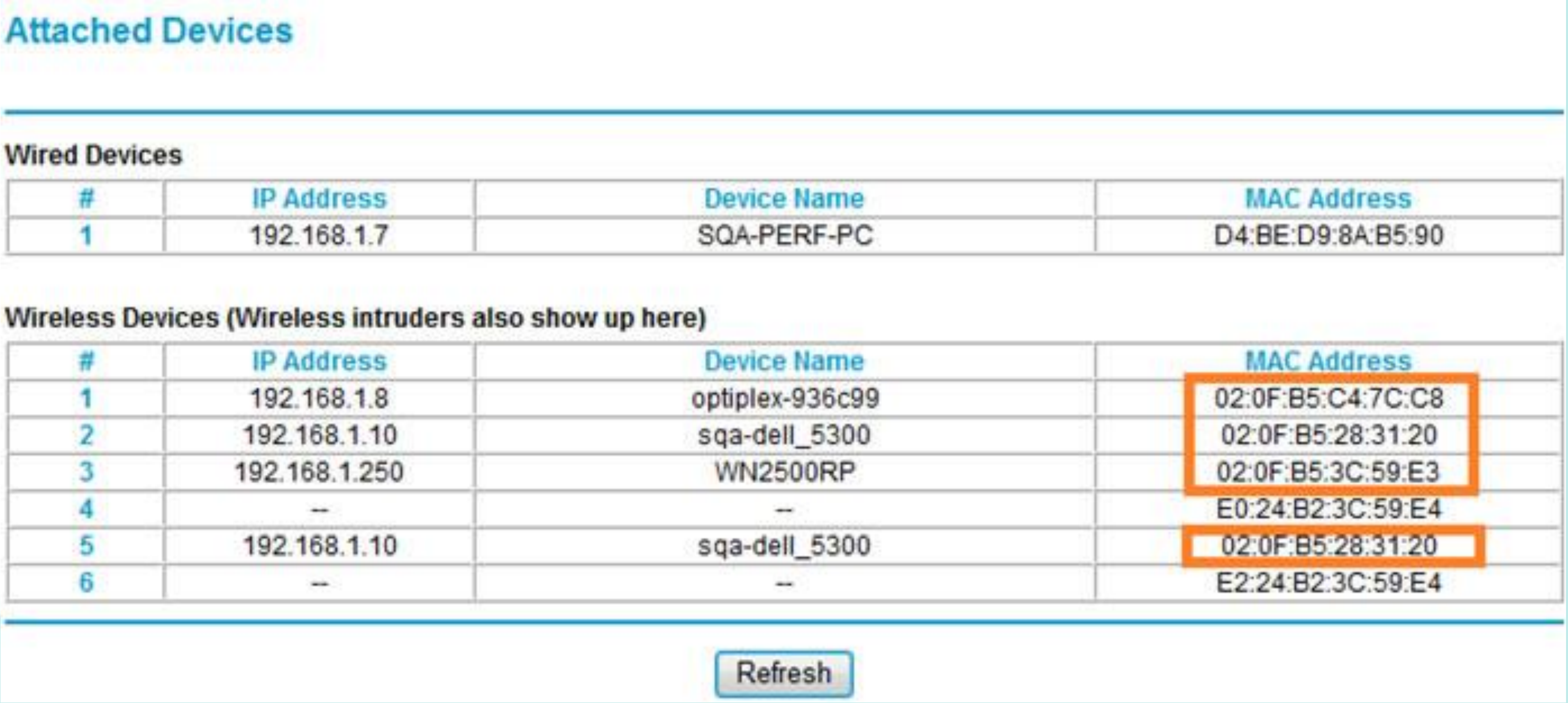
Use Encryption

- WEP (Wireless Equivalent Protocol)
  - Introduced in 1997 and cracked in 2001
  - DO NOT USE WEP, can be cracked within 10 mins
- WPA/WPA2 (Wi-Fi Protected Access)
  - TKIP (Temporal Key Integrity Protocol)
  - AES (Advanced Encryption Standard)



