Modern iOS Pentesting:

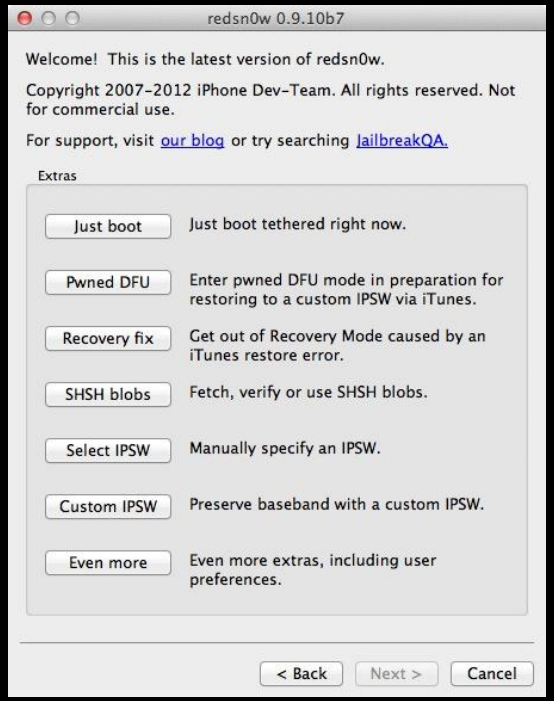
No Jailbreak Needed

presented by Noah Farmer, Senior AppSec Engineer at Dvuln

Some stuff you'll probably recognise

JailbreakMe (2011) - iOS 4

@comex

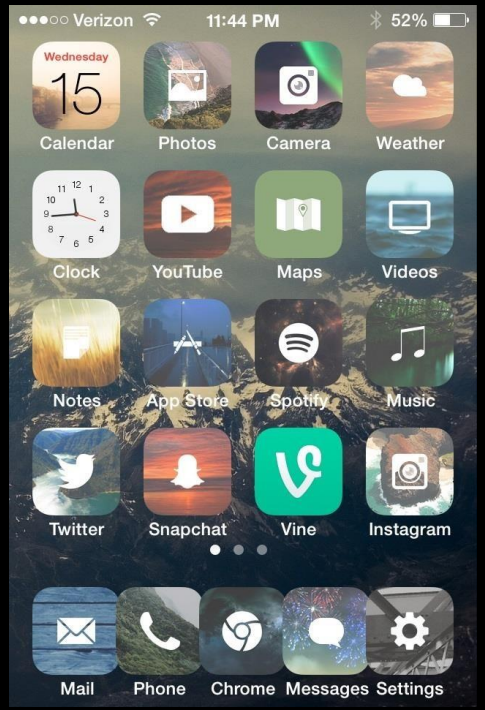


redsn0w (2012) - iOS 4 - 6

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?

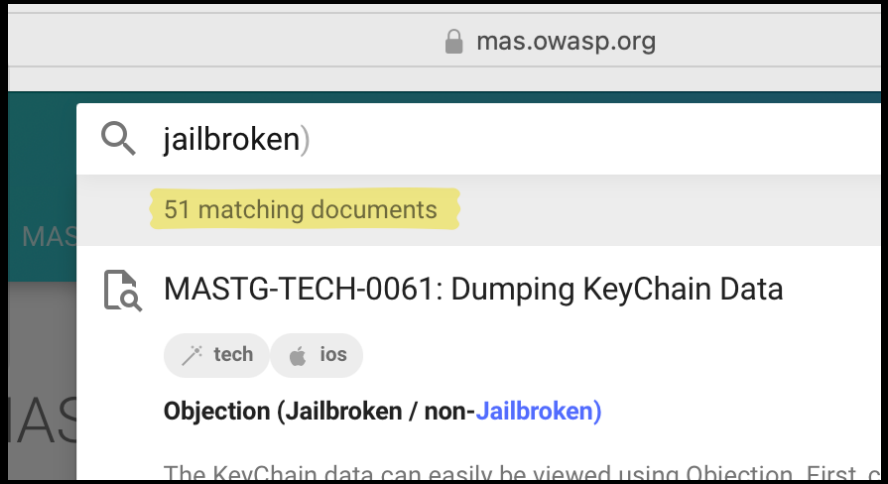
- Had a Minecraft Pocket Edition server shared with classmates in year 5
- Annoyed with being locked in survival mode, wanted free diamonds
- Did some Googling...

