Security in Computing & Information Technology

Lecture 10

Mobile Computing

Lecture Schedule

Foundations

1. Introduction
2. Vulnerabilities, Threats, Attacks

Basic mechanisms

3. Security mechanisms, Elementary cryptography
4. Authentication
5. Access control

Major computing security areas

6. Operating systems
7. Databases
8. Networks
9. Web
10. Mobile computing

Applications

11. Privacy
12. Internet banking

Lecture Topics

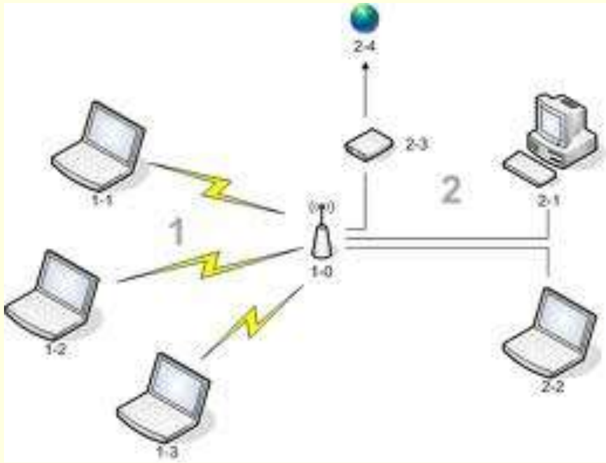
- Wireless and mobility technology
  - Infrastructure
  - WiFi
  - Bluetooth
  - Smartphones
- Mobile malware

Mobile Computing

- Mobile devices
  - Portable computing equipment
  - Used pervasively
  - Have many different forms

    Laptop/notebook/netbook computers, smart phones

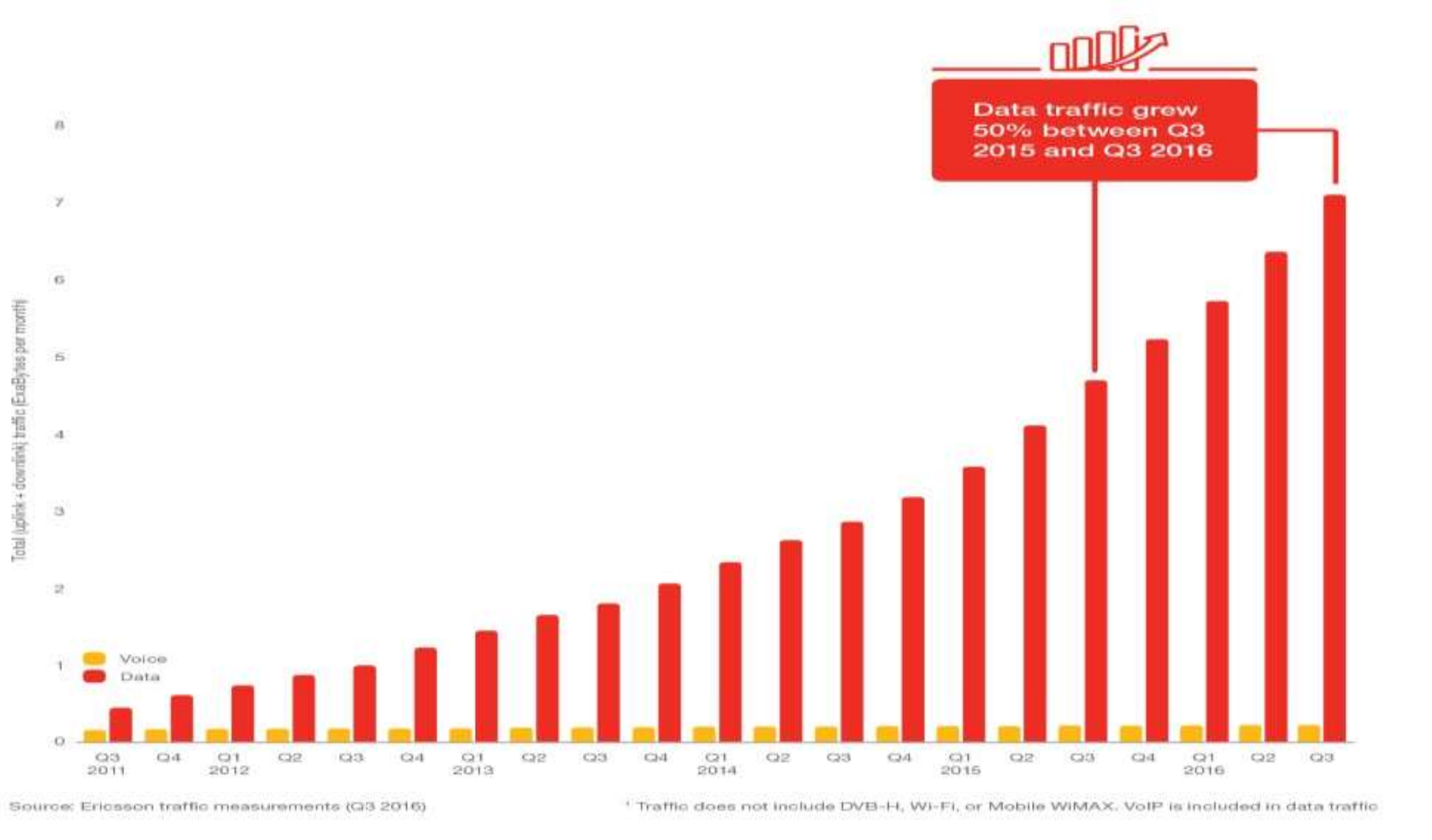
- Mobility infrastructure
  - Network access
    - Wireless network



