RANDORISEC

Mobile Hacking Workshop – iOS

June 30th & July 1st 2022

Pre requisites

No setup, no VM, only a **web browser** (Chrome recommended for H264 video streaming support), a **command line** and a **brain**

1. Send your email adress to **davy@randorisec.fr** for your Corellium  account creation

2. Log in Corellium (you'll receive a mail with the link)

3. Get the **materials**  on your laptop

```
git clone https://github.com/randorisec/HIP2022-Workshops
```

Agenda

1. Testing environment
2. Basics
3. Static analysis – 2 labs
4. Data Security – 3 labs
5. Execution analysis – 2 labs
6. Transport Security – 1 lab

Legend

Lab: practical exercice

OWASP M2 Insecure data storage

OWASP Top10 item covered

Basics

Main steps of a security iOS application assessment

1. Review the codebase or reverse engineer the binary
2. Run the app on a jailbroken device
3. Inspect and manipulate the app via instrumentation
4. Manipulate the runtime
5. MiTM all the network communications

What is an IPA ?

- iOS App Store Package
- Archive (can be renamed to .zip and unzipped)
- Binary and static files (signed)

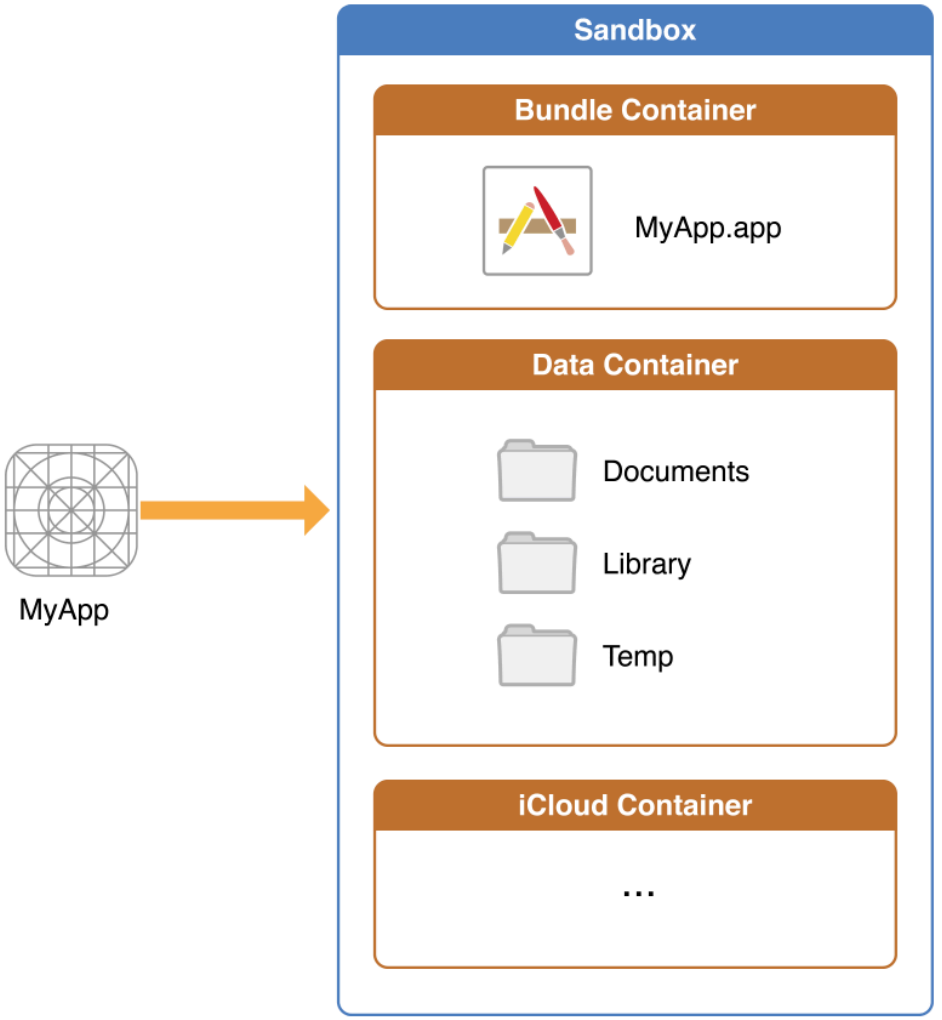
```
480B May 25  2018 Frameworks
1.1M May 25  2018 iGoat-Swift
 15K May 25  2018 embedded.mobileprovision
 96B May 25  2018 ..
 96B May 25  2018 _CodeSignature
372B May 25  2018 archived-expanded-entitlements.xcent
128B May 25  2018 Base.lproj
1.4K May 25  2018 Info.plist
  8B May 25  2018 PkgInfo
189K May 25  2018 Assets.car
128B May 25  2018 CrossSiteScriptingExerciseVC.nib
128B May 25  2018 HTMLViewController.nib
3.0K May 25  2018 AppIcon29x29@2x.png
5.3K May 25  2018 AppIcon29x29@3x.png
```

Filesystem: **System applications**

/Applications

```
iPhone:/Applications root# ls -al
total 0
drwxr-xr-x  76 root wheel 2432 May 31 06:20 ./
drwxr-xr-x  27 root wheel  864 May 31 06:18 ../
drwxrwxr-x  46 root admin 1472 May 21 20:47 AXUIViewService.app/
drwxrwxr-x   7 root admin  224 May 21 20:47 AccountAuthenticationDialog.app/
drwxrwxr-x   7 root admin  224 May 21 20:47 ActivityMessagesApp.app/
drwxrwxr-x   9 root admin  288 May 21 20:47 AdPlatformsDiagnostics.app/
drwxrwxr-x  52 root admin 1664 May 21 20:47 AppStore.app/
drwxrwxr-x  47 root admin 1504 May 21 20:47 AskPermissionUI.app/
drwxrwxr-x   7 root admin  224 May 21 20:47 BusinessExtensionsWrapper.app/
drwxrwxr-x  46 root admin 1472 May 21 20:47 CTCarrierSpaceAuth.app/
drwxrwxr-x  58 root admin 1856 May 21 20:47 Camera.app/
drwxrwxr-x  47 root admin 1504 May 21 20:47 CheckerBoard.app/
drwxrwxr-x  46 root admin 1472 May 21 20:47 CompassCalibrationViewService.app/
drwxrwxr-x   8 root admin  256 May 21 20:46 ContinuityCamera.app/
drwxrwxr-x  49 root admin 1568 May 21 20:46 CoreAuthUI.app/
drwxr-xr-x 124 root wheel 3968 May 31 01:37 Cydia.app/
drwxrwxr-x  46 root admin 1472 May 21 20:46 DDActionsService.app/
```

Filesystem: **User applications**



Filesystem: **User applications**

/private/var/containers/Bundle/Application

```
iPhone:/private/var/containers/Bundle/Application root# ls -al
total 0
drwxr-xr-x 29 _installd _installd 928 Jun 15 09:48 ./
drwxr-xr-x  6 _installd _installd 192 May 31 01:38 ../
drwxr-xr-x  5 _installd _installd 160 Jun 10 03:54 07B03D18-01A1-4F1E-A355-F000AC9B9F35/
drwxr-xr-x  5 _installd _installd 160 May 31 01:39 121F8420-4F80-4398-8C22-240CEFEF6F54/
drwxr-xr-x  5 _installd _installd 160 May 31 01:39 1E1ACAAC-CD00-47D2-BD0D-68A23A68A85A/
drwxr-xr-x  5 _installd _installd 160 May 31 02:19 277F19A6-D521-48ED-B75E-9D1E8FCA8C90/
drwxr-xr-x  5 _installd _installd 160 May 31 01:52 27FFB5C0-7872-4552-894D-D2374A0ACDD9/
drwxr-xr-x  5 _installd _installd 160 Jun 10 03:51 2E2449F1-AE2A-44A1-8A71-2FBF132852BD/
drwxr-xr-x  5 _installd _installd 160 May 31 01:38 43B016BC-5984-45A5-A4A5-B315E5046993/
drwxr-xr-x  5 _installd _installd 160 May 31 01:39 62784C25-81EB-4CCA-9BDE-C71AE162EA0A/
drwxr-xr-x  5 _installd _installd 160 May 31 01:39 65A879DB-CC9B-4AC6-8DB9-EFABC3DCDF90/
drwxr-xr-x  5 _installd _installd 160 May 31 01:39 7D73F79E-78CF-487B-8C9E-7A3B15CE13E0/
drwxr-xr-x  5 _installd _installd 160 May 31 01:38 81A56A73-B663-4566-8687-2EBE4C04ADD7/
```