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

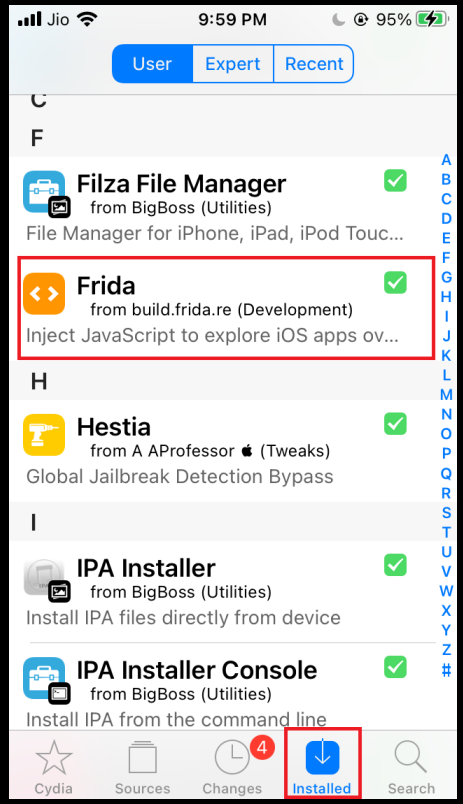
- Supports both iOS and Android.
- Inspect and interact with container file systems.
- Bypass SSL pinning.
- Dump keychains.
- Perform memory related tasks, such as dumping & patching.
- Explore and manipulate objects on the heap.
- And much, much more...

Screenshots are available in the wiki.