Mobile Computing Devices

- Computing services
  - Service level similar to fixed devices
- Portability constraints
  - Battery operated
    - Limited power
  - Limited processing capacity, memory
  - User interface issues
    - Small screen, unusual keyboard

Mobile Traffic



Data traffic grew 50% between Q3 2015 and Q3 2016

Source: Ericsson traffic measurements (Q3 2016)

¹ Traffic does not include DVB-H, Wi-Fi, or Mobile WiMAX. VoIP is included in data traffic

Image source: https://www.ericsson.com/mobility-report/mobile-traffic-statistics-q3-2016

Operating Systems' Market Share Overall

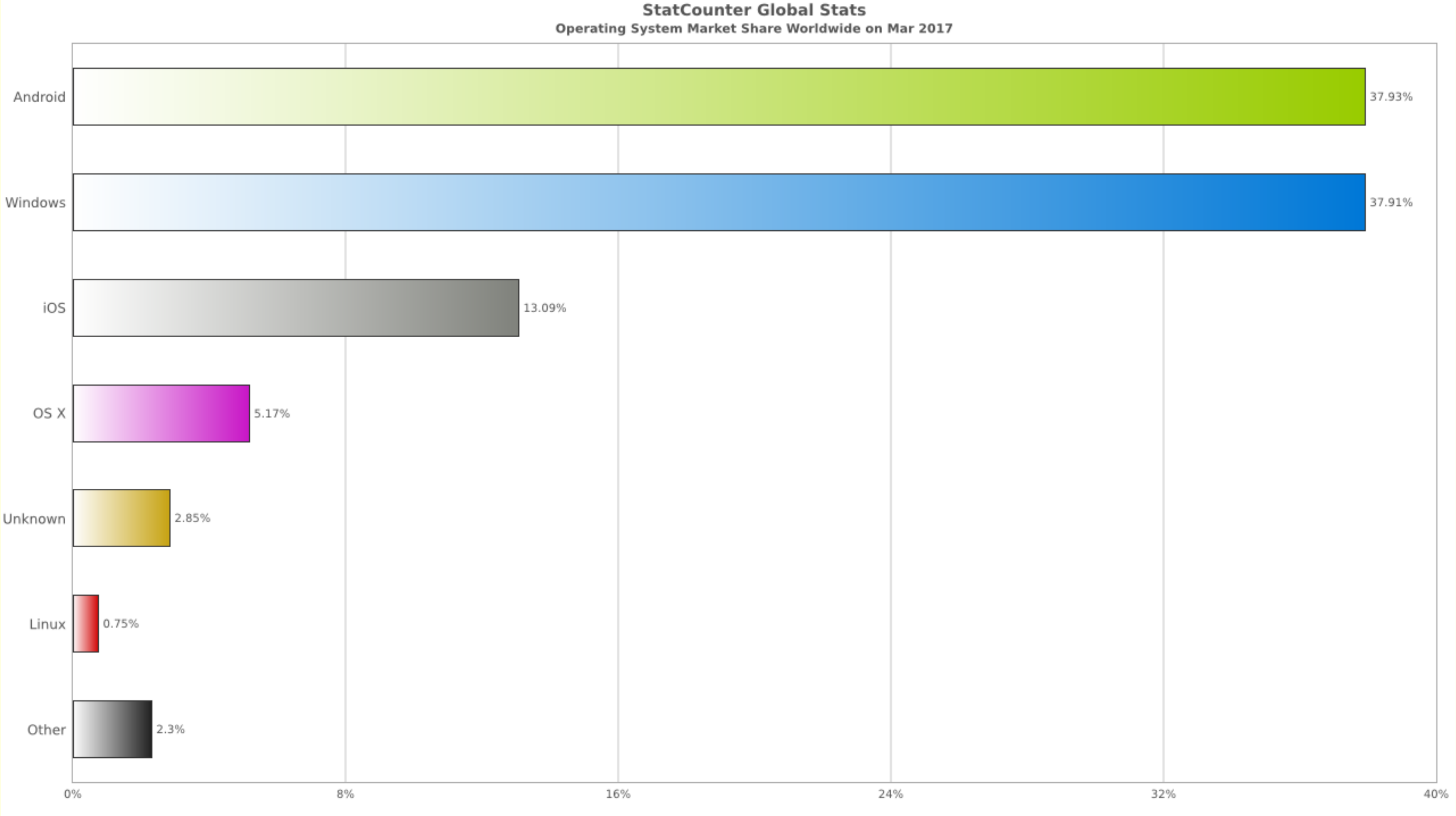


Image source: http://gs.statcounter.com/os-market-share#monthly-201703-201703-bar

