Mobile Platform Security Models

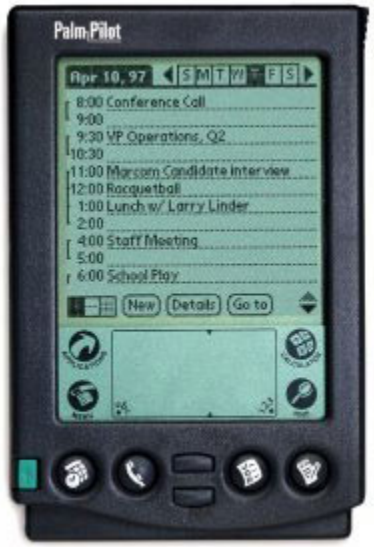
Outline

- Introduction: platforms and attacks
- Apple iOS security model
- Android security model
- Windows 7, 8 Mobile security model

Announcement: See web site for second homework, third project

Change takes time

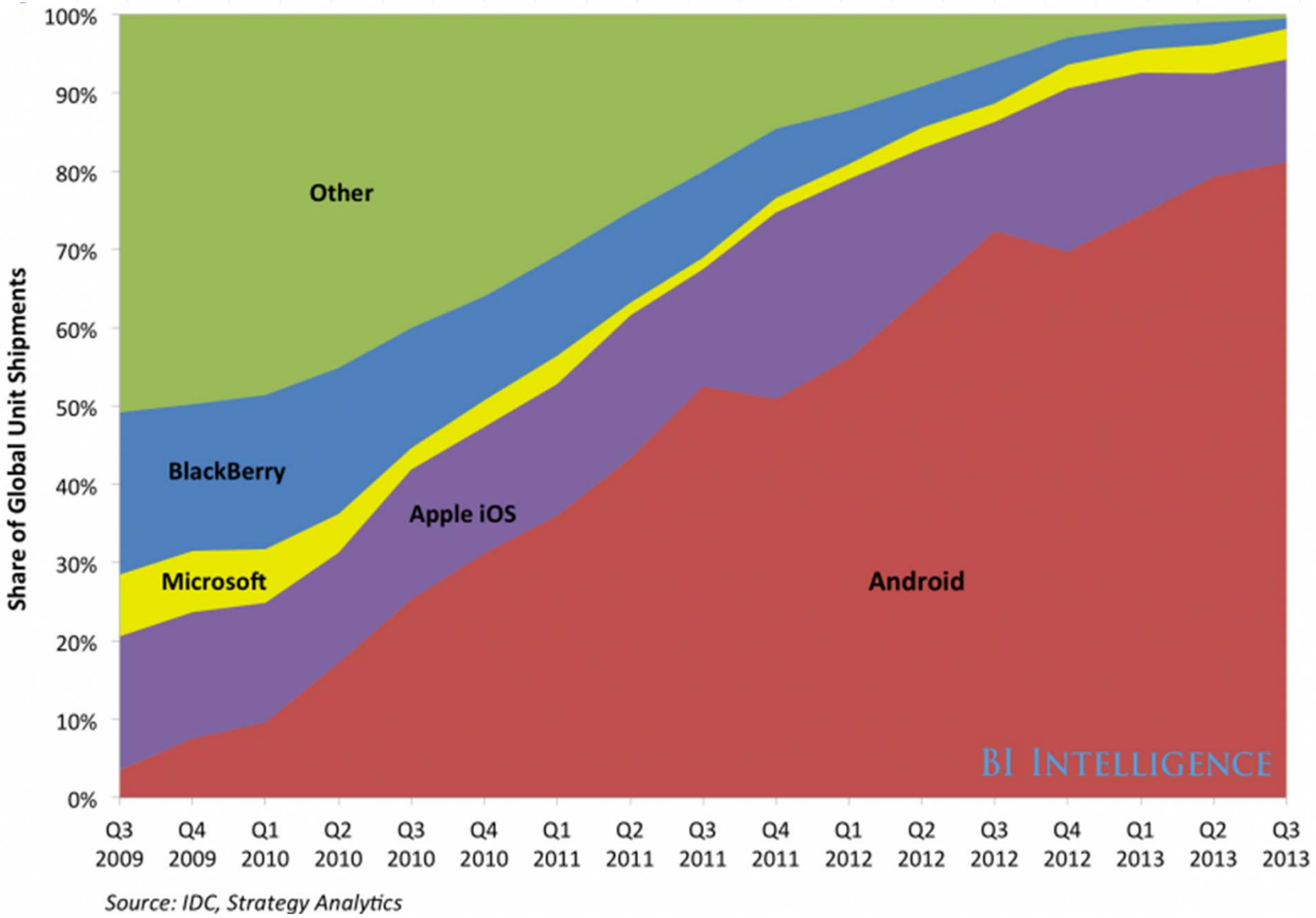
Apple Newton, 1987



Palm Pilot, 1997

iPhone, 2007

Global smartphone market share



Zillions of apps

Two attack vectors

- Web browser
- Installed apps

Both increasing in prevalence and sophistication

Mobile malware attacks

- Unique to phones:
  - Premium SMS messages
  - Identify location
  - Record phone calls
  - Log SMS
- Similar to desktop/PCs:
  - Connects to botmasters
  - Steal data
  - Phishing
  - Malvertising

Kaspersky: Aug 2013 – Mar 2014

- 3,408,112 malware detections 1,023,202 users.
- 69,000 attacks in Aug 2013 -> 644,000 in Mar 2014
- 35,000 users -> 242,000 users
- 59.06% related to stealing users' money
- Russia, India, Kazakhstan, Vietnam, Ukraine and Germany have largest numbers of reported attacks
- Trojans sending SMS were 57.08% of all detections

Typical scenario

- Cybercriminals create an affiliate website and invite Internet users to become their accomplices
- A unique modification of the malware and a landing page for download is created for each accomplice
- Participants of the affiliate program trick Android users into installing malicious application
- Infected device sends SMS messages to premium numbers, making money for the cybercriminals
- Part of money is paid to the affiliate partners

http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf

Mobile malware examples

- DroidDream (Android)
  - Over 58 apps uploaded to Google app market
  - Conducts data theft; send credentials to attackers
- Ikee (iOS)
  - Worm capabilities (targeted default ssh pwd)
  - Worked only on jailbroken phones with ssh installed
- Zitmo (Symbian,BlackBerry,Windows,Android)
  - Propagates via SMS; claims to install a “security certificate”
  - Captures info from SMS; aimed at defeating 2-factor auth
  - Works with Zeus botnet; timed with user PC infection

Comparison between platforms

- Operating system (recall security features from lecture 5)
  - Unix
  - Windows
- Approval process for applications
  - Market: Vendor controlled/Open
  - App signing: Vendor-issued/self-signed
  - User approval of permission
- Programming language for applications
  - Managed execution: Java, .Net
  - Native execution: Objective C

