iOS Testing Tools

David Lindner
Director of Mobile and IoT Security
Who is this guy?

David Lindner

- @golfhackerdave
- david.lindner@nvisium.com
- 15+ years consulting experience
- I hack and golf, sometimes at the same time.
• Web Assessments
• Code Remediation
• Secure Development

• Training
• Continuous Security
• Mobile & IoT Assessments

Expertise in ...
Disclaimer

Hacking of App Store apps is not condoned or encouraged in any way. What you do on your own time is your responsibility. @golfhackerdave & nVisium take no responsibility if you use knowledge shared in this presentation for unsavory acts.
Agenda

- Proxy Traffic
- Runtime Analysis
- Memory Analysis
- Binary Analysis
Proxy iOS

• Step 1 – Pick your Proxy
Proxy iOS

• Step 2 – Add CA to device

You Can Remove them

This works too but not as easy to manage!
Proxy iOS

• Step 3 – Set your system proxy
  – Settings -> WiFi -> YourNetwork
iOS Proxy Success!

Happy Happy Happy Happy
iOS – Certificate Pinning bypass

• SSLKillSwitch
  – https://github.com/iSECPartners/ios-ssl-kill-switch

“MobileSubstrate extension to disable certificate validation within NSURLConnection in order to facilitate black-box testing of iOS Apps.”
Runtime Analysis and Manipulation

• Monitor and modify the running application.
• Essentially “debugging.”
• Use cases:
  – Client-only applications.
  – Custom protocol (non-HTTP) communication.
Runtime Analysis: iOS

• iOS: Need a jailbroken device
  – Pangu for iOS 9-9.0.2
  – Possible to deploy to simulator (clunky, ugly)
  – Great tools for testing on devices

• Current Tools:
  – idb
  – cycript
  – snoop-it

• Resources
  – http://www.slideshare.net/jasonhaddix/pentesting-ios-applications
idb Features

• **File System Access**
  – View all current and created files
  – Keychain access
  – Check for auto screenshots
  – Check iOS Logs
  – Check iOS Pasteboard

• **App Analysis**
  – Analyze app binary for encryption, PIE, ARC, etc
  – Run strings on App
  – Dump class information
idb: Installing

- Requires a ruby environment
Live Demo: idb
Snoop-it

https://code.google.com/p/snoop-it/
Snoop-it Features

• **Monitoring**
  - File system access (print data protection classes)
  - Keychain access
  - HTTP(S) connections (NSURLConnection)
  - Access to sensitive API (address book, photos etc.)
  - Debug outputs (NSLog)
  - Tracing App internals (objc_msgSend)

• **Analysis/Manipulation**
  - Fake hardware identifier (UDID, Wireless MAC, etc.)
  - Fake location/GPS data
  - Explore and force display of available ViewController
Snoop-it: Installing

1. Add the Cydia repository repo.nesolabs.de and install the provided snoop-it package
2. After installing, run the Snoop-it Configuration App by tapping the Snoop-it icon on SpringBoard
3. Using the Snoop-it Configuration App, select the Apps to analyze.
4. Adjust the Snoop-it settings if desired (like e.g. the listening port of the web interface, authentication, tracing, etc.)
5. Run the selected App & point the browser in a computer to the Snoop-it web interface.
Live Demo: Snoop-it

Enter Passcode

1  2  3
4  5  6
7  8  9
0  A  B  C
D  E  F
G  H  I
J  K  L
M  N  O
P  Q  R
S  T  U
V  W  X
Y  Z
“Cycript allows developers to explore and modify running applications on either iOS or Mac OS X using a hybrid of Objective-C++ and JavaScript syntax through an interactive console that features syntax highlighting and tab completion.”

http://www.cycript.org/
iOS Execution Flow
What is Cycript

- A programming language designed to blend Objective-C and JavaScript.
- Allows hooking into an iOS process or application.
- It grants access to all of the classes and instance variables and methods within the application.
- Can write and execute scripts.
Cycrypt: How?

• Available for jailbroken iOS devices (Cydia installation)
• Command line interface.
Cycrypt: Why?

- Bypass client-side validations.
- Obtain sensitive data stored on memory (passwords, private keys, certificates, etc).
- Call methods directly.
- Overwrite methods (aka Method Swizzling).
- Similar capabilities to editing HTML/JS on a Web App (but much more complicated).
Cycrypt: Installing

• Cycrypt is available in Cydia:
  1. Open cydia on a jailbroken iOS device
  2. In case cycrypt is now showing up in the search results page make sure the “Developer” option is selected under “Manage”->”Settings”.
  3. Select the cycrypt package and install it.

• If the Cycrypt package is not seen in Cydia:
  1. Navigate to http://www.cycrypt.org/debs/ and download the latest available.
  2. Copy this file to the iDevice by using SFTP.
  3. SSH into the iDevice and install it, you may need root/sudo for this:
     # dpkg -i cycrypt_iphoneos-arm.deb
  4. Verify the installation by executing the following command:
     # cycrypt
  5. If the installation was successful a cycrypt interactive shell will be displayed:
     cy#
Cycrypt: Usage

• Obtain command line access to the device using SSH.
• Cycrypt needs to be attached/hooked to a process.

    # cycrypt -p Application

• Where “Application” is the name of the application running on the device

• If cycrypt is not able to start a process, an ID can be provided.

    # ps aux
    # cycrypt -p {process id}

• Get the name of the application delegate class.

    cy# UIApp.delegate
    #"<AppDelegate: 0x28a600>"
    cy# UIApp.keyWindow.rootViewController
Cycript: Usage Continued

• Dump all classes
  cy# ObjectiveC.classes

• Get a class memory address
  cy# choose(SomeClass)
  "<SomeClass: 0x28a600>"

• Attach to instance of Class
  cy# var somcls = new Instance(0x28a600)

• Run Methods in Class
  cy# [somcls someMethod: someParm]
Cycript Common Functions

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

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;
}

function methodsMatching(cls, regexp) {
    return [[new Selector(m).type(cls), m] for (m in cls.messages) if (!regexp || regexp.test(m))];
}
```

http://iphonedevwiki.net/index.php/Cycript_Tricks
Cycrypt Method Swizzling

cy# SomeClass.messages

cy# SomeClass.messages[‘someMethod’] = function(){return true;}
Live Demo: Cycrypt

```cy
# 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;
}
```
What About Swift

- No tools…yet
- Write custom hooks through Mobile Substrate
  - https://www.securify.nl/blog/SFY20150302/hooking_swift_methods_for_fun_and_profit.html
Memory Dumping and Analysis

• Why do we care about memory?
  – What type of info is retained? How long?
  – Is it necessary?
  – Could an attacker recover it if lost / stolen?
Memory Analysis: iOS

• Back to Snoop-it/Cycript/idb
iOS Binary Analysis

- iOS binaries are native code (read: cannot decompile).
- IPA files from iTunes have their binary code encrypted with Fairplay.
- Disassembler tools:
  - IDA pro [https://www.hex-rays.com/products/ida/](https://www.hex-rays.com/products/ida/)
- Resources:
  - [https://rstforums.com/forum/79368-ios-app-decompilation.rst](https://rstforums.com/forum/79368-ios-app-decompilation.rst)
  - [http://resources.infosecinstitute.com/penetration-testing-for-iphone-applications-part-5/](http://resources.infosecinstitute.com/penetration-testing-for-iphone-applications-part-5/)
But the app is encrypted???

- idb FTW!
- Uses dumpdecrypted

![App Binary Table]

- Encryption? : true
- Cryptid : true
- PIE : true
- Stack Canaries : true
- ARC : true
Other Tools

• **Methods**
  – class-dump
  – nm
  – strings

• **Logging**
  – idevicesyslog

• **Networking**
  – rvictl
  – iproxy
david.lindner@nvisium.com
@golfhackerdave
https://linkedin.com/in/dlindner