Operating Systems' Market Share Mobile

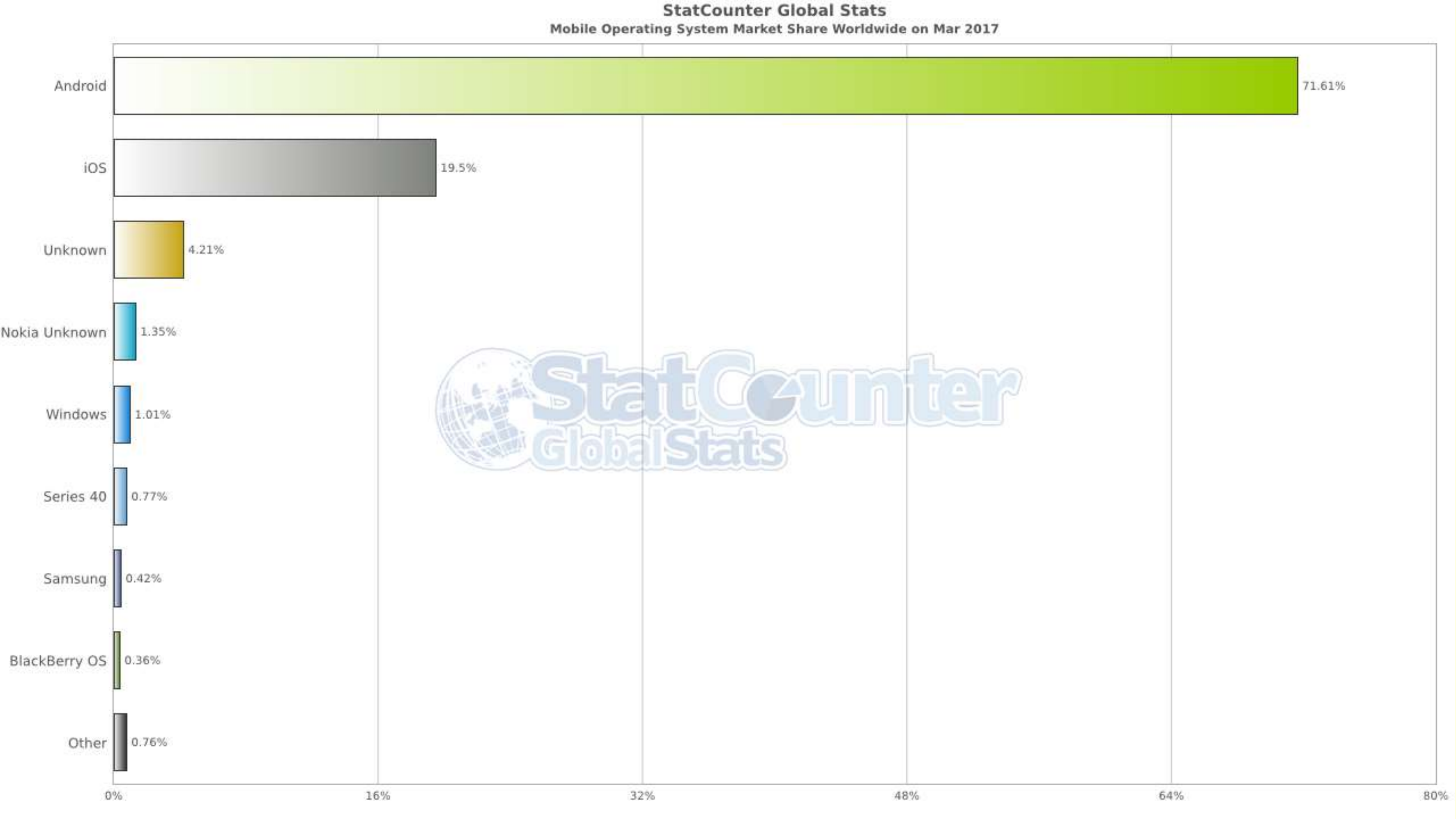


Image source: http://gs.statcounter.com/os-market-share#monthly-201703-201703-bar

Mobile Device Security

- Physical security
  - Easy to steal or lose
  - Easy to temper with, if left unattended
    - Access by unauthorised users
- Software security
  - Computers
    - The same as fixed hosts
    - Additional malware, mostly related to location privacy
  - Phones
    - Smart phones are mostly affected

