

SecurityTube iOS Security Expert



SecurityTube iOS Security Expert

Online Training: <http://www.Securitytube-Training.com>

Introduction to iOS

Vivek Ramachandran

Founder, SecurityTube.net

Training: <http://securitytube-training.com>

Course Requirements

- Hardware
 - Jailbroken iPhone / iPad
 - Any version of iOS \geq 5.1.1
 - No Support for Jailbreaking (warranty void?)
 - <http://jailbreak-me.info/>
- Software
 - Windows / Linux / OS X

Can I follow the course without a device?

- Absolutely!
- Will not be able to do the demos
- Concept Oriented and Practical
 - will not be boring to watch 😊

iOS

iPhone



iPad



iPod



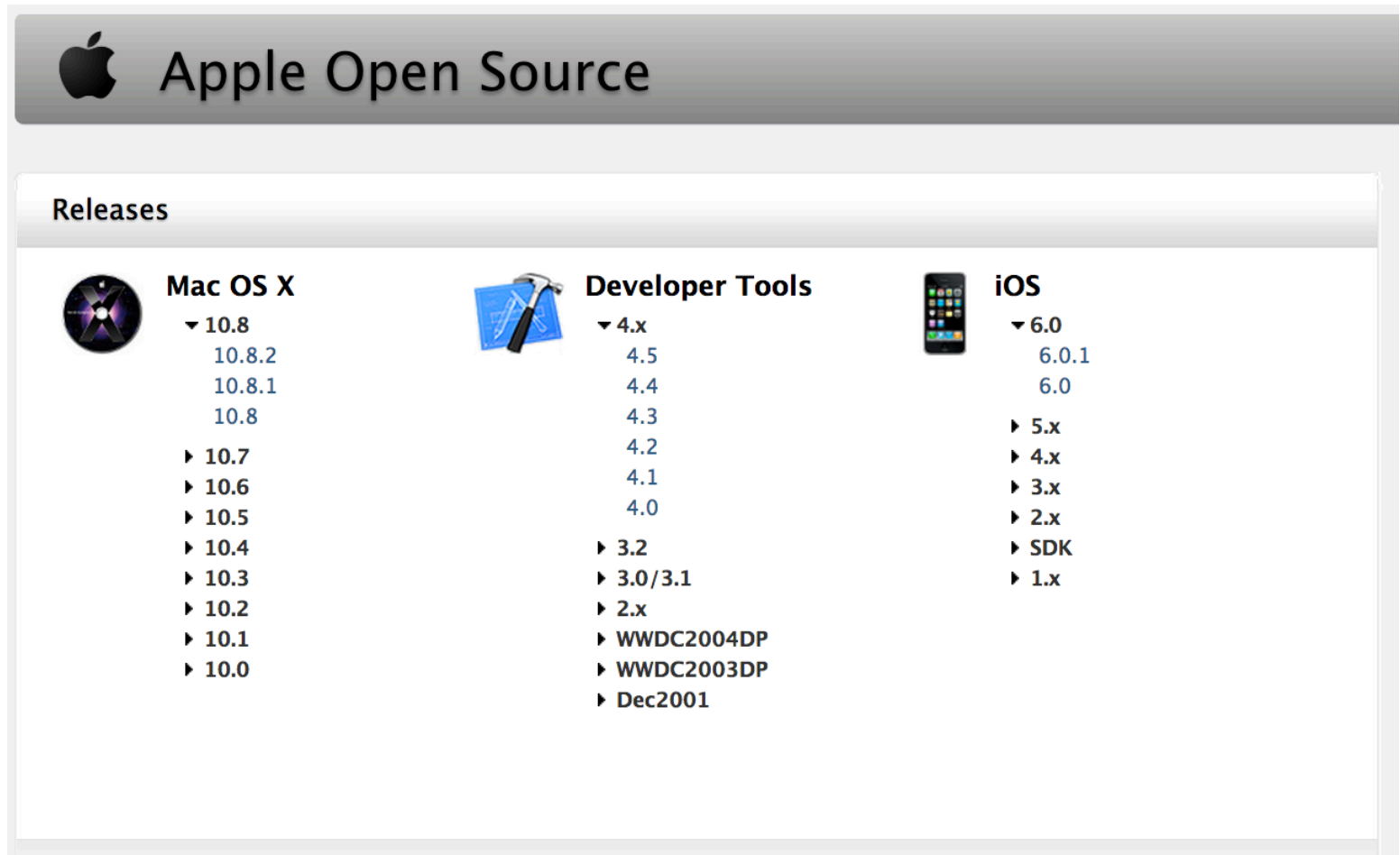
iOS Operating System

What is iOS really?

iOS is derived from **OS X**, with which it shares the **Darwin** foundation, and is therefore a **Unix** operating system. iOS is Apple's mobile version of the **OS X** operating system used on Apple computers.

