

Differences Between Rooting and Jailbreaking

TechRounder PDF Edition

Live article: <https://www.techrounder.com/mobile/differences-between-rooting-and-jailbreaking/>

By Vipin PG | Published March 22, 2024 | Updated March 26, 2024 | Format: Article | 5 min read

In brief

If you're a tech enthusiast and naturally curious like most people are, you've probably come across the terms "rooting" and "jailbreaking".

If you're a tech enthusiast and naturally curious like most people are, you've probably come across the terms "rooting" and "jailbreaking". These two terms often spark mystery and curiosity, often regarded as almost "illegal" ways to get smartphone devices to perform functions outside of those assigned by the device manufacturer. In this quick article, we aim to demystify the meaning of these two terms while discussing their implications in their different ecosystems. In the end, you'll understand what rooting and jailbreaking are from a technical perspective and get some ideas.

Understanding the Basics

Android rooting and iOS jailbreaking are two methods used to bypass device restrictions imposed by the manufacturer or vendor. Rooting is primarily associated with Android devices, while iOS jailbreaking is exclusive to Apple devices. Commonly, these restrictions by the manufacturer effectively limit what the user can do outside of the assigned ecosystem. For example, in iOS, the user cannot install themes, plugins, and other apps outside of the Apple App Store. In earlier versions of iOS, the Apple device was limited to a specific carrier, i.e., AT&T, which had a poor 2G network and unfriendly service charges. Therefore, the entire purpose of rooting or jailbreaking devices is to grant the user more permissions to customize the device as a "super user". However, the exact methodology for achieving these new permissions differs for Android and iOS.

The History of Rooting and Jailbreaking

In Android rooting, the user is granted "root access," nearly similar to a computer user being granted administrator privileges. With these new superuser privileges, the user is free to modify system files, install a custom OS, install apps outside of those the device manufacturer allows, and use other advanced functionalities. Rooting has its roots in Android's open-source nature, as a kernel built on Linux/Unix, which are both open-source. This initiative is powered by the Android Open-Source Project (AOSP), which encourages developers to customize or even create their own firmware. On the other hand, jailbreaking stemmed from the closed-source nature of Apple devices and the iOS ecosystem that treats device owners as users rather than admins. Due to this closed nature of the OS, jailbreaking doesn't involve modifying the device firmware to grant the user super privileges. Instead, security vulnerabilities in the firmware are exploited to bypass restrictions. Thus, users can access apps outside the App Store through sideloading. In a sense, then, rooting goes more than just customization and, in many instances, is encouraged. This is especially true for developers who need to test apps extensively. Some device manufacturers provide devices with unlocked bootloaders, allowing for custom firmware installation. For iOS, jailbreaking is often a cat-and-mouse game that Apple actively discourages by releasing numerous patches to fix the vulnerabilities. Additionally, Apple has integrated many of the extensions and features that can be accessed on jailbroken phones into its App Store.

Comparing and Contrasting Jailbreaking and Rooting

Rooting involves a major modification of the system permissions to grant the user superuser privileges. This can be achieved in different ways. For example, security vulnerabilities can be exploited, manufacturer tools can be used, or even custom software can be flashed on the device to provide new firmware. On the other hand, jailbreaking often involves bypassing iOS security features by exploiting security vulnerabilities. Apps outside of the official App Store can be installed via side loading, and some custom modifications to the UI can be performed. However, deeper system modifications are not possible. The normal process for jailbreaking is to use a package manager such as Cydia and a jailbreak tool such as Chekra1n. This should be done with a compatible iOS version since most newer iOS versions after iOS 14 are unsupported. Jailbreaking newer iPhone models is becoming increasingly tougher since Apple prevents downgrades to older firmware. Android rooting usually involves unlocking the bootloader, downloading and flashing stock firmware on the device, and extracting the firmware zip files. The firmware's boot image is then patched using a tool such as Magisk Manager, and the patched boot image is flashed using a tool like Odin. As is clear, rooting grants deep access to the underlying Android system, and the user can modify core features and functionalities. Jailbreaking focuses on circumventing app store restrictions and customizing the user interface.

What Are the Risks Involved?

Both jailbreaking and rooting pose security restrictions. In particular, devices can be exposed to security vulnerabilities, compromising their stability. In both instances, the device warranty can be voided. For rooting, improper modifications can brick the device, i.e., render it unusable. However, depending on the type of rooting used, the implications can be moderate to severe. Jailbreaking carries higher risks due to the exploitation of security vulnerabilities. Although not illegal, it technically violates Apple's terms of service. However, you can revert to a previous version of the firmware with a jailbroken device, thus restoring your warranty.

What Are the Benefits of Jailbreaking Versