



Hong Kong Computer Emergency Response Team  
Coordination Centre  
香港電腦保安事故協調中心

# Safe Mobile Computing

Presented by  
Roland Cheung, Frankie Wong  
HKCERT

26-Nov-2012



# Agenda

- Introduction
  - Mobile characteristics
  - Statistics
- Mobile malware/threats
  - Why mobile malware?
  - Mobile malware trends
  - Infection channels



# Agenda (cont'd)

- Demo
  - Premium SMS
  - USSD vulnerability
  - Privacy Advisor
- Safeguard your mobile phone
- Future trends
- HKCERT Services



Hong Kong Computer Emergency Response Team  
Coordination Centre  
香港電腦保安事故協調中心



# Introduction





# Introduction

- Mobile Device

- Smartphone
- Tablet

- Mobile OS

- Apple – iOS
- Google – Android
- Windows – Windows Phone
- RIM – BlackBerry OS





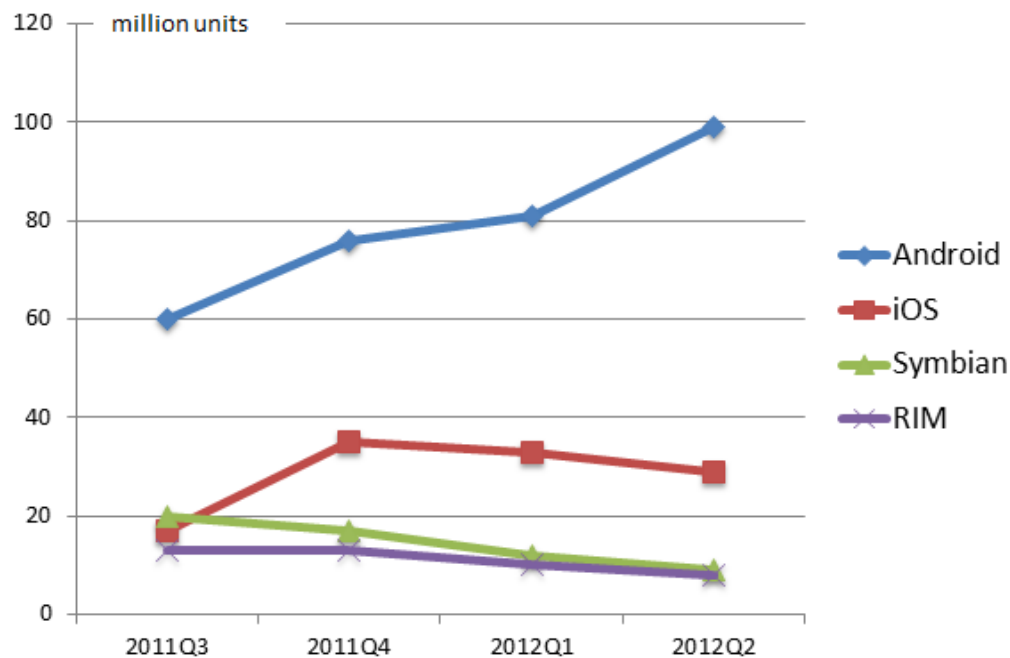
# Mobile characteristics

- Portable
- Store a lot of personal data
- Wireless connection  
(e.g. 3G, Wi-Fi, Bluetooth, NFC, GPS)
- Email, Facebook, Twitter, Weibo client, etc.
- App install available
- Mobile browser
- Support financial services
- Game center
- Multimedia center