Filesystem: User applications: **Bundle** Directory

/private/var/containers/Bundle/Application/UUID/App.app

```
iPhone:/private/var/containers/Bundle/Application/4E1CB17B-5A86-468D-AD57-F92C9F11A5B2/DamnVulnerableIOSApp.app root# ls -al
total 6456
drwxr-xr-x 38 _installd _installd    1216 Oct 26 18:49 ./
drwxr-xr-x  5 _installd _installd     160 Oct 26 18:49 ../
-rw-r--r--  1 _installd _installd   11553 Dec  2  2014 120x120.png
-rw-r--r--  1 _installd _installd   13907 Dec  2  2014 152x152.png
-rw-r--r--  1 _installd _installd    6525 Dec  2  2014 57x57.png
-rw-r--r--  1 _installd _installd  375699 Dec  2  2014 640_960_SplashScn.png
-rw-r--r--  1 _installd _installd  464522 Dec  2  2014 640x1136_SplashScn.png
-rw-r--r--  1 _installd _installd    7893 Dec  2  2014 72x72.png
-rw-r--r--  1 _installd _installd    8464 Dec  2  2014 76x76.png
-rw-r--r--  1 _installd _installd   11292 Dec  2  2014 AppIcon40x40\@2x.png
-rw-r--r--  1 _installd _installd   11553 Dec  2  2014 AppIcon60x60\@2x.png
drwxr-xr-x  3 _installd _installd      96 Oct 26 18:49 Base.lproj/
-rwxr-xr-x  1 _installd _installd 4483296 May 26 11:32 DamnVulnerableIOSApp*
-rw-r--r--  1 _installd _installd     423 May 26 11:32 DamnVulnerableIOSApp.entitlements
-rw-r--r--  1 _installd _installd    1410 Jan  1  1980 Info.plist
-rw-r--r--  1 _installd _installd  464522 Dec  2  2014 LaunchImage-700-568h\@2x.png
```

- Static files (signed):
- Binary
- Images
- Properties

Filesystem: User applications: Bundle Directory

Info.plist

```
plconvert Info.plist Info.txt
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>CFBundleName</key>
        <string>DamnVulnerableIOSApp</string>
        <key>DTSDKName</key>
        <string>iphoneos8.1</string>
        <key>DTXcode</key>
        <string>0610</string>
        <key>DTSDKBuild</key>
        <string>12B411</string>
        <key>CFBundleDevelopmentRegion</key>
        <string>en</string>
        <key>CFBundleVersion</key>
        <string>1.0</string>
        <key>BuildMachineOSBuild</key>
        <string>14B25</string>
        <key>DTPlatformName</key>
        <string>iphoneos</string>
        <key>CFBundleShortVersionString</key>
        <string>1.3</string>
```

Filesystem: User applications: **Data** Directory

/private/var/mobile/Containers/Data/Application/UUID

```
iPhone:/private/var/mobile/Containers/Data/Application/AA7D5264-12B6-4109-A397-C007299AB958 root# ls -al
total 4
drwxr-xr-x  7 mobile mobile  224 May 31 01:52 ./
drwxr-xr-x 81 mobile mobile 2592 Jun 15 09:48 ../
-rw-r--r--  1 root   mobile  211 May 31 01:52 .com.apple.mobile_container_manager.metadata.plist
drwxr-xr-x  3 mobile mobile   96 Jun 11 10:45 Documents/
drwxr-xr-x  5 mobile mobile  160 Jun 11 02:14 Library/
drwxr-xr-x  2 mobile mobile   64 May 31 01:52 SystemData/
drwxr-xr-x 25 mobile mobile  800 Jun 15 16:25 tmp/
iPhone:/private/var/mobile/Containers/Data/Application/AA7D5264-12B6-4109-A397-C007299AB958 root# du -ah
12K     ./Documents/credentials.sqlite
12K     ./Documents
4.0K    ./.com.apple.mobile_container_manager.metadata.plist
52K     ./Library/Caches/com.swaroop.iGoat/Cache.db
0       ./Library/Caches/com.swaroop.iGoat/Cache.db-wal
32K     ./Library/Caches/com.swaroop.iGoat/Cache.db-shm
84K     ./Library/Caches/com.swaroop.iGoat
40K     ./Library/Caches/Snapshots/com.swaroop.iGoat/600E684E-7B24-4386-947A-FDF646E30248@2x.atx
36K     ./Library/Caches/Snapshots/com.swaroop.iGoat/downscaled/D29866C1-7955-4271-B34A-5F63AF19BB65@2x.atx
36K     ./Library/Caches/Snapshots/com.swaroop.iGoat/downscaled
76K     ./Library/Caches/Snapshots/com.swaroop.iGoat
76K     ./Library/Caches/Snapshots
160K    ./Library/Caches
0       ./Library/Preferences
4.0K    ./Library/Cookies/com.swaroop.iGoat.binarycookies
```

- User data
- Settings
- Cookies
- Cached files
- Temp files

Filesystem: to sum up

Bundle directory
`/private/var/containers/Bundle/Application/UUID/App`
Data directory
`/private/var/mobile/Containers/Data/Application/UUID`

Ex:
Bundle directory
`/private/var/containers/Bundle/Application/E69C6843-CD63-41C7-9AA8-120177BACA73/<AppName>.app`
Data directory
`/private/var/mobile/Containers/Data/Application/31D5446F-A320-4C83-B592-84783B3F68FF`

OWASP MSTG+MASVS+Checklist

OWASP Mobile Security Testing Project

Project = standard + checklist + guide

GitHub, Inc. [US] | https://github.com/OWASP/owasp-mstg

README.md

OWASP Mobile Security Testing Guide

Follow 542

owasp lab project build passing

This is the official GitHub Repository of the OWASP Mobile Security Testing Guide (MSTG). The MSTG is a comprehensive manual for mobile app security testing and reverse engineering. It describes technical processes for verifying the controls listed in the OWASP Mobile Application Verification Standard (MASVS). You can also read the MSTG on Gitbook or download it as an e-book.

MASVS (Mobile AppSec Verification **Standard**)

V1 Architecture, design and threat modelling
V2 Data Storage and Privacy
V3 Cryptography
V4 Authentication and Session Management
V5 Network Communication
V6 Platform Interaction
V7 Code Quality and Build Settings

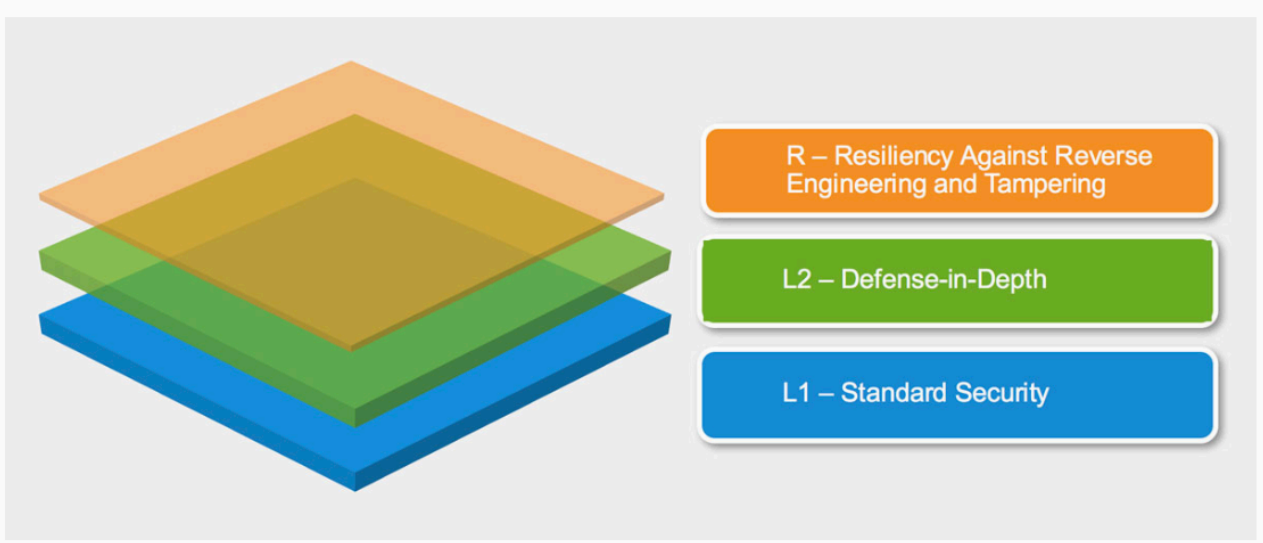
Last version: version 1.4.2 (jan 2022)

