

# RSA<sup>®</sup>Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: MBS-T09

## Exploring the Foundations of Mobile Trust



Connect to  
Protect

### **Josh Thomas**

Founding Partner  
Atredis Partners  
@m0nk\_dot

### **Charles Holmes**

Principal Consultant  
Atredis Partners  
@afrocheese

@atredis



#RSAC

- Security Consulting Driven by Applied Research
- Speakers:
  - Josh Thomas
  - Charles Holmes
- The slides will be available for download:
  - [www.atredis.com/RSA2016.pdf](http://www.atredis.com/RSA2016.pdf)

A High Level Talk About Low Level Bugs

... or ...

A Low Level Talk About High Level Bugs

# Flow of this talk



- Foundational Introduction
- Market Share:
  - OS / OEM / Processors and SoCs
- Impacts of Problems at the Hardware Layer
  - The last 18 months of issues
  - The last 18 months of impacts
- Take Away and Planning Forward

# What is Mobile Trust?

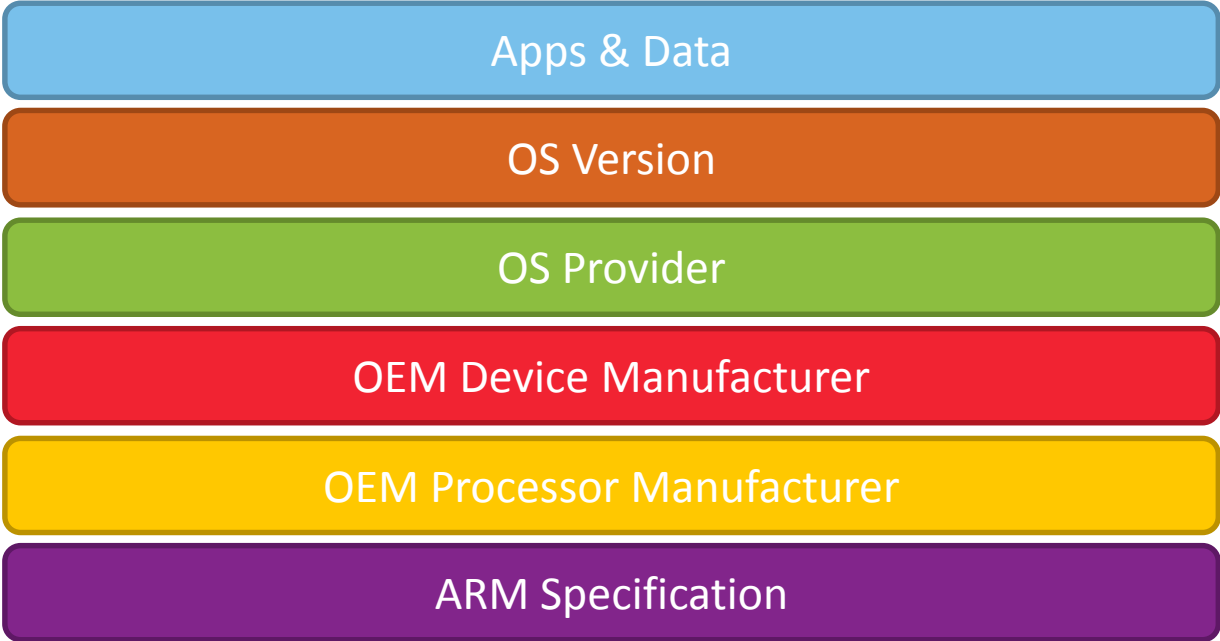


- Realistic Ability to Secure Data
- Realistic Ability to Validate Environment

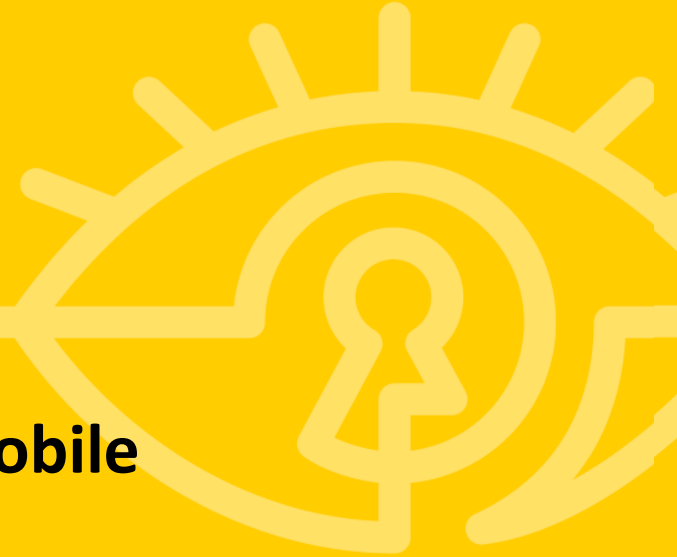
# Foundations of Mobile Trust



#RSAC



## What Is Expected in a Talk about Mobile



# Common Talking Points: Data



Apps & Data

OS Version

OS Provider

OEM Device Manufacturer

OEM Processor Manufacturer

ARM Specification

- Data
  - Protected by App or OS
- App
  - Written for OS and OS version
  - Moderated by Platform App Store
  - Constrained by Platform API