<http://en.wikipedia.org/wiki/IOS>



Is iOS Open Source?



<http://opensource.apple.com/>

Only Selected Components

iOS 6.0.1 Source

● Project	Licenses	Downloads
● JavaScriptCore-1097.3.3	BSD LGPL	
WTFEmbedded-20	LGPL	
● WebCore-1640.1	BSD LGPL	
cctools-836	APSL GPL	
gdb-1822	GPL	
ld64-134.9	APSL	
libiconv-35	LGPL	
libstdcxx-56	GPL	

<http://opensource.apple.com/release/ios-601/>

Does it look any different than Linux?

- Lets login to an Jailbroken iPhone

SecurityTube iOS Security Expert



SecurityTube iOS Security Expert

Online Training: <http://www.Securitytube-Training.com>

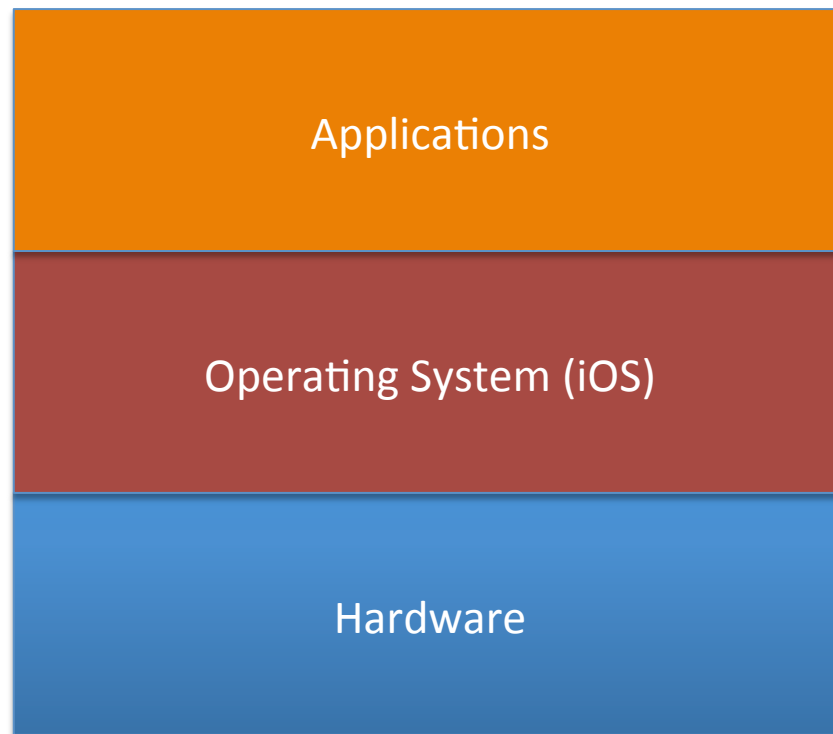
iOS Application Basics

Vivek Ramachandran

Founder, SecurityTube.net

Training: <http://securitytube-training.com>

iXXX



iOS Applications



How does one Develop iOS Applications?

- Xcode using Objective-C
- iPhone / iPad simulator
- Run on actual device to test

HelloWorld

- Customary Hello World Program

SecurityTube iOS Security Expert



SecurityTube iOS Security Expert

Online Training: <http://www.Securitytube-Training.com>

MVC and Event Driven Architecture

Vivek Ramachandran

Founder, SecurityTube.net

Training: <http://securitytube-training.com>

SecurityTube iOS Security Expert



SecurityTube iOS Security Expert

Online Training: <http://www.Securitytube-Training.com>

ARM Processor

Vivek Ramachandran

Founder, SecurityTube.net

Training: <http://securitytube-training.com>

iDevice Processors

- SoC – System on a Chip
- iDevices
 - License ARM cores (< iPhone 5)
 - License ARM instruction set to build own code (> iPhone 5)

[http://www.anandtech.com/show/6292/
iphone-5-a6-not-a15-custom-core](http://www.anandtech.com/show/6292/iphone-5-a6-not-a15-custom-core)

ARM anyone?

