Please Complete Speaker Feedback Surveys

Advanced iOS Application Pentesting

Vivek Ramachandran
Founder, SecurityTube.net

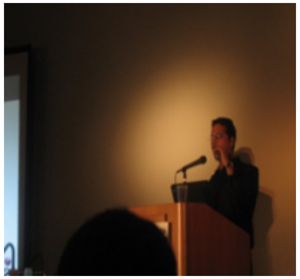
vivek@securitytube.net

Vivek Ramachandran

B.Tech, ECE
IIT Guwahati

802.1x, Cat65k
Cisco Systems

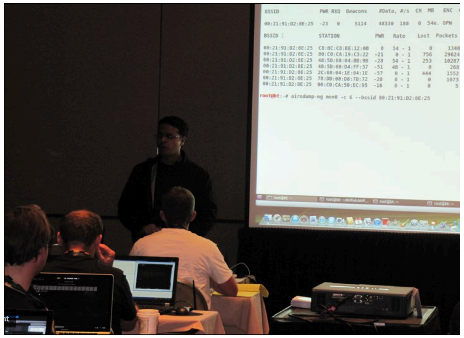
WEP Cloaking
Defcon 19



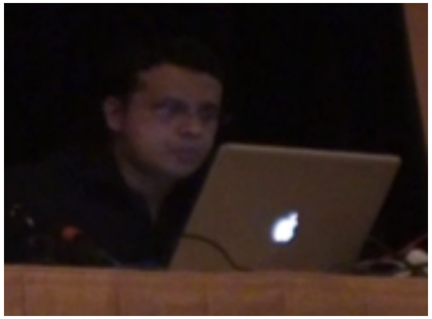
Caffe Latte Attack
Toorcon 9

Media Coverage
CBS5, BBC

Microsoft
Security Shootout

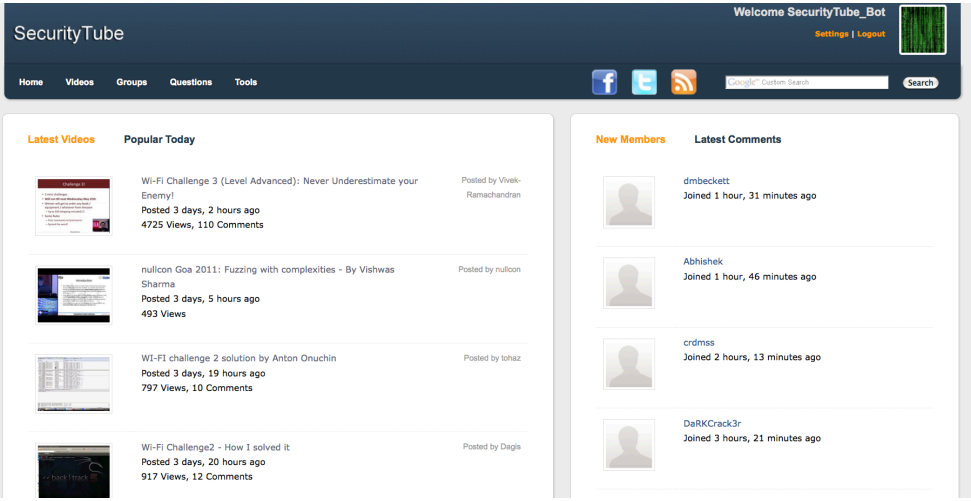


Trainer, 2011



Wi-Fi Malware, 2011

SecurityTube.net



SecurityTube

Welcome SecurityTube_Bot

Settings | Logout

Latest Videos Popular Today

Wi-Fi Challenge 3 (Level Advanced): Never Underestimate your Enemy!
Posted 3 days, 2 hours ago
4725 Views, 110 Comments
Posted by Vivek-Ramachandran

nullcon Goa 2011: Fuzzing with complexities - By Vishwas Sharma
Posted 3 days, 5 hours ago
493 Views
Posted by nullcon

WI-FI challenge 2 solution by Anton Onuchin
Posted 3 days, 19 hours ago
797 Views, 10 Comments
Posted by tohaz

Wi-Fi Challenge2 - How I solved it
Posted 3 days, 20 hours ago
917 Views, 12 Comments
Posted by Dagis

New Members Latest Comments

dmbeckett
Joined 1 hour, 31 minutes ago

Abhishek
Joined 1 hour, 46 minutes ago

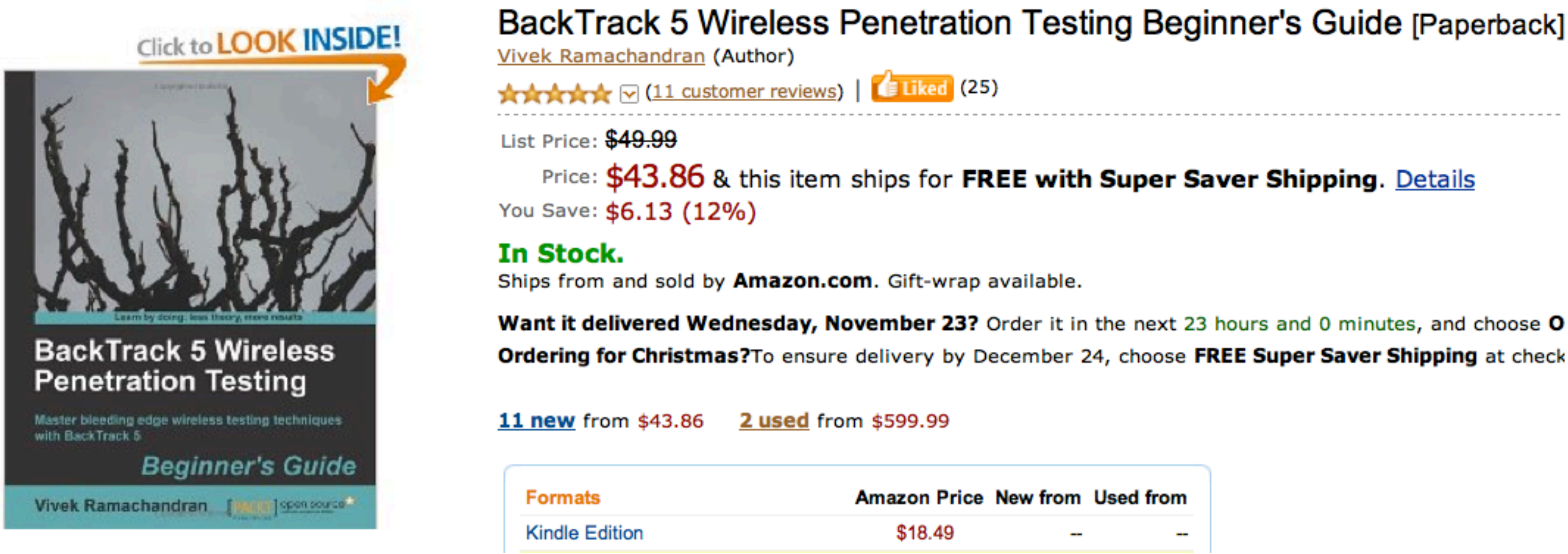
crdmss
Joined 2 hours, 13 minutes ago

DaRKCrack3r
Joined 3 hours, 21 minutes ago

Asia
North America
Atlantic Ocean
Africa
South America
cific ean
Indian Ocean
Australia

Students in 65+ Countries

Backtrack 5 Wireless Penetration Testing


Click to LOOK INSIDE!
Learn by doing: less theory, more results
BackTrack 5 Wireless Penetration Testing
Master bleeding edge wireless testing techniques with BackTrack 5
Beginner's Guide
Vivek Ramachandran
PACKT open source

BackTrack 5 Wireless Penetration Testing Beginner's Guide [Paperback]

Vivek Ramachandran (Author)

★★★★★ (11 customer reviews) | Liked (25)

List Price: ~~$49.99~~

Price: $43.86 & this item ships for **FREE with Super Saver Shipping**. Details

You Save: $6.13 (12%)

In Stock.

Ships from and sold by **Amazon.com**. Gift-wrap available.

Want it delivered Wednesday, November 23? Order it in the next 23 hours and 0 minutes, and choose **O**

Ordering for Christmas?To ensure delivery by December 24, choose **FREE Super Saver Shipping** at check

11 new from $43.86 2 used from $599.99

Formats	Amazon Price	New from	Used from
Kindle Edition	$18.49	--	--

http://www.amazon.com/BackTrack-Wireless-Penetration-Testing-Beginners/dp/184951558I/

©SecurityTube.net

SecurityTube iOS Security Expert

SecurityTube iOS Security Expert

Teaching iOS Pentesting to Hackers from 50+ Countries!

iOS

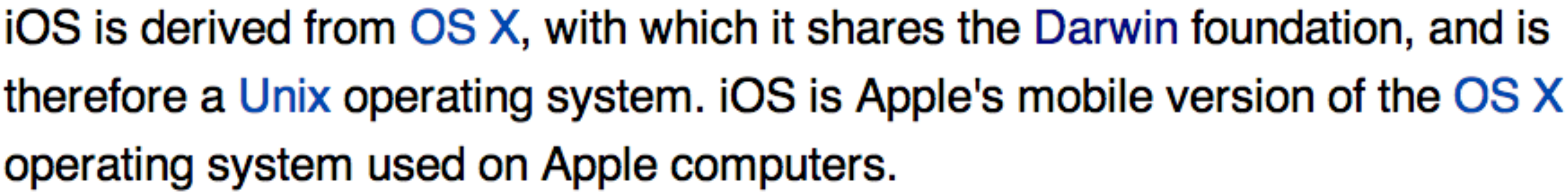
iPhone

iPad

iPod

iOS Operating System

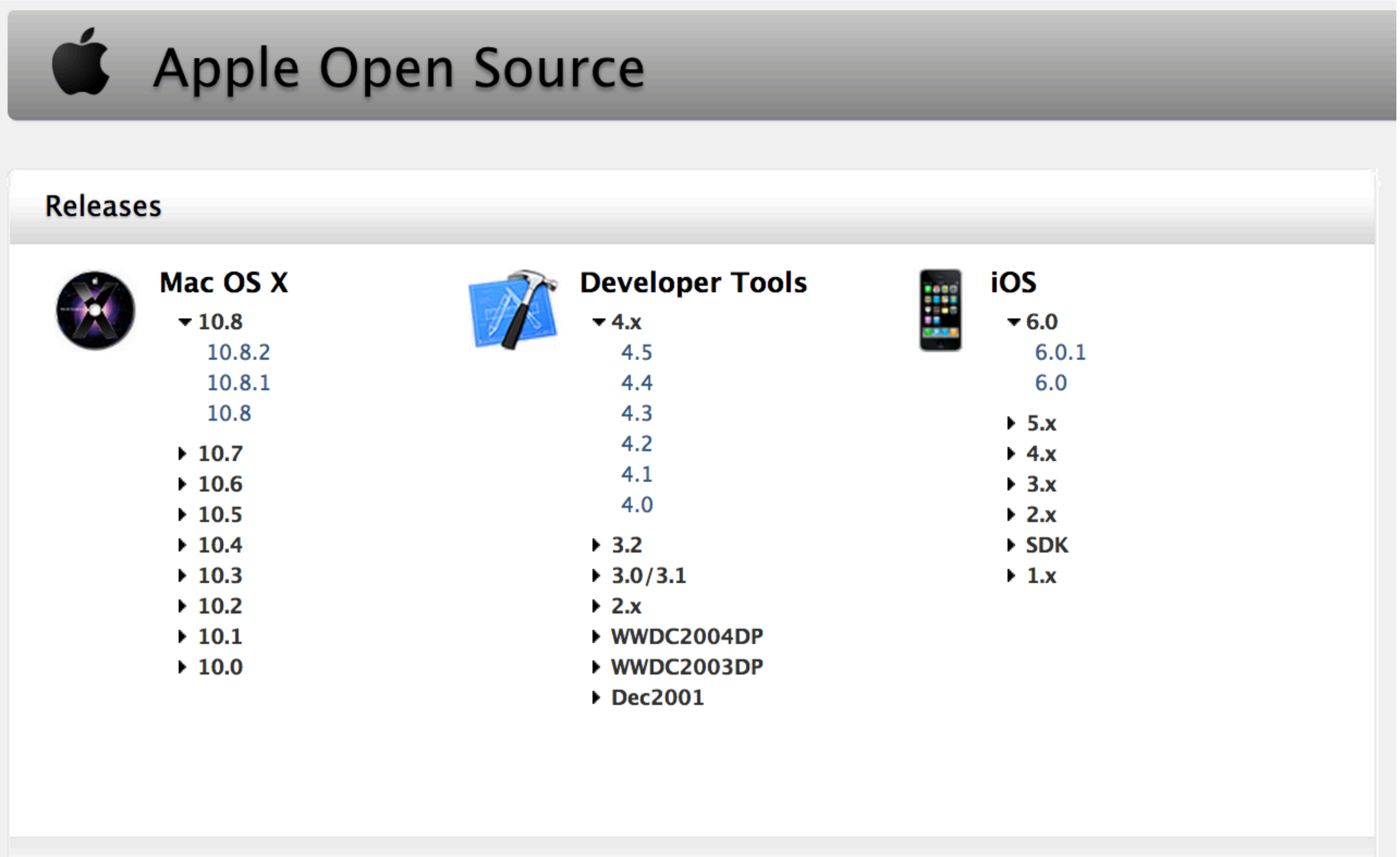
What is iOS really?



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?



Apple Open Source

Releases

Mac OS X

- ▾ 10.8
  - 10.8.2
  - 10.8.1
  - 10.8
- ▸ 10.7
- ▸ 10.6
- ▸ 10.5
- ▸ 10.4
- ▸ 10.3
- ▸ 10.2
- ▸ 10.1
- ▸ 10.0

Developer Tools

- ▾ 4.x
  - 4.5
  - 4.4
  - 4.3
  - 4.2
  - 4.1
  - 4.0
- ▸ 3.2
- ▸ 3.0/3.1
- ▸ 2.x
- ▸ WWDC2004DP
- ▸ WWDC2003DP
- ▸ Dec2001