Mobile Networks and Attacks

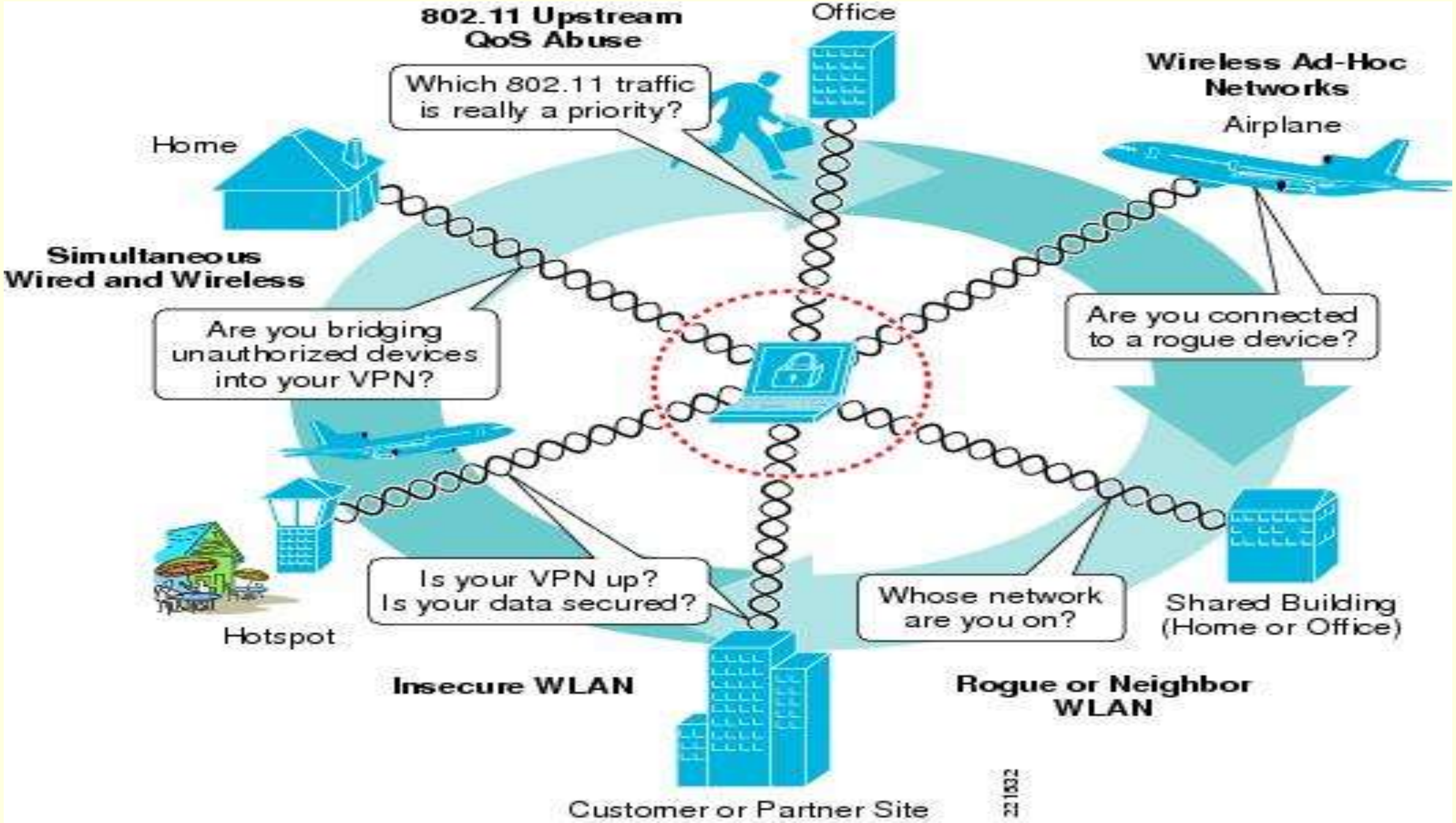

802.11 Upstream QoS Abuse
Which 802.11 traffic is really a priority?
Office
Wireless Ad-Hoc Networks
Airplane
Home
Simultaneous Wired and Wireless
Are you bridging unauthorized devices into your VPN?
Are you connected to a rogue device?
Hotspot
Is your VPN up? Is your data secured?
Whose network are you on?
Shared Building (Home or Office)
Insecure WLAN
Rogue or Neighbor WLAN
Customer or Partner Site
221532

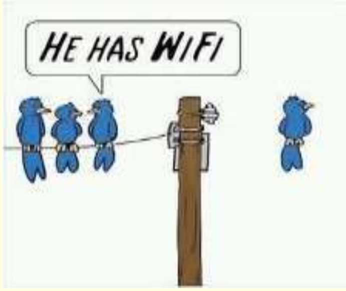
Image source http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/csa_mobile_secure.html

Mobility Infrastructure

- Wired networks
  - “Road warriors”
    - Away from home network
    - Have access to wired networks (e.g. in hotel)
  - Security issue: connection to home network goes via public routes

- Wireless networks
  - Advantages
    - Freedom of user movement
    - No cabling costs
    - Less weight (important e.g. in an aeroplane)
  - Security issue: communication channel is wide open

Wired vs Wireless



- Wireless network applications
  - Logically should be no different – only the communication medium differs
  - In practice
    - Performance is different (higher error rate, lower speed)
    - Signal interference is common

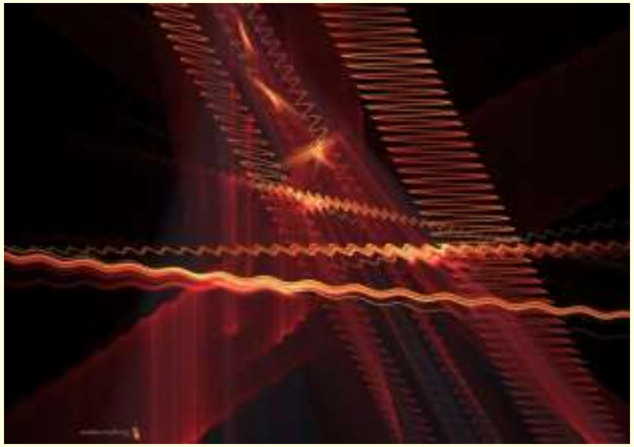
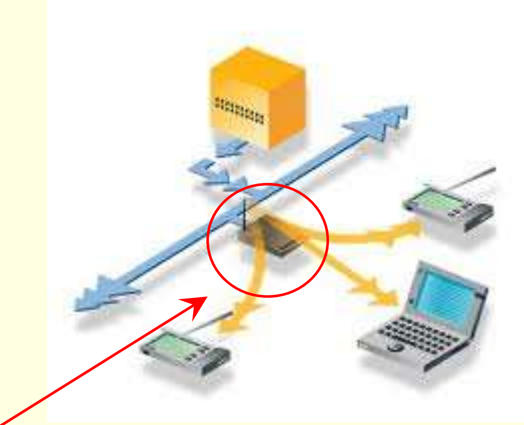


Image source: http://wikis.lib.ncsu.edu/index.php/Wireless_Communication_Interferences

Wireless Computer Networks
Local Area Networks (LANs)

- Features
  - Covers a limited area
  - Fairly high-speed communication
  - Access is restricted to local users (employees, students, affiliates etc)



- Network access
  - Service access point (SAP)
    Interface between wired and wireless network segments
  - Transmission methods
    - Radio waves - WiFi (most popular)
      - Hotspot: public SAP
    - Infrared (outdated)
      - Line of sight is needed for good reception
      - Still used where radio interference is an issue

Wireless Computer Networks
Metropolitan Area Networks (MANs)

“Mobile broadband”

- Features
  - Covers larger geographical area (max. 50km)
  - Provides medium-speed communication
    - Speed comparable to wired MANs when close to SAP
    - Speed decreases and error rate increases with distance
  - Access is available to all valid subscribers
- Network access
  - Several competing technologies