# Statistics

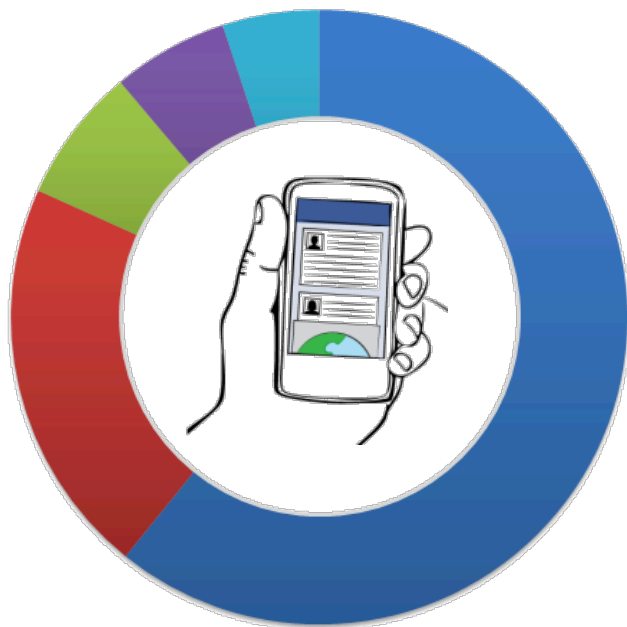
- Worldwide Smartphone Sales Trends
  - 2011 Q3 - 2012 Q2





# Statistics

- Worldwide Smartphone Sales Ratio
  - 2012 Q1 – 2012 Q2



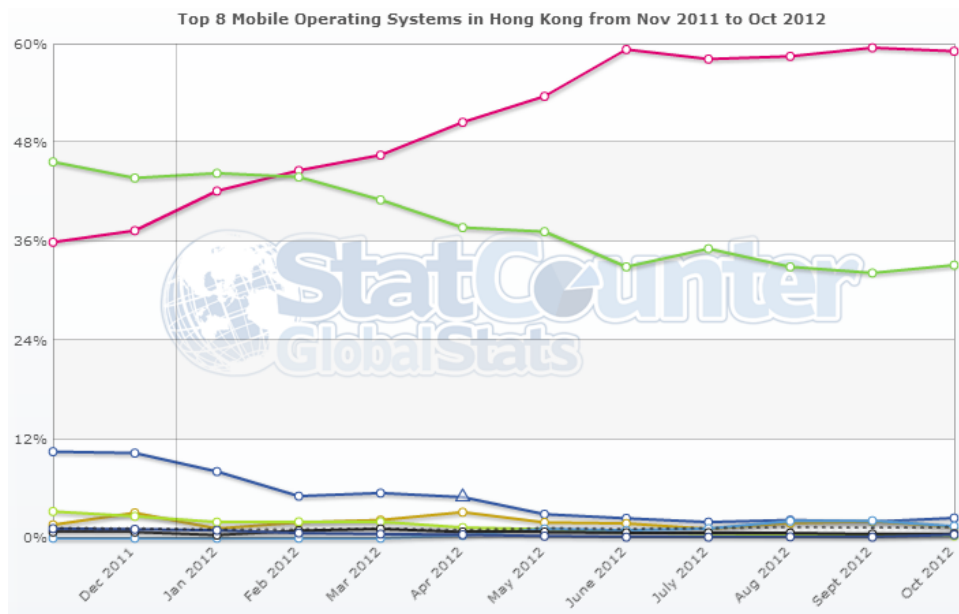
- Android – 61%
- iOS – 21%
- Symbian – 7%
- RIM – 6%
- Others – 5%





