iOS Application Security Testing

COLUMBUS OWASP - NOV 21, 2019

HANS WEISHEIMER

Email: weisheimer@gmail.com

Twitter and Github: @hweisheimer

Slides will be on Github later if you want them

Web is: Stable

Backwards Compatibility > *

Protocols are 20+ years old

HTML5 is as old as the iPhone

Burp Suite is 15 years old

Mobile is: “Evolving”

iOS is “only” 12 years old

New version every year
New security features every year

Objective-C is stable, Swift is still changing

Web is: Transparent (Thanks F12)

HTTP Requests & Responses
Cookies & JS Local Storage
JS Debugging
JS Console & REPL
DOM Manipulation

Mobile is: Opaque

Apps are sandboxed, data access is limited

What's in the KeyChain? 

Is this app's API connection encrypted? 

Is the app *data* encrypted? ¯_(ツ)_/¯

iOS Tools of Past

Some early tools came from the Jailbreak scene

Many *required* a Jailbroken device

New iOS releases would lock things down, break tools

Jailbreaks eventually got *really* hard

Goals

- Off-the-Shelf hardware
- No jailbreaks required
- Free software
- Free accounts/subscriptions

Low Hanging Fruit

What can we inspect that's relatively low effort?

- Web APIs
- Compiler options
- Permissions
- Transport security settings
- Certificate pinning
- Root and Jailbreak detection
- Stored data (files, SQLite, KeyChain, UserDefaults)

Prerequisites: Hardware

Mac of some kind

iOS device and USB cable

Mac & iDevice connected to same WiFi

Prerequisites: XCode

Install XCode from the App Store

Run `xcode-select --install`

Preferences -> Components -> DL iOS Simulator

Register as an Apple Developer (free tier is fine)

Create a code signing certificate

Prerequisites: Third-Party

Proxy of your choice (Burp, ZAP, Charles, …)

Package manager such as Homebrew

```
brew install usbmuxd libimobiledevice python
pip install virtualenv
virtualenv ~/venv-objection &&
    source ~/venv-objection/bin/activate
pip install objection frida frida-tools
```

Network Inspection: HTTP

Use an intercepting proxy

Supported on: WiFi, Cellular

Ineffective on the iOS Simulator

Testing strategies are similar to web

Network Inspection: Everything Else

Remote Virtual Interfaces
(`rvictl` command)

Attach Wireshark to the new virtual adapter

Extra installation step as of XCode 11

Meet your new friends

FRIDA

Instrumenting an App

We'll use Frida in "embedded" mode, a.k.a Frida Gadget

* Jailbroken devices can use "injected" mode w/ Frida Server

Working from source? Add dylib to project

Run on device from XCode

Working from an IPA? Use **`objection patchipa`**

Sideload with ios-deploy or distribute as desired

Test the Plumbing

Run **`frida-ls-devices`** – you should see a USB device

Run the application – it will appear to hang

Attach with **`objection explore`**

Finding Loot: Filesystem

Find the DocumentsDirectory location:

```
env
cd [location-from-output]
```

Use **`ls`**, download interesting files to inspect:

```
file download name-on-device name-on-mac
!cat name-on-mac
```

Built-in helpers exist for things like plists

Finding Loot: SQLite DBs

Try the Caches directory, too

Open: **`sqlite connect [file]`**

Show tables: **`.tables`**

Query: **`sqlite execute select * from loot;`**

Finding Loot: KeyChain Entries

The KeyChain is often thought to be magically secure

Challenge this assumption with:

`ios keychain dump`

May need to respond to TouchID/FaceID prompt

(OK, that part *is* magic)

Passive Shenanigans

Simulate Jailbreak status, or bypass common checks

Bypass certificate pinning

Bypass weak biometric authentication

Monitor method calls and print the arguments

Resources: Docs

Frida:

https://frida.re/docs

@fridadotre @oleavr

Objection:

https://github.com/sensepost/objection/

Wiki is good (also on Github)

@leonjza

Resources: More Tools

Passionfruit

Slick Web UI, does a lot of what we've seen today

https://github.com/chaitin/passionfruit

MobSF

Web app, automated analysis for iOS and Android

https://github.com/MobSF/Mobile-Security-Framework-MobSF

Resources: Better Talks Than This

Kev Cody - How to Frida Good

SnowFROC 2019, mDevCamp 2019

https://slideslive.com/38916544/how-to-frida-good?locale=en

Leon Jacobs - Meticulously Modern Mobile Manipulations

DEFCON 27

https://www.youtube.com/watch?v=7LKXSYFrYAM

Resources: Better Guides Than This

OWASP Mobile Security Testing Guide

https://mobile-security.gitbook.io/mobile-security-testing-guide/

OWASP Mobile Application Security Verification Standard

https://mobile-security.gitbook.io/masvs/

Next Up: Codemash

Jan 7th or 8th

Four hour hands-on session if you have a 4-day ticket

Bring a MacBook if you can

Corellium virtual devices provided

Jan 9th or 10th

This talk again

Send feedback, don't let me look like an ass