    WiFi – with compromises on radial coverage

    3G/LTE/4G phone (UMTS) – phone / mobile broadband

    WiMAX –mobile broadband

Wireless Security

- Problems
  - No physical protection
    - Physical access is not limited

      No need to plug into a socket

  - Broadcast communication
    - Transmissions can be overheard by anyone within the range
    - Anyone can transmit messages that
      - can be received by all others within the range
      - interfere with other transmissions and prevent correct reception (jamming)
- Security implications

  It is easy to

  - eavesdrop (Google Street View cars did that)
  - inject bogus messages
  - replay recorded messages
  - launch a denial-of-service attack by jamming

Wireless LAN (WiFi)

- Hotspots
  - Public access points
  - Can be free or fee-paying
  - Universal technology – interoperable devices
- Home networks
  - Wireless routers

    Share access to one external Internet connection by several local devices

  - Wireless devices

    Computers, printers, gaming hardware, …

WiFi Security Issues

- Hotspots
  - Typically default to open (non-protected) mode
  - Channel pollution

    WiFi networks too close to each other may interfere with each other's operation
- Home networks
  - Hacking
    - WarXing (war driving, war walking, …)

      Searching for WiFi networks without using its services

      Problems: Ethical and legal questions, privacy concerns
    - Piggybacking

      Connecting to a network and using it without explicit authorisation
  - Easy attack launch by intruders

    E.g. DNS (URL to IP address) spoofing

    The intruder can reply to a local query faster than the real DNS server

WiFi Security Protocols

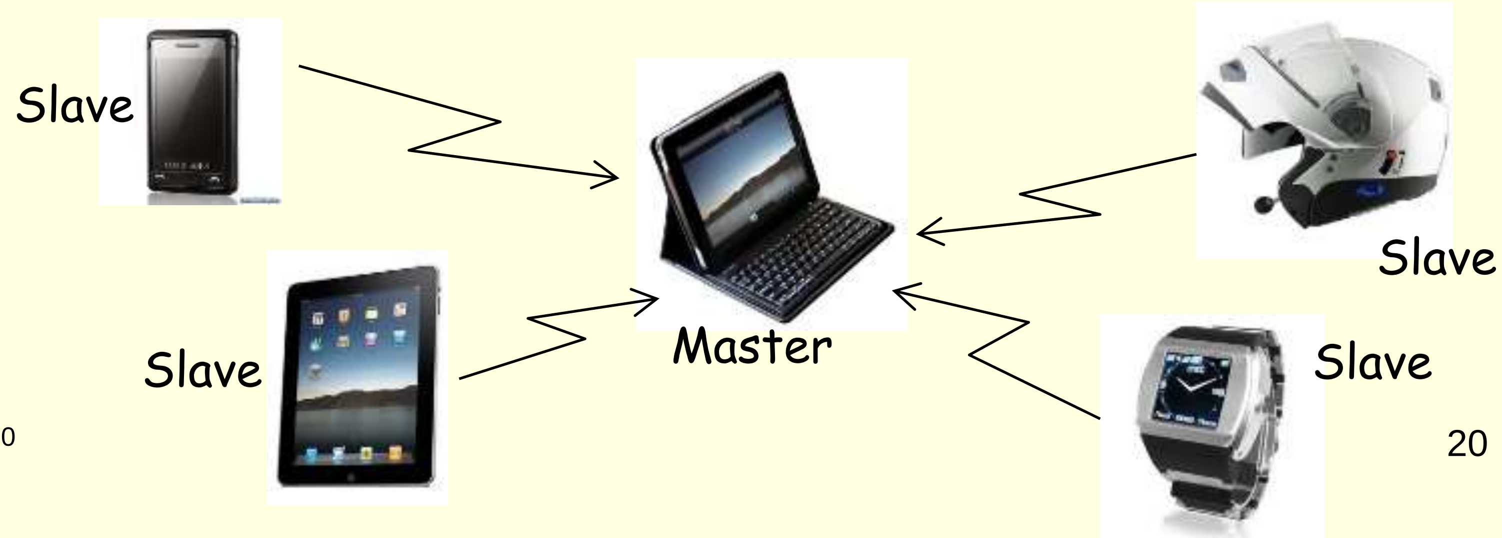
- Wired equivalent privacy (WEP)
  - Aim: make a wireless network as secure as a wired network (i.e. not strong security)
  - Services: access control, message confidentiality and integrity
  - Deprecated (has many flaws) Don't use it!
    - Authentication is one way only (mobile device to access point)
    - The same secret key is used for authentication and encryption
    - Device can be impersonated
    - No re-play protection
    - Message integrity check is ineffective
    - …
- WiFi protected access (WPA – WPA2)
  - Improved data encryption
    - Temporal key integrity protocol (TKIP): default for WPA, supported by WPA2 for backward compatibility
    - AES: default for WPA2
  - Improved authentication via the extensible authentication protocol (EAP)

Bluetooth

- Short-range wireless communication
  - Typical distance is 10m (or for extended range 100m)
- Designed to avoid interference with other wireless networks (automatic search for an idle channel)
- Low to medium speed connection
  - Basic: 1 Mbps, recent standards allow up to 24 Mbps
  - Higher speeds consume more power
- Offers basic security only

Bluetooth Networks

- Bluetooth devices can form ad-hoc networks (piconets)
  - Networks that are established dynamically and automatically by mobile devices
  - A master device provides synchronisation for slave devices in the piconet



Bluetooth Security

- Security services
  - Authentication
  - Authorisation
  - Confidentiality (encryption)

      Stream cipher with a 128 bit link-key (stored in the device), a 128 bit random number and a value negotiated during authentication
- Security levels
  - Services
    - Authentication and authorisation required
    - Authentication only
    - Open access
  - Devices
    - Trusted
    - Untrusted
- Access modes
  - Non-secure
  - Service-level enforced security
  - Link-level enforced security