# Statistics

- Smartphone web browsing in Hong Kong
  - Nov 2011 – Oct 2012



- Android – 59%
- iOS – 33%
- Symbian – 2%



# Mobile malware/threats





# Why mobile malware?

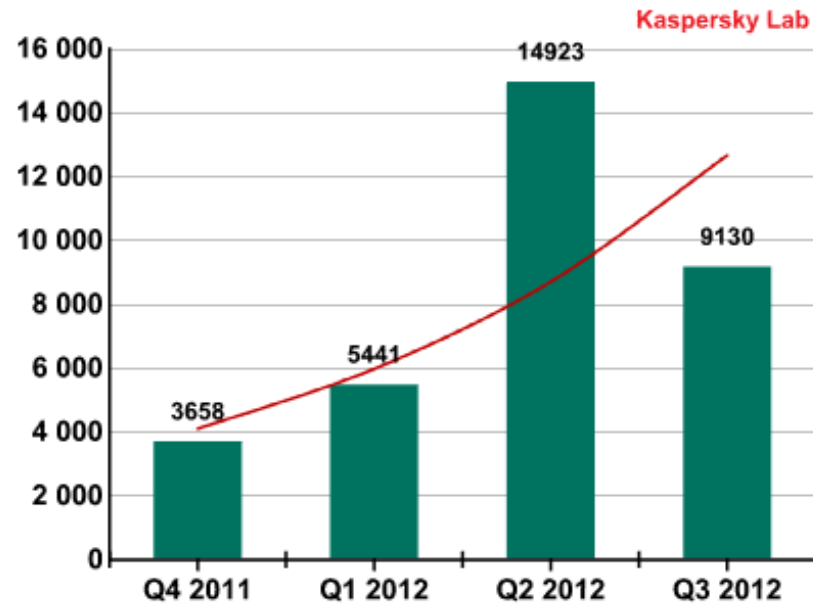
- Growth in mobile device
  - to be malware author target
  - additional channels to infect (e.g. QR Code, NFC)
- Always-connected network
  - 3G / LTE data network
- Store a lot of personal data
  - personal data worth
  - additional information (e.g. Camera, GPS)
- Mobile commercial growth
  - significant rise in the number of mobile shoppers





# Mobile malware/threats trends

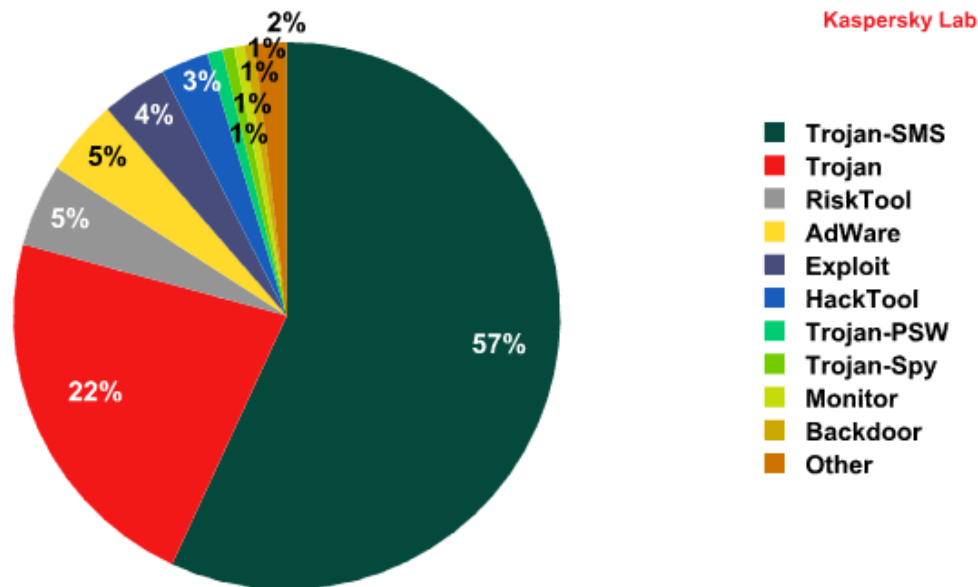
- The number of malware modifications (targeting Android OS)
  - The number of new files detected was in line with the trend





# Mobile malware/threats trends

- Distribution of malware (targeting Android OS)
  - Trojan-SMS is more than one half





# Mobile malware/threats

- Infection channels
  - OS vulnerability exploit
  - Application vulnerability exploit
  - Jailbreak / root
  - Unofficial marketplaces
  - Bluetooth, Wi-Fi, NFC, QR Code
  - Email, Messaging