# Aside about BOYD & MDM



#RSAC

- Based on the Lowest Common Denominator of Security Assumptions
- Written for Cross Platform Use
- Rarely take advantage of OS or Hardware Security Capabilities

# Common Talking Points: OS & OS Version



#RSAC

Apps & Data

OS Version

OS Provider

OEM Device Manufacturer

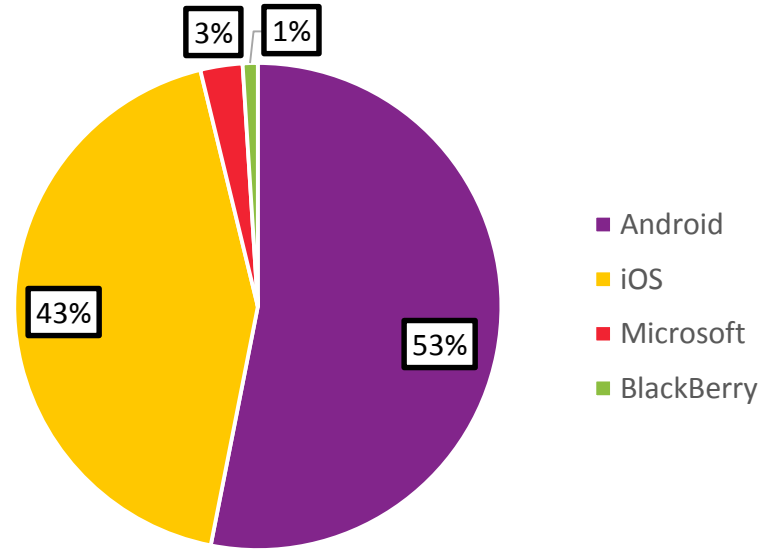
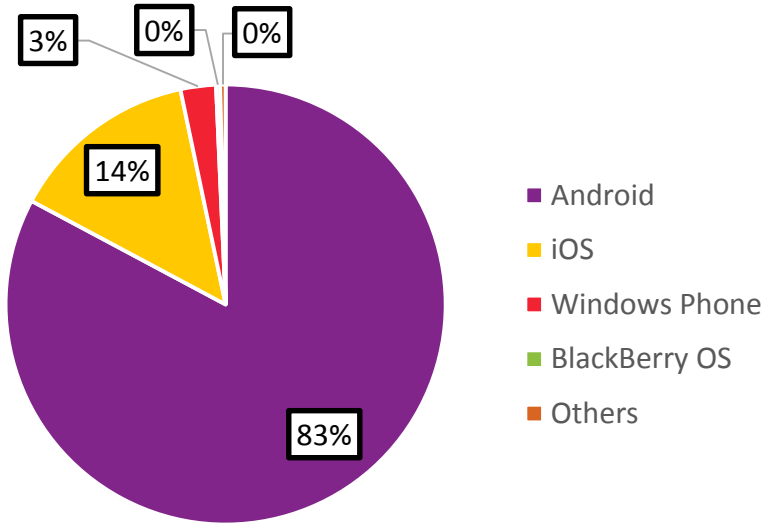
OEM Processor Manufacturer