Device Management

- Device authentication
  - Pre-register Wi-Fi devices (MAC address of Wi-Fi interface)
  - Regular review the device list (Trusted devices)
  - Record the usage of Wi-Fi device



Attached Devices

Wired Devices

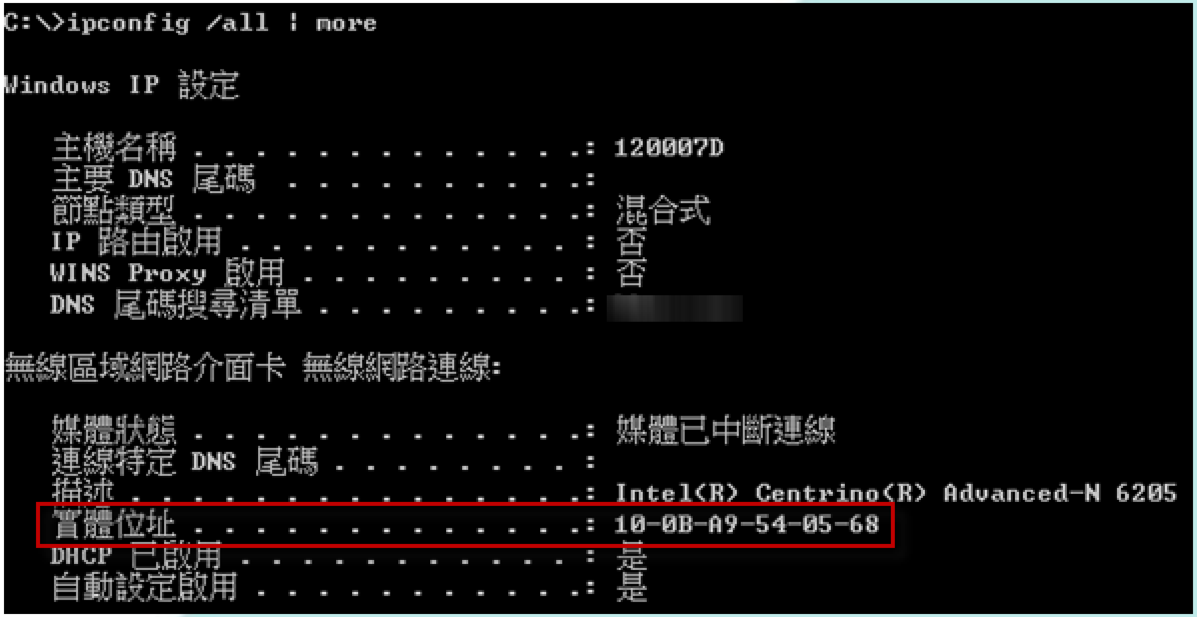
#	IP Address	Device Name	MAC Address
1	192.168.1.7	SQA-PERF-PC	D4:BE:D9:8A:B5:90

Wireless Devices (Wireless intruders also show up here)

#	IP Address	Device Name	MAC Address
1	192.168.1.8	optiplex-936c99	02:0F:B5:C4:7C:C8
2	192.168.1.10	sqa-dell_5300	02:0F:B5:28:31:20
3	192.168.1.250	WN2500RP	02:0F:B5:3C:59:E3
4	--	--	E0:24:B2:3C:59:E4
5	192.168.1.10	sqa-dell_5300	02:0F:B5:28:31:20
6	--	--	E2:24:B2:3C:59:E4