The **ARM** architecture describes a family of computer processors designed in accordance with a **RISC** CPU design developed by British company **ARM Holdings**. ARM architecture has been in development since the 1980s and is the most widely used **32-bit** instruction set architecture, in numbers produced.^{[2][3]} ARM was an **acronym** for *Advanced RISC Machine* (previously known as *Acorn RISC Machine*).^[4]

http://en.wikipedia.org/wiki/ARM_architecture

Demo

- Attaching to a Running Program
- View disassembly

SecurityTube iOS Security Expert



SecurityTube iOS Security Expert

Online Training: <http://www.Securitytube-Training.com>

iOS Security Mechanisms

Vivek Ramachandran

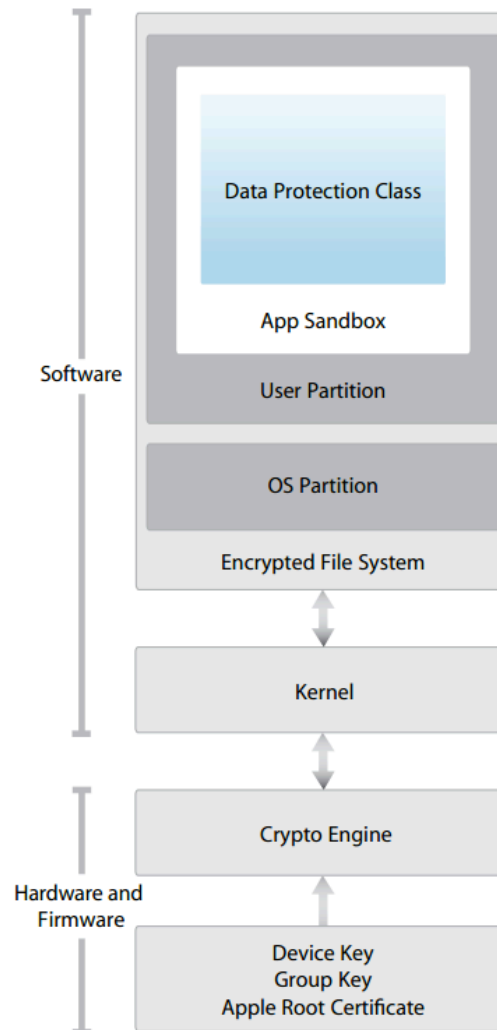
Founder, SecurityTube.net

Training: <http://securitytube-training.com>

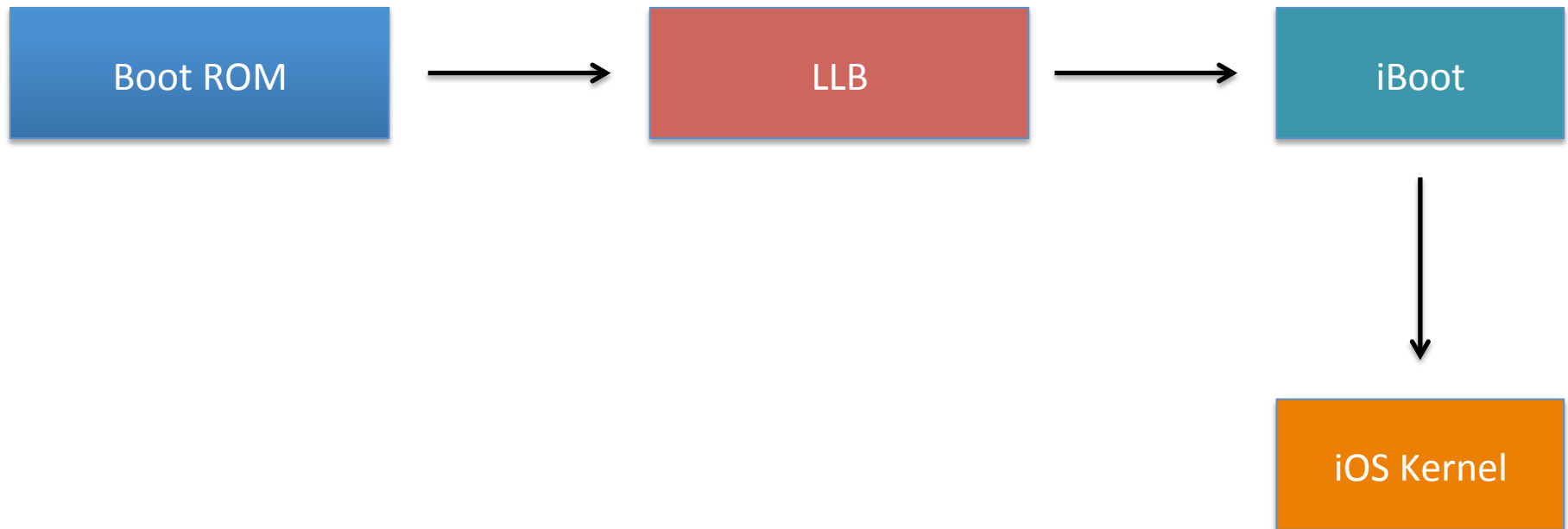
iOS Security Mechanisms

- Pretty much shrouded in mystery
- First public disclosure:
http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf
- Talk at Blackhat 2012
 - Rehash of the PDF above