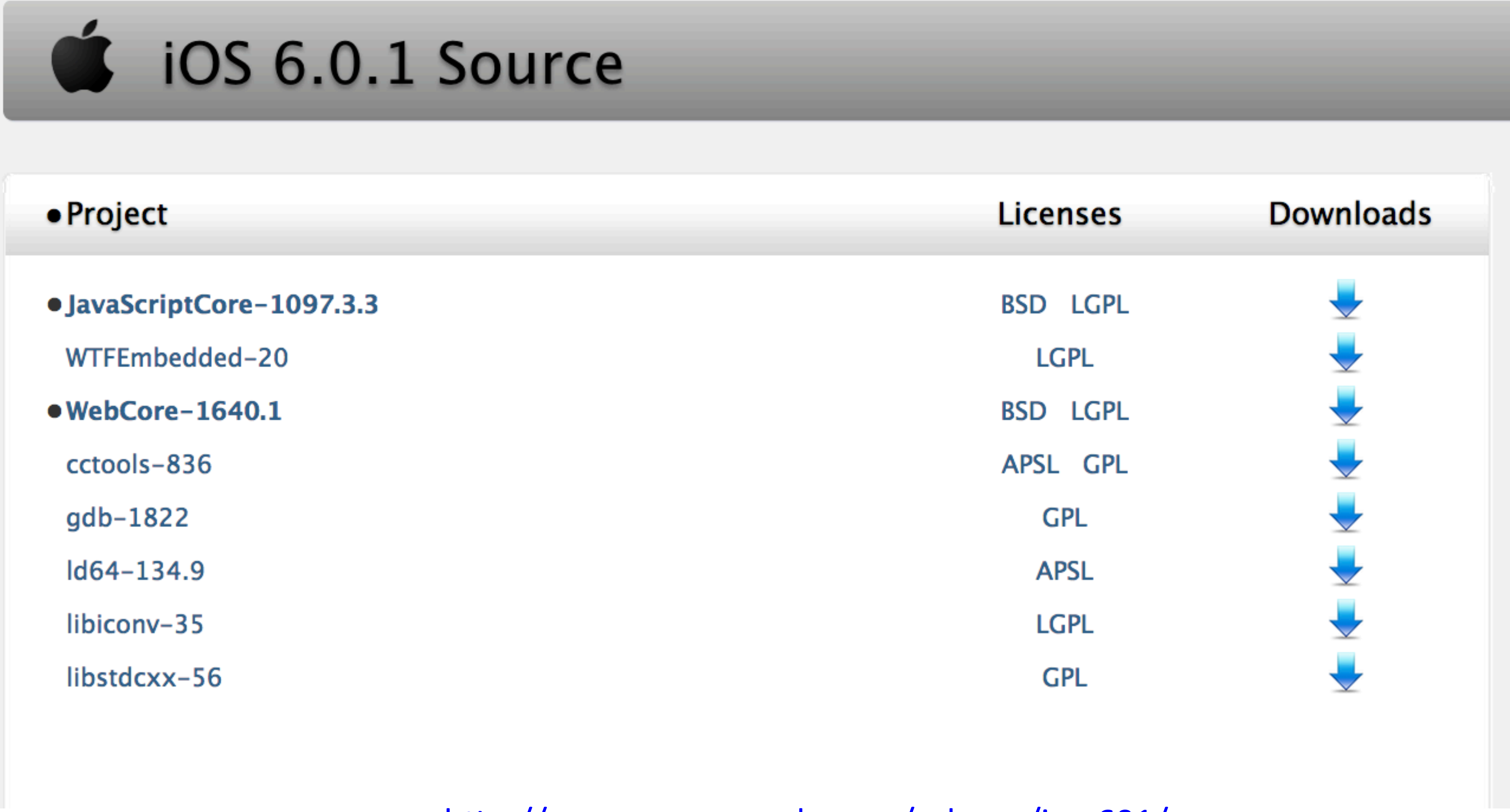
iOS

- ▾ 6.0
  - 6.0.1
  - 6.0
- ▸ 5.x
- ▸ 4.x
- ▸ 3.x
- ▸ 2.x
- ▸ SDK
- ▸ 1.x

http://opensource.apple.com/

©SecurityTube.net

Only Selected Components

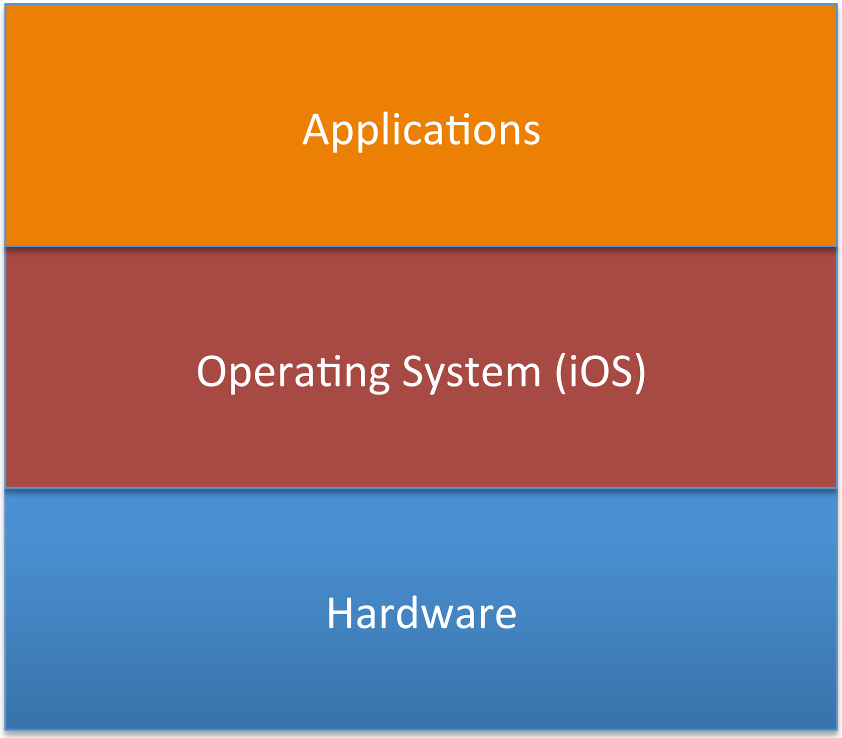


iOS 6.0.1 Source

●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/

iXXX



Applications

Operating System (iOS)

Hardware

iOS Applications

How does one Develop iOS Applications?

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

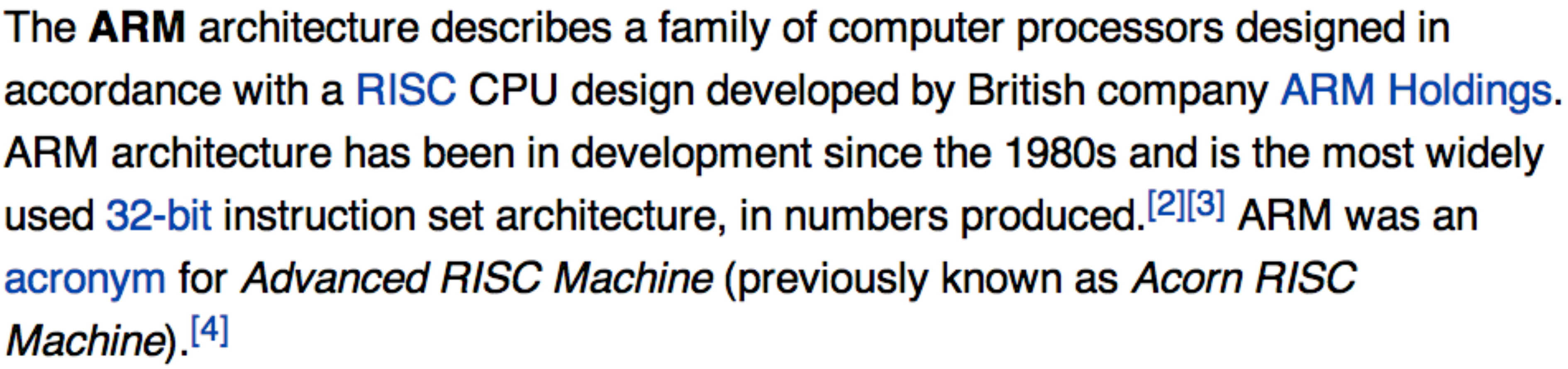
iDevice Processors

- 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

ARM anyone?



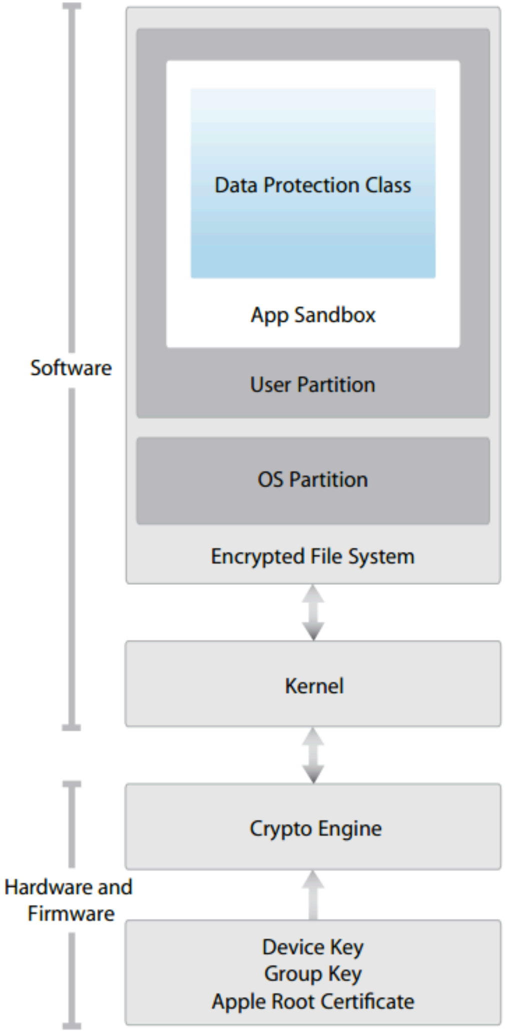
The **ARM** architecture describes a family of computer processors designed in accordance with a RISC CPU design developed by British company ARM Holdings. ARM architecture has been in development since the 1980s and is the most widely used 32-bit instruction set architecture, in numbers produced.[2][3]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

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

iOS Security Mechanisms

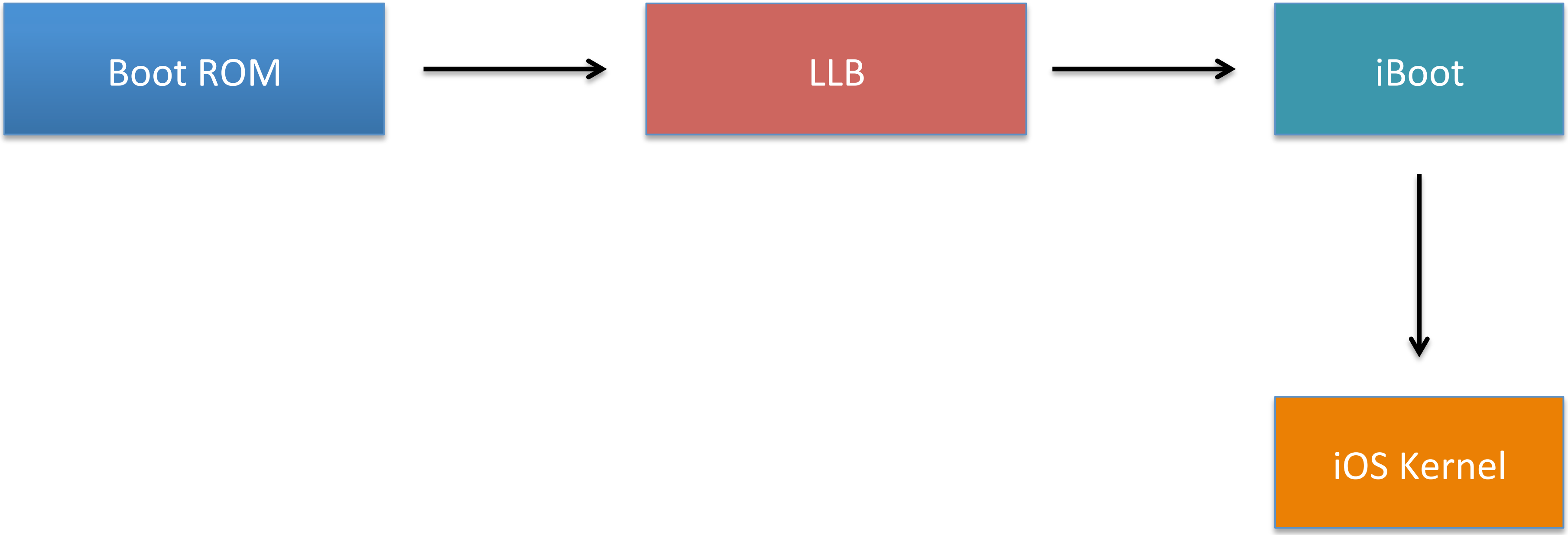
- Pretty much shrouded in mystery
- First public disclosure: http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf
- Talk at Blackhat 2012
  - Rehash of the PDF above

