Can you trust me now?
The Current State of Mobile Security

Black Hat USA
August 2016
Atredis Partners
Overview

**Bene Diagnoscitur, Bene Curatur**
- “That which is well diagnosed is well cured.”
- Research Driven Security Consulting
- Advanced Secure Design & Development
- Advanced Penetration Testing
- Advanced Risk Consulting

**Josh Thomas**
- 16 Years in the field
- Focus on mobile devices, development, hardware design, architecture

**Shawn Moyer**
- 20 years in the field
- Focus on industrial, software and network security
Today’s Focus

Mobile Layers and Landscape
  • What are the actual components and layers of a production mobile device?

BYOD and Market share
  • What to expect when we allow anything to happen

Android versus iOS
  • The little engine that could train a generation to break trusted boot

Hardware and components
  • Reuse and architecture limitations

MDM
  • A false sense of stability
Mobile Layers and Landscape

The foundations of mobile trust

Apps & Data
OS Version
OS Provider
OEM Device Manufacturer
OEM Processor Manufacturer
ARM Specification
Functional Layers: App & Data

- **Data**
  - Protected by App or OS

- **App**
  - Written for OS and OS version
  - Moderated by Platform App Store
  - Constrained by Platform API
Functional Layers:
OS & OS Version

- OS Version
  - Incremental Approach to Security
  - Incremental Approach to Functionality

- OS
  - Fundamental Approach to Security
  - Fundamental Approach to Functionality

Diagram:
- Apps & Data
- OS Version
- OS Provider
- OEM Device Manufacturer
- OEM Processor Manufacturer
- ARM Specification
Functional Layers: OEM

- OEM
  - Design of Hardware
  - Selection of Secure Components
  - Approach to Market
  - Solution Customization
Functional Layers: System on Chip

- **SoC**
  - Design of Component Hardware
  - Control of Trust
  - Control of Security

- **SoC Version**
  - Similar to OS Version
  - Incremental updates driven by platform vision
Common Talking Points: Specification

- ARM Specification
- Core Design of Security
- Applied Academic Design
- As Much Theory as Reality
Who Writes The Software?

Apps & Data
OS Version
OS Provider
OEM Device Manufacturer
OEM Processor Manufacturer
ARM Specification

Service Provider
OEM
OS Vendor
Netflix & DRM
MDM
App Dev
You
OS Market Share

OS Global Market Share (2015 Q2)
- Android: 83%
- iOS: 14%
- Windows Phone: 3%
- BlackBerry OS: 1%
- Others: 3%

OS US Market Share (2015 Q3)
- Android: 53%
- iOS: 43%
- Microsoft: 3%
- BlackBerry: 1%
- Others: 3%
Trending Toward Irrelevance With Subscribers

Global Market Share: Smartphone Operating Systems

- Android
- iOS
- Microsoft
- RIM
- Bada*
- Symbian
- Other

[Graph showing market share trends over time for each operating system from Q1 '09 to Q3 '15]
Trending Toward Irrelevance With Sales

Global Smartphone Sales By Operating System

- Android
- iOS
- RIM
- Symbian
- Microsoft
- Bada
- Other

Millions

2009 2010 2011 2012 2013 2014
Android: Plagued by Version Fragmentation
Apple: Version Fragmentation
Market Share of the Leaders
Foundations of Mobile Trust

OEM SoC Market Share

- Qualcomm: 60%
- Samsung LSI: 18%
- MTK: 20%
- Intel: 18%
- Nvidia: 1%
- Other: 1%
Android versus iOS

- Security Capabilities
  - Android tries things first, enters the market with partial implementations
  - iOS enters the market with finished software
  - Iterative Android releases accidentally help train security professionals to beat iOS protections
Layers of Security
Mobile Security Starts Here
System on a Chip
What OS Does This Run?