ARM Specification

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



## OS Global Market Share (2015 Q2) OS US Market Share (2015 Q3)

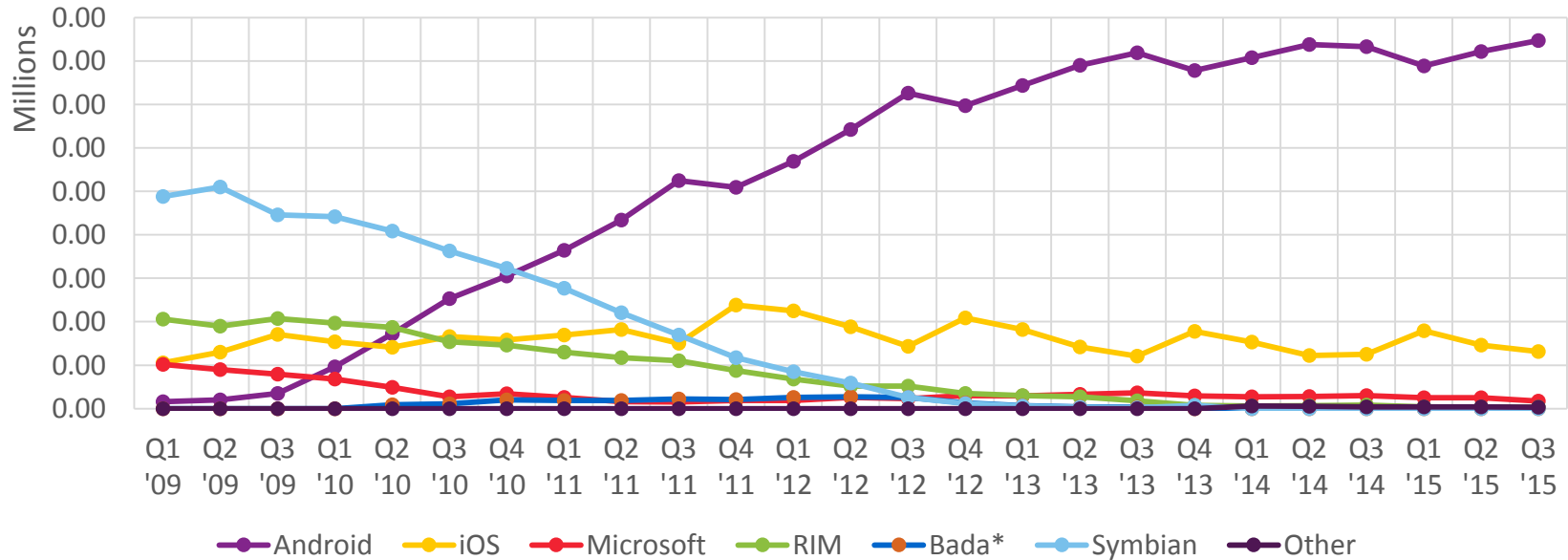


# Trending Toward Irrelevance With Subscribers



#RSAC