Security Architecture

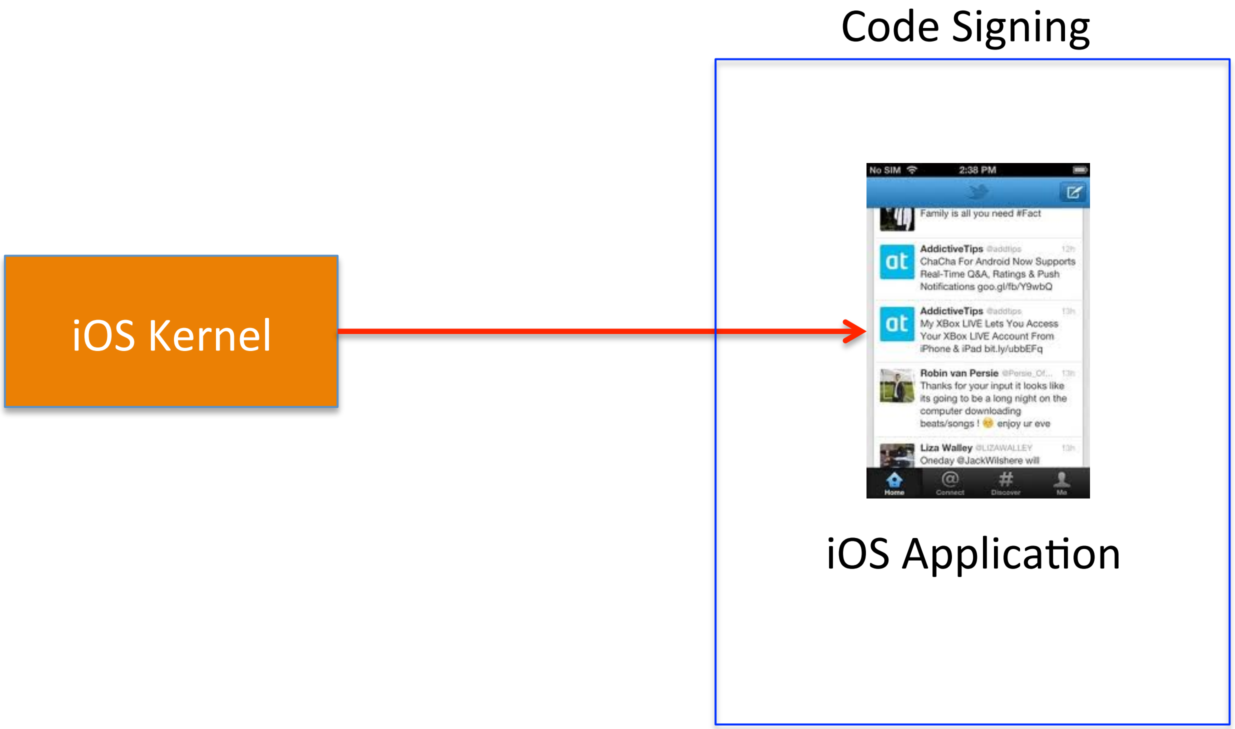


Source: Apple Inc.

Secure Boot Chain



Loading Trusted Applications



Family is all you need #Fact

AddictiveTips @addtips 12h
ChaCha For Android Now Supports Real-Time Q&A, Ratings & Push Notifications goo.gl/fb/Y9wbQ

AddictiveTips @addtips 13h
My XBox LIVE Lets You Access Your XBox LIVE Account From iPhone & iPad bit.ly/ubbEFq

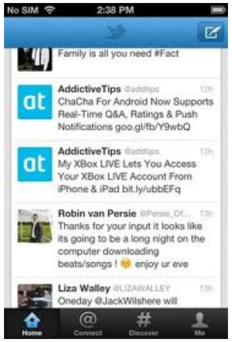
Robin van Persie @Persie_Of... 13h
Thanks for your input it looks like its going to be a long night on the computer downloading beats/songs ! 😊 enjoy ur eve

Liza Walley @LIZAWALLEY 13h
Oneday @JackWilshere will

©SecurityTube.net

Application Isolation

Code Signing



Family is all you need #Fact

AddictiveTips @addtips 12h
ChaCha For Android Now Supports Real-Time Q&A, Ratings & Push Notifications goo.gl/fb/Y9wbQ

AddictiveTips @addtips 13h
My XBox LIVE Lets You Access Your XBox LIVE Account From iPhone & iPad bit.ly/ubbEFq

Robin van Persie @Persie_Of... 13h
Thanks for your input it looks like its going to be a long night on the computer downloading beats/songs ! 😊 enjoy ur eve

Liza Walley @LIZAWALLEY 13h
Oneday @JackWilshere will

Application 1

Sandbox

Code Signing

Jorn van Dijk
Product Designer at Facebook
Studied at Hogeschool Rotterdam

Jorn van Dijk via Jasper Hauser
Announcing f8 2011
developers.facebook.com
Friday at 7:25pm
1 person

Jorn van Dijk and Michael Eyal Sharon are now friends.

Application 2

Sandbox

©SecurityTube.net

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?

Why do we need to Jailbreak?

- 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?

Jailbreaking

- Breaking through the “Jail” to allow for
  - running any application
  - file system access with root privileges
- May void Warranty!!
- In reality privilege escalation from mobile -> root

How does Jailbreaking work?

- Similar to any other exploitation

- How do you exploit Chrome on Windows?
  - Run browser_autopwn in Metasploit
  - If vulnerable Chrome, then gets exploited

- How do you exploit an iPhone
  - Find a vulnerability
  - Exploit it
  - Install your tools to maintain access

History of Jailbreaking Exploits

- Definitive List:

http://theiphonewiki.com/wiki/index.php?title=jailbreak

Types of Jailbreaks

- Untethered

- Tethered

Really depends on the Jailbreaking exploit used

Jailbreaking

- Hardware
  - Jailbroken iPhone / iPad
  - Any version of iOS >= 5.1.1
  - **No Support for Jailbreaking (warranty void?)**
  - **Do at your own risk**
  - http://jailbreak-me.info/

- Software
  - Windows / Linux / OS X

Cydia

Appstore for Jailbroken iPhones

Logging into your Jailbroken Device

- Install Open SSH server
- Connect to Wi-Fi and SSH over IP
- Connect via USB Multiplexer such as usbmuxd

Install the Following

- Erica Utilities
- Wget
- unzip
- adv-cmds
- cycript
- …

Sqlite Databases

- Sqlite is a file based database
- Does not have a server process associated with it
- Core Data files are Sqlite files
- Most common database type for both iOS and Android

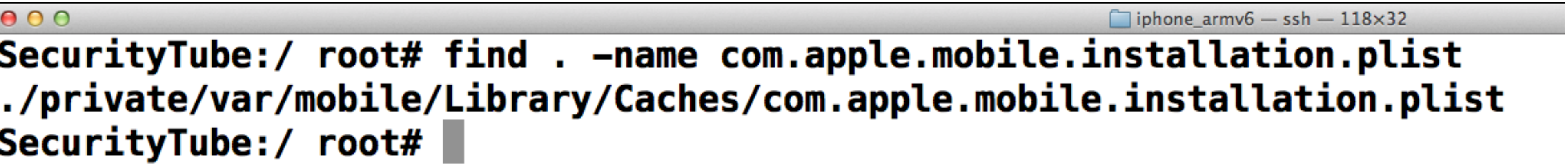
Sqlite Commands

- .headers ON – to make headers visible
- .tables – to list all available tables
- select * from table_name – to list all data in table name

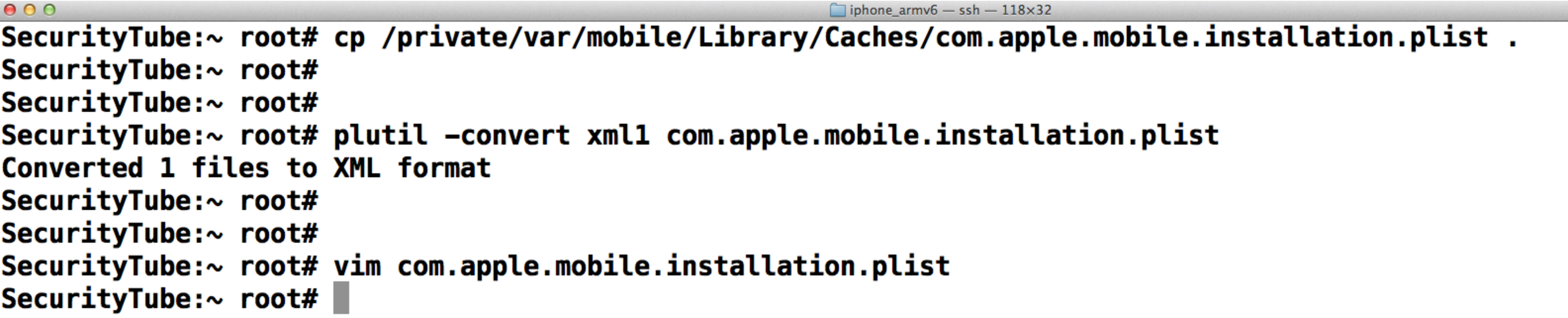
Property List Files

- used to store application and user settings
- data is serialized
- plutil tool to inspect and convert plist files
- Further Reading: http://en.wikipedia.org/wiki/Property_list

List of Applications



```
SecurityTube:/ root# find . -name com.apple.mobile.installation.plist
./private/var/mobile/Library/Caches/com.apple.mobile.installation.plist
SecurityTube:/ root# 
```



```
SecurityTube:~ root# cp /private/var/mobile/Library/Caches/com.apple.mobile.installation.plist .
SecurityTube:~ root#
SecurityTube:~ root#
SecurityTube:~ root# plutil -convert xml1 com.apple.mobile.installation.plist
Converted 1 files to XML format
SecurityTube:~ root#
SecurityTube:~ root#
SecurityTube:~ root# vim com.apple.mobile.installation.plist
SecurityTube:~ root# 
```