FRIDA

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

Installing was pretty simple...




```
[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!

     _   _         _   _
 ___| |_|_|___ ___| |_|_|___ ___
| . | . | | -_|  _|  _| | . |   |
|___|___| |___|___|_| |_|___|_|_|
      |___|(object)inject(ion) v1.11.0

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

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

Ready to test!

...but now?

bcredeur97 • 1y ago

Game of cat and mouse, but the cat won

10 Reply Award Share ...

r/jailbreak • 6 mo. ago

Glum-Substance-3356

Ho

Disc

/jailbreak • 1 yr. ago

lightOwlEyes

give up? Iphone 13 plus ios 16

Discussion

r/jailbreak • 7 days ago

Puzzleheaded-Land-56

bscribe

Jailbreaking is dead and you know it

Discussion

ome back in 3

ears on condition you stop updating your iPhone

8 Reply ...

Nonja999 OP • 3h ago

MOBILE

Is iPhone ja

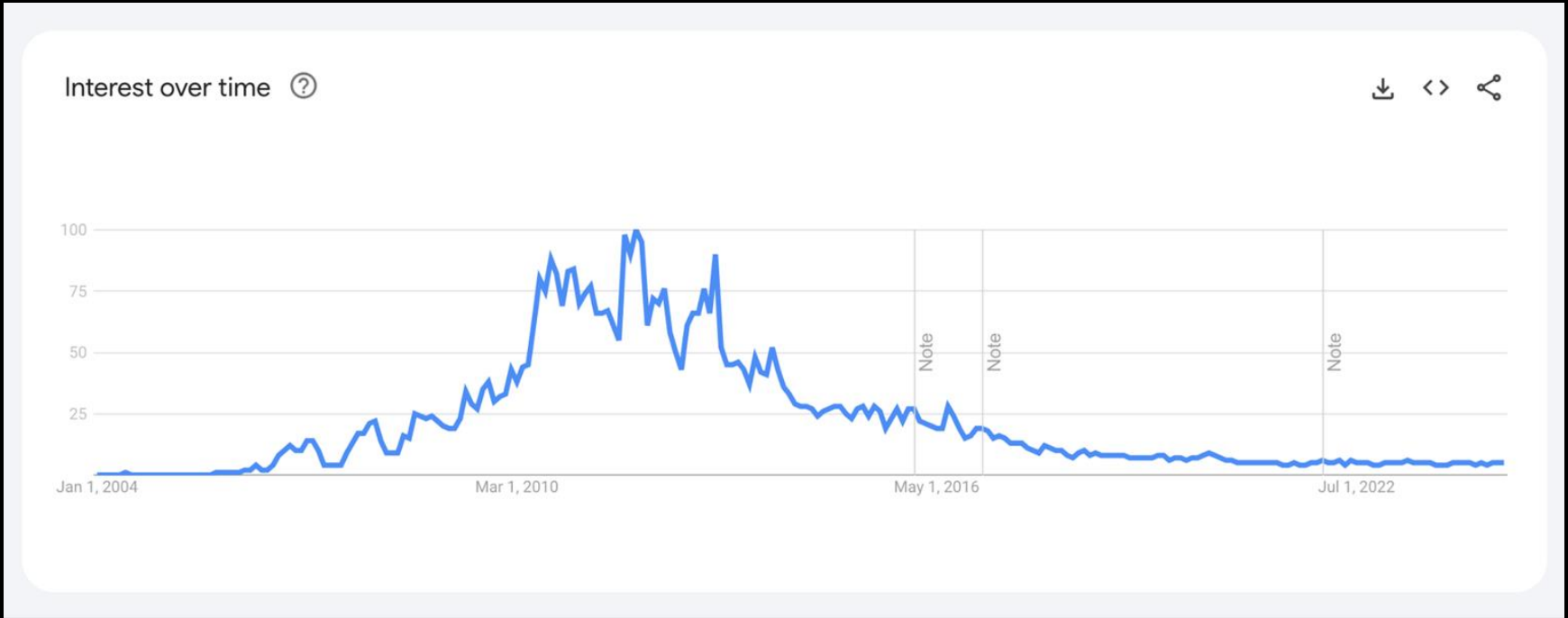
community looks like in 2023

Everyone wanted to jailbreak their iPhone in the 2010s, so why has the hype died down?

By Calvin Wankhede • April 13, 2023

Unfortunately,
jailbreaking has lost its community.

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

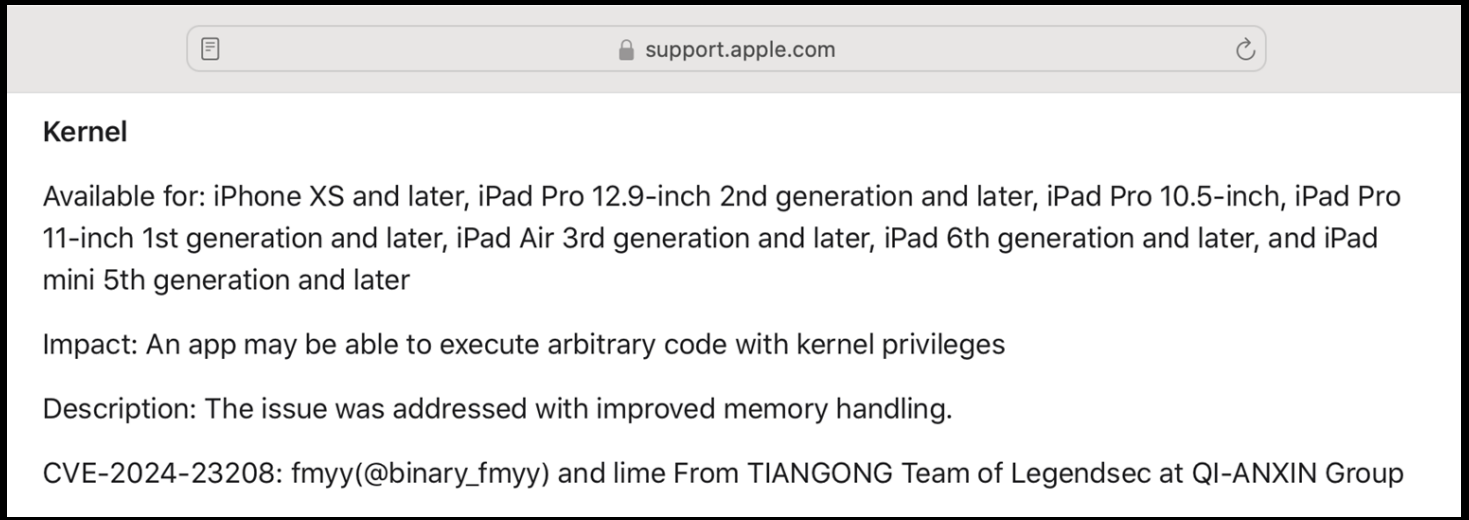


Apple’s security bounties are among some of the highest in the industry

Network attack without 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

Example: CVE-2024-23208

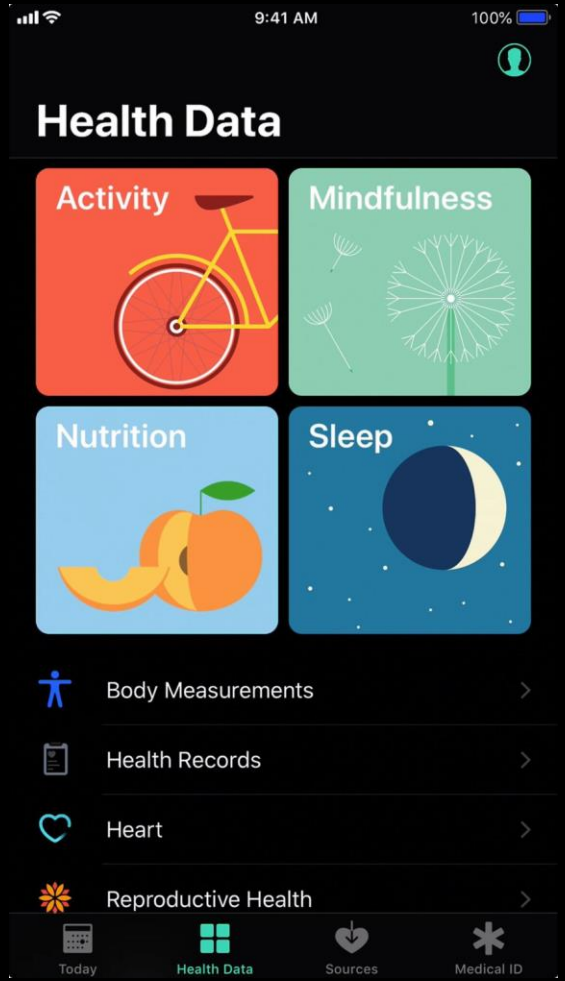
- Affected iOS (iPad/iPhone), macOS, tvOS, and watchOS
- Allows arbitrary code execution with kernel privileges.. also known as a **jailbreak**
- Submitted to Apple, and patched in iOS 17.3 :(



Tweaks are now Features

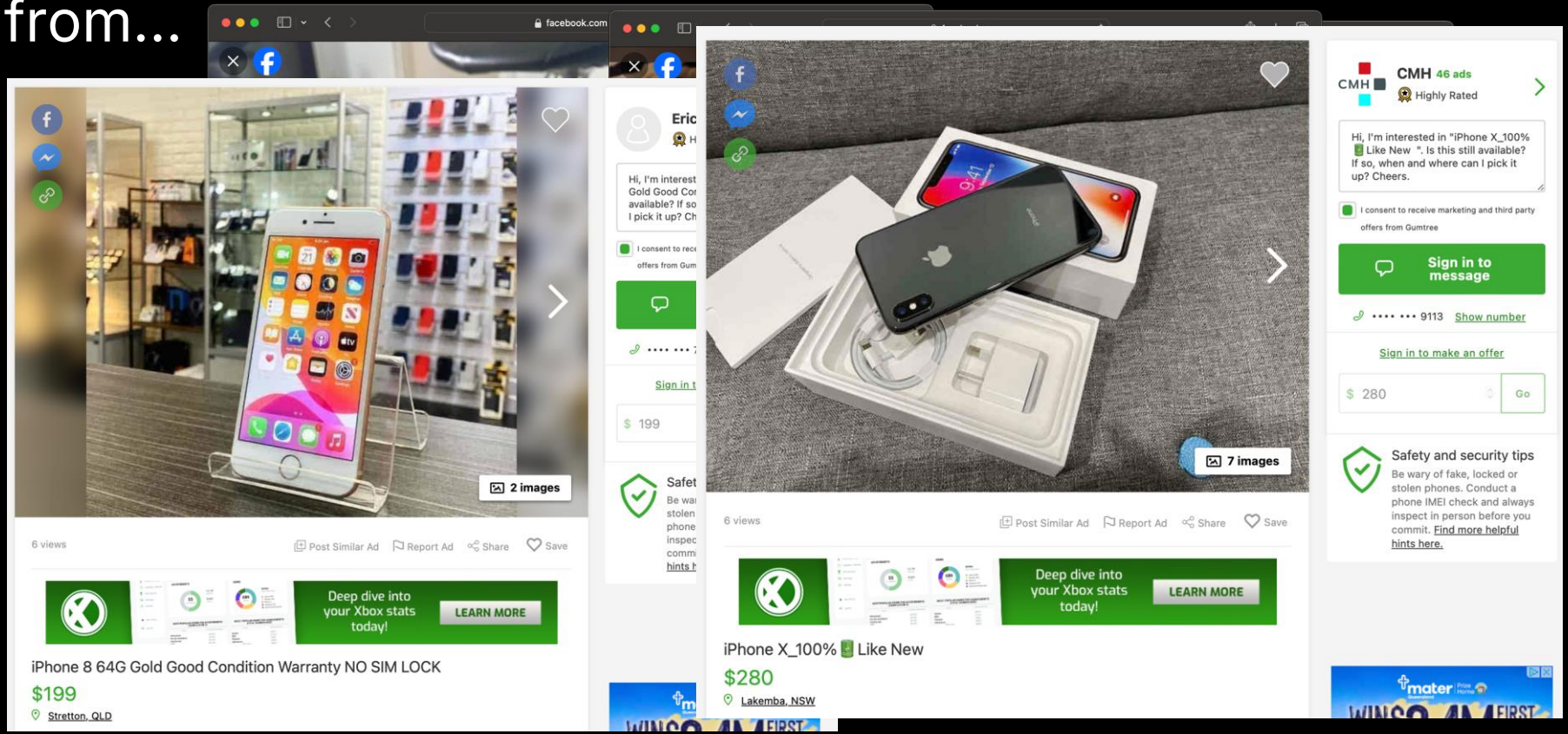
