Mobile Handsets: 
A Panoramic Overview

Adam C. Champion and Dong Xuan
Department of Computer Science & Engineering
The Ohio State University
Autumn 2012
Outline

• Introduction
• Mobile Handset Architecture
• Mobile Handset Operating Systems
• Networking
• Applications
• Mobile Handset Security
Mobile Handset Definition

- Mobile handsets (*mobiles*): electronic devices that provide services to users:
  - Internet
  - Games
  - Contacts
- Form factors: tablets, smartphones, consoles
- Mobile: arguably, your next computer system
Mobile Handsets: Business

• Meteoric sales and growth:
  – $\geq 5$ billion mobile phone subscriptions worldwide
  – Some people have *multiple* phones!
  – Mobile handsets & industries: $5$ trillion [3]

• Mobile phones are replaced every 6 months in S. Korea (just *phones*) [4]

• We can’t ignore these numbers

• Note: mobiles are *computer systems*
What’s Inside a Mobile Handset?

Figure D.17  Circuit board from a Nokia cell phone. (Courtesy HowStuffWorks, Inc.)

Source: [5]
Handset Architecture (1)

- Handsets use several hardware components:
  - Microprocessor
  - ROM
  - RAM
  - Digital signal processor
  - Radio module
  - Microphone and speaker
  - Hardware interfaces
  - LCD display
Handset Architecture (2)

• Handsets store system data in electronically-erasable programmable read-only memory (EEPROM)
  – Mobile operators can reprogram phones without physical access to memory chips
• OS is stored in ROM (nonvolatile memory)
• Most handsets also include *subscriber identity module* (SIM) cards
Handset Microprocessors

- Handsets use *embedded processors*
  - Intel, ARM architectures dominate market. Examples include:
    - BlackBerry 8700, uses Intel PXA901 chip [6]
    - iPhone 3G, uses Samsung ARM 1100 chip [7]
  - Low power use and code size are crucial [5]
  - Microprocessor vendors often package *all* the chip’s functionality in a single chip (*package-on-package (PoP)) for maximum flexibility
  - Apple A4 uses a PoP design [10]
Example: iPhone 3G CPU

- The iPhone: a real-world MH [7–9]
  - Runs on Samsung S3C6400 chip, supports ARM architecture
  - Highly modular architecture

Source: [8]
Mobile Handset OSes (1)

• **Key mobile OSes:**
  – Google Android
  – Apple iOS
  – BlackBerry OS
  – Windows Phone 7 (formerly Windows Mobile)

• **Others include:**
  – Symbian OS
  – HP Palm webOS
  – Samsung bada

*U.S. market share. Source: [25]*
Mobile Handset OSes (2)

- **Symbian OS (ARM only)**
  - Closed-source (Nokia/Accenture)
  - Multitasking
  - Programming: C++, Java ME, Python

- **BlackBerry OS (?)**
  - Proprietary (RIM)
  - Multitasking
  - Many enterprise features
  - Programming: Java ME

- **iOS (ARM only)**
  - Proprietary (Apple)
  - Multitasking
  - Multi-touch interface
  - Programming: Objective-C

- **Windows Phone 7/8 (ARM only)**
  - Proprietary (Microsoft)
  - No multitasking
  - Programming: Silverlight, XNA, .NET Compact Framework, native C/C++ (WP8)

- **Android (ARM, x86, …)**
  - Open-source
  - Multitasking
  - Programming: Java (Apache Harmony)

- **Other OS features**
  - Most require app code signing
  - Many support Adobe Flash Lite, multitasking
  - ARM is predominant ISA
Mobile Handset Networking

• Handsets communicate with each other and with service providers via many networking technologies

• Two “classes” of these technologies:
  – Cellular telephony
  – Wireless networking

• Most handsets support both, some also support physical connections such as USB
Cellular Telephony Basics (1)

• Many mobile handsets support cellular services
• Cellular telephony is radio-based technology, radio waves propagated by antennas
• Most cellular frequency bands: 800, 850, 900, 1800, 1900, 2100 MHz

Source: [5]
Cellular Telephony Basics (2)

• Cells, base stations
  – Space divided into *cells*, each has *base station* (tower, radio equipment)
  – Base stations coordinate so mobile users can access network
  – Move from one cell to another: *handoff*
Cellular Telephony Basics (3)

• Statistical multiplexing
  – Time Division Multiple Access (TDMA)
    • Time & frequency band split into time slots
    • Each conversation gets the radio a fraction of the time
  – Frequency Division Multiple Access (FDMA) analogous
Wireless Networking (1)

• Bluetooth (BT)
  – Frequency-hopping radio technology: hops among frequencies in 2.4 GHz band
  – Nearly ubiquitous on mobile handsets
  – Personal area networking: master device associate with ≤ 7 slave devices (piconet)
  – Pull model, not push model:
    • Master device publishes services
    • BT devices *inquire* for nearby devices, *discover* published services, *connect* to them
  – Latest version: 4.0; latest mobiles 3.0, 4.0 [12]
Wireless Networking (2)