Class-Dump-Z

- Dumping class information from an iOS application
- Allows for guessing class utility
- Great help when using cycript or GDB
- Documentation: http://code.google.com/p/networkpx/wiki/class_dump_z

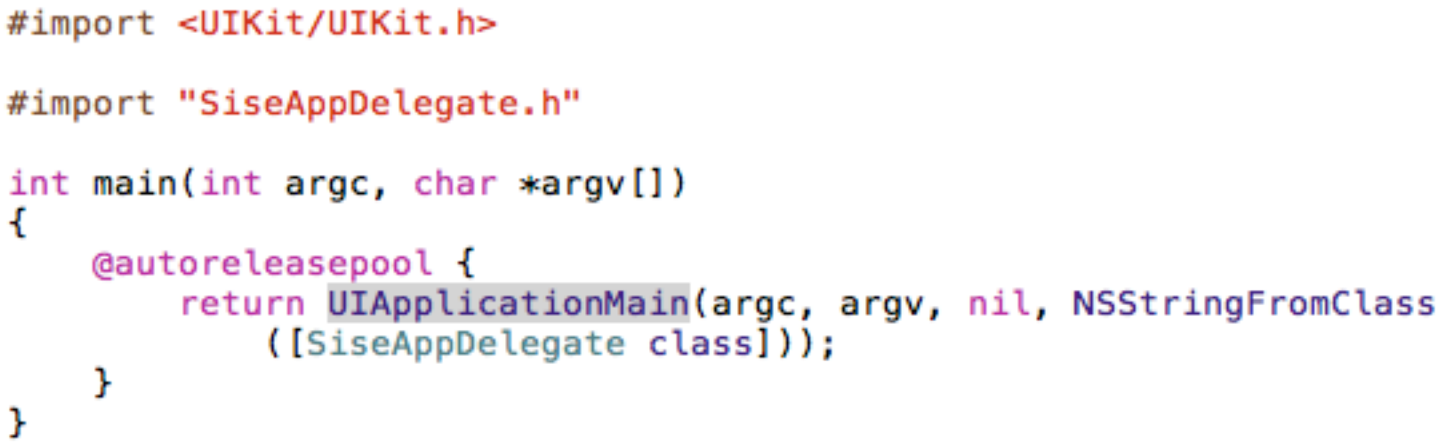
Cycript

- Runtime Injection and Modification of control flow
- Can view / modify data and code
- Documentation: http://www.cycript.org/

Installing HelloWorld

- Upload zip file to phone
- unzip and install in /Applications
- Already signed, hence will work

The Life Cycle of an iOS Application

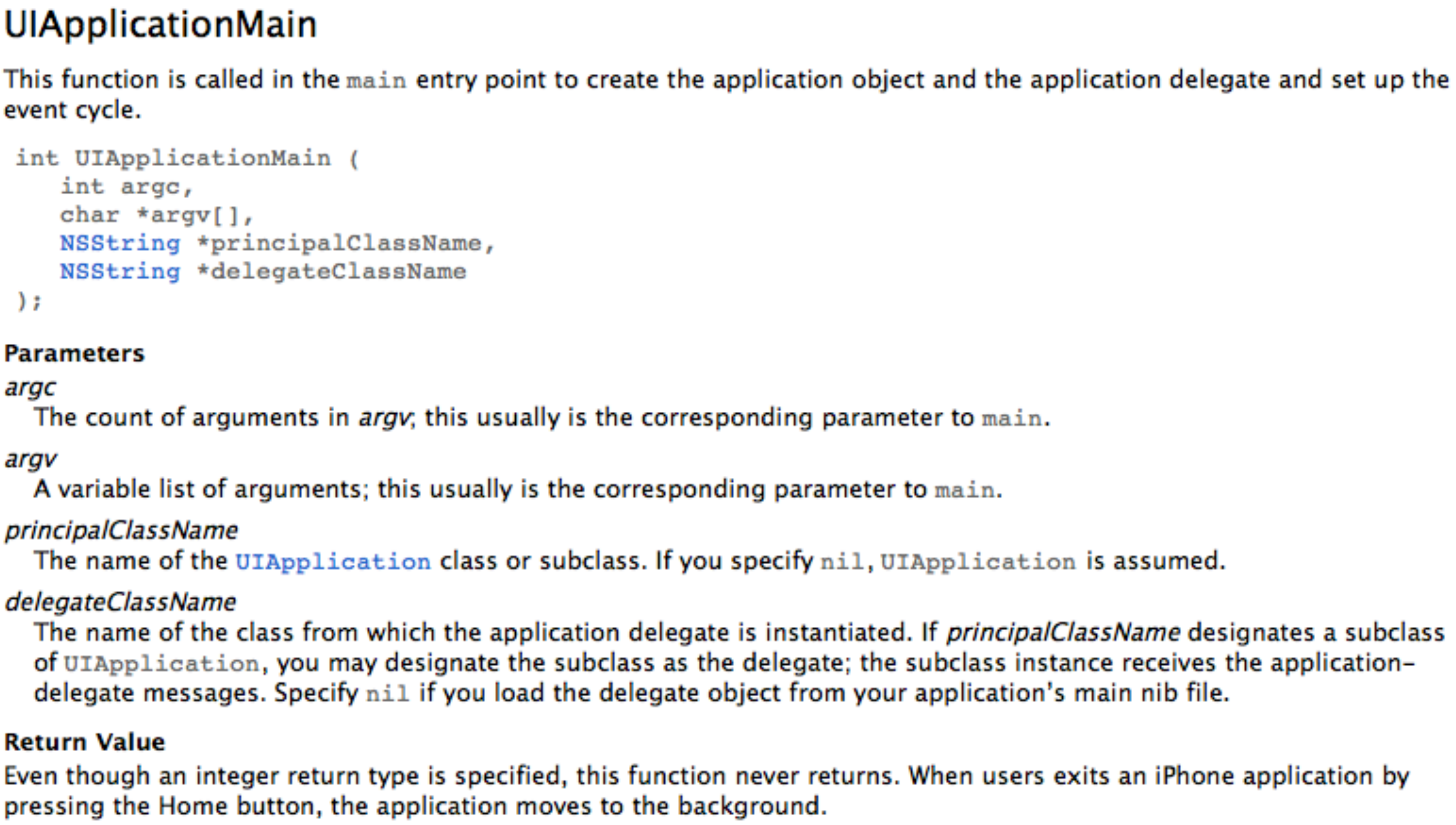


```
#import <UIKit/UIKit.h>

#import "SiseAppDelegate.h"

int main(int argc, char *argv[])
{
    @autoreleasepool {
        return UIApplicationMain(argc, argv, nil, NSStringFromClass
            ([SiseAppDelegate class]));
    }
}
```

UIApplicationMain



UIApplicationMain

This function is called in the `main` entry point to create the application object and the application delegate and set up the event cycle.

```
int UIApplicationMain (
    int argc,
    char *argv[],
    NSString *principalClassName,
    NSString *delegateClassName
);
```

Parameters

argc
The count of arguments in *argv*; this usually is the corresponding parameter to `main`.

argv
A variable list of arguments; this usually is the corresponding parameter to `main`.

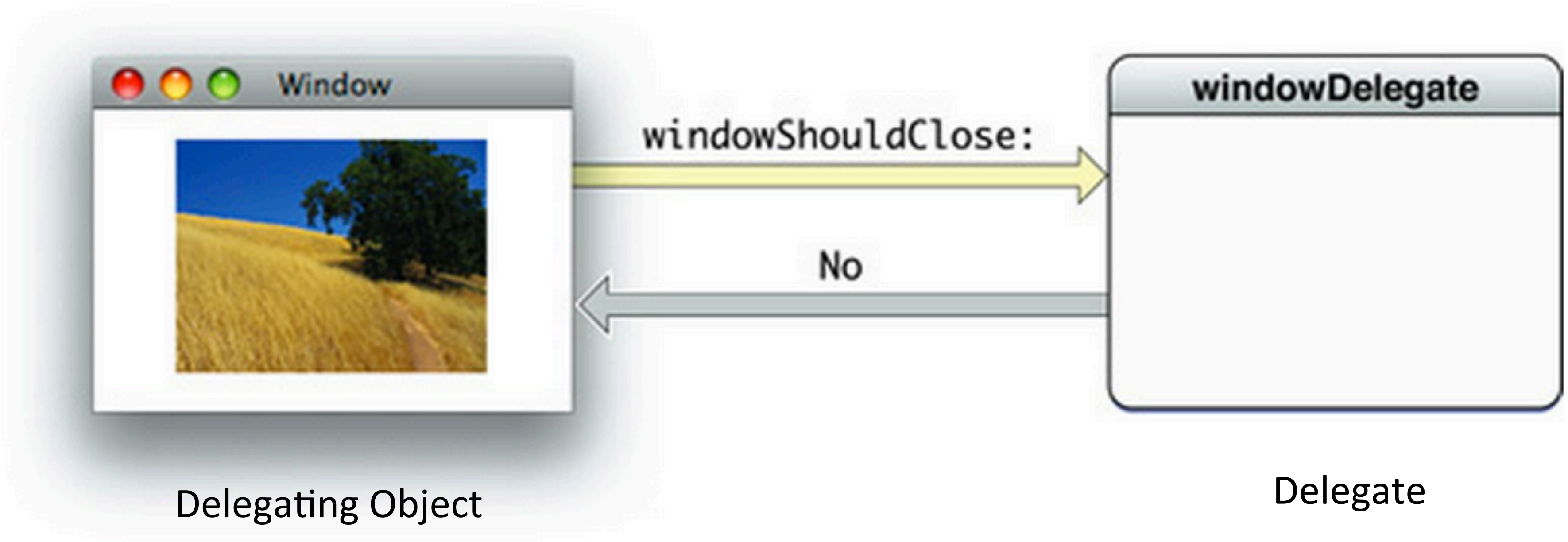
principalClassName
The name of the `UIApplication` class or subclass. If you specify `nil`, `UIApplication` is assumed.

delegateClassName
The name of the class from which the application delegate is instantiated. If *principalClassName* designates a subclass of `UIApplication`, you may designate the subclass as the delegate; the subclass instance receives the application-delegate messages. Specify `nil` if you load the delegate object from your application's main nib file.

Return Value

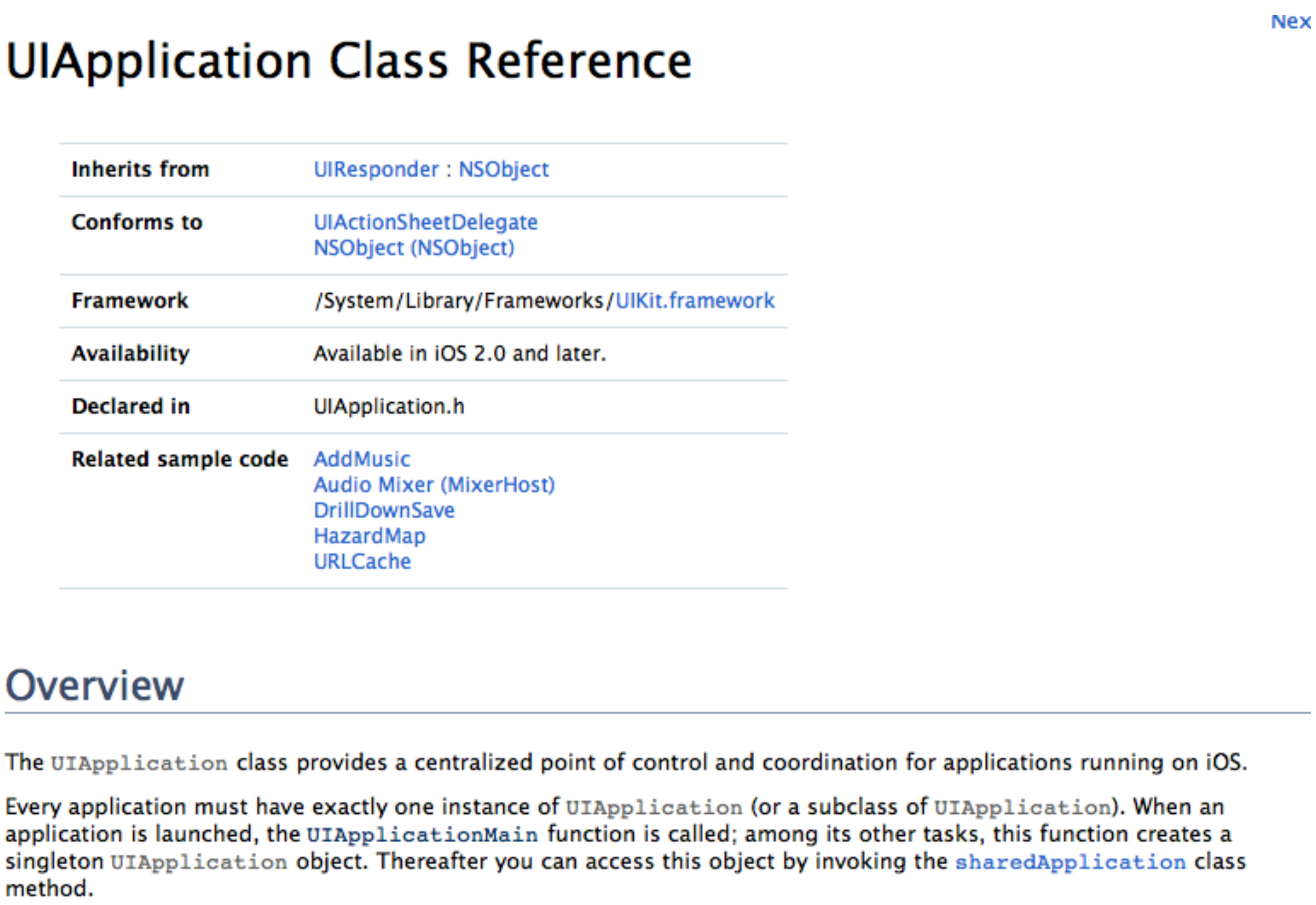
Even though an integer return type is specified, this function never returns. When users exits an iPhone application by pressing the Home button, the application moves to the background.

Delegation? Huh?



http://developer.apple.com/library/ios/#documentation/General/Conceptual/DevPedia-CocoaCore/Delegation.html

UIApplication



Nex

UIApplication Class Reference

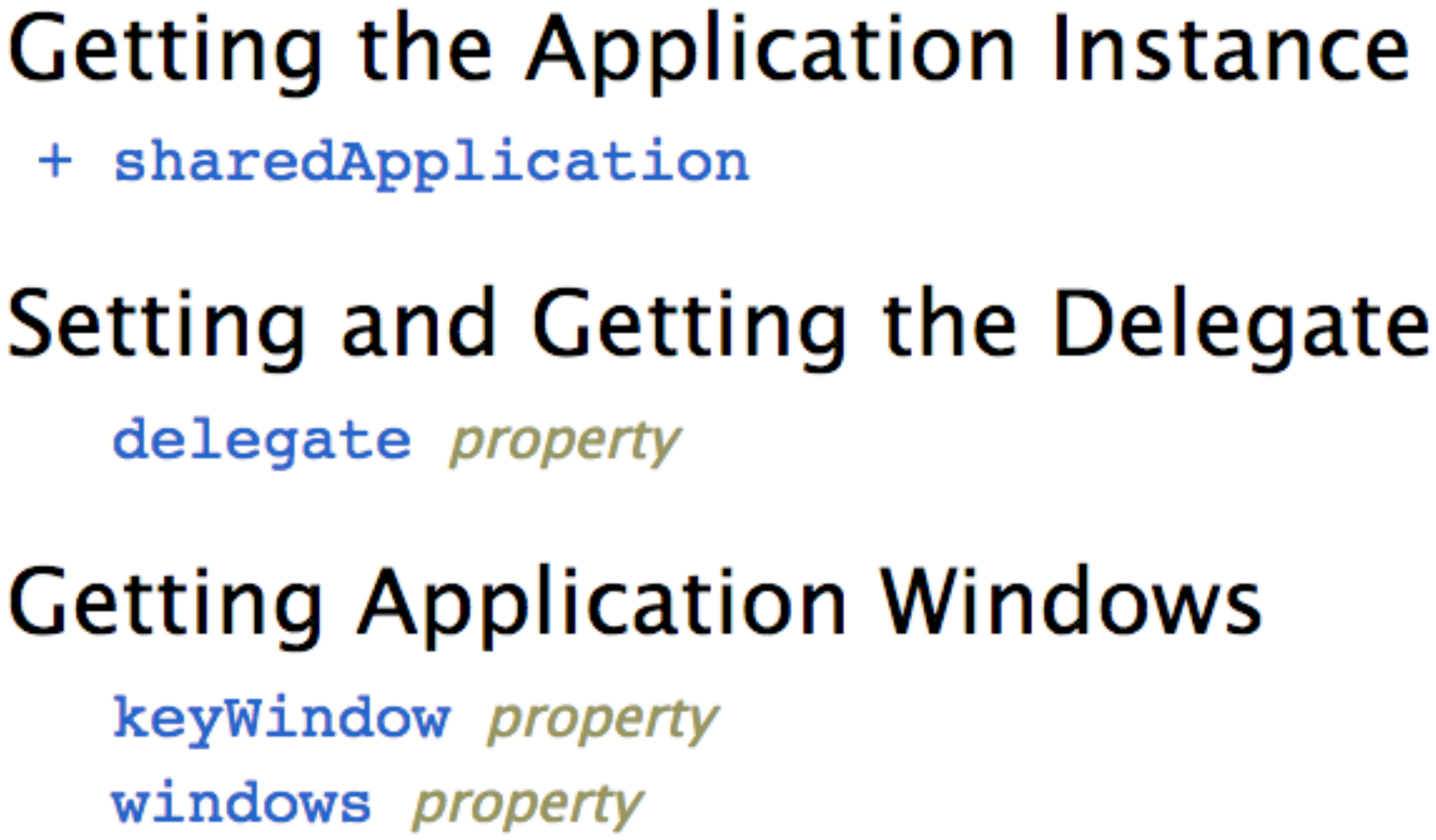
Inherits from	UIResponder : NSObject
Conforms to	UIActionSheetDelegate NSObject (NSObject)
Framework	/System/Library/Frameworks/UIKit.framework
Availability	Available in iOS 2.0 and later.
Declared in	UIApplication.h
Related sample code	AddMusic Audio Mixer (MixerHost) DrillDownSave HazardMap URLCache

Overview

The `UIApplication` class provides a centralized point of control and coordination for applications running on iOS.