- Vmoji by @vintendo became “Emoji” in iOS 5
- SBSettings by @BigBoss became “Control Center” in iOS 7
- StickerMe by Alexander Laurus became “Stickers” in iOS 10
- Noctis by @LaughingQuoll became “Dark Mode” in iOS 13

...you get the point



Yes, it’s still a thing. But...

Here's where your pentesting devices are coming from...



Even if you had these devices...

Passkey API
iOS 16+

Focus Filters
iOS 16+

SharePlay API
iOS 15+

...just to name a few

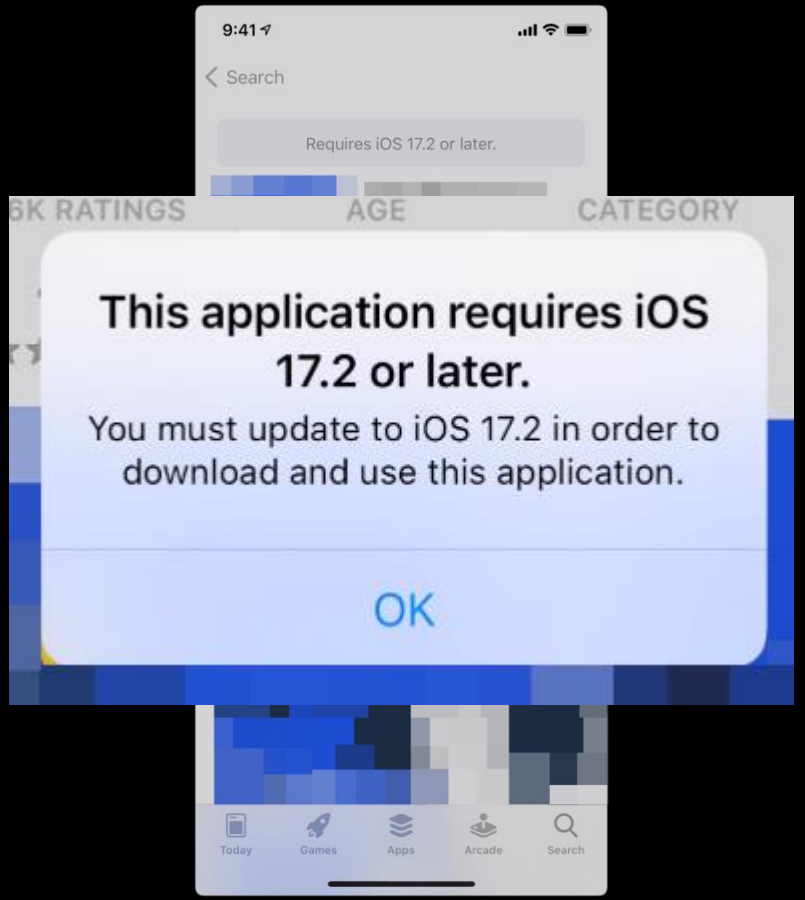
The usual setup

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.

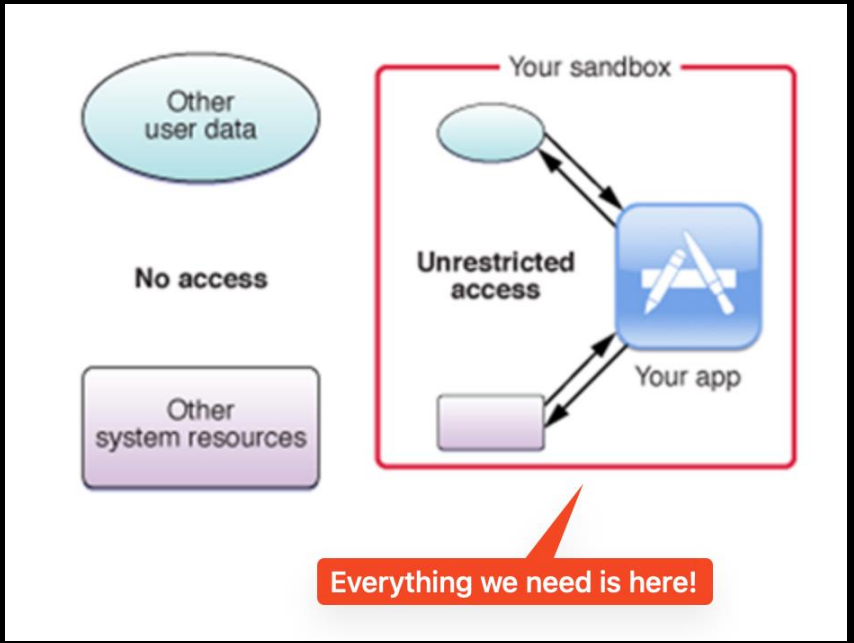
What does this have to do with jailbreaking?

- 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.

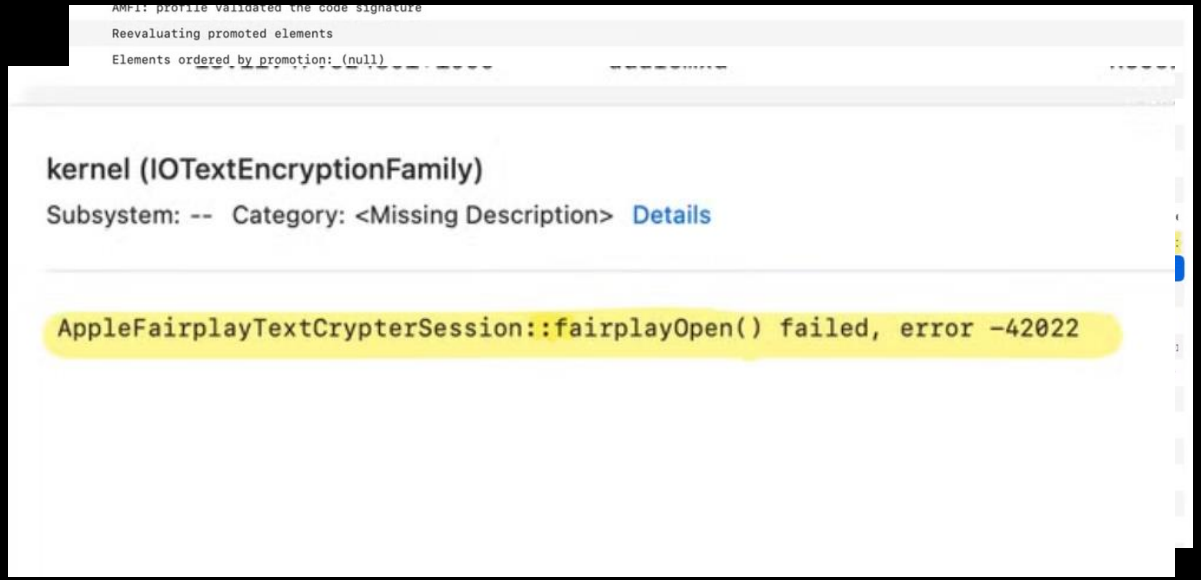
If we can re-sign an application with this `get_task_allow` entitlement...