OWASP Mobile AppSec **Checklist**

Data Storage and Privacy Requirements

ID	MSTG-ID	Detailed Verification Requirement	L1	L2	R	Android	iOS	Status
2.1	MSTG-STORAGE-1	System credential storage facilities need to be used to store sensitive data, such as PII, user credentials or cryptographic keys.	■	■		Test Case	Test Case	
2.2	MSTG-STORAGE-2	No sensitive data should be stored outside of the app container or system credential storage facilities.	■	■		Test Case	Test Case	
2.3	MSTG-STORAGE-3	No sensitive data is written to application logs.	■	■		Test Case	Test Case	
2.4	MSTG-STORAGE-4	No sensitive data is shared with third parties un						

Last version: 1.4 (jan 2022)



OWASP Mobile Security Testing **Guide**

The guide:

- 3 sections:
  - General (common to Android and iOS)
  - Android
  - iOS
- + 500 pages

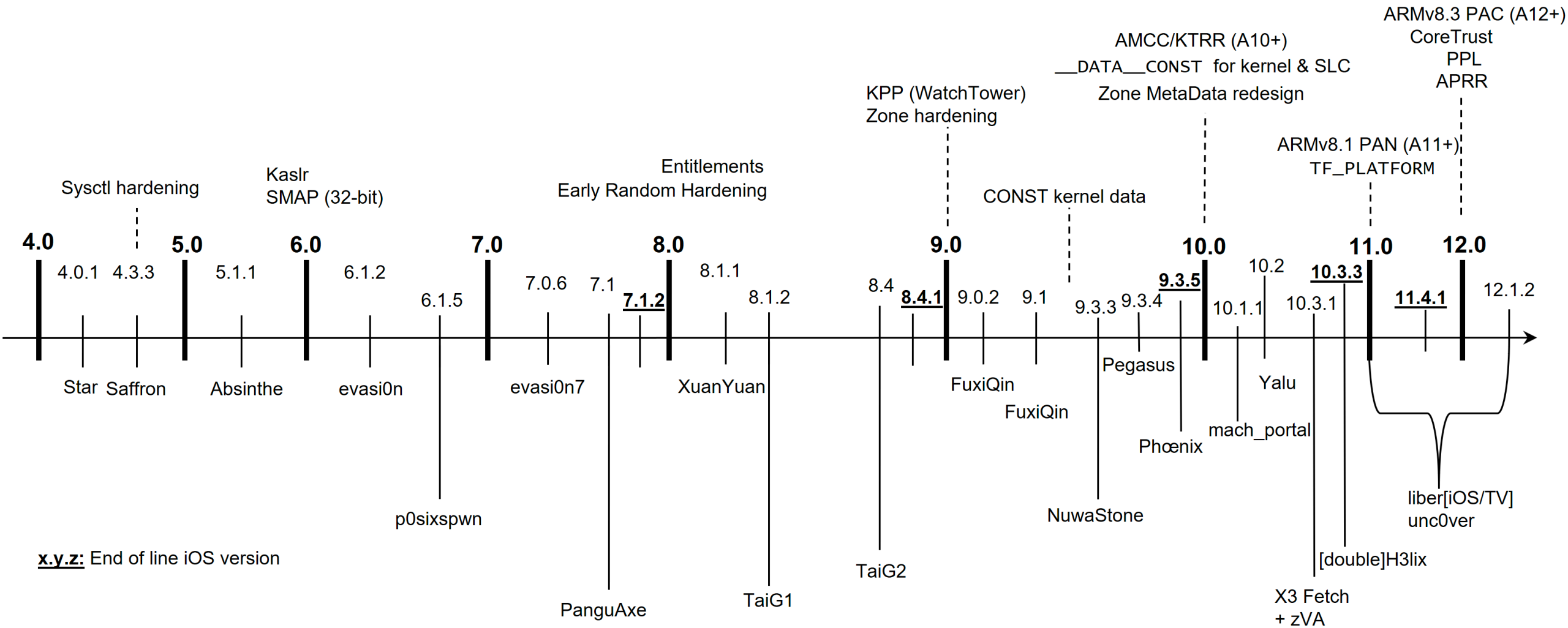
- Last printed version: 1.1.3 (aug 2019)
- **Last gitbook version: 1.4.0 (jan 2022)**

OWASP - Top10 Mobile Risks - 2016

OWASP M1 Improper Platform Usage	OWASP M2 Insecure Data Storage	OWASP M3 Insecure Communication	OWASP M4 Insecure Authentication
OWASP M5 Insufficient Cryptography	OWASP M6 Insecure Authorization	OWASP M7 Client code quality	OWASP M8 Code Tampering
	OWASP M9 Reverse engineering	OWASP M10 Extraneous Functionality	

Jailbreaks

Jailbreak history



Source: http://newosxbook.com

Jailbreaks: iOS 12 -> too old

iOS	Jailbreak Tool	Tool Version	Device															
			iPhone 5s	iPhone 6	iPhone 6 Plus	iPhone 6s	iPhone 6s Plus	iPhone SE (1st generation)	iPhone 7	iPhone 7 Plus	iPhone 8	iPhone 8 Plus	iPhone X	iPhone XR	iPhone XS	iPhone XS Max	iPod touch (6th generation)	iPod touch (7th generation)
12.0	Chimera	1.4.0	Yes															N/A
	unc0ver	5.2.0																
12.0.1	Chimera	1.4.0	Yes															
	unc0ver	5.2.0																
12.1	Chimera	1.4.0	Yes															
	unc0ver	5.2.0																
12.1.1	Chimera	1.4.0	Yes															
	unc0ver	5.2.0																
12.1.2	Chimera	1.4.0	Yes														N/A	
	unc0ver	5.2.0																
12.1.3	Chimera	1.4.0	Yes											Partial			Yes	
	unc0ver	5.2.0	Yes															
12.1.4	Chimera	1.4.0	Yes											Partial			Yes	
	unc0ver	5.2.0	Yes															
12.2	Chimera	1.4.0	Yes											Partial			Yes	
	unc0ver	5.2.0	Yes															
12.3	checkra1n	0.10.2 beta	Yes (Semi-Tethered)											No			Yes (Semi-Tethered)	
	unc0ver	5.3.0	Yes			No												
12.3.1	checkra1n	0.10.2 beta	Yes (Semi-Tethered)											No			Yes (Semi-Tethered)	
	unc0ver	5.3.0	Yes			No												
12.3.2	checkra1n	0.10.2 beta	N/A									Yes (Semi-Tethered)	N/A					
12.4	checkra1n	0.10.2 beta	Yes (Semi-Tethered)											No			Yes (Semi-Tethered)	
	Chimera	1.4.0	Yes											Partial			Yes	

Source: https://www.theiphonewiki.com/wiki/Jailbreak

Jailbreaks: iOS 13 -> too old

iOS	Jailbreak Tool	Tool Version	Device															
			iPhone 6s	iPhone 6s Plus	iPhone SE	iPhone 7	iPhone 7 Plus	iPhone 8	iPhone 8 Plus	iPhone X	iPhone XR	iPhone XS	iPhone XS Max	iPhone 11	iPhone 11 Pro	iPhone 11 Pro Max	iPhone SE (2nd generation)	iPod touch (7th generation)
13.0	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No						N/A	
	unc0ver	4.3.1	Yes															
13.1	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
	unc0ver	4.3.1	Yes															Yes
13.1.1	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
	unc0ver	4.3.1	Yes															Yes
13.1.2	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
	unc0ver	4.3.1	Yes															Yes
13.1.3	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
	unc0ver	4.3.1	Yes															Yes
13.2	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
	unc0ver	4.3.1	Yes														N/A	Yes
13.2.2	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
	unc0ver	4.3.1	Yes															Yes
13.2.3	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
	unc0ver	4.3.1	Yes															Yes
13.3	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
	unc0ver	4.3.1	Yes															Yes
13.3.1	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
13.4	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)
13.4.1	checkra1n	0.10.1 beta	Yes (Semi-Tethered)								No							Yes (Semi-Tethered)

Source: https://www.theiphonewiki.com/wiki/Jailbreak

Jailbreaks: iOS 14 -> ok

iOS	Jailbreak Tool	Tool Version	Device																		
			iPhone 6s	iPhone 6s Plus	iPhone SE (1st generation)	iPhone 7	iPhone 7 Plus	iPhone 8	iPhone 8 Plus	iPhone X	iPhone XR	iPhone XS	iPhone XS Max	iPhone 11	iPhone 11 Pro	iPhone 11 Pro Max	iPhone SE (2nd generation)	iPhone 12 mini	iPhone 12	iPhone 12 Pro	iPhone 12 Pro Max	iPod touch (7th generation)
14.0	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No							N/A				Yes[1]
	unc0ver	6.1.2	Yes																			Yes
	Taurine	1.0.4																				
14.0.1	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No											Yes[1]
	unc0ver	6.1.2	Yes															Yes				
	Taurine	1.0.4																				
14.1	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No											Yes[1]
	unc0ver	6.1.2	Yes																			
	Taurine	1.0.4																				
14.2	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No											Yes[1]
	unc0ver	6.1.2	Yes																			
	Taurine	1.0.4																				
14.2.1	unc0ver	6.1.2	N/A															Yes				N/A
	Taurine	1.0.4																				
14.3	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No											Yes[1]
	unc0ver	6.1.2	Yes																			
	Taurine	1.0.4																				
14.4	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No											Yes[1]
14.4.1	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No											Yes[1]
14.4.2	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No											Yes[1]
14.5	checkra1n	0.12.3 beta	Yes[1]					Yes[1][2]			No											Yes[1]
14.5.1	checkra1n	0.12.3 beta[3]	Yes[1]					Yes[1][2]			No											Yes[1]
14.6	checkra1n	0.12.3 beta[3]	Yes[1]					Yes[1][2]			No											Yes[1]