Every application must have exactly one instance of `UIApplication` (or a subclass of `UIApplication`). When an application is launched, the `UIApplicationMain` function is called; among its other tasks, this function creates a singleton `UIApplication` object. Thereafter you can access this object by invoking the `sharedApplication` class method.

UIApplication Tasks



Getting the Application Instance

`+ sharedApplication`

Setting and Getting the Delegate

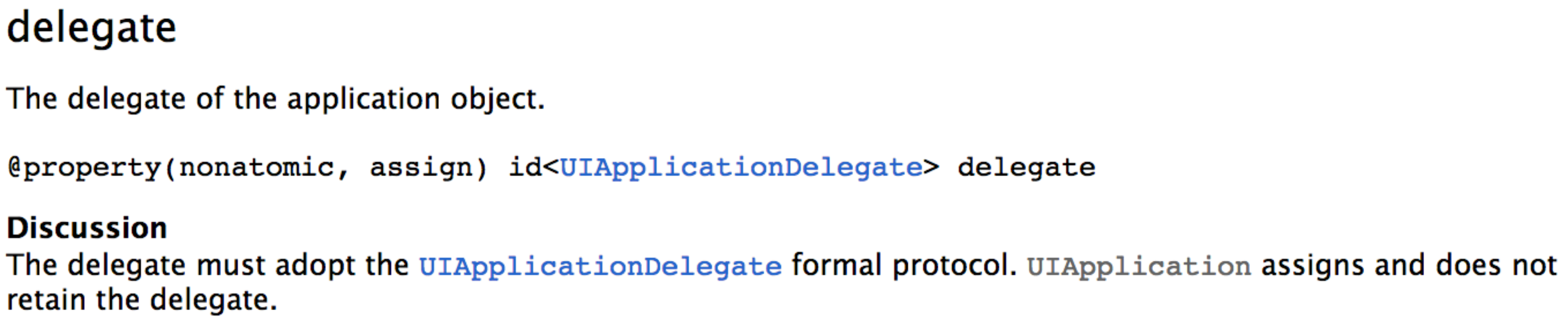
`delegate` *property*

Getting Application Windows

`keyWindow` *property*

`windows` *property*

UIApplication Delegate



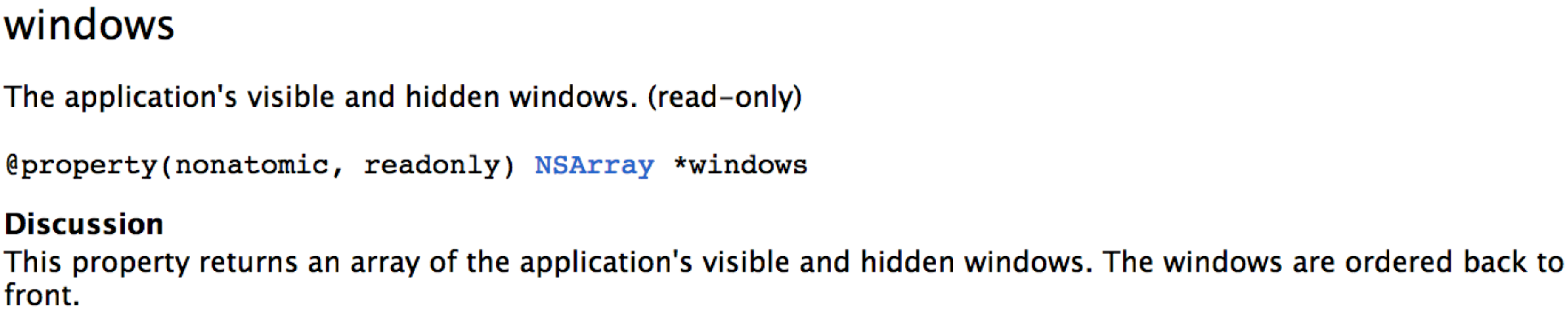
delegate

The delegate of the application object.

```
@property(nonatomic, assign) id<UIApplicationDelegate> delegate
```

Discussion
The delegate must adopt the `UIApplicationDelegate` formal protocol. `UIApplication` assigns and does not retain the delegate.

UIApplication windows



windows

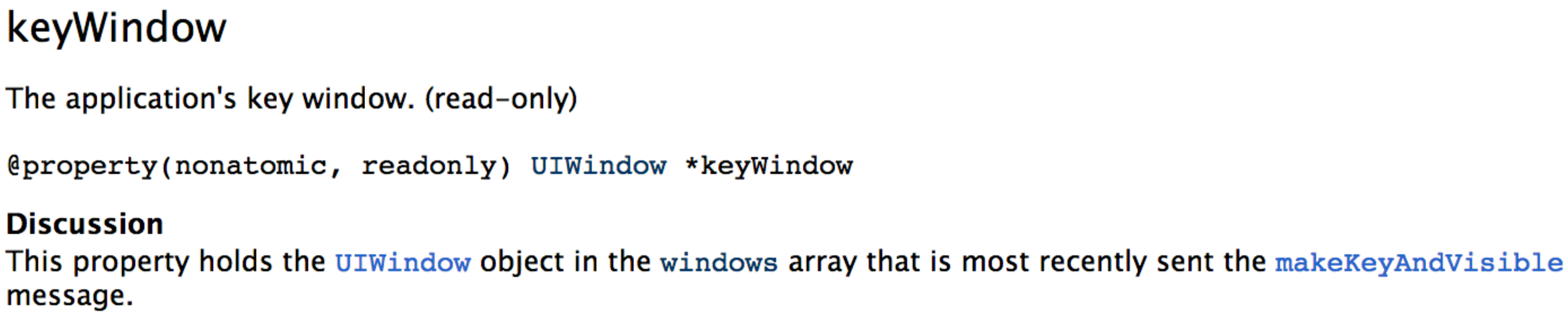
The application's visible and hidden windows. (read-only)

```
@property(nonatomic, readonly) NSArray *windows
```

Discussion

This property returns an array of the application's visible and hidden windows. The windows are ordered back to front.

Which is the active window?



keyWindow

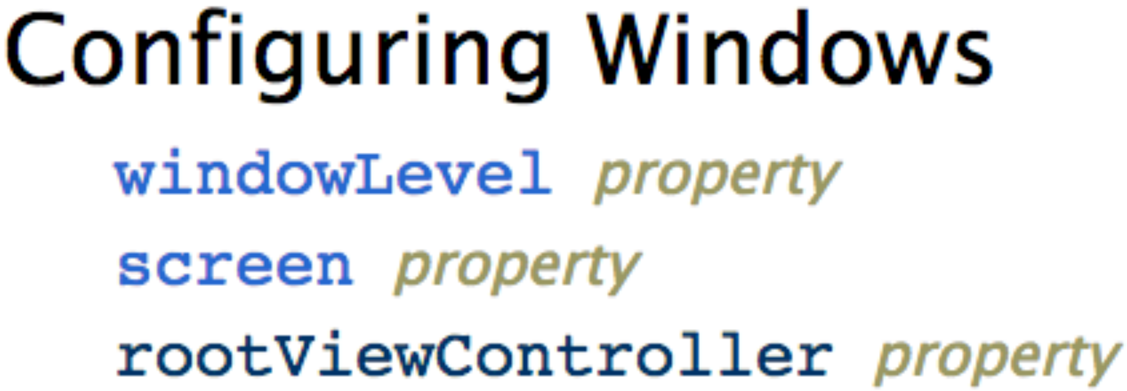
The application's key window. (read-only)

```
@property(nonatomic, readonly) UIWindow *keyWindow
```

Discussion

This property holds the `UIWindow` object in the `windows` array that is most recently sent the `makeKeyAndVisible` message.

UIWindow



Configuring Windows

windowLevel *property*

screen *property*

rootViewController *property*

http://developer.apple.com/library/ios/#DOCUMENTATION/UIKit/Reference/UIWindow_Class/UIWindowClassReference/UIWindowClassReference.html#//apple_ref/occ/cl/UIWindow

Cycript

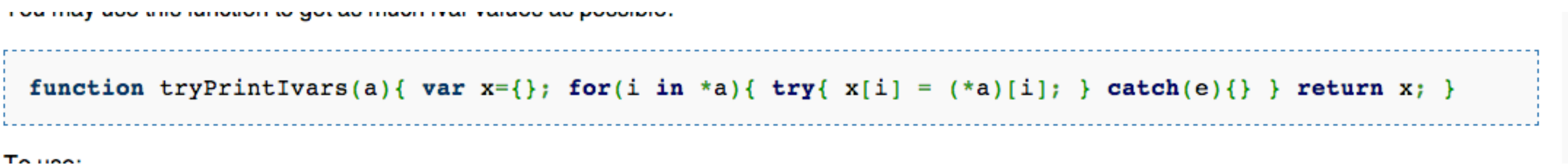
- Tricks:

http://iphonedevwiki.net/index.php/Cycript_Tricks

- Detailed Information:

http://iphonedevwiki.net/index.php/Cycript

Print iVars (Instance Variables)

