Modern iOS Pentesting: No Jailbreak Needed

presented by Noah Farmer, Senior AppSec Engineer at Dvuln

Some stuff you'll probably recognise

ildb 🛜	23:03	59
	JailbreakMe	2
	Cydia ay Freeman (saurik) ailbreak by comex.	FREE
JailbreakN your devid be, fully c with every imagine.	le is the easiest wa ce. Experience iOS a ustomizable, theme v tweak you could p	y to free as it could eable, and ossibly
Safe and o restore in control ov takes a m completel	completely reversib iTunes), jailbreakin er the device you o inute or two, and a y free.	le (just g gives you wn. It only s always, it's
Please ma	ike an iTunes backu	up before
<	> + C	n c

JailbreakMe (2011) - iOS 4

@comex

	redsn0w 0.9.10b7			
Welcome! This is t	he latest version of redsn0w.			
Copyright 2007–20 for commercial use	12 iPhone Dev-Team. All rights reserved. Not			
For support, visit <u>o</u>	ur blog or try searching JailbreakQA.			
Extras				
Just boot	Just boot tethered right now.			
Pwned DFU	Enter pwned DFU mode in preparation for restoring to a custom IPSW via iTunes.			
Recovery fix	Get out of Recovery Mode caused by an iTunes restore error.			
SHSH blobs	Fetch, verify or use SHSH blobs.			
Select IPSW	Manually specify an IPSW.			
Custom IPSW	Preserve baseband with a custom IPSW.			
Even more	Even more extras, including user preferences.			

redsnOw (2012) - iOS 4 - 6 iPhone Dev-Team

Why did *most* people jailbreak?

- Custom themes (changing the look of the entire device)
- Super cool tweaks (remember Barrel/Cylinder??)
- Carrier unlocking





So.. what got *me* into jailbreaking?

- Had a Minecraft Pocket Edition server shared with classmates in year 5
- Annoyed with being locked in survival mode, wanted free diamonds
- Did some Googling...





Fast forward to today...

 Here I am working in cybersecurity, often tasked with pentesting mobile applications

MASTG

Mobile Application Security Testing Guide



My toolsuite

objection - Runtime Mobile Exploration

objection is a runtime mobile exploration toolkit, powered by Frida, built to help you assess the security posture of your mobile applications, without needing a jailbreak.

twitter @leonjza pypi package 1.11.0 Black Hat Arsenal Europe 2017 Black Hat Arsenal USA 2019

- · Supports both iOS and Android.
- Inspect and interact with container file systems.
- Bypass SSL pinning.
- Dump keychains.
- Perform memory related tasks, such as dumping & patching.
- Explore and manipulate objects on the heap.
- And much, much more

Screenshots are available in the wiki.

OBJECTION
EXPLORATION
GIT.IO/OBJECTION

FSIDA

These help to cover pretty much every MASTG checklist item, and more...

Installing was pretty simple...

• II Jio 🗢 9:59 PM € 🖲 95% 🛃	[noshformer@Noshe MasPook Dro no isilbreak required & objection g cam cup? modernics evalers
User Expert Recent	Checking for a newer version of objection Using USB device `iPhone` Agent injected and responds ok!
Filza File Manager from BigBoss (Utilities) File Manager for iPhone, iPad, iPod Touc	
Frida from build.frida.re (Development) Inject JavaScript to explore iOS apps ov	Runtime Mobile Exploration by: @leonjza from @sensepost
H	[tab] for command suggestions
From A AProfessor & (Tweaks) Global Jailbreak Detection Bypass	com.cyn8.modernios on (iPhone: 17.6.1) [usb] #
l S	
IPA Installer from BigBoss (Utilities) Install IPA files directly from device	Ready to test!
From BigBoss (Utilities) Install IPA from the command line	
Cydia Sources Changes Installed Search	

...but now?

MOBILE



Unfortunately, jailbreaking has lost its community.

Google Trends data for "iOS Jailbreaking" shows a pretty obvious decline... why?



Apple's security bounties are among some of the highest in the industry

Network attack Device & without user-ins user interaction	Zero-click radio to kernel with physical proximity	\$5,000 – \$500,000	~	
	Zero-click unauthorized access to sensitive data	\$5,000 – \$500,000	~	~
	Zero-click kernel code execution with persistence and kernel PAC bypass	\$100,000 - \$1,000,000	~	~
			<u></u>	

Example: CVE-2024-23208

- Affected iOS (iPad/iPhone), macOS, tvOS, and watchOS
- Allows arbitrary code execution with kernel privileges.. also known as a jailbreak
- Submitted to Apple, and patched in iOS 17.3 :(

Ē	support.apple.com	5
Kernel		
Available for: iPhone XS and later, iPad Pro 1 11-inch 1st generation and later, iPad Air 3rd mini 5th generation and later	2.9-inch 2nd generation and later, iPad Pro 10.5- generation and later, iPad 6th generation and la	-inch, iPad Pro ter, and iPad
Impact: An app may be able to execute arbit	rary code with kernel privileges	
Description: The issue was addressed with in	mproved memory handling.	
CVE-2024-23208: fmyy(@binary_fmyy) and	lime From TIANGONG Team of Legendsec at QI	-ANXIN Group

Tweaks are now Features

- Vmoji by @vintendo became "Emoji" in iOS 5
- SBSettings by @BigBoss became "Control Center" in iOS 7
- StickerMe by Alexander Laurus became "Stickers" in iOS 10
- Noctis by @LaughingQuoll became "Dark Mode" in iOS 13

...you get the point



Yes, it's still a thing. But...

Here's where your pentesting devices are coming

from... ●**○**● □ - < A facebook.com CMH 46 ads CMH **Highly Rated** Eric 😥 н Hi, I'm interested in "iPhone X_100% Like New ". Is this still available? If so, when and where can I pick it up? Cheers. Hi, I'm interest Gold Good Cor available? If so I consent to receive marketing and third party I pick it up? Ch offers from Gumtree I consent to rece 0 Sign in to offers from Gum \frown message \bigcirc J 9113 Show number 2 Sign in to make an offer Sign in t \$ 280 \$ 199 Safety and security tips 3 7 images ~ Be wary of fake, locked or Safet 2 images stolen phones. Conduct a ~ Be war phone IMEI check and always stolen inspect in person before you 6 views 1 Post Similar Ad Report Ad Share Save phone commit. Find more helpful 🕒 Post Similar Ad 🖓 Report Ad 👒 Share 🖤 Save inspec hints here. 6 views commi hints h 0 Deep dive into vour Xbox stats LEARN MORE Deep dive into todav! your Xbox stats LEARN MORE today! iPhone X_100% 🔄 Like New iPhone 8 64G Gold Good Condition Warranty NO SIM LOCK \$280 thmater 📖 🕤 \$199 Lakemba, NSW WINCO AN AFIRST Stretton, QLD

WINCO AN FIRST

Go

Even if you had these devices...



iOS 16+

Focus Filters iOS 16+ SharePlay API iOS 15+

...just to name a few

The usual setup



iPhone X running iOS 14.4.1

Can pentest most apps: 🔽

...but not this time

- Contract signed
- Testing dates locked in
- iOS device jailbroken and ready
- No IPA provided (black-box), so we'll install the app from the App Store...



Dead end?

Apple's gift to pentesting: get_task_allow

- Special entitlement, which you can enable when signing (or re-signing) an application
- Allows external processes, like a debugger, to attach themselves to the application using a special function called task_for_pid().
- Once attached, we can read/write memory, and inject our own code into the application.

What does this have to do with jailbreaking?

- What's the first thing a jailbreak has to achieve? tfp0
- tfp0 (short for task_for_pid(0)), gives you access to read & write memory of the kernel (pid = 0)
- If you can read/write the kernel's memory, you have the foundations for a full device jailbreak!

But, we don't need a full-device jailbreak.

If we can re-sign an application with this get_task_allow entitlement... we can achieve code execution, memory read/write, and more... just for that single application.

Therefore, this entitlement allows us to gain a "jailbreak-like" state, limited to a single application sandbox.



Not fair, FairPlay!

- Unfortunately, you can't just pull the application, resign it with that entitlement, and go about your day.
- If you did, your app sadly won't open, and you'll be greeted nice little messages like these:

ption> Details	
:fairplayOpen() failed, e	rror -42022
	ption> Details

Why does this happen?

- Apple encrypts App Store applications with FairPlay DRM
- When you download from the App Store, the IPA is encrypted with a key tied to your Apple ID
- When re-signing (entitlements or not), you break the digital signature of the IPA, and thus:

AppleFairplayTextCrypterSession::fairplayOpen() failed, error -42022

No application for you!

Fortunately, all is not lost

- Yes, FairPlay is annoying but it is crucial for protecting IP
- There are a number of methods to decrypt and remove FairPlay DRM, such as frida-ios-dump, Clutch, FoulDecrypt, and Iridium - all of which require a jailbreak

But wait!

- The app won't run on my jailbroken iOS 14 device
- We need the decrypted IPA to go any further...
- Decrypting requires a jailbreak... are we stuck? No!
- The solution?

Static Decryption!