Authorized / Trusted devices

- Allow only pre-registered device.
  - MAC filtering



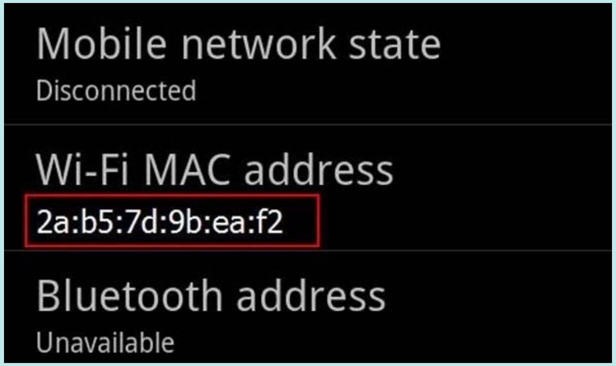
```
C:\>ipconfig /all | more

Windows IP 設定

   主機名稱 . . . . . . . . . . . . . . : 120007D
   主要 DNS 尾碼 . . . . . . . . . . . :
   節點類型 . . . . . . . . . . . . . . : 混合式
   IP 路由啟用 . . . . . . . . . . . . : 否
   WINS Proxy 啟用 . . . . . . . . . . : 否
   DNS 尾碼搜尋清單 . . . . . . . . . . : [redacted]

無線區域網路介面卡 無線網路連線:

   媒體狀態 . . . . . . . . . . . . . . : 媒體已中斷連線
   連線特定 DNS 尾碼 . . . . . . . . . :
   描述 . . . . . . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   實體位址 . . . . . . . . . . . . . . : 10-0B-A9-54-05-68
   DHCP 已啟用 . . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . . : 是
```



Mobile network state
Disconnected

Wi-Fi MAC address
2a:b5:7d:9b:ea:f2

Bluetooth address
Unavailable

Device Management

- Provided and Managed by organization
  - System and application installation and update
  - Security Software
- Bring Your Own Device (BYOD)

BYOD Security Guidelines

Bring Your Own Device

「自攜裝置」保安指引

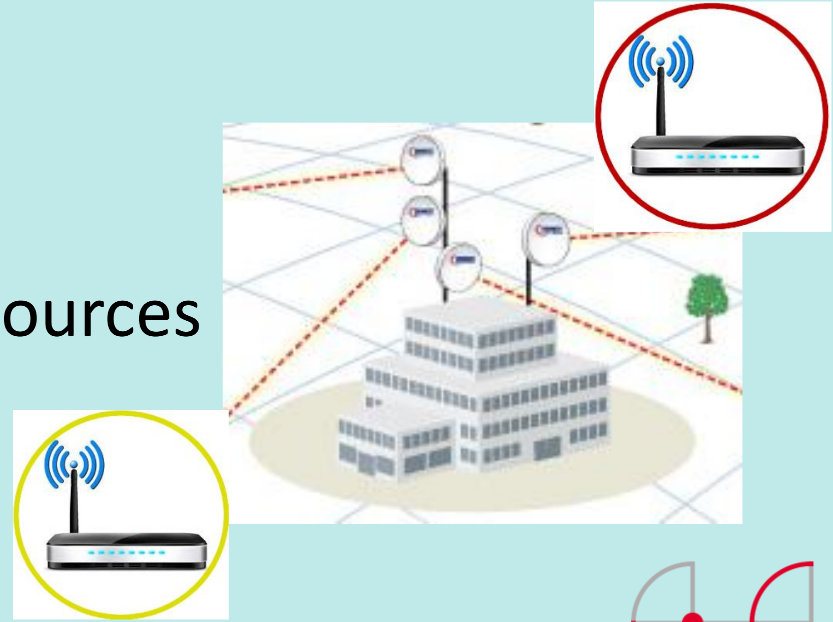
  - Define policies on BYOD
  - Organization and employee agree and understand the policies
  - Bring Your Own Device (BYOD) Security Guidelines

    https://www.hkcert.org/my_url/en/guideline/13092602

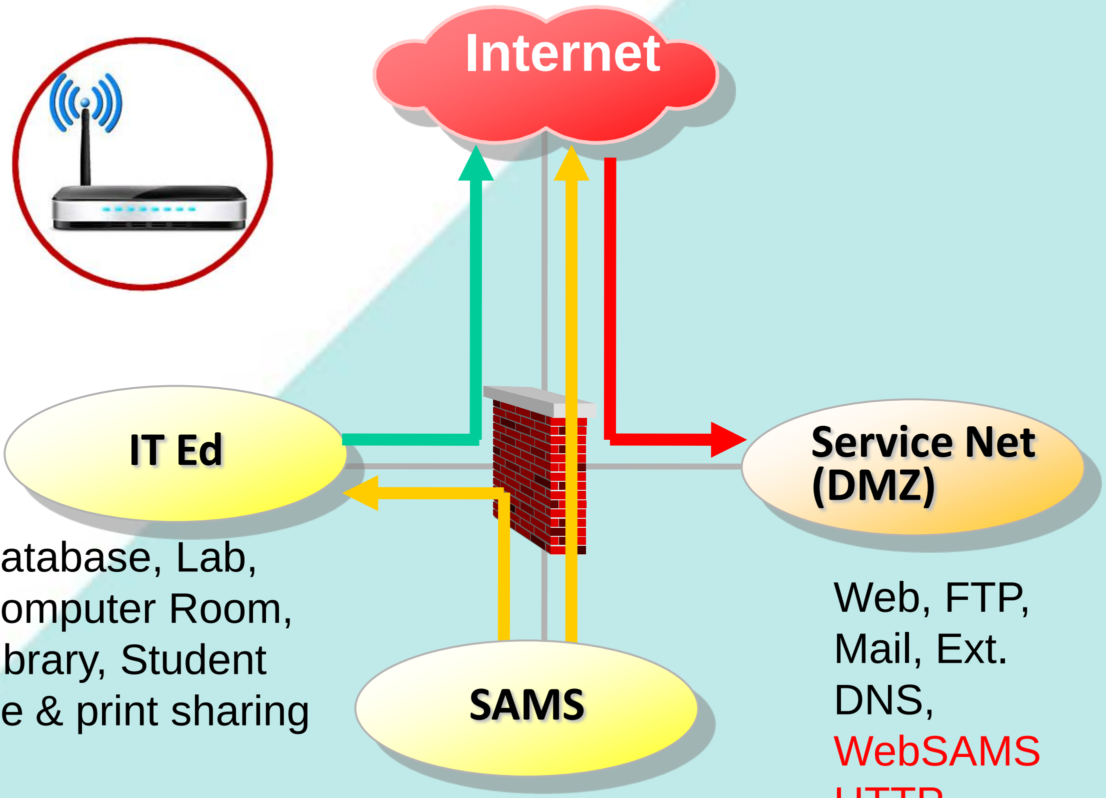
Network Segmentation

- Isolated Network
  - No connection to school network
  - Avoid Malware spreads to Internal Network

- Restricted Network
  - Only allow connection to
  - Limited access right on resources
    - Ex: Read Only
  - Access log



Network Segmentation



Internet

IT Ed

Service Net (DMZ)

SAMS

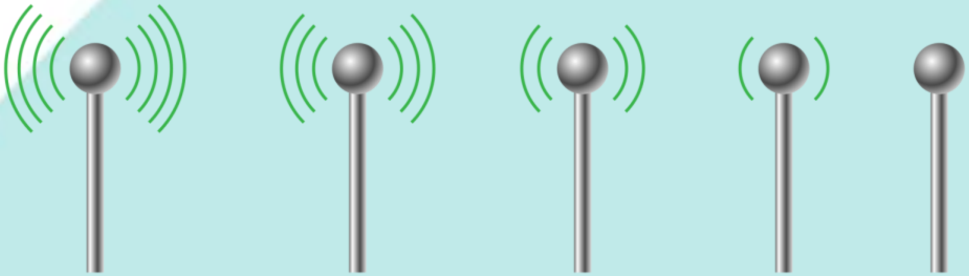
Database, Lab, Computer Room, Library, Student file & print sharing