- WiFi (IEEE 802.11)
  - Variants: 802.11b, g, n, etc.
  - Radio technology for WLANs: 2.4, 3.6, 5 GHz
  - Some mobile handsets support WiFi, esp. premium ones!
  - Two modes: infrastructure and ad hoc
    - Infrastructure: mobile stations communicate with deployed base stations, e.g., OSU Wireless
    - Ad hoc: mobile stations communicate with each other without infrastructure
  - Most mobiles support infrastructure mode
Mobile Handset Applications

• Mobile apps span many categories, e.g.:  
  – Games: Angry Birds, Assassin’s Creed, etc.  
  – Multimedia: Pandora, Guitar Hero, etc.  
  – Utilities: e-readers, password storage, etc.  
• Many apps are *natively* developed for one mobile OS, e.g., iOS, Android  
  – *Cross-platform* native mobile apps can be developed via middleware, e.g., Rhodes [13], Titanium [14]  
  – Can also build (HTML5) Web apps, e.g., Ibis Reader [15], Orbium [16]  
• We’ll discuss mobile app development next
Native Mobile App Development

• Mobile apps can be developed *natively* for particular mobile handset OSes
  – iOS: Xcode/Interface Builder; Mac only
  – Android: Eclipse; Windows/Mac/Linux
  – Windows Phone: Silverlight, XNA, Visual Studio 2010+; Windows only
  – Symbian: Eclipse, NetBeans; Windows only
  – BlackBerry: Eclipse, Visual Studio; Windows only
Other Mobile App Development

• Middleware
  – Rhodes: Ruby/HTML compiled for all mobile OSes
  – Titanium: HTML/JS + APIs compiled for iOS, Android
  – Still dependent on native SDK restrictions

• Web development: HTML5, CSS, JS
  – Works on most mobile browsers
  – Can develop on many IDEs, Win/Mac/Linux

• SMS/cellular promotions
Business Opportunities

- Virtually every mobile OS supports app sales via stores, e.g., iOS App Store, Google Play (Android Market), MS App Hub
- Devs sign up for accounts, download SDKs
  - Costs: $99/yr (iOS, App Hub), $25 once (Google Play)
Mobile Handset Security Issues

- People store much info on their mobiles
- “Smartphones are the new computers….2 billion…will be deployed by 2013” – M.A.D. Partners [18]
- Handsets are targets for miscreants:
  - Calls
  - SMS/MMS messages
  - E-mail
  - Multimedia
  - Calendars
  - Contacts
  - Phone *billing system* [18]
Handset Malware History (1)

• Hackers are already attacking handsets
  – Most well-known case: a 17-year-old broke into Paris Hilton’s Sidekick handset [19]
  – Less well-known: worms, viruses, and Trojans have targeted handsets since 2004
  • 2004: [20]
    – Cabir worm released by “29A,” targets Symbian phones via Bluetooth
    – Duts virus targets Windows Mobile phones
    – Brador Trojan opens backdoor on Windows Mobile [24]
Handset Malware History (2)

• 2005: [21]
  – CommWarrior worm released; replicates via Bluetooth, MMS to all contacts
  – Doomboot Trojan released; claims to be “Doom 2” video game, installs Cabir and CommWarrior
• 2006: [20, 21]
  – RedBrowser Trojan released; claims to be a Java program, secretly sends premium-rate SMS messages to a Russian phone number
  – FlexiSpy spyware released; sends log of phone calls, copies of SMS/MMS messages to Internet server for third party to view
• 2008: [22]
  – First iPhone Trojan released
• 2009–2010: iPhone “Rickrolling”, Android SMS malware, etc.

“The single biggest thing threatening any enterprise today on a security basis is mobile. Furthermore, mobile phone application stores are the greatest malware delivery system ever invented by man” – Robert Smith, CTO, M.A.D. Partners [18]
Key Handset Threats, Attacks

- Info theft [23]
  - Transient info: user location
  - Static info: bluesnarfing attacks, WEP & WPA cracks [24]
- Service/$ theft, *e.g.*, premium-rate calls/SMS [23]
- Denial-of-service attacks [23]
  - Flooding attacks overload handset radio with garbage
  - Power-draining attacks attempt to drain battery
- Botnets and DoS attacks against networks [22]
- Exploiting the human factor (see HW 1)
- We’ll discuss risk management strategies
Risk Management Strategies

• Organizations must:
  – Understand rapidly-evolving threatspace [18]
  – Understand applicable laws & regulations
  – Understand employee demand for handsets and balance this against the risk they pose
  – Institute CSO policies to achieve compliance (and get top management on board!)
  – Inform employees about policies (change mgmt)
  – Implement the policies with tech and people
Risk Management Tactics

- To implement strategies, organizations must:
  - Decide whether to distribute handsets to employees for business purposes, allow use
  - Encrypt device data
  - Remote data wipe as needed
  - Procure, install anti-malware, firewall products
  - Require VPN use, strong passwords, inventory mgmt.
  - Monitor employee handset use to detect attacks
  - Educate employees about the threatspace, train them to treat handsets as any other computer system
  - Prevent, detect, and respond appropriately
Discussion and Questions

Thank you
References [1]

References [2]

15. Ibis Reader LLC, http://ibisreader.com