1 extern int mremap_encrypted(caddr_t addr, size_t len, 2 uint32_t cryptid, uint32_t cputype, 3 uint32_t cpusubtype);

Static Decryption

- We use a system function, mremap_encrypted(), to decrypt a binary
 on the disk.
- That means, the app doesn't have to be able to run, and we don't need to dump it from memory.
- All we need is a jailbroken environment to run the function.

So, what does that mean?

To decrypt, all we have to do is:

- 1. Trick the device into installing the app by changing the minimum required iOS version
- 2. Use a decryption tool that utilises mremap_encrypted() such as Iridium, FlexDecrypt, or FoulDecrypt
- 3. Profit!

For the sake of simplicity...





Jailbreak 2.0 - Adding our entitlements

- Now, we can take the final crucial step, enabling the get-task-allow entitlement.
- Fortunately, iOS App Signer (available on GitHub), makes this pretty easy:

• • •	iOS App Signer					
Input File:	File path or URL accepted	Browse				
Signing Certificate:	Apple Development: Noah Farmer	0				
Provisioning Profile:	iOS Team Provisioning Profile: com.cyn8.modernios					
New Application ID:	com.cyn8.modernios					
App Display Name:	This changes the app title on the home screen					
App Version:	This changes the app version number 🛛 Ignore Plu	ıglns folder				
	✓ No get-ta	sk-allow				
App Short Version:	This changes the app short version number	Start				
Selected provisionin	ng profile com.cyn8.modernios					

Jailbreak 2.0 - Time to hook!

[noahfarmer@Noahs-MacBook-Pro no-jailbreak-required % objection -g com.cyn8.modernios explore Checking for a newer version of objection...

Using USB device `iPhone`

Agent injected and responds ok!



We have execution on the latest iOS!

Runtime Mobile Exploration by: @leonjza from @sensepost

[tab] for command suggestions com.cyn8.modernios on (iPhone: 17.6.1) [usb] #

Feels like home :-)

[noahfarmer@Noahs-MacBook-Pro no-jailbreak-required % objection -g com.cyn8.modernios explore Using USB device `iPhone`



MASTG covered: 🗹 Pentest completed: 🜌

Runtime Mobile Exploration by: @leonjza from @sensepost

[tab] for c	command	suggestions							
[com.cyn8.mc	odernios	on (iPhone: 17.6.	1) [us	b] # pw	/d				
Current dir	ectory:	/private/var/cont	ainers	/Bundle	Application/EB			. app	
[com.cyn8.mc	odernios	on (iPhone: 17.6.	1) [us	b] # ls					
NSFileType	Perms	NSFileProtection	Read	Write	Owner	Group	Size	Creation	Name
Regular	420	None	True	False	_installd (33)	_installd (33)	21.9 KiB	2024-05-21 08:22:52 +0000	.png
Regular	420	None	True	False	_installd (33)	_installd (33)	2.0 KiB	2024-05-21 08:22:52 +0000	ng
Regular	420	None	True	False	_installd (33)	_installd (33)	33.3 KiB	2024-05-21 08:22:52 +0000	The second se
Directory	493	None	True	False	installd (33)	installd (33)	96.0 B	1970-01-01 00:00:00 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	8.2 KiB	2024-05-21 08:22:52 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	262.8 KiB	2024-05-21 08:22:52 +0000	
Directory	493	None	True	False	installd (33)	installd (33)	128.0 B	1970-01-01 00:00:00 +0000	
Directory	493	None	True	False	installd (33)	installd (33)	96.0 B	1970-01-01 00:00:00 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	92.3 KiB	2024-05-21 08:22:52 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	2.8 KiB	2024-05-21 08:22:52 +0000	
Directory	493	None	True	False	installd (33)	installd (33)	128.0 B	1970-01-01 00:00:00 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	241.4 KiB	2024-05-21 08:22:52 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	9.0 KiB	2024-05-21 08:22:52 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	262.3 KiB	2024-05-21 08:22:52 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	9.0 KiB	2024-05-21 08:22:52 +0000	
Regular	420	None	True	False	installd (33)	installd (33)	225 0 KiB	2024-05-21 08:22:52 +0000	State and a state of the state

Summary

- Black-box pentest, no IPA file given
- Can't use jailbroken device, as app doesn't support it
- Can't use main device, as no jailbreaks existed
- We patched the IPA to install on our older device, even though it wouldn't run
- Used that device to decrypt the IPA
- Resigned the IPA with the get-task-allow entitlement
- Installed it on our main device (iPhone 14 Pro)
- Achieved code execution in our application's sandbox

In closing...

Thanks!