we can achieve code execution, memory read/write, and more...
just for that single application.

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:



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:

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!

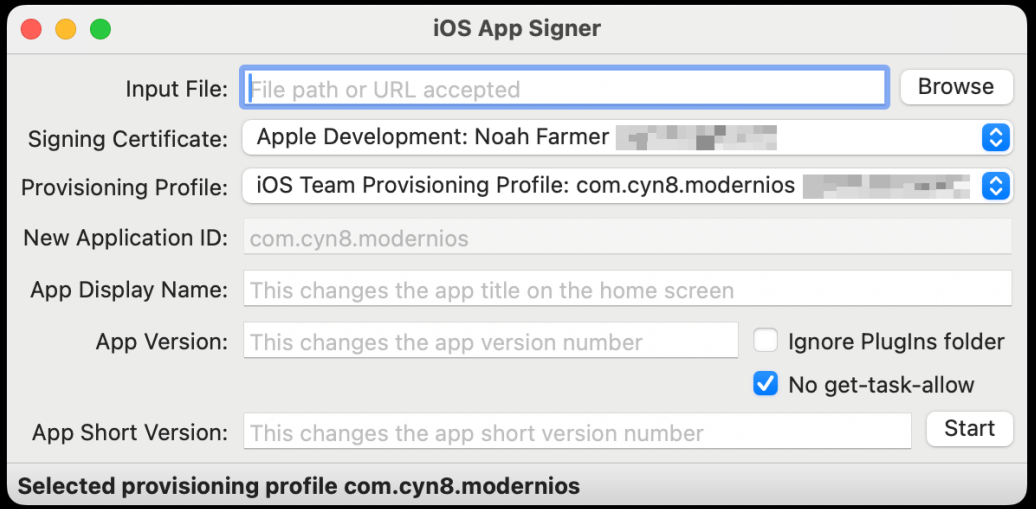
For the sake of simplicity...

[redacted]-decrypted.ipa

30.18 MB

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:



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!

     _   _                 _   _
 ___| |_|_|___ ___ ___| |_|_|___ ___
| . | . | | -_|  _|  _| | . |   |
|___|___| |___|___|_| |_|___|_|_|_|
      |___|(object)inject(ion) v1.11.0

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

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

We have execution on the latest iOS!

Feels like home :-)

MASTG covered: ✅
Pentest completed: ✅