Web, FTP, Mail, Ext. DNS, WebSAMS HTTP

HR Data, Financial Data, Student Record, Exam Paper, Staff file sharing

Wi-Fi Signal

- Broadcast SSID
- Wi-Fi Coverage – signal strength



Access Control

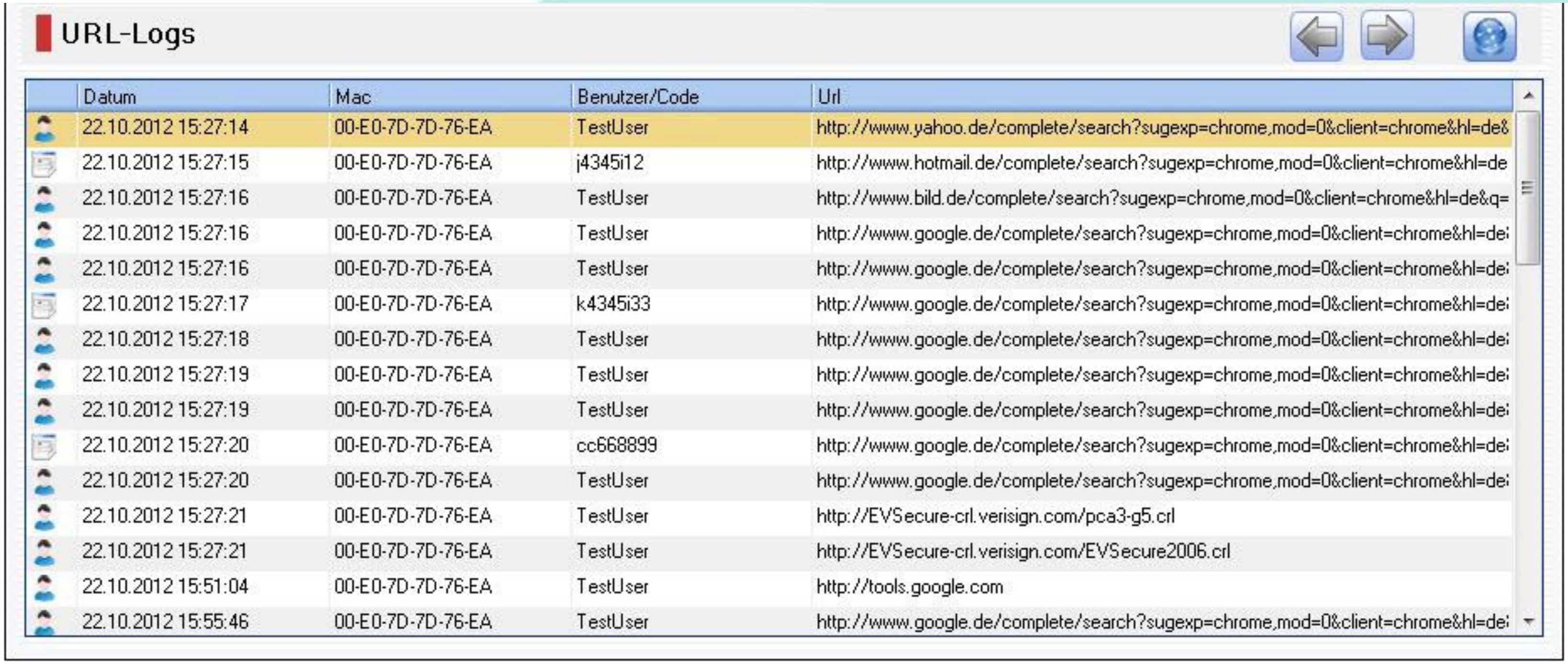
- Wi-Fi Network Operation Hour
  - Turn off in non-office hr
  - Guest ?

- Internet access control
  - Services, ex: web browsing and email
  - Web content filtering

- Intranet access control
  - Data classification
  - Not allow access via Wi-Fi connection

Audit Trail

- Bandwidth usage
- Connection record (IP and MAC address)
- User logon record
- Access record (URL, server, services, etc.)