Hong Kong Computer Emergency Response Team  
Coordination Centre  
香港電腦保安事故協調中心



# Demo

DEMO





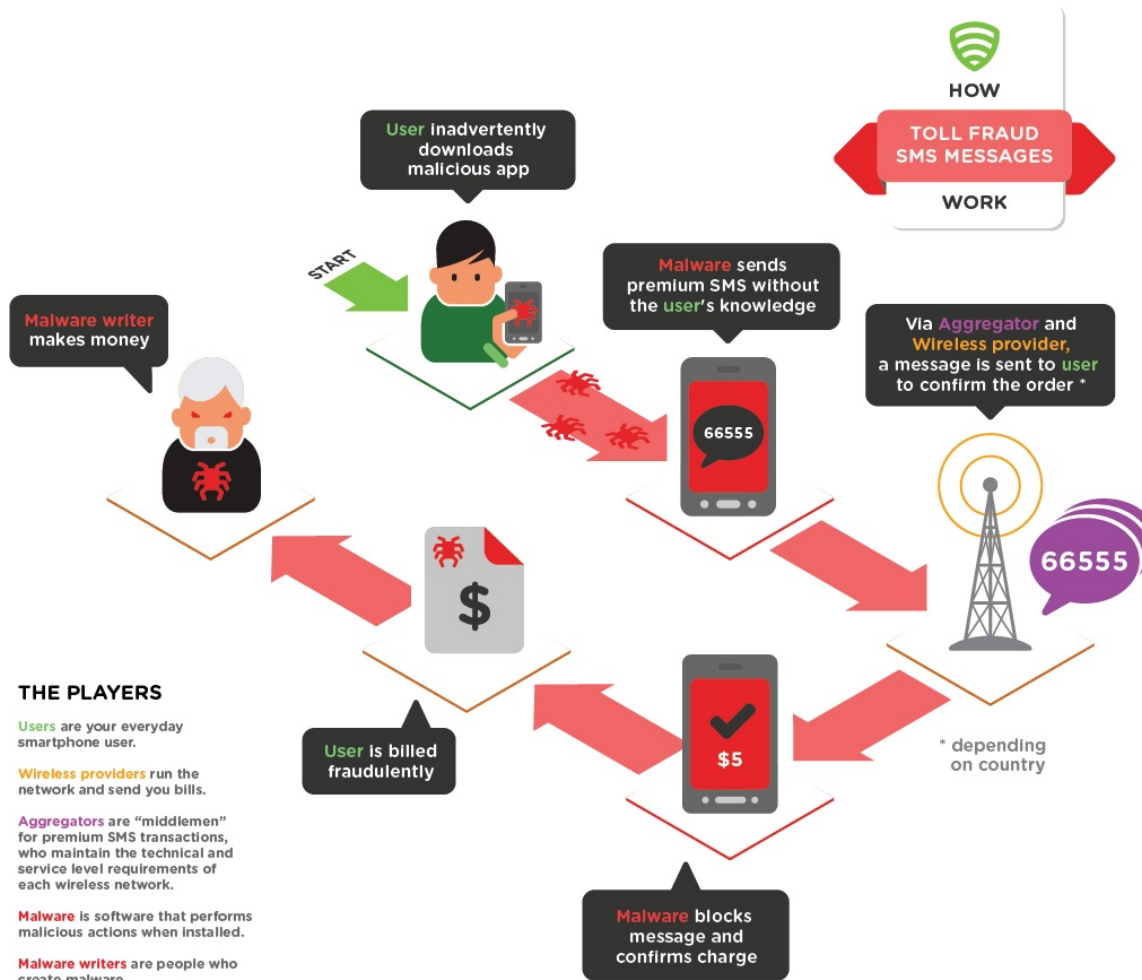
# Demo1 - Premium SMS

- Demo





# Demo1 - Premium SMS





# Demo1 - Premium SMS

- Anti-malware tools





## Demo2 - USSD attack via QR Code

- What is USSD?
  - USSD is a code to communicate with Service Provider or perform phone actions.
    - E.g. `*#06#` - retrieve IMEI code
  - Some phone manufactories have specified USSD codes to perform factory reset.
  - The attack is targeted to Dialer flaw