## Global Market Share: Smartphone Operating Systems

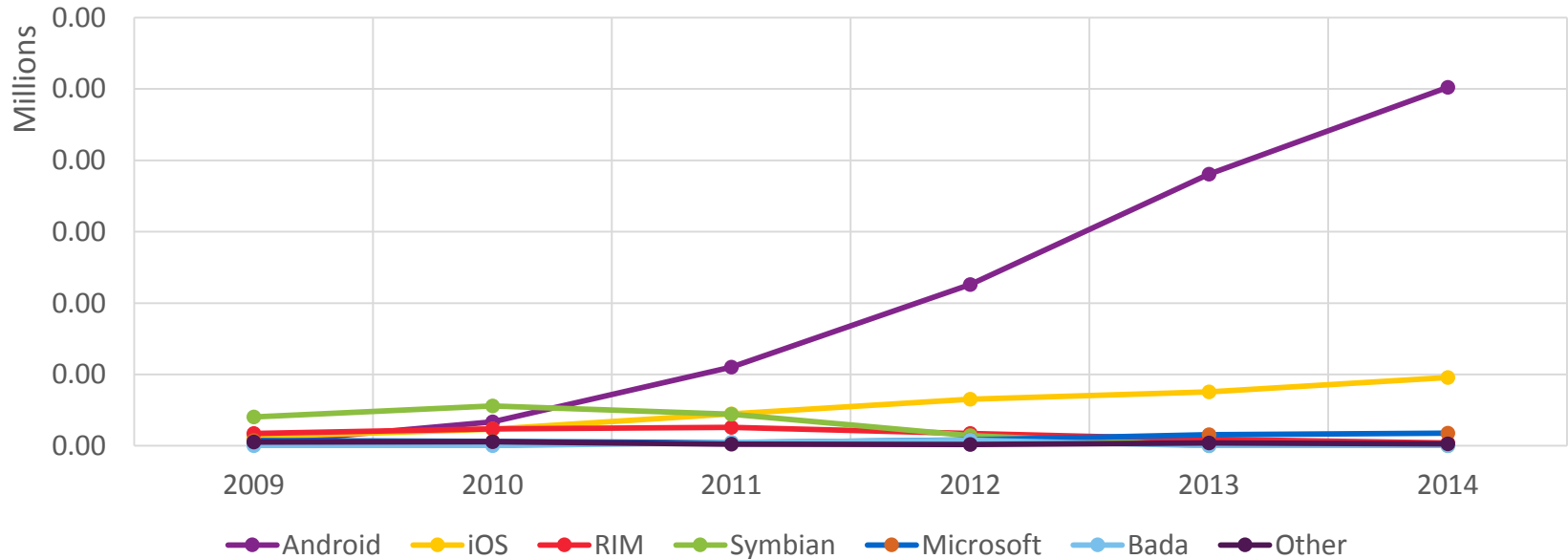


# Trending Toward Irrelevance With Sales



#RSAC

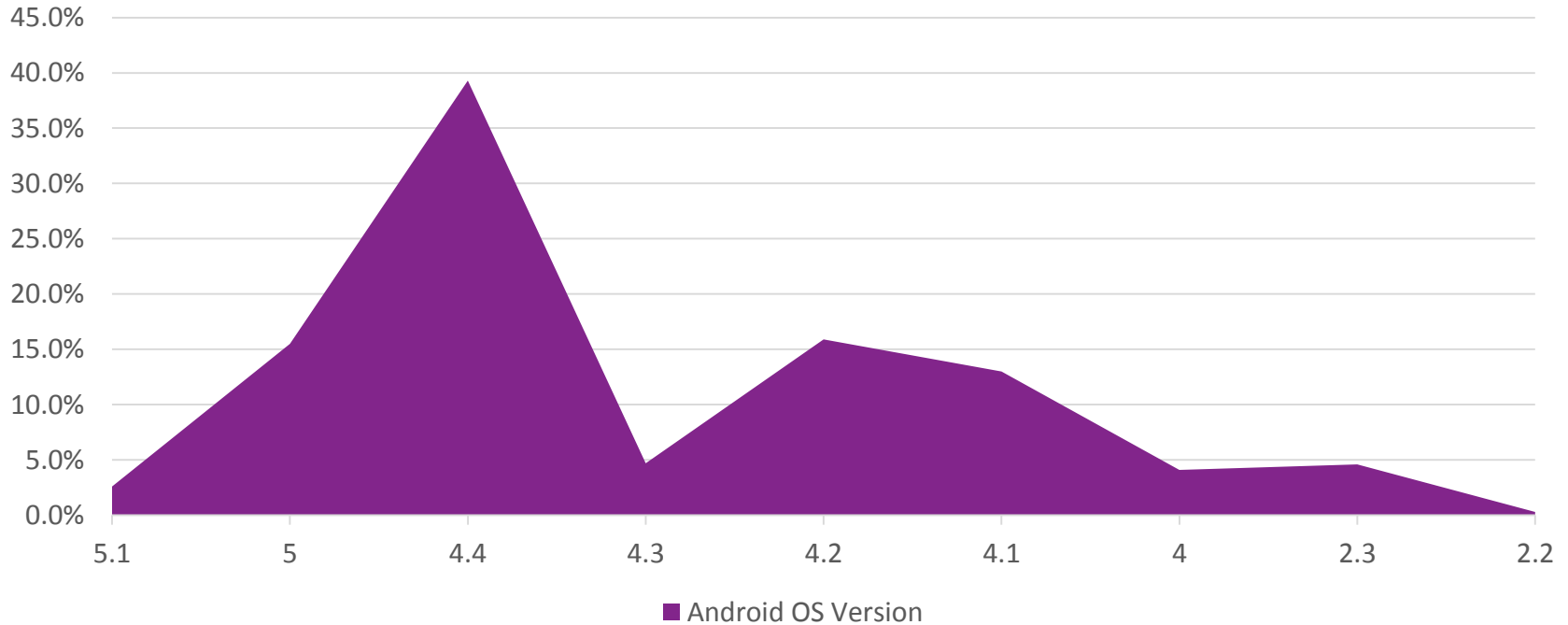
## Global Smartphone Sales By Operating System