Source: https://www.theiphonewiki.com/wiki/Jailbreak

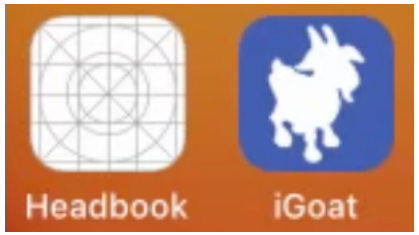
Jailbreaks: iOS 15 -> no public jailbreak !

iOS	Jailbreak Tool	Tool Version	Device																								
			iPhone 6s	iPhone 6s Plus	iPhone SE (1st generation)	iPhone 7	iPhone 7 Plus	iPhone 8	iPhone 8 Plus	iPhone X	iPhone XR	iPhone XS	iPhone XS Max	iPhone 11	iPhone 11 Pro	iPhone 11 Pro Max	iPhone SE (2nd generation)	iPhone 12 mini	iPhone 12	iPhone 12 Pro	iPhone 12 Pro Max	iPhone 13 mini	iPhone 13	iPhone 13 Pro	iPhone 13 Pro Max	iPhone SE (3rd generation)	iPod touch (7th generation)
15.0	No Tool Available													No													No
15.0.1	No Tool Available													No													No
15.0.2	No Tool Available													No												N/A	No
15.1	No Tool Available													No													No
15.1.1	No Tool Available		N/A															No								N/A	
15.2	No Tool Available													No													No
15.2.1	No Tool Available													No												N/A	No
15.3	No Tool Available													No													No
15.3.1	No Tool Available													No													No
15.4	No Tool Available														No												
15.4.1	No Tool Available														No												
15.5	No Tool Available														No												

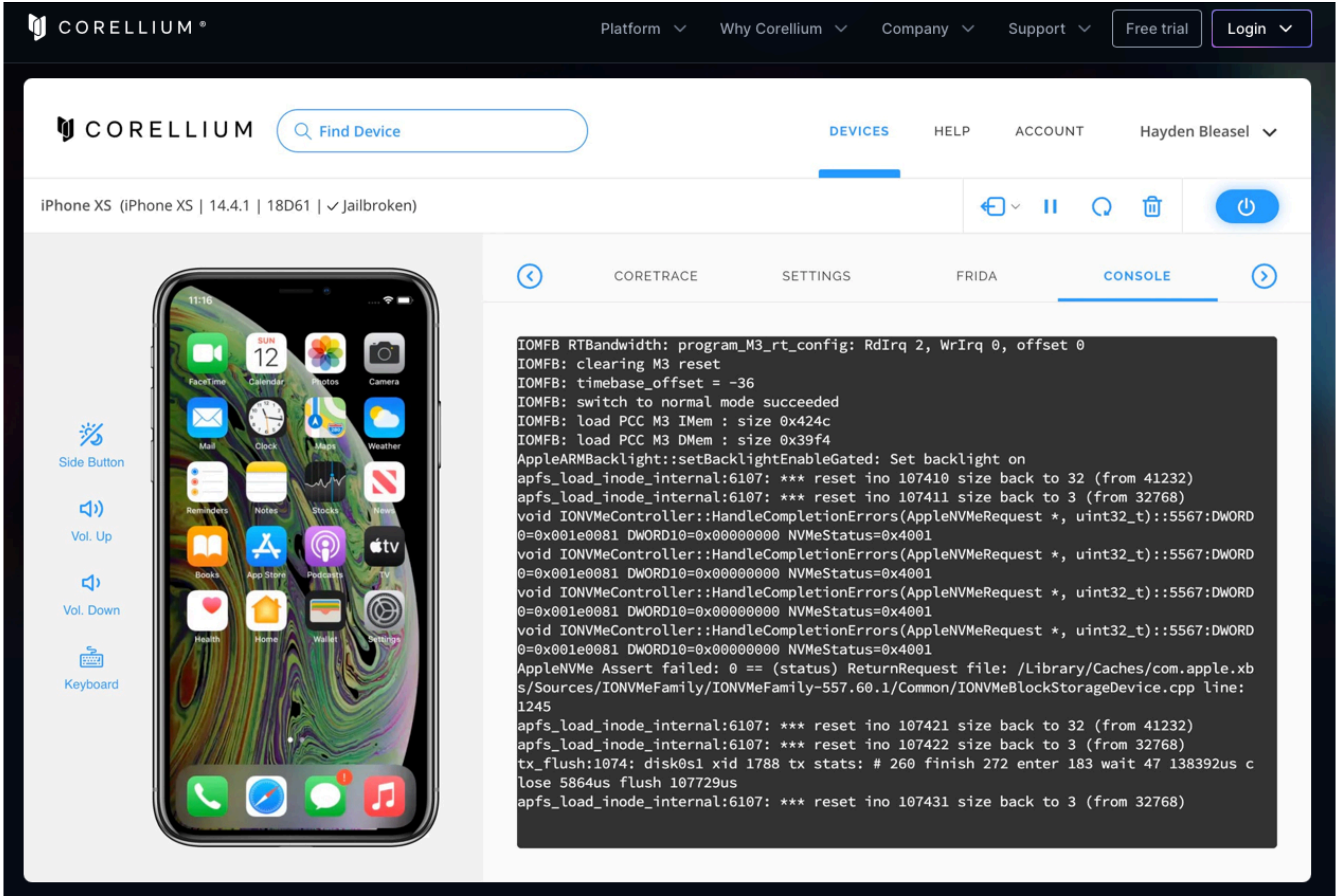
Source: https://www.theiphonewiki.com/wiki/Jailbreak

Testing environnement

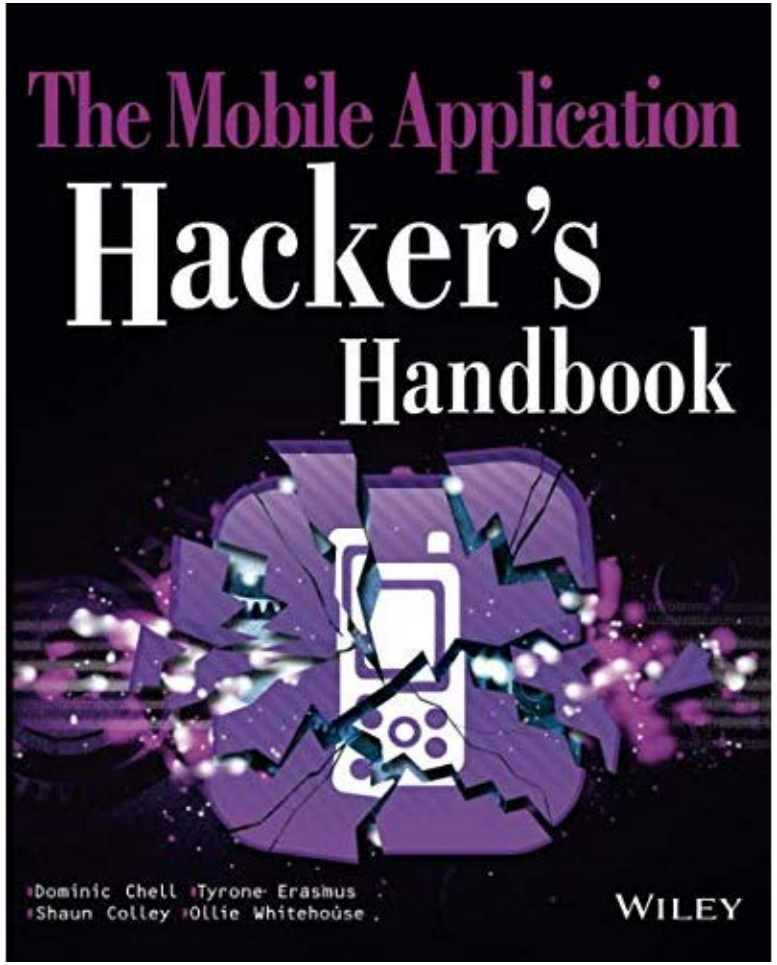
- For this workshop, we are going to use