Bluetooth Vulnerabilities

There are many

- Encryption

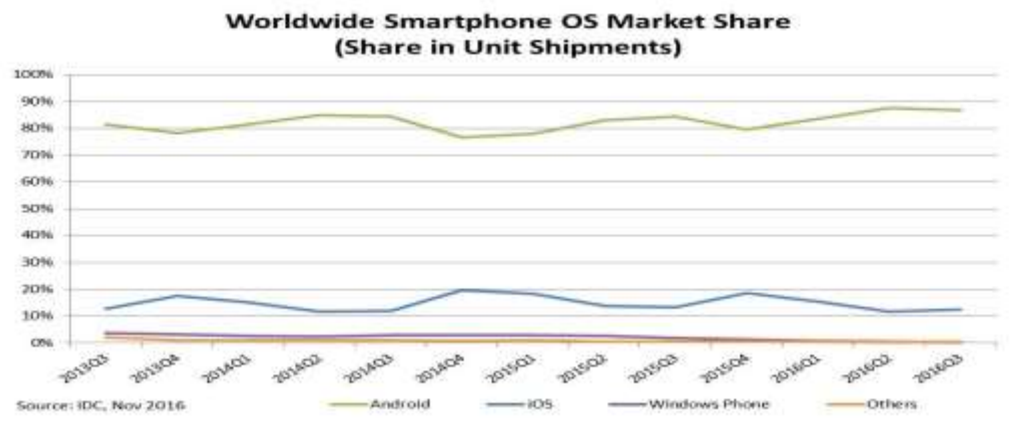
  Keys are negotiated and can be short, device keys can be shared, cipher algorithm is weak …
- Authentication

  Attempts have no limits, no user authentication, …
- Threats
  - Bluejacking: sending unsolicited messages
  - Bluesnarfing: unathorized access of information via Bluetooth
  - Bluebugging: attacker takes over the device by exploiting some flaws in firmware of older devices
  - Denial of service
  - Fuzzing attacks: sending malformed messages/data to discover device firmware vulnerabilities

Mobile Devices (Smartphones)

- Considerable capabilities of mobile devices
  - Resources: CPU, memory, storage devices (e.g. SD card)
  - Efficient interfaces: GUI, touch screen, QWERTY keyboard
  - Connectivity: local (Bluetooth), wide area (HSDPA)
- Good support
  - Applications (Apple shop, Android market)

    Platform popularity



Source: IDC, Nov 2016

Image source: http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Security Considerations

- Platforms
  - Variety of operating systems
    - Android, iOS (iPhone), Symbian, Palm OS, Windows mobile, Blackberry
- Large population of devices
  - Makes them attractive targets for malware
- Attack profile different from computers
  - Less value for using them in botnets
  - More valuable private data
- Vulnerabilities
  - Technical exploits
  - Social aspects (more vulnerable user population)
- Services may be running in the background
  - E.g. the phone may not deactivate WiFi and Bluetooth radios when disconnecting devices or from the network (iOS 11)