# Demo2 - USSD attack via QR Code

- Demo



# Demo2 - USSD attack via QR Code

- USSD protection tools

- **avast!** Mobile Security



- **Avira** USSD Exploit Blocker



- **Bitdefender** USSD Wipe Stopper



- **ESET** USSD Control



- **Norton** Halt USSD Code Blocker



- **Sophos** Mobile Security





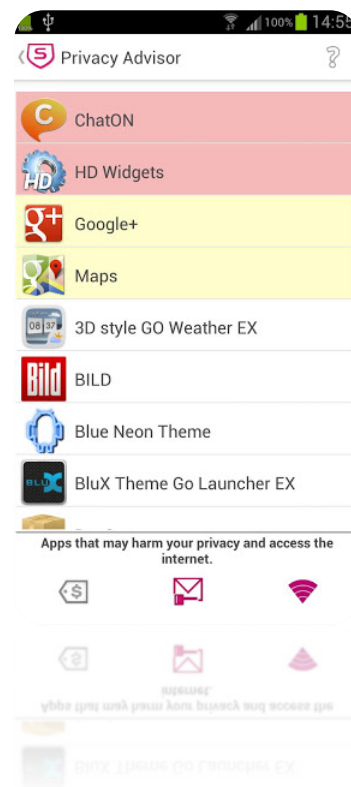
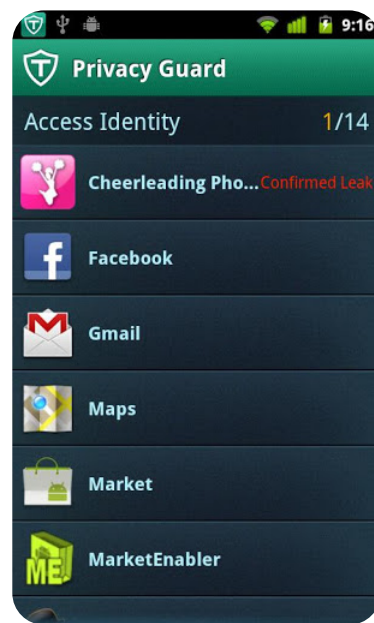
# Demo3 - Privacy Advisor

- Demo



# Demo3 - Privacy Advisor

- Privacy Advisor tools





# Safeguard your mobile phone







# Safeguard your mobile phone

- Setup Passcode / Screen Lock
  - If lost or stolen, data is much difficult to access
- Trusted Sources
  - Only install apps from trusted stores and markets
- Clicking on web links
  - Pay close attention if the website ask to enter account or login information



# Safeguard your mobile phone

- Firmware updates
  - Install firmware/application updates as soon as they are available
- Check your phone bill
  - Be alert for unusual behaviors on your phone
    - Suspicious charges
    - Unusual messages (SMS, WhatsApp, LINE, etc.)
    - Suddenly decreased battery life



# Safeguard your mobile phone

- Physical security
  - Take care of your smart devices
- Security App
  - Install a mobile security app
    - Scan every app you downloaded for malware and spyware
    - Help to locate a lost or stolen device
    - Protect from unsafe websites
    - Data monitoring



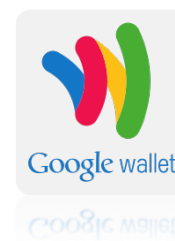
# Future trends





# Future trends

- NFC
  - Payment over NFC
  - Mobile payment
- GPS
  - Physical location
- Mobile OS
  - BlackBerry 10
  - Windows Phone 8