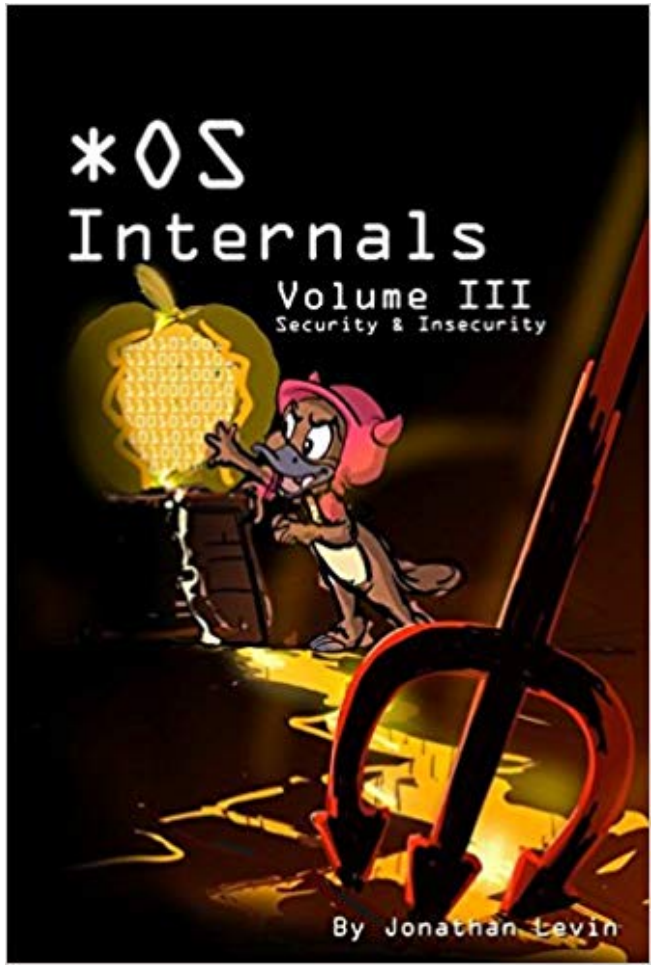


- No setup, no VM, only a web browser (Chrome recommended for H264 video streaming support)


CORELLIUM
Platform
Why Corellium
Company
Support
Free trial
Login
CORELLIUM
Find Device
DEVICES
HELP
ACCOUNT
Hayden Bleasel
iPhone XS (iPhone XS | 14.4.1 | 18D61 | ✓ Jailbroken)
Side Button
Vol. Up
Vol. Down
Keyboard
CORETRACE
SETTINGS
FRIDA
CONSOLE
IOMFB RTBandwidth: program_M3_rt_config: RdIrq 2, WrIrq 0, offset 0
IOMFB: clearing M3 reset
IOMFB: timebase_offset = -36
IOMFB: switch to normal mode succeeded
IOMFB: load PCC M3 IMem : size 0x424c
IOMFB: load PCC M3 DMem : size 0x39f4
AppleARMBacklight::setBacklightEnableGated: Set backlight on
apfs_load_inode_internal:6107: *** reset ino 107410 size back to 32 (from 41232)
apfs_load_inode_internal:6107: *** reset ino 107411 size back to 3 (from 32768)
void IONVMeController::HandleCompletionErrors(AppleNVMeRequest *, uint32_t)::5567:DWORD0=0x001e0081 DWORD10=0x00000000 NVMeStatus=0x4001
void IONVMeController::HandleCompletionErrors(AppleNVMeRequest *, uint32_t)::5567:DWORD0=0x001e0081 DWORD10=0x00000000 NVMeStatus=0x4001
void IONVMeController::HandleCompletionErrors(AppleNVMeRequest *, uint32_t)::5567:DWORD0=0x001e0081 DWORD10=0x00000000 NVMeStatus=0x4001
void IONVMeController::HandleCompletionErrors(AppleNVMeRequest *, uint32_t)::5567:DWORD0=0x001e0081 DWORD10=0x00000000 NVMeStatus=0x4001
AppleNVMe Assert failed: 0 == (status) ReturnRequest file: /Library/Caches/com.apple.xbs/Sources/IONVMeFamily/IONVMeFamily-557.60.1/Common/IONVMeBlockStorageDevice.cpp line: 1245
apfs_load_inode_internal:6107: *** reset ino 107421 size back to 32 (from 41232)
apfs_load_inode_internal:6107: *** reset ino 107422 size back to 3 (from 32768)
tx_flush:1074: disk0s1 xid 1788 tx stats: # 260 finish 272 enter 183 wait 47 138392us close 5864us flush 107729us
apfs_load_inode_internal:6107: *** reset ino 107431 size back to 3 (from 32768)

To go further 📚

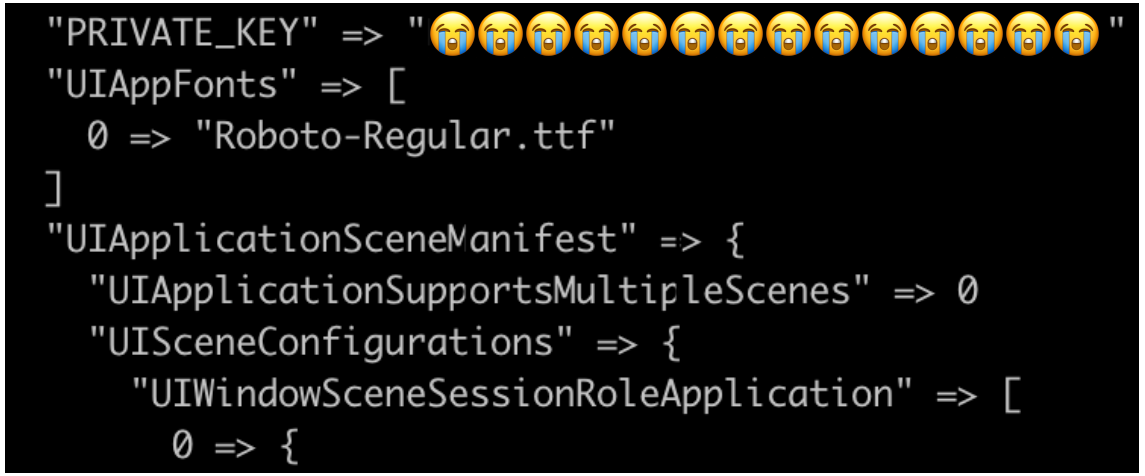




Static analysis

Example of requirement: **MSTG-CRYPTO-1**

The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.



OWASP M5
Insufficient
Cryptography

Lab1: App metadata

OWASP M9 Reverse engineering

Goal: analyze Info.plist

If it is not installed**, install **`Headbook`

1. *On the "Apps" tab and click on "Install"*
2. *Select the **`Headbook.ipa`** file (IPA file is in the GitHub repo)*

1. Open **`Info.plist`** (no need to launch the app on the GUI)

   `plconvert Info.plist Info.plist.txt`

   But where is **`Info.plist`** ??? (see next slide to find it)

2. Submit the flag to https://ctf.ivrodriguez.com

Lab2: Find the Bundle directory

OWASP M9 Reverse engineering

Goal: find the Bundle directory and Info.plist

1. Find the bundle directory for **Headbook** – **the manual way**:

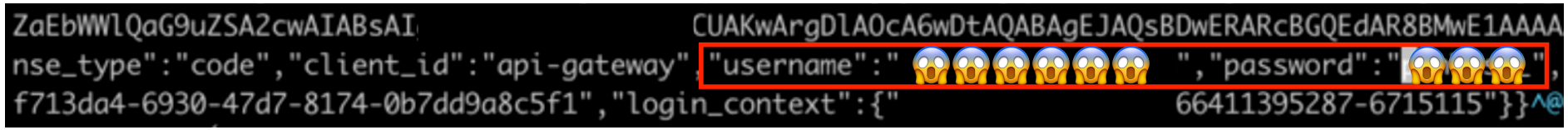
iOS10 and over = **/User/Library/FrontBoard/applicationState.db**

```
iPhone:~ root# sqlite3
/User/Library/FrontBoard/applicationState.db
sqlite> select * from kvs;
(…)
165|98|3|bplist00□Tguid_installInstanceIDTvers_$37341D29-82CE-
4E70-ADDF-
DC16E277AA9D_afile:///private/var/containers/Bundle/Application/
D3A516AB-C416-4E42-803C-06E0347950C5/Headbook.app
(…)
```

Data security

Example of requirement: **MSTG-STORAGE-1**

System credential storage facilities are used appropriately to store sensitive data, such as PII, user credentials or cryptographic keys.