# Android: Plagued by Version Fragmentation



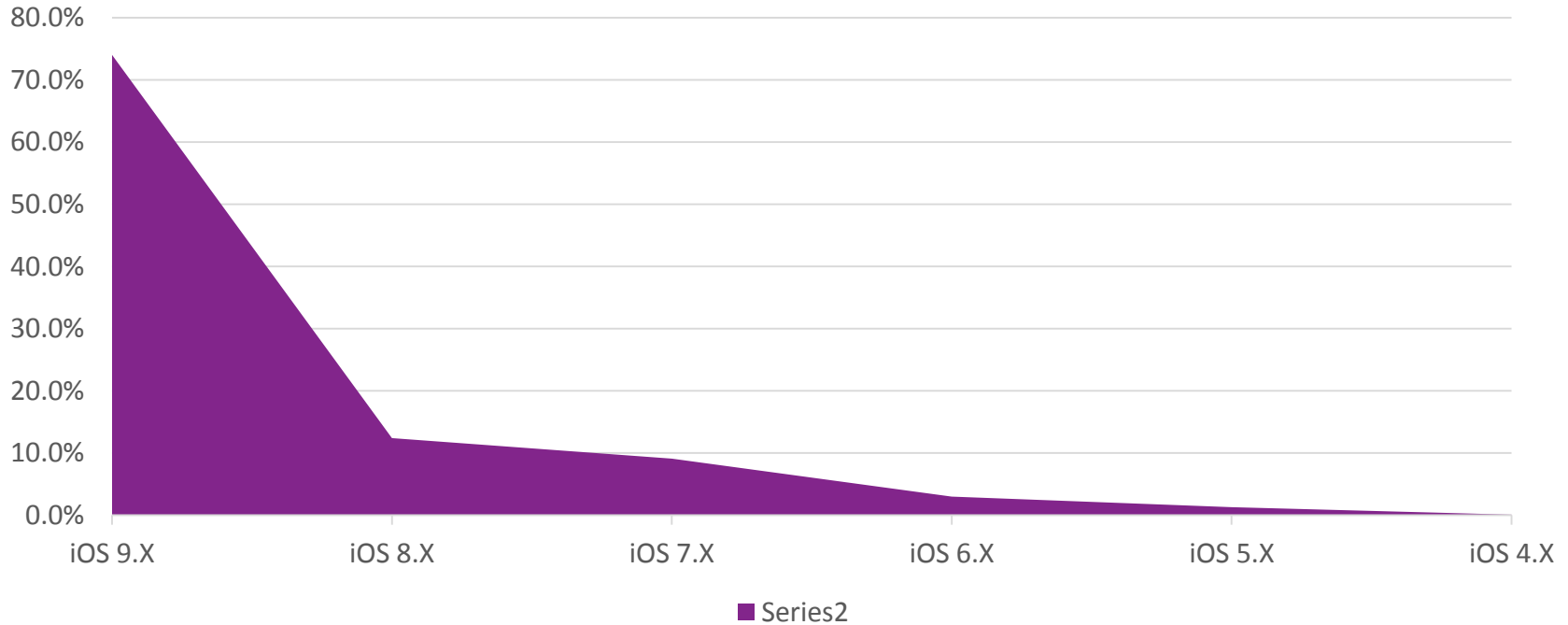
#RSAC



# Apple: Version Fragmentation



#RSAC



# Common Talking Points: OEM



Apps & Data

OS Version

OS Provider

OEM Device Manufacturer

OEM Processor Manufacturer

ARM Specification

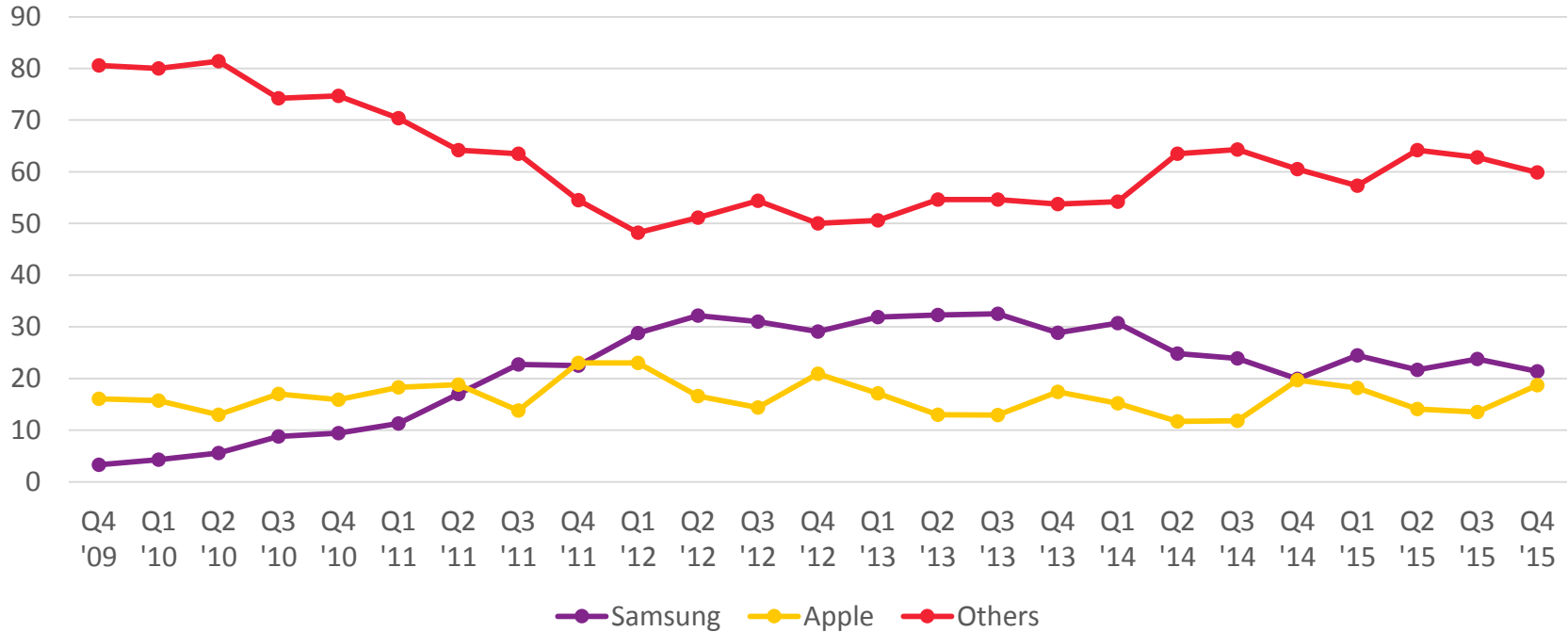
- OEM
  - Design of Hardware
  - Selection of Secure Components
  - Approach to Market
  - Solution Customization