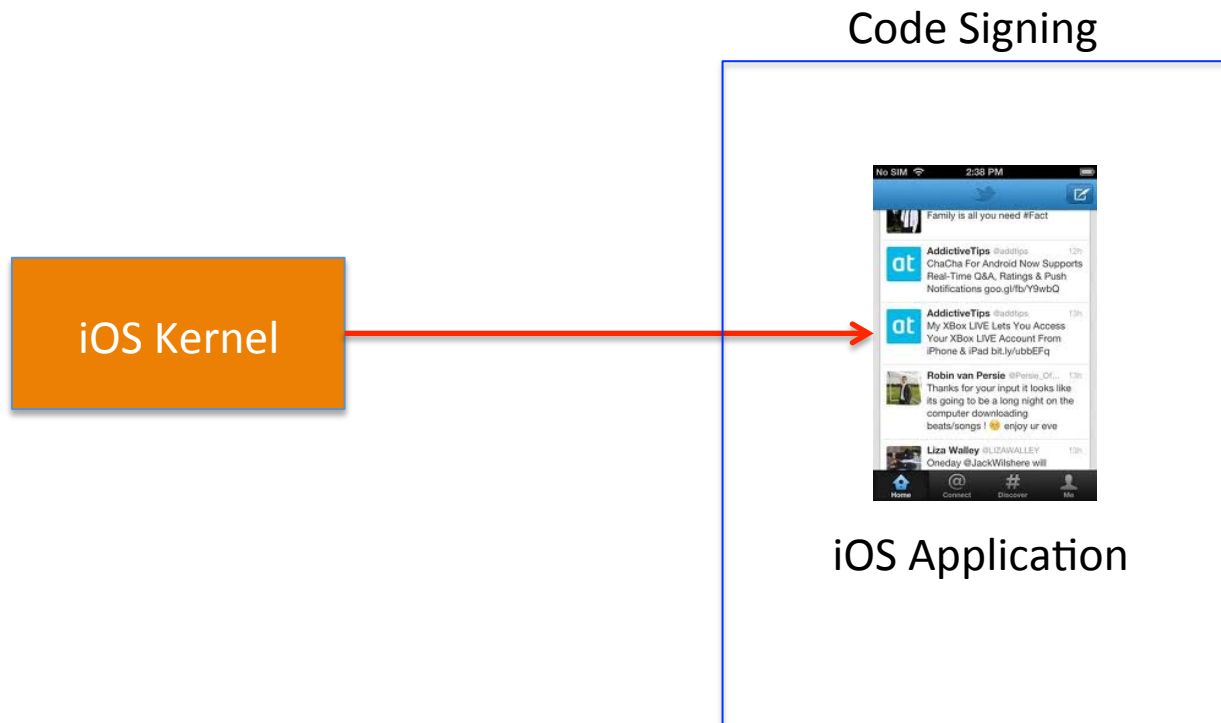
Security Architecture



Secure Boot Chain

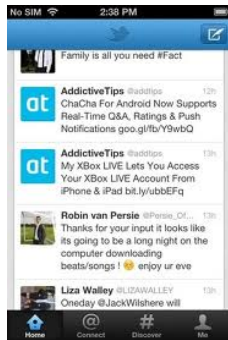


Loading Trusted Applications



Application Isolation

Code Signing



Application 1

Sandbox

Code Signing



Application 2

Sandbox

Data Encryption

- Hardware Crypto
 - UID and GID keys
- Data and File Protection
 - Keychain
 - Keybags
 - File Encryption

Network Security

- Built in support for:
 - SSL and TLS
 - VPN
 - Wifi
 - Enterprise (EAP-TLS, TTLS, PEAP etc.)
 - Bluetooth

Why is this relevant to Application Pentesting?

- How can you audit an application if the platform has so many restrictions?
- How do you gain access to the filesystem?
- How do decrypt data from keychain, file etc.?
- How do you monitor the application while it is running?