OWASP M2 Insecure data storage

Lab3: Cleartext Property List Files (Plist)

OWASP M2 Insecure data storage

Goal: find credentials stored in cleartext

***If it is not installed**, install `iGoat`*

1. *On the "Apps" tab and click on "Install"*
2. *Select the `iGoat.ipa` file (IPA file is in the GitHub repo)*

1. Open **iGoat**
2. Go to "Data Protection (Rest) / **Plist Storage** "
3. Click "Start", enter random credentials & click "Verify"

Solution: the credentials are stored in `Documents/Credentials.plist`

But where is `Credentials.plist` ??? (see next slide to find it)

Lab4: Find the Data directory

OWASP M2 Insecure data storage

Goal: find the Data directory

1. On the “Frida” tab, select “iGoat” and “Attach”
2. On the “Scripts” tab load **`frida.js`** script (JS file is in the GitHub repo) and “Execute”, go back to “Console” tab and type **`appInfo()`**

```
[Remote::PID::607]-> appInfo()
{
    "Binary": "/private/var/containers/Bundle/Application/D1A2A1C1-7E07-4B4A-AD10-68F6996F99F9/iGoat.app/iGoat",
    "Bundle": "/private/var/containers/Bundle/Application/D1A2A1C1-7E07-4B4A-AD10-68F6996F99F9/iGoat.app",
    "Bundle ID": "com.swaroop.iGoat",
    "Data": "/private/var/mobile/Containers/Data/Application/CEDEB20A-65BA-4207-A353-CF690563A900",
    "Name": "iGoat",
    "Version": "1"
}
```

Lab5: fsmon-ios

OWASP M2 Insecure data storage

Goal: find files used by an app

1. Open **iGoat**
2. Go to “Data Protection (Rest) / **Cookie Storage** ”
3. Click “Start”
4. Enter info
5. Click “Verify”
6. Where is stored the answer ?

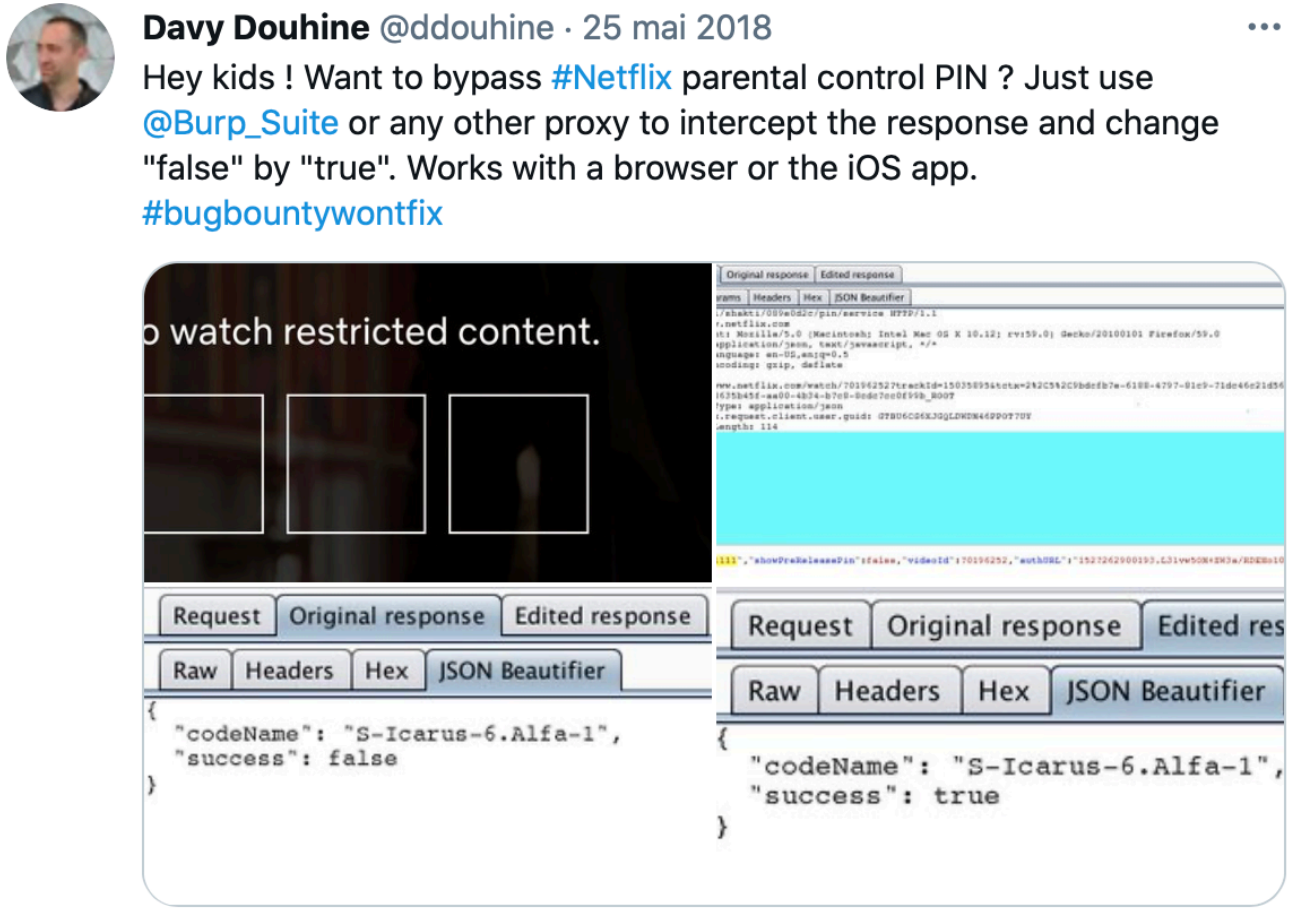
Use **`fsmon-ios`** to find it:

```
/var/root/fsmon-ios -P iGoat
```

Execution analysis

Example of requirement: **MSTG-ARCH-2**

Security controls are never enforced only on the client side



OWASP M8 code tampering

Hooking

cycript

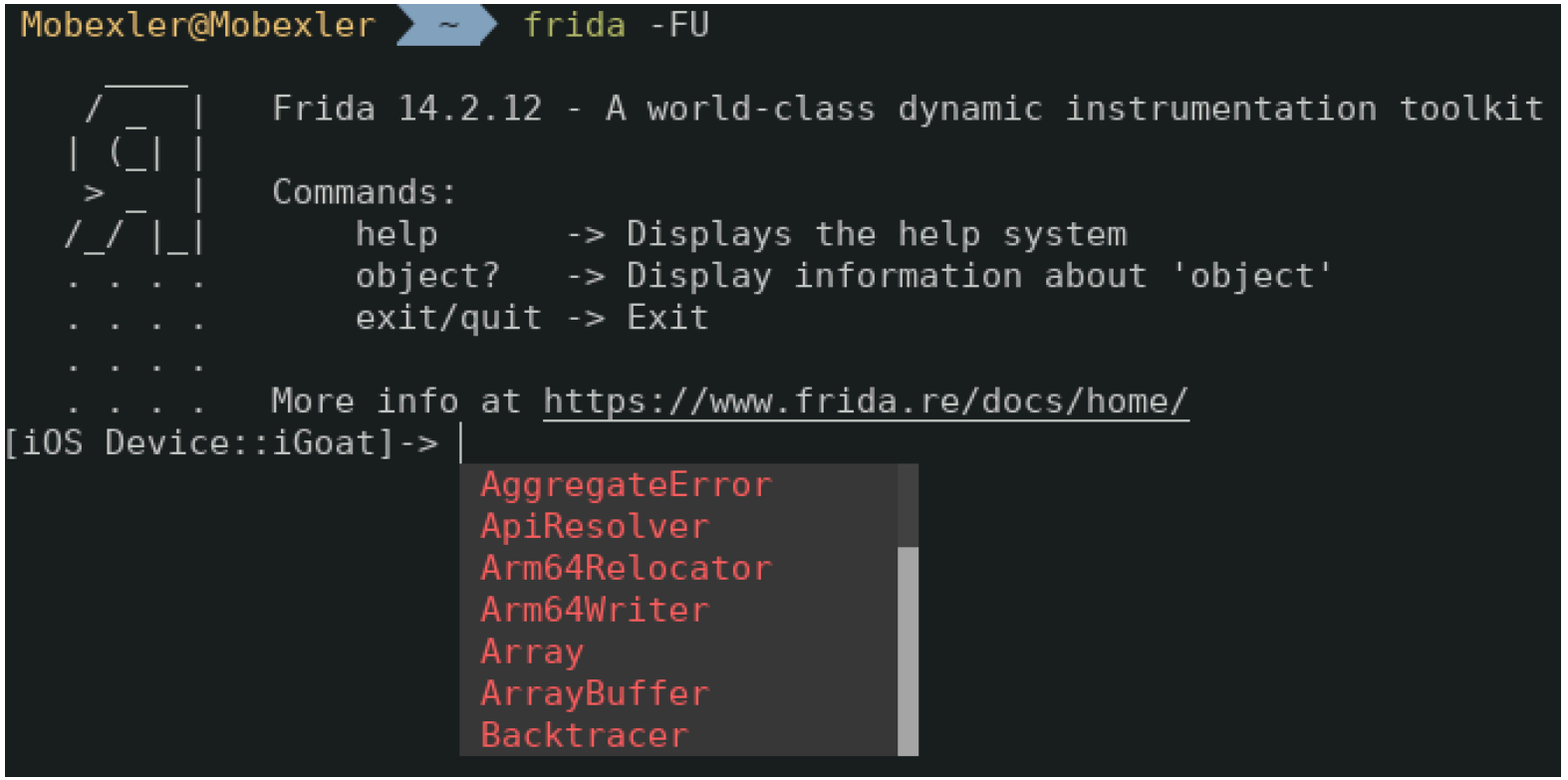
Cycript allows developers to explore and modify running applications on either iOS or Mac OS X using a hybrid of Objective-C++ and JavaScript syntax through an interactive console that features syntax highlighting and tab completion.
(It also runs standalone on Android and Linux and provides access to Java, but without injection.)