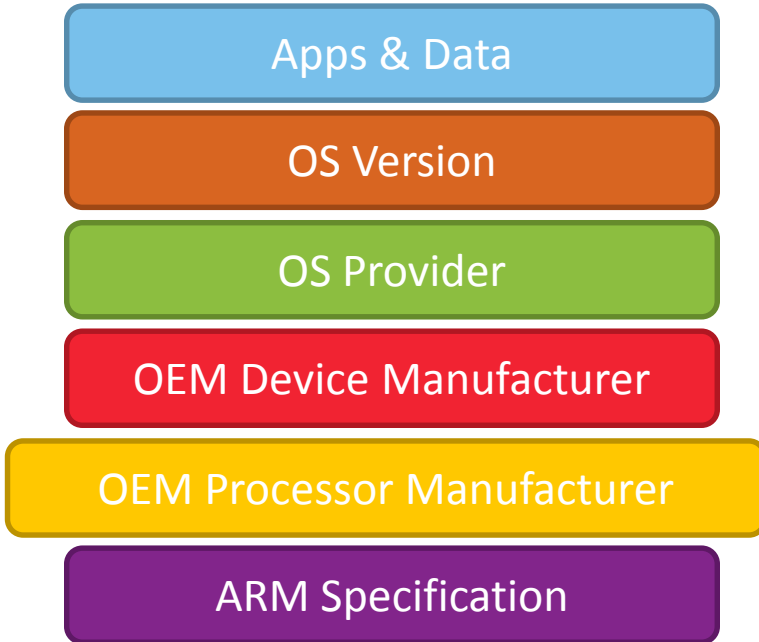
# Market Share of the Leaders



#RSAC



# Common Talking Points: System on Chip



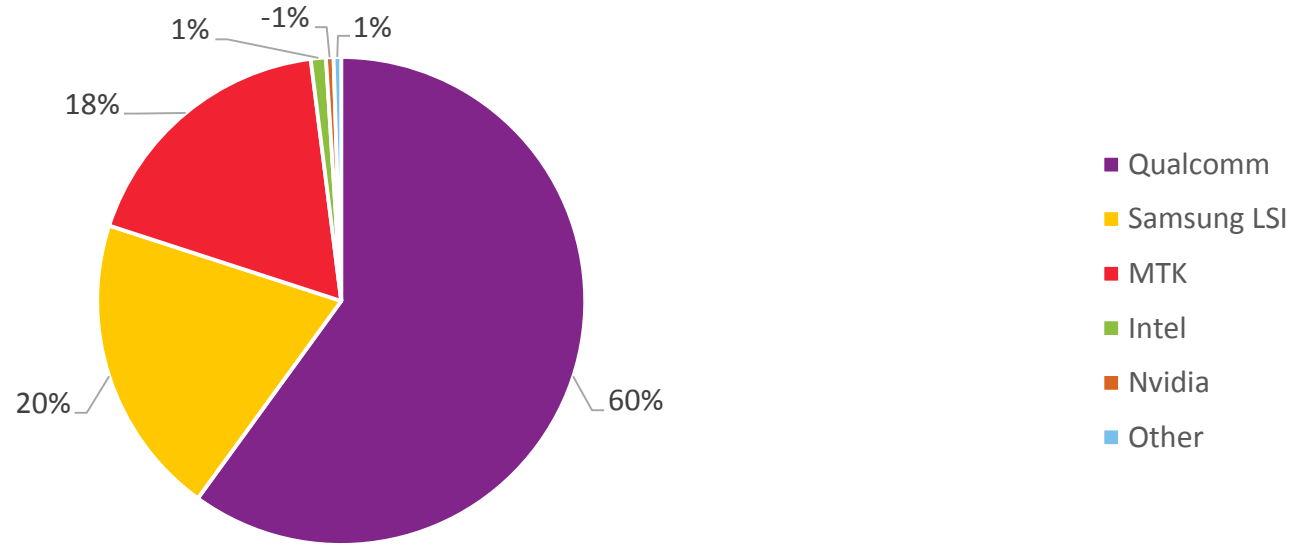
- SoC
  - Design of Component Hardware
  - Control of Trust
  - Control of Security
- SoC Version
  - Similar to OS Version
  - Incremental updates driven by platform vision