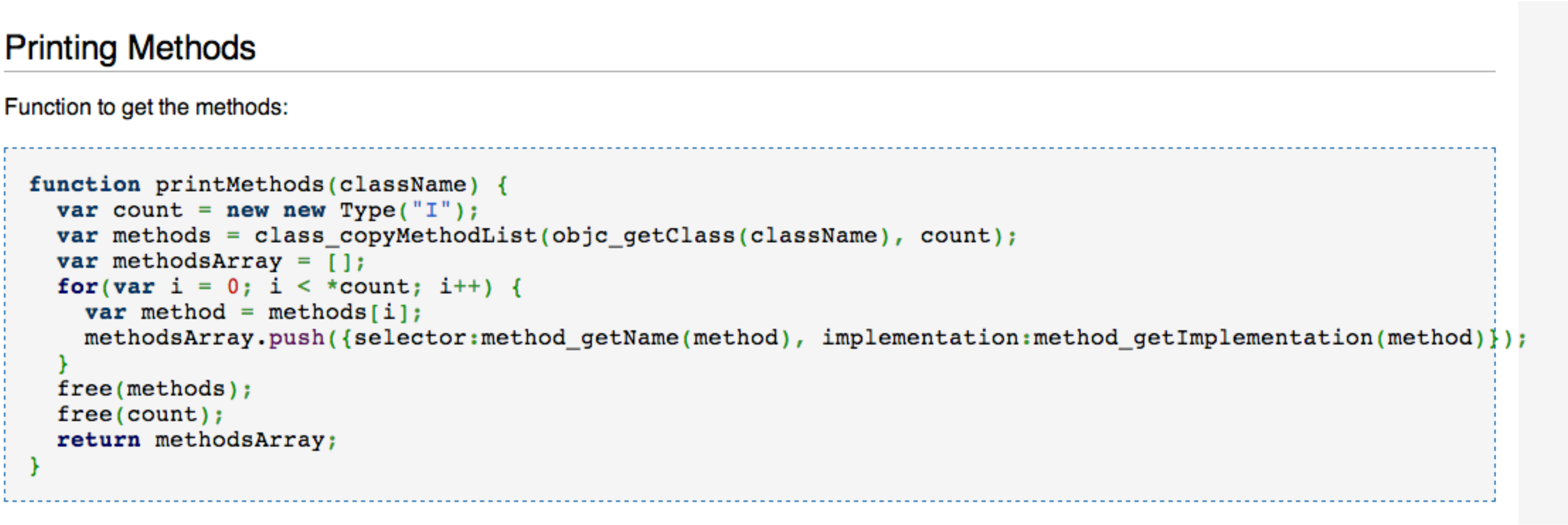


You may use this function to get as much ivar values as possible.

```
function tryPrintIvars(a){ var x={}; for(i in *a){ try{ x[i] = (*a)[i]; } catch(e){} } return x; }
```

To use:

Printing Methods

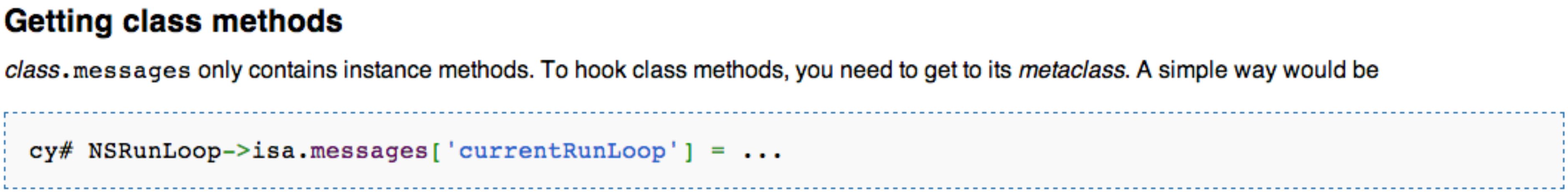


Printing Methods

Function to get the methods:

```
function printMethods(className) {
  var count = new new Type("I");
  var methods = class_copyMethodList(objc_getClass(className), count);
  var methodsArray = [];
  for(var i = 0; i < *count; i++) {
    var method = methods[i];
    methodsArray.push({selector:method_getName(method), implementation:method_getImplementation(method)});
  }
  free(methods);
  free(count);
  return methodsArray;
}
```

Replacing Functions



Getting class methods

class.messages only contains instance methods. To hook class methods, you need to get to its *metaclass*. A simple way would be

```
cy# NSRunLoop->isa.messages['currentRunLoop'] = ...
```

Application Encryption?

- All Applications we have used till now were not encrypted
  - out custom apps: already signed
  - Apple apps

- What about applications from the App Store?
  - Encrypted and Signed

Decrypting Applications with GDB

- Load process in GDB
- Dump memory and patch file header
- http://hackulo.us/wiki/IOS_Cracking#Using_GDB_to_Dump

Clutch

- Used for iOS application decryption
- Can be run from the command line
- ~~Documentation: http://hackulo.us/wiki/Clutch~~

Clutch

- Used for iOS application decryption
- Can be run from the command line
- ~~Documentation: http://hackulo.us/wiki/Clutch~~
- Clutch source code and other tools: http://cloud.uhelios.com/1t1y2z0M2B0d (Thanks to Paul!)
- Clutch binary included in this directory

GNU Debugger

- SecurityTube GNU Debugger Expert
  - Course videos
  - Slides
  - Exercises

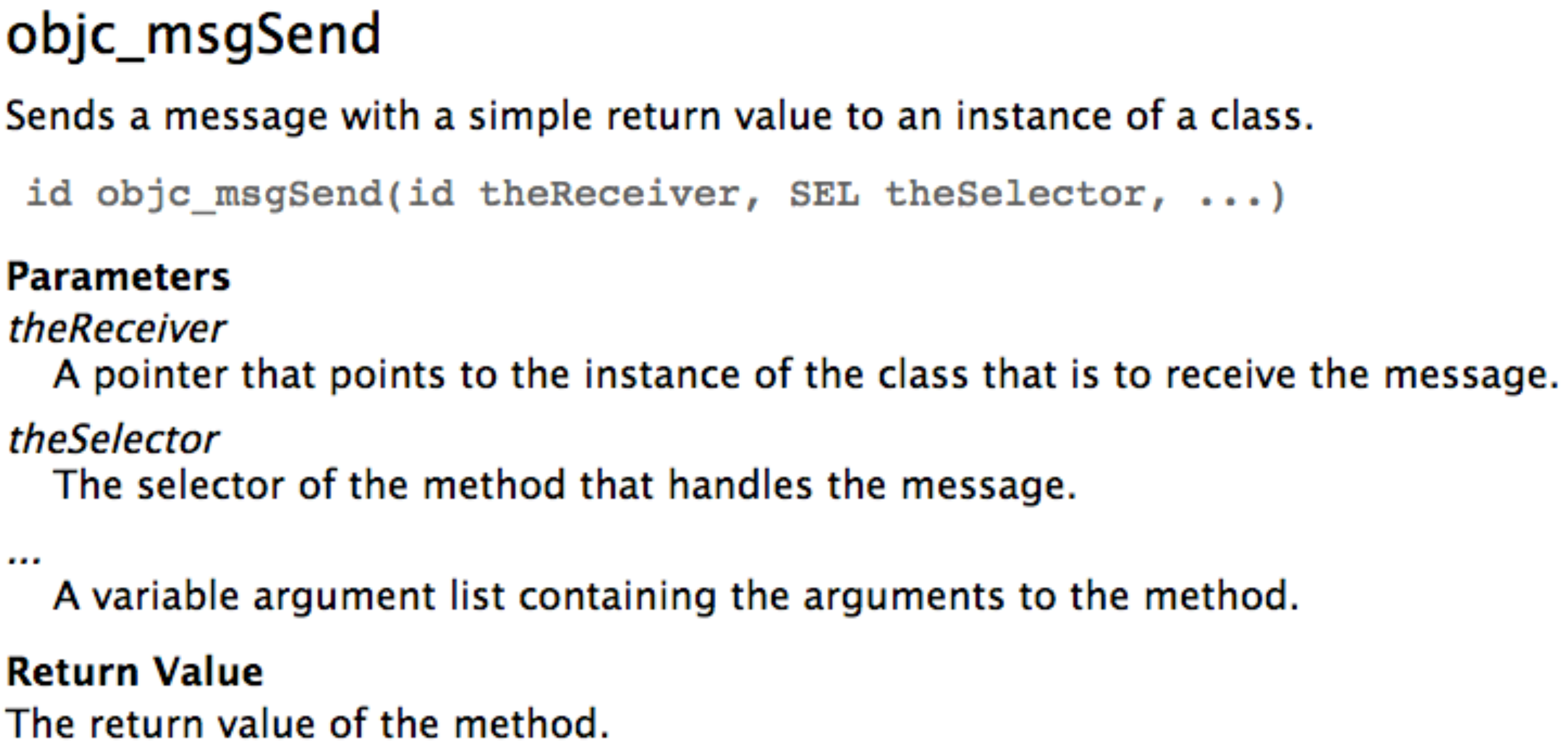
- GDB-Primer directory inside Module-3

- Please do it first before proceeding further

Cydia GDB Broken ☹

- pod2g: http://www.pod2g.org/2012/02/working-gnu-debugger-on-ios-43.html
- GDB included in module-3 directory
- upload to phone

objc_msgSend



objc_msgSend

Sends a message with a simple return value to an instance of a class.

```
id objc_msgSend(id theReceiver, SEL theSelector, ...)
```

Parameters

theReceiver

A pointer that points to the instance of the class that is to receive the message.

theSelector

The selector of the method that handles the message.

...

A variable argument list containing the arguments to the method.

Return Value

The return value of the method.

Source: Apple.com

Demos and Questions

Please Complete Speaker Feedback Surveys