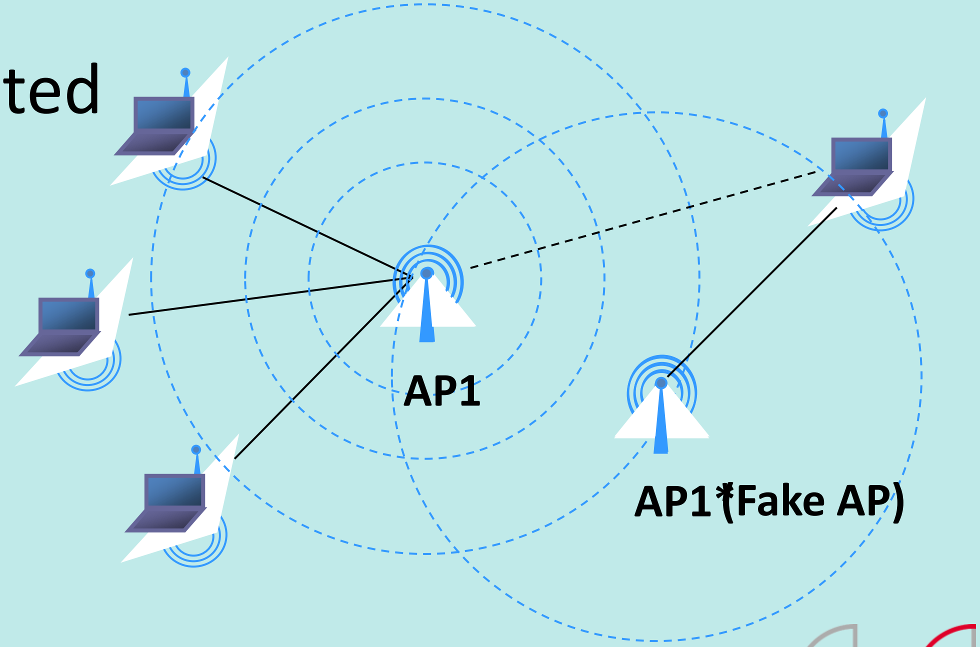


URL-Logs

Datum	Mac	Benutzer/Code	Url
22.10.2012 15:27:14	00-E0-7D-7D-76-EA	TestUser	http://www.yahoo.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:15	00-E0-7D-7D-76-EA	j4345i12	http://www.hotmail.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de
22.10.2012 15:27:16	00-E0-7D-7D-76-EA	TestUser	http://www.bild.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&q=
22.10.2012 15:27:16	00-E0-7D-7D-76-EA	TestUser	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:16	00-E0-7D-7D-76-EA	TestUser	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:17	00-E0-7D-7D-76-EA	k4345i33	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:18	00-E0-7D-7D-76-EA	TestUser	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:19	00-E0-7D-7D-76-EA	TestUser	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:19	00-E0-7D-7D-76-EA	TestUser	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:20	00-E0-7D-7D-76-EA	cc668899	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:20	00-E0-7D-7D-76-EA	TestUser	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&
22.10.2012 15:27:21	00-E0-7D-7D-76-EA	TestUser	http://EVSecure-crl.verisign.com/pca3-g5.crl
22.10.2012 15:27:21	00-E0-7D-7D-76-EA	TestUser	http://EVSecure-crl.verisign.com/EVSecure2006.crl
22.10.2012 15:51:04	00-E0-7D-7D-76-EA	TestUser	http://tools.google.com
22.10.2012 15:55:46	00-E0-7D-7D-76-EA	TestUser	http://www.google.de/complete/search?sugexp=chrome,mod=0&client=chrome&hl=de&

Security Awareness

- Beware of Fake Access Point
- Do not disclose Wi-Fi password to others
- Use **https** connection
- Enable Password protected
- Turn off Wi-Fi when not in use