# Foundations of Mobile Trust

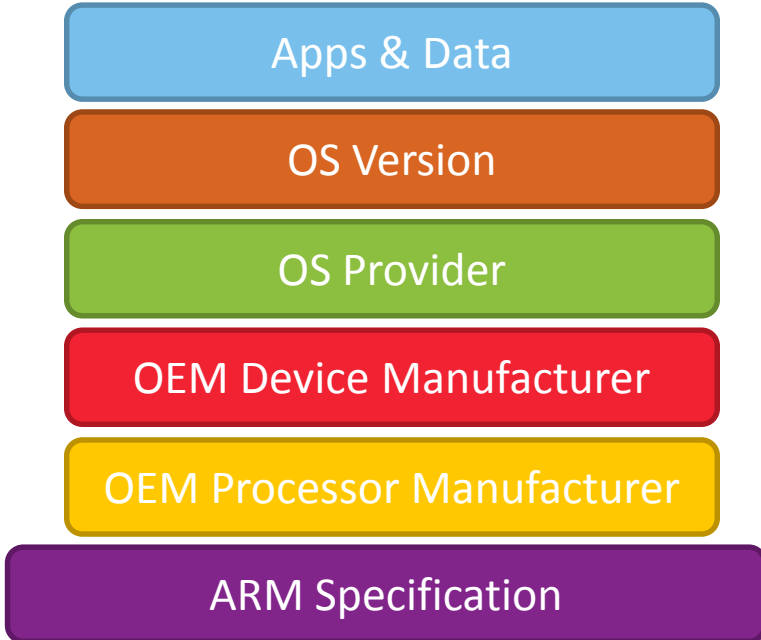


#RSAC

## OEM SoC Market Share

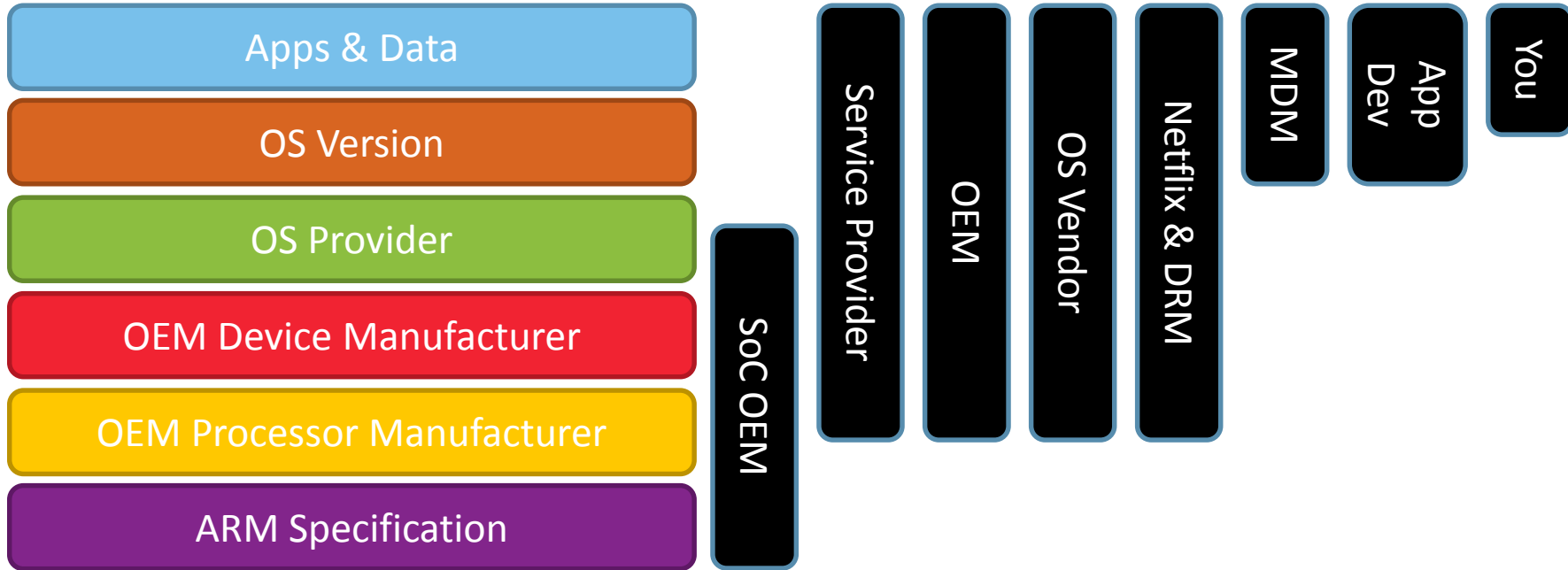


# Common Talking Points: Specification



- ARM Specification
  - Core Design of Security
  - Applied Academic Design
  - As Much Theory as Reality