- Android
- Little Kernel
- REX
- QuRT
- QSEE
Physical Attack Surface

- Direct memory access, Modem, TrustZone, power management
- USB often exposes diagnostic or factory test modes
- JTAG, UART, FIQ debugging cables
- $2,000
Remote Attack Surface

- Modem, TrustZone, HLOS
- Large attack surface between DRM and cellular protocols
- $2,000 + time fighting software
Trusted Execution Environments

- Provide a separate execution environment
- Closed source blobs

- Key storage
- DRM
- How trusted are they?
TrustZone TEE

- TrustZone can introspect and interact with the mobile operating system
- The mobile operating system cannot introspect TrustZone
- Controls sensitive information from keys to secure boot
- Handles DRM and parses video and audio data
- Vulnerability affects large quantities of devices
- Imagine malware that could…
Simcard TEE

- Simcards are another example of a mobile TEE
- Provide key storage for network encryption
- GSM networks have privacy but not authentication

- IMSI Catchers
- Eavesdropping
- Passive and Active
- Base station controlled
Modem

Figure 3: Illustrative baseband architecture
Modem

- Contains stacks for telephony protocols
- Direct access to peripherals and buses
- Mostly ignored outside of law enforcement and unlockers
Modem

- Local exploitation via proprietary protocols between application and baseband processors
  - QMI, MMI, AT, Diag
- Remote exploitation via proprietary telephony stacks
  - GSM: LAPDm, SNDCP, RLC, MAC, CM, MM, RR
  - LTE: PDCP, NAS, RRC, IP
- Network exploitation
  - IMSI Catchers
  - Eavesdropping
Boot Loader / Secure Boot

- Android traditionally runs Little Kernel bootloaders
- Contains “apps” that implement fastboot, recovery, android debugging bridge
- OEM-specific bootloaders contain other proprietary protocols for debugging, fault analysis, or engineering
QFUSES

• Software programmable fuses for one-time programmable configuration

• Device keys, carrier keys, OEM keys

• Security features toggles
  • Normally accessible only via interface to TrustZone
  • Often exploitation of TrustZone related to desire to blow fuses
Cross Device Impacts

- One bug to cross OEMs?
- No Problem
- One bug to cross Operating Systems?
- Likely
Aside about BYOD & MDM

- Based on the Lowest Common Denominator of Security Assumptions
- Written for Cross Platform Use
- Rarely take advantage of OS or Hardware Security Capabilities
A Brief History of Failure: Logic Flaws
A Brief History of Failure: Debugging and Backdoors
A Brief History of Failure: Authorization, Crypto, Bootloaders
Q&A
Be Apple, not Android

<table>
<thead>
<tr>
<th>Device</th>
<th>Release-Discontinued Date</th>
<th>1st Year After Release</th>
<th>2nd Year After Release</th>
<th>3rd Year After Release</th>
<th>4th Year After Release</th>
<th>5th Year After Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 5</td>
<td>Sep 2012 - Sep 2013</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 4S</td>
<td>Oct 2011 - Currently available</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 4</td>
<td>Jun 2010 - Sep 2013</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>iPhone 3GS</td>
<td>Jun 2009 - Sep 2012</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Nexus 4</td>
<td>Nov 2012 - Nov 2013</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Samsung Galaxy Note 2</td>
<td>Nov 2012 - Currently available</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Motorola Atrix HD</td>
<td>Jul 2012 - May 2013</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Samsung Galaxy S3</td>
<td>Jul 2012 - Currently available</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HTC One X</td>
<td>May 2012 - Apr 2013</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HTC One S (TMobile)</td>
<td>Apr 2012 - Feb 2013</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Samsung Galaxy Note*</td>
<td>Feb 2012 - Jun 2013</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Galaxy Nexus</td>
<td>Nov 2011 - Oct 2012</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Motorola Atrix 2</td>
<td>Oct 2011 - Aug 2012</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Samsung Galaxy S2</td>
<td>Oct 2011 - May 2012</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HTC Amaze 4G</td>
<td>Oct 2011 - Feb 2012</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>LG G2x (TMobile)</td>
<td>Apr 2011 - Jan 2012</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Motorola Atrix 4G</td>
<td>Mar 2011 - Sep 2011</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HTC Inspire 4G</td>
<td>Feb 2011 - Apr 2012</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Nexus S</td>
<td>Dec 2010 - Nov 2011</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Samsung Captivate</td>
<td>Jul 2010 - Oct 2011</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Legend:
- On current major version
- 1 major version behind
- 2 major versions behind
- 3 major versions behind
- 4 major versions behind
- 4+ major versions behind
- Actively for sale
- Getting support updates