Ben Westphal

Ms. Bennett

English 11th

05/04/2023

Jailbreaking

Apple’s iOS operating system has been around since mid-2007 with the release of the first ever iPhone running iPhone OS 1.0. Ever since then, users have been trying to enhance their experience through the use of jailbreaks. Back then, the iPhone did not have the Apple App Store that we all know and not necessarily love. Instead, users downloaded third-party apps through an app called Cydia which could only be acquired by jailbreaking their device. Cydia, created by Jay Freeman, is a graphical user interface of APT for iOS which enables users to find and install software on their iPhone not authorized by Apple (Freeman *Cydia*). Freeman launched Cydia on the 28th of February 2008. Apple introduced their App Store on July 10th the same year. Ever since the release of the first jailbreak, Apple has been at war with the jailbreaking community constantly doing anything they can to prevent users from jailbreaking their devices, though jailbreakers persevere and jailbreaking remains something users still do today.

How does one Jailbreak? Jailbreaking is the act of getting around software restrictions installed on your device by Apple through the use of an exploit, or a series of exploits, so that you can manage your device at an administrator level. Most modern jailbreaks such as unc0ver or Taurine are extremely simple to use and only require that the user “sideload” an app onto their device and press a button within the app. These jailbreaks are known as “semi-untethered” jailbreaks because the user will have to re-open the jailbreak app and press the jailbreak button again every time their device reboots. However, with each new version of iOS, Apple patches the vulnerabilities that make these jailbreaks possible. Jailbreaking hasn’t always been this way though, early iOS versions were able to be jailbroken in a way that left the kernel of the operating system permanently patched, allowing the jailbreak to persist even after a reboot. Some jailbreaks worth mentioning that fall under this category would be Spirit for iOS 3.1.2-3.2.0 developed by Nicholas Allegra, otherwise known as Comex, as well as evasi0n for iOS 6.0-6.1.2 developed by evad3rs, a team of hackers consisting of four individuals (*Jailbreak - The iPhone Wiki*).

Why do users jailbreak? Jailbreaking allows users to install third-party software onto their iOS device with ease. Notable software that many jailbreakers use include Snowboard by SparkDev, a theming engine that allows users to change the look of their icons on their home screen. Many users may also like to change their system font, a tweak called A-Font can do just that. However, there is also a side to jailbreaking that is looked down upon by most of the community, this of course being piracy. With a tweak installed called AppSync Unified, a user can install any unsigned .ipa file (iOS application package) they want. This makes it incredibly easy to download any app you want completely for free (similar to Android with .apk files). There are many reasons one would want to jailbreak, primarily for customization purposes, but some people do some unfavorable things with jailbreaks as well.

Why and how does Apple try to stop jailbreaking? Jailbreaking gives users more control over their device. This directly goes against how they designed the iPhone to be used in the first place. With every new update to the operating system, Apple patches more security vulnerabilities which makes it so that hackers have to find other ways to exploit the operating system. In iOS 15, Apple introduced a new security feature known as Signed System Volume. This new SSV security feature verifies system files on boot and rejects anything that does not have a valid cryptographic signature from Apple. (*Signed system volume security in iOS, iPadOS, and macOS*). Upon attempting to jailbreak iOS 15 using checkra1n (an un-patchable bootrom exploit based jailbreak), the device will enter DFU mode (Device Firmware Upgrade mode) resulting in the user having to restore their device through iTunes, effectively uninstalling the jailbreak. This means that jailbreaks for iOS 15 and newer must be rootless (install jailbreak files somewhere that won’t interfere directly with the root filesystem). Despite this, there are jailbreaks out now for both iOS 15 and iOS 16 that do just that. Those being Dopamine by opa334 for iOS 15.0-15.4.1 (*OPA334/dopamine*) and palera1n for older devices running iOS 15.0-16.4 by the palera1n team (*PALERA1N*).

Apple once attempted to take extreme measures to eradicate jailbreaking. In 2009, Apple made the argument that jailbreaking infringes on their copyright and was a DMCA violation. These comments were made by apple with the Copyright Office during the DMCA rulemaking in 2009. As stated in an online article from EFF.org, “Apple's copyright infringement claim starts with the observation that jailbroken iPhones depend on modified versions of Apple's bootloader and operating system software… courts have long recognized that copying software while reverse engineering is a fair use when done for purposes of fostering interoperability with independently created software, a body of law that Apple conveniently fails to mention” (Lohmann *Apple says iPhone jailbreaking is illegal*). Thus, jailbreaking was granted DMCA exemption and is 100% legal, at least in the United States.

Is jailbreaking still worth it today? Many features that were once exclusive to jailbreak tweaks were eventually added officially in later releases of iOS. It’s always possible that Apple may adopt more features such as icon themes in the future. They’ve already shown that they like to take inspiration from the jailbreak community when adding new features to the operating system. Most notably dark mode with iOS 13 which used to be a tweak called Eclipse for iOS 7 and newer. More recently, Apple has added lock screen customization extremely similar to the iOS tweaks Jellyfish and Complications which affect the lock screen clock and the widgets users are able to put under the clock respectively. Apple has also recently added the ability to have your battery percentage show on the battery icon in the status bar rather than having to check the control center. This functionality has been available for jailbroken devices since iOS 12 by using a tweak called Juice. In short, the user is willing to wait patiently and has hope that Apple will eventually implement the functionality of their favorite jailbreak tweak into iOS, there is no reason to jailbreak. However, for users who like to live on the edge and wish for their iOS device to stand out amongst a crowd, then jailbreaking is a good option. However, when running literal malware on a device, it is important to use caution to only download packages from trusted sources. Other than that, there are really no true risks to jailbreaking as long as the user is careful and knows what he or she is doing.

Though jailbreaking has been around almost as long as the iOS operating system itself, there is little to no chance that it will be going away any time soon. Over the years, jailbreaking has evolved considerably to keep up with the development of iOS. Despite Apple’s attempts to eradicate jailbreaking, it seems it’s here to stay. Though this may be for the best, as without jailbreaks, there would be no extremely talented developers creating third-party software for iPhones. If there were no one making tweaks for jailbroken devices, there would be no good features for Apple to emulate. Apple may not approve of jailbreaking, but they likely recognize that without it, it’s probable iOS wouldn’t be as successful or well-known as it is today.

Works Cited

➤ Freeman, Jay. *Cydia*, 28 Feb. 2008, [cydia.saurik.com/](http://cydia.saurik.com/).

*➤ Jailbreak - The iPhone Wiki*, [www.theiphonewiki.com/wiki/Jailbreak](http://www.theiphonewiki.com/wiki/Jailbreak).

➤ Lohmann, Fred von. “Apple Says iPhone Jailbreaking Is Illegal.” *Electronic Frontier Foundation*, 12 Feb. 2009, <https://www.eff.org/deeplinks/2009/02/apple-says-jailbreaking-illegal>.

➤ opa334. “OPA334/Dopamine.” *GitHub*, 2023, [github.com/opa334/Dopamine](https://github.com/opa334/Dopamine).

➤ “PALERA1N.” *palera1n*, palera1n, 2022, [palera.in/](https://palera.in/).

➤ “Signed System Volume Security in iOS, iPadOS, and MacOS.” *Apple Support*, Apple, 2021, [support.apple.com/en-gu/guide/security/secd698747c9/web](https://support.apple.com/en-gu/guide/security/secd698747c9/web).