# Who Writes The Software?



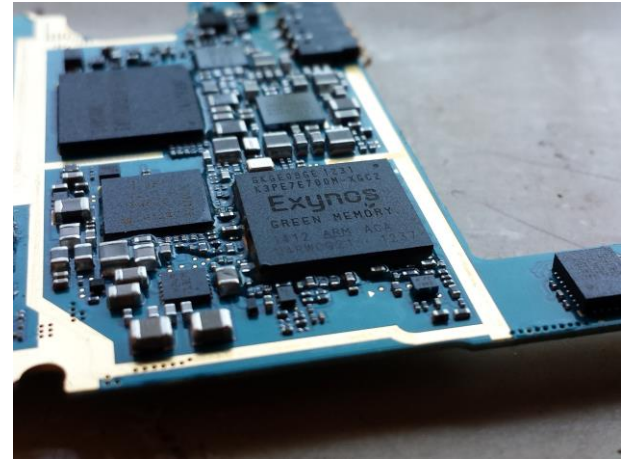
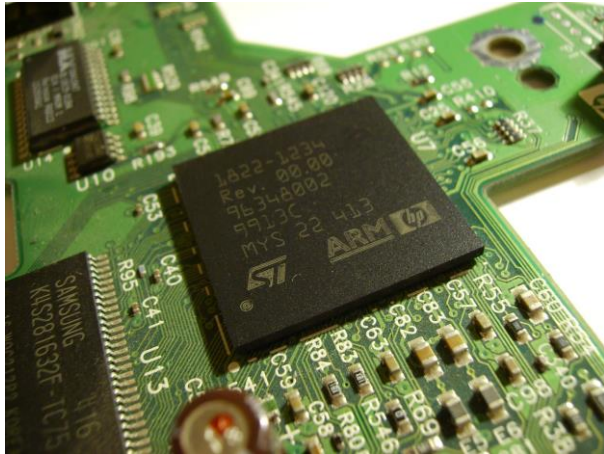
# Foundational Problems



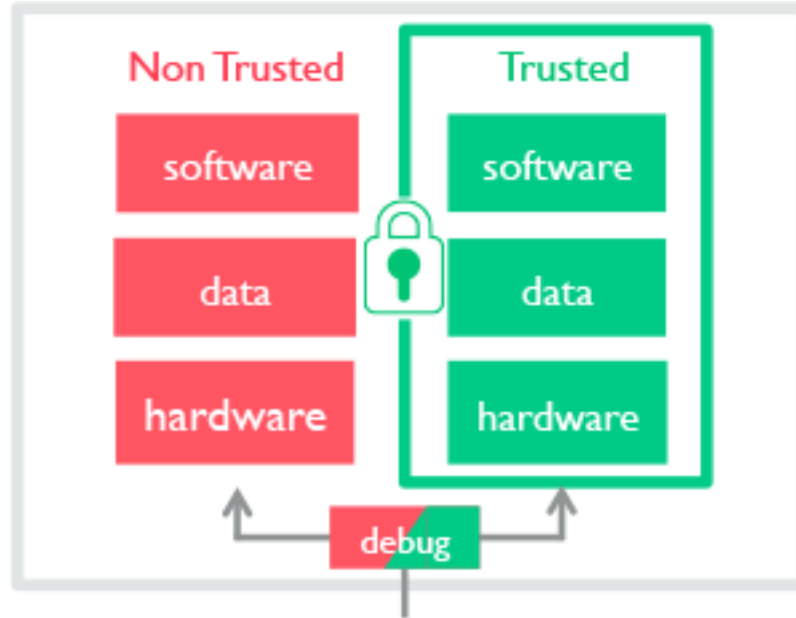
# Mobile Security Starts Here



#RSAC



# Introduction to Embedded Trust





# TrustZone Bugs in the Wild



#RSAC

- In the past 18 months the following vulnerabilities in Mobile Processors have made public
  - Holmes & Keltner – Recon 2015
  - Rosenberg – BlackHat 2015
  - Xxx
  - Yyy
  - Zzz

# 1-2 Slides per Security Vulnerability



- What is was
- How it worked
- Who was at fault
- What was the impact?
- **Currently finishing these slides**
- **While it does not seem like it right now, this will be at least ½ the talk time on stage once setup is complete**
- **There will be few slides though.. More of a conversation about bugs and impacts**

# Cross Device Impacts



- One bug to cross OEMs?
  - No Problem
- One bug to cross Operating Systems?
  - Likely

**Transition from fear to action**



# “Apply” Slide



- This Week
  - Think about what hardware you are using
  - Think about what you are actually protecting
  - Ask your MDM Vendor if the use OS Security
- This Quarter
  - Know your hardware based exposure
  - Track known hardware issues against that exposure
- This Year
  - Focus on device patching and disallowing certain chipsets in your environment

**Questions?**



# References



- All Statistics pulled from
  - Statista: <http://www.statista.com/>
  - Open Signal: <https://opensignal.com/>