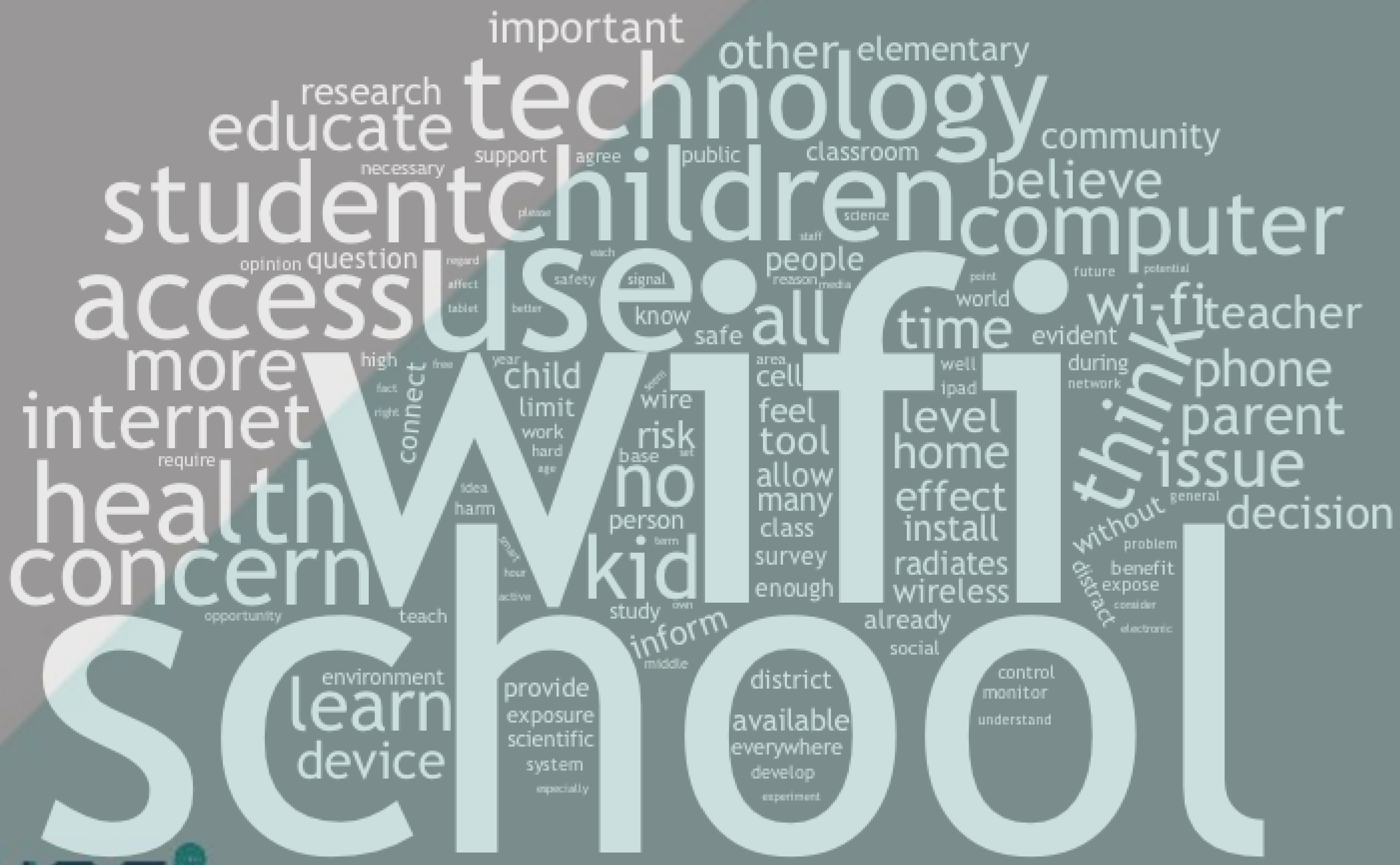
HKPC

HKCERT

HKCERT

- Hotline: 8105-6060
- Email: hkcert@hkcert.org
- Website: www.hkcert.org
- Guideline - Guideline for Safety Using Wireless LAN
  https://www.hkcert.org/my_url/en/guideline/12040201
- Hong Kong Google Play Store's Apps Security Risk Report
  https://www.hkcert.org/play-store-srr

Q&A



HKPC

HKCERT