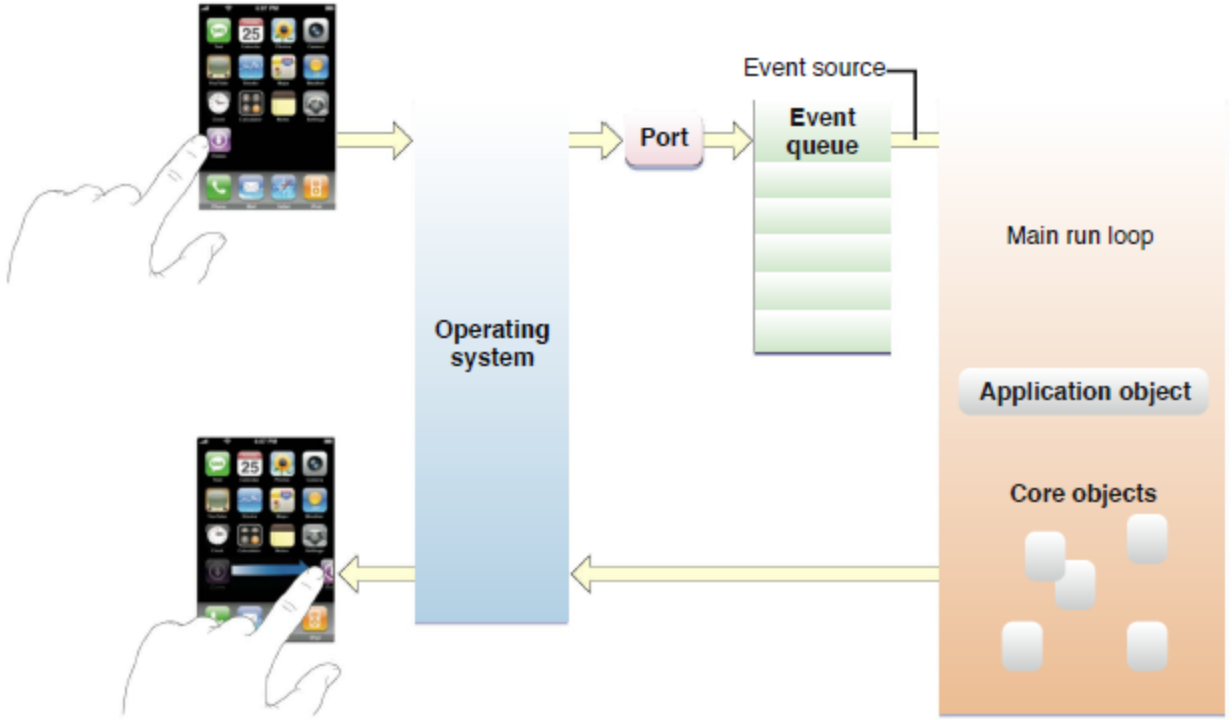
Outline

- Introduction: platforms and attacks
- Apple iOS security model
- Android security model
- Windows 7 Mobile security model

Apple iOS

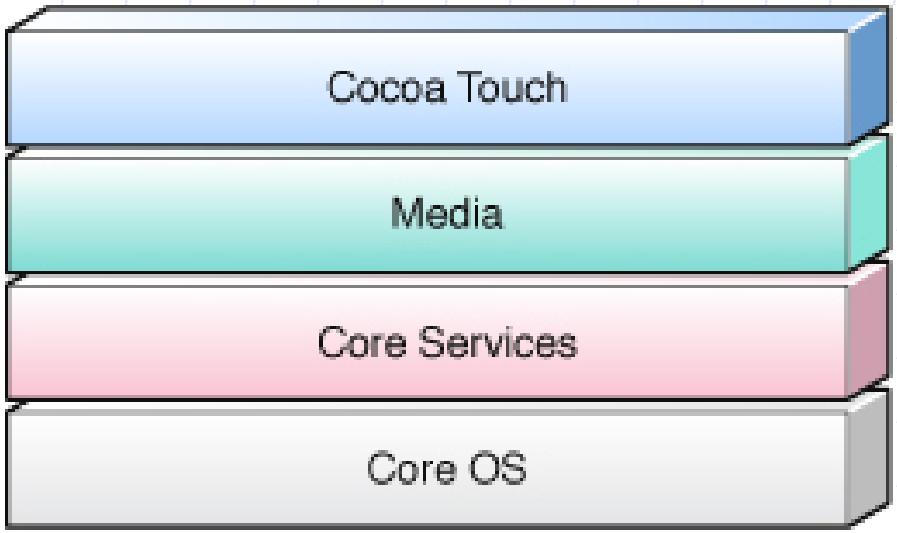
From: iOS App Programming Guide

iOS Application Development



- Apps developed in Objective-C using Apple SDK
- Event-handling model based on touch events
- Foundation and UIKit frameworks provide the key services used by all iOS applications

iOS Platform



- Cocoa Touch: Foundation framework, OO support for collections, file management, network operations; UIKit
- Media layer: supports 2D and 3D drawing, audio, video
- Core OS and Core Services: APIs for files, network, ... includes SQLite, POSIX threads, UNIX sockets
- Kernel: based on Mach kernel like Mac OS X

Implemented in C and Objective-C