FRIDA

OVERVIEW DOCS NEWS CODE CONTACT

Inject JavaScript to explore native apps on Windows, macOS, Linux, iOS, Android, and QNX.

Frida


Mobexler@Mobexler ~ frida -FU
Frida 14.2.12 - A world-class dynamic instrumentation toolkit
Commands:
help -> Displays the help system
object? -> Display information about 'object'
exit/quit -> Exit
More info at https://www.frida.re/docs/home/
[iOS Device::iGoat]->
AggregateError
ApiResolver
Arm64Relocator
Arm64Writer
Array
ArrayBuffer
Backtracer

Frida: CodeShare

iOS DataProtection

7 | 4K

Uploaded by: @ay-kay

List iOS file data protection classes (NSFileProtectionKey) of an app

PROJECT PAGE

aesinfo

7 | 5K

Uploaded by: @dzonerzy

Show useful info about AES encryption/decryption at application runtime

PROJECT PAGE

frida-multiple-unpinning

5 | 4K

Uploaded by: @akabe1

Another Android ssl certificate pinning bypass script for various methods (https://gist.github.com/akabe1/5632cbc1cd49f0237cbd0a93bc8e4452)

PROJECT PAGE

ObjC method observer

4 | 8K

Uploaded by: @mrmacete

Observe all method calls to a specific class (e.g. observeClass('LicenseManager')) , or dynamically resolve methods to observe using ApiResolver (e.g. observeSomething('*[* *Password:*]')). The script tries to do its best to resolve and display input parameters and return value. Each call log comes with its stacktrace.

PROJECT PAGE

Frida: CodeShare: ObjC-method-observer

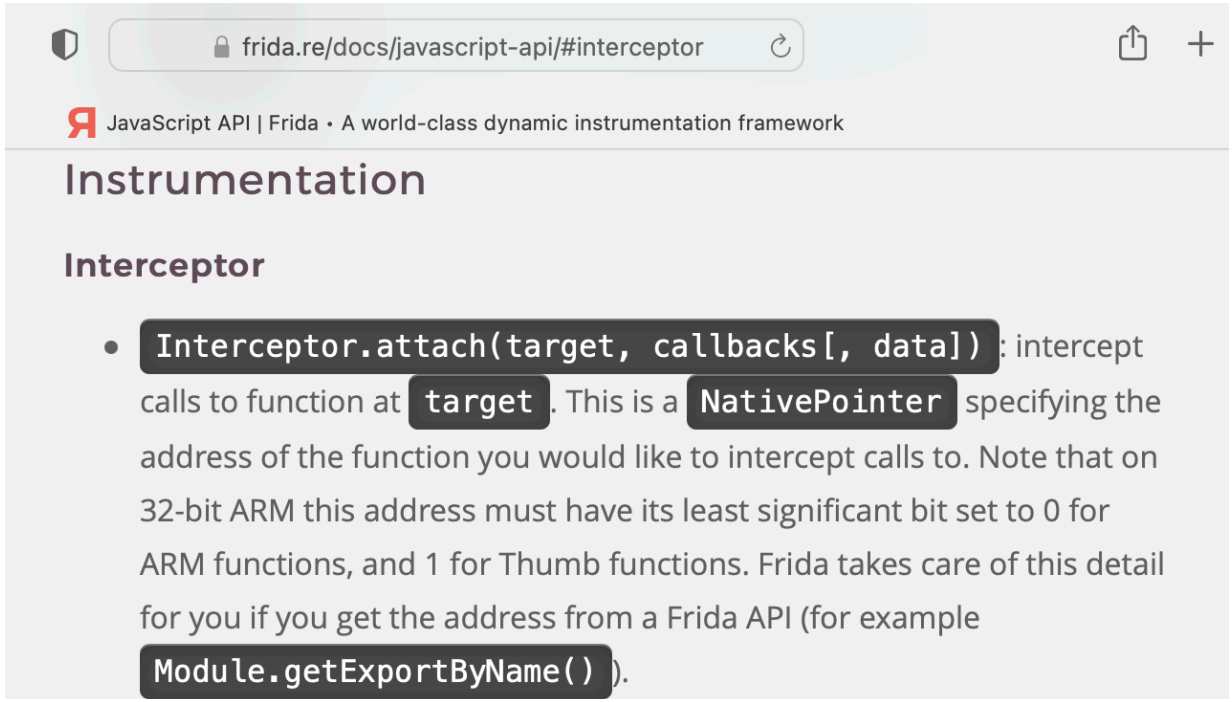
```
Mobexler@Mobexler ~ frida -FU -l frida.js

     ____
    / _  |   Frida 14.2.12 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://www.frida.re/docs/home/
[iOS Device::iGoat]-> observeSomething('*[* *fileExists*]');
Observing  -[NSURL cls_fileExists]
Observing  -[PFUbiquityLocation fileExistsAtLocation]
Observing  -[PFUbiquityLocation fileExistsAtLocationWithLocalPeerID:error:]
Observing  +[CIRedEyeRepair2 fileExistsAtPath:]
Observing  -[NSFileManager fileExistsAtPath:]
Observing  -[NSFileManager fileExistsAtPath:isDirectory:]
Observing  -[NSFileManager _web_fileExistsAtPath_nowarn:isDirectory:traverseLink:]
Observing  -[MBFileManager fileExistsAtPath:]
[iOS Device::iGoat]->
```

Frida: CodeShare: ObjC-method-observer

```
[Remote::iGoat]-> (0x28387c060)  -[NSFileManager fileExistsAtPath:]
fileExistsAtPath: /var/mobile/Containers/Data/Application/87057B91-EC0F-4EDB-917C-B237619AFBF1/Documents/Credentials.plist (NSPathStore2)
0x102aaeff0 iGoat!0xd6ff0
0x1a41f1448 UIKitCore!-[UIViewController _sendViewDidLoadWithAppearanceProxyObjectTaggingEnabled]
0x1a41f5f58 UIKitCore!-[UIViewController loadViewIfRequired]
0x1a41f6360 UIKitCore!-[UIViewController view]
0x102a6a074 iGoat!0x92074
0x102a69dbc iGoat!0x91dbc
0x102a5eb6c iGoat!0x86b6c
0x1a4965e3c UIKitCore!-[UIStoryboardSegueTemplate _performWithDestinationViewController:sender:]
0x1a4965d4c UIKitCore!-[UIStoryboardSegueTemplate _perform:]
0x1a4966018 UIKitCore!-[UIStoryboardSegueTemplate perform:]
0x1a48119ac UIKitCore!-[UIApplication sendAction:to:from:forEvent:]
0x1a3f0e318 UIKitCore!-[UIBarButtonItem(UIInternal) _sendAction:withEvent:]
0x1a48119ac UIKitCore!-[UIApplication sendAction:to:from:forEvent:]
0x1a4247fbc UIKitCore!-[UIControl sendAction:to:forEvent:]
0x1a4248320 UIKitCore!-[UIControl _sendActionsForEvents:withEvent:]
0x1a4248450 UIKitCore!-[UIControl _sendActionsForEvents:withEvent:]
RET: 0x1
```

Frida: Interceptor



The `callbacks` argument is an object containing one or more of:

- `onEnter(args)`: callback function given one argument `args` that can be used to read or write arguments as an array of `NativePointer` objects. {: #interceptor-onenter}
- `onLeave(retval)`: callback function given one argument `retval` that is a `NativePointer`-derived object containing the raw return value. You may call `retval.replace(1337)` to replace the return value with the integer `1337`, or `retval.replace(ptr("0x1234"))` to replace with a pointer. Note that this object is recycled across *onLeave* calls, so do not store and use it outside your callback. Make a deep copy if you need to store the contained value, e.g.: `ptr(retval.toString())`.