Malware Example

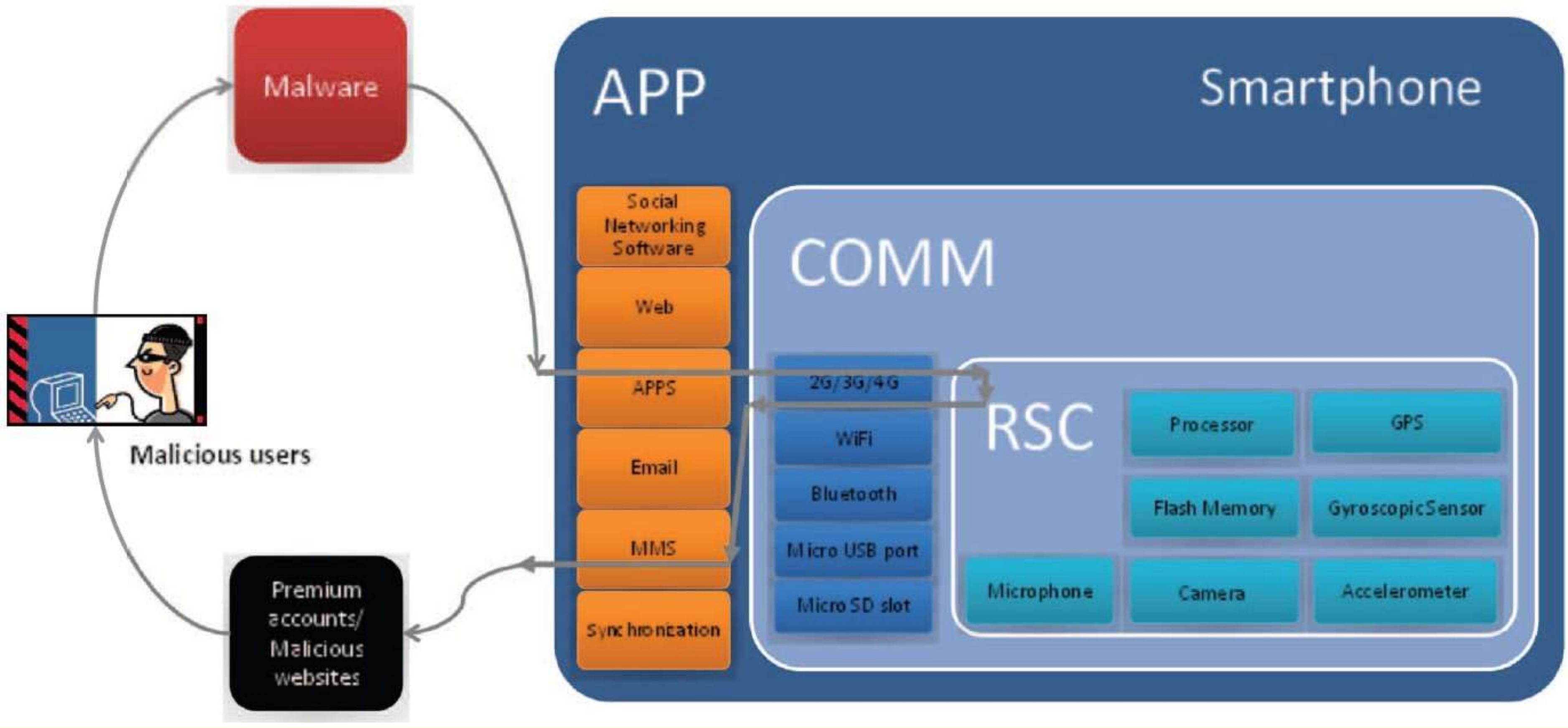


Image source: IEEE Computer, 12/2012

Mobile Phone Protection

Platform dependent security measures

- Closed platform (e.g. iPhone)
  - Applications run in a sandbox (cannot access other programs' data)
  - Applications are signed by Apple or by the developer using an Apple certificate
  - Jailbreak: enabling the iPhone to run applications not approved by Apple
    - Large number of new applications
    - Security/protection is switched off
- Antivirus software
  - Major vendors have phone support

    E.g. Kaspersky for Symbian, Windows
- Inherited protection methods

  E.g. Android: Linux + Java

Mobile Phones and Malware

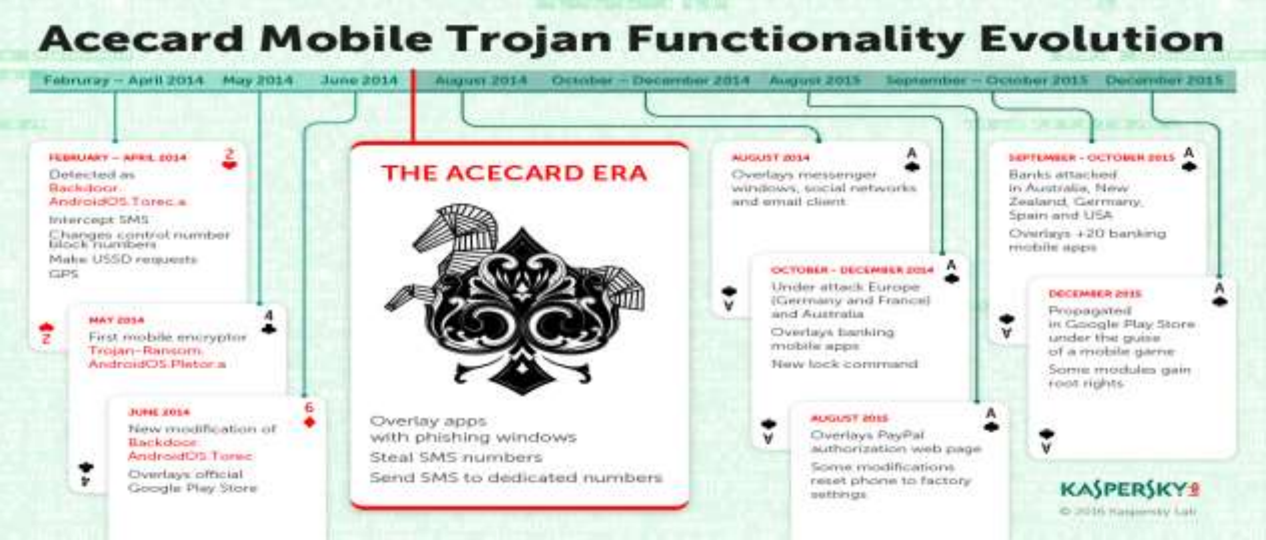
- Mobile malware has become a profitable business
- Malware distribution techniques are diversifying

  They spread via

  - Drive-by-downloads
  - Email
  - Bluetooth file transfers
  - Multimedia messages (MMS), ringtones
  - Infected memory cards
  - SMS download links

Malware Evolution

- Trojans subscribe people to unnecessary services
- Fake mobile banks steal money
  - E.g. Trojans overlaying a phishing screen over a legitimate banking application (clickjacking)
- Evolution
  - Criminals release skeleton with simple functions (to mislead security researchers)
  - Malicious functionality is added
  - Massive attack campaign begins



Acecard Mobile Trojan Functionality Evolution

Februray – April 2014 | May 2014 | June 2014 | August 2014 | October – December 2014 | August 2015 | September – October 2015 | December 2015

FEBRUARY – APRIL 2014
Detected as Backdoor. AndroidOS.Torec.a
Intercept SMS
Changes control number block numbers
Make USSD requests
GPS

MAY 2014
First mobile encryptor Trojan-Ransom. AndroidOS.Pletor.a

JUNE 2014
New modification of Backdoor. AndroidOS.Torec
Overlays official Google Play Store

THE ACECARD ERA
Overlay apps with phishing windows
Steal SMS numbers
Send SMS to dedicated numbers

AUGUST 2014
Overlays messenger windows, social networks and email client

OCTOBER – DECEMBER 2014
Under attack Europe (Germany and France) and Australia
Overlays banking mobile apps
New lock command

AUGUST 2015
Overlays PayPal authorization web page
Some modifications reset phone to factory settings

SEPTEMBER – OCTOBER 2015
Banks attacked in Australia, New Zealand, Germany, Spain and USA
Overlays +20 banking mobile apps