Hong Kong Computer Emergency Response Team  
Coordination Centre  
香港電腦保安事故協調中心



# HKCERT Services





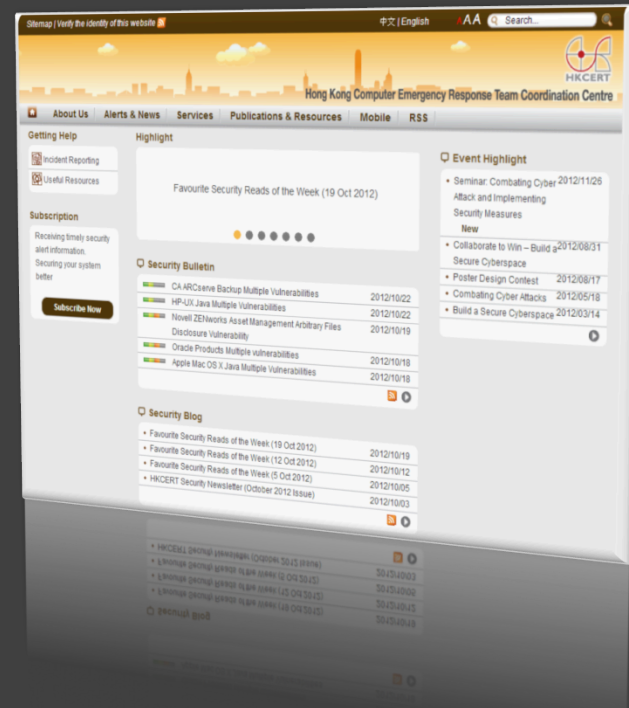
## HKCERT Services

- Incident Response service
  - **Hotline: 8105-6060**
- Mobile Security Tools on Android
  - <https://www.hkcert.org/mobile-security-tools>
- Security Blog on Mobile
  - <https://www.hkcert.org/security-blog>
- Mobile security guideline (coming soon)





Hong Kong Computer Emergency Response Team  
Coordination Centre  
香港電腦保安事故協調中心



# Q & A Section

Thank you

Website: [www.hkcert.org](http://www.hkcert.org)

Hotline: 8105-6060



Search: HKCERT







# Supplement





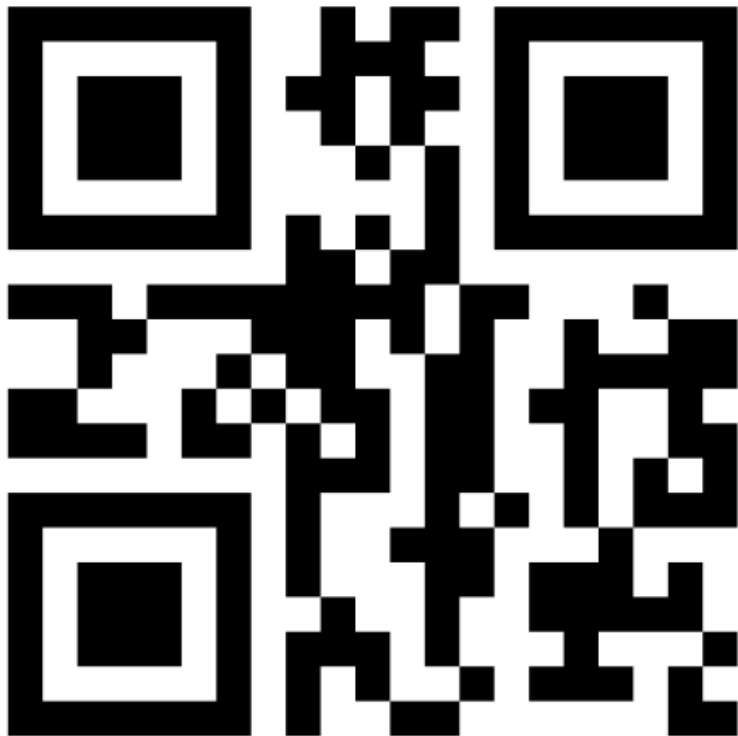
## Dialer Vulnerability Test

### 撥號器漏洞測試

(No harm 沒有損害指令)

QR Code – USSD: \*#06#

Show IMEI code 顯示 IMEI 碼



- Test

- Your Android phone is safe
  - If it does NOT show IMEI in the Dialer application after scanning
- Install a USSD protection tool is necessary
  - If a 15-digit IMEI shows immediately in the Dialer application after scanning

- References

- Blog article:
  - [https://www.hkcert.org/my\\_url/zh/blog/12092801](https://www.hkcert.org/my_url/zh/blog/12092801)
- USSD protection tools
  - [Page 21](#), or
  - <https://www.hkcert.org/mobile-security-tools>