Frida basics

List running processes on a **device connected on the network**

```
frida-ps -H <IP>
```

List running processes on a **device connected with USB**

```
frida-ps -U
```

Inject Frida in appName's process

```
frida -U <appName>
```

Inject Frida in appName's process and load `frida.js` file

```
frida -U <appName> -l frida.js
```

Inject Frida in the foreground app process and load `frida.js` file

```
frida -FU -l frida.js
```

Frida scripts (credit: https://github.com/interference-security)

Show binarycookies

Script: `show_binarycookies.js`

Usage: `show_binarycookies()`

Show classes

Script: `find-app-classes.js`

Usage: `show_app_classes_only()`

Show classes and their methods

Script: `find-app-classes-methods.js`

Usage: `show_app_classes_methods_only()`

Frida scripts (credit: https://github.com/interference-security)

Find a method

Script: **find-specific-method.js**

Usage: **find_specific_method_in_all_classes("function_name_here")**

Ex:

```
[Remote::PID::607]->
find_specific_method_in_all_classes("checkPin")
[*] Started: Find Specific Method in All Classes
[Remote::PID::607]-> [+] Class: BruteForce
        [-] Method: - checkPin:
                [-] Arguments Type: pointer,pointer,pointer
                [-] Return Type: bool
[*] Completed: Find Specific Method in All Classes
```

Frida scripts (credit: https://github.com/interference-security)

Modify a return value

Script: **`show-modify-method-return-value.js`**

Usage: **`show_modify_function_return_value("CLASS",”METHOD")`**

Ex: **`show_modify_function_return_value("BruteForce",”-checkPin:")`**

```
//For modifying the return value
var newretval = ptr("0x0") //your new return value here
retval.replace(newretval)
```

Return value is hardcoded :/

-> You’ll have to modify the script to meet your specific goal.

Frida scripts (credit: https://github.com/interference-security)

```
function modify_function_return_value(className_arg, funcName_arg, returnvalue_arg)
{
    var className = className_arg;
    var funcName = funcName_arg;
    var returnvalue = returnvalue_arg;
```

Modify a return value

Script: **modify-method-return-value.js**

Usage: **modify_function_return_value("CLASS","METHOD","VALUE")**

Ex:

```
[Re::PID::607]-> modify_function_return_value("BruteForce","-checkPin:","1")
[*] Class Name: BruteForce
[*] Method Name: - checkPin:
        [-] Type of return value: object
        [-] Return Value: 0x0
        [-] New Return Value: 1
```

Lab6: PIN bypass with Frida

OWASP M8 code tampering

Goal: bypass a security check using Frida

Steps:

1. Open **iGoat**
2. Go to “Runtime Analysis” / “**Runtime Brute force attack**” and “Start”
3. Find the **class** and the **method** used to check the PIN code
4. Instrument iGoat using `frida` to modify the value

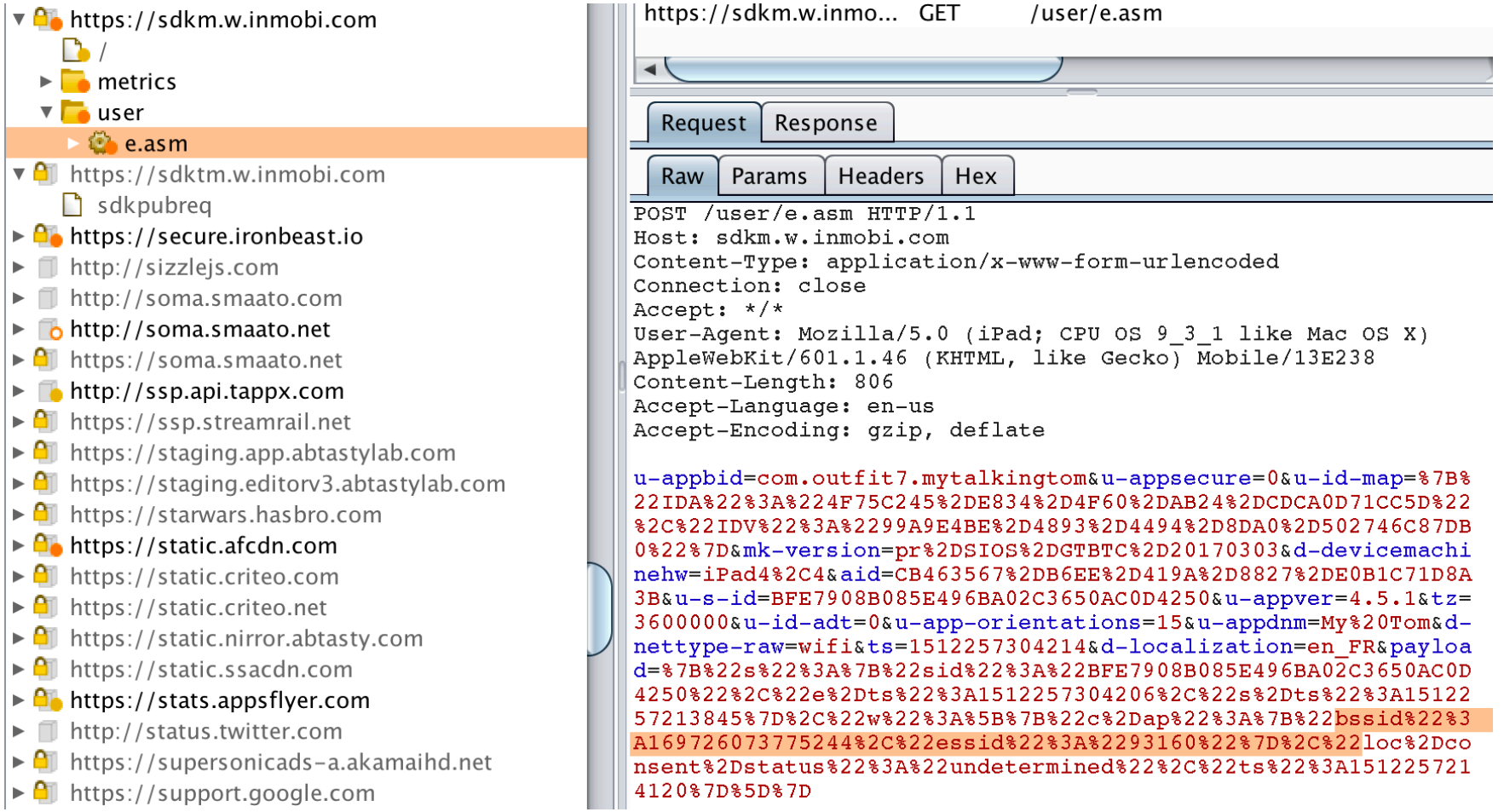
Transport security

iOS - Network monitoring techniques

Technique	Tool	SSL/TLS decryption	iOS support	Mac needed ?	Jailbreak needed ?	Limitations /remarks
Proxying	Proxy (Burp)	No	Any	No	No	No traffic if pinning or if app doesn't use system proxy settings
Proxying + SSL pinning bypass	Proxy (Burp) + SSL KillSwitch or Frida	Yes	Any	No	Yes	No traffic if app doesn't use system proxy settings
Proxying + SSL pinning bypass	Proxy (Burp) + Frida	Yes	Any	Yes	No	No traffic if app doesn't use system proxy settings
Mirroring	rvictl	No	Any	Yes	No	Can't repeat traffic
Mirroring	rvi_capture	No	Any	No	No	Can't repeat traffic
Mirroring	Named pipes	No	Any	No	Yes	Can't repeat traffic
VPN	iOS app (eg: Charles Proxy)	Yes	Any	No	No	Can't repeat traffic
WebView hooking	NetworkSniffer	Yes	Any	Yes	Yes	Can't repeat traffic

Example of requirement: **MSTG-STORAGE-4**

No *sensitive data is shared third parties*



OWASP M3
Insecure Communication

Lab7: network capture with **Frida**

OWASP M3
Insecure Communication

Goal: analyze network communications

Steps:

1. Open **iGoat**
2. Go to “Data Protection (Transit)” / “**Public Key Pinning**” and “Start”
3. On the “Scripts” tab load `spit_ios.js` script (JS file is in the GitHub repo) and “Execute”, go back to “Console” tab
4. Click on Submit

Questions