DECEMBER 2015
Propagated in Google Play Store under the guise of a mobile game
Some modules gain root rights

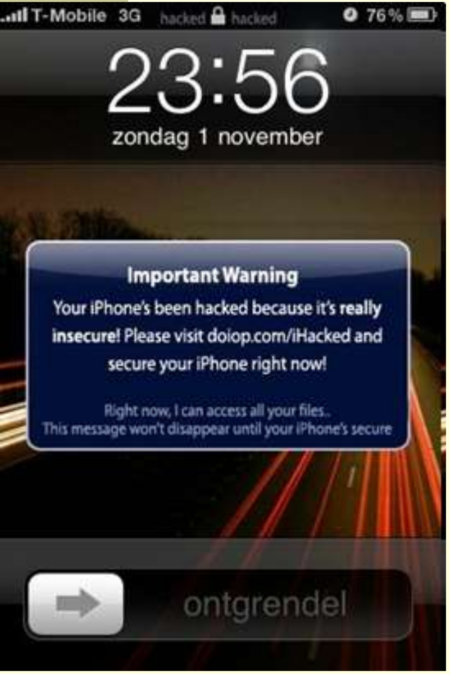
© 2016 Kaspersky Lab

Viruses

- Spreading
  - MMS replication, similar to email
    - Message with social engineering content
    - Trusted source: message comes from known sender
    - Rapid local outbreak, easily noticed (and blocked) by network operators

Worms

- Spreading
  - Selects the next victim from local address book
  - SMS download links spammed with worm installation file (appear to come from trusted source)
- Motivations
  - Vendor error
    - HatiHati: intended anti-theft program, locks the phone if SIM card is changed and sends SMS with info on new SIM card. Sent SMS in an infinite loop, due to a bug in the code.
  - Getting people’s attention
    - Ikee: jailbroken iPhones with SSH installed and having the default root password are getting infected (limited to Australia)
  - Attack tools
    - Duh: uses the same method as ikee, but malicious. First malware to turn a mobile phone to a zombie (e.g. for DDoS attacks)



Important Warning

Your iPhone's been hacked because it's really insecure! Please visit doiop.com/iHacked and secure your iPhone right now!

Right now, I can access all your files..
This message won't disappear until your iPhone's secure

Trojans

- Most frequent malware
- For profit
  - Active Trojan

    Trojan sends SMS to micropayment systems or premium rate numbers
  - Callback scheme

    Phone rings only once. When returning the call, user is connected to a premium rate number. Long messages (with bad call quality) tries to keep the user connected as long as possible.

Spam and Phishing

- Spam via SMS

  E.g. entice to subscribe to expensive SMS services

  Problem: Unwanted advertising uses up limited resources

- Phishing

  Aims to extract private information

  E.g. banking details, via spoofed sites

  Problem: may look more genuine because phone numbers are less public than email addresses

Spytools

- Applications sending out information from the victim's phone
- Used by
  - spouses, private investigators, managers, industrial spies etc.
  - criminals (phone banking)

- Information accessed
  - SIM card information
  - SMS, MMS, email traffic information (called number, time) & content
  - Voice call information and content, including call interception & recording
  - Geographical location (GPS)
  - Key logging
- Work on most platforms (Windows, Android, Unix …)

Spytool Example: RCSAndroid

- A sophisticated, real-world surveillance and hacking tool that can
  - Capture screenshots
  - Collect passwords for Wi-Fi networks and online accounts (Skype, Facebook, etc)
  - Record using the microphone
  - Collect SMS, MMS, and Gmail messages
  - Record location
  - Capture photos using the front and back cameras
  - Collect contacts and decode messages from IM accounts
  - Capture real-time voice calls in any network or app by hooking into the “mediaserver” system service
- Infection methods
  - Specially crafted SMS and email messages contain URLs to infected sites
  - Applications (e.g. BeNews) on the official Google Play Store install the spyware

Mobile Spyware: Detection

- Users
  - Any extra charges on my bill? (no tools can trick the operator’s billing system)
  - Has my phone opened unexpected connections?
  - When rebooting, are there screens/dialogs that flash and disappear instantaneously?
- Experts
  - Check network connections
    - TCP/IP traffic monitoring
  - Check every process running on the phone
    - Most system-like processes should start from ROM
    - Check where the image was loaded from
  - File system analysis
    - Check autostart programs
    - Check all executables
    - Is the device jailbroken?
    - Investigate suspicious files

Mobile Spyware: Defence

- Spyware vendors make efforts to avoid attention of security companies
  - Security companies may not have a full picture of mobile spyware
- Prevention
  - Apply updates (OS, applications), possibly re-install OS periodically
  - Use only signed applications
  - Have a lock code, personalise your phone (to avoid quick swapping), don't leave it out of sight

Defence Tools

- Anti-virus products
- Encrypted communication
  - VoIP (not using the phone connection)
  - Protects the conversation only
  - E.g.
    - Secfone
      - 2048-bit RSA for server authentication
      - 1024-bit RSA for peer authentication
      - 448-bit Blowfish CBC for voice communication and data flow
    - Cryptalk
      - EC Diffie-Hellman for key exchange
      - AES-256 for data exchange
      - RSA 2048 signature

Virtual Private Networks (VPN)

- The number of Android VPN applications significantly increased in the last few years
- Many of them do not provide sufficient security (or security at all)
  - Fail to encrypt
  - Use third party tracking applications
  - Close to 40% contain malware
  - Use traffic interception nodes (including TLS traffic), in-path proxies, or manipulate traffic
  - Source: https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf

Summary

- Wireless technologies have inherent security issues
- Resource-constrained devices offer less support for security services
- Conventional malware adapted to the new platform