```
noahfarmer@Noahs-MacBook-Pro no-jailbreak-required % objection -g com.cyn8.modernios explore
Using USB device `iPhone`
Agent injected and responds ok!

     _   _         _   _
 ___| |_|_|___ ___| |_|_|___ ___
| . | . | | -_|  _|  _| | . |   |
|___|___| |___|___|_| |_|___|_|_|
      |___|(object)inject(ion) v1.11.0

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
com.cyn8.modernios on (iPhone: 17.6.1) [usb] # pwd
Current directory: /private/var/containers/Bundle/Application/EB[redacted].app
com.cyn8.modernios on (iPhone: 17.6.1) [usb] # 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  [redacted].png
Regular       420  None              True  False  _installd (33)  _installd (33)  2.0 KiB    2024-05-21 08:22:52 +0000  [redacted]ng
Regular       420  None              True  False  _installd (33)  _installd (33)  33.3 KiB   2024-05-21 08:22:52 +0000  [redacted]
Directory     493  None              True  False  _installd (33)  _installd (33)  96.0 B     1970-01-01 00:00:00 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  8.2 KiB    2024-05-21 08:22:52 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  262.8 KiB  2024-05-21 08:22:52 +0000  [redacted]
Directory     493  None              True  False  _installd (33)  _installd (33)  128.0 B    1970-01-01 00:00:00 +0000  [redacted]
Directory     493  None              True  False  _installd (33)  _installd (33)  96.0 B     1970-01-01 00:00:00 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  92.3 KiB   2024-05-21 08:22:52 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  2.8 KiB    2024-05-21 08:22:52 +0000  [redacted]
Directory     493  None              True  False  _installd (33)  _installd (33)  128.0 B    1970-01-01 00:00:00 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  241.4 KiB  2024-05-21 08:22:52 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  9.0 KiB    2024-05-21 08:22:52 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  262.3 KiB  2024-05-21 08:22:52 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  9.0 KiB    2024-05-21 08:22:52 +0000  [redacted]
Regular       420  None              True  False  _installd (33)  _installd (33)  225.0 KiB  2024-05-21 08:22:52 +0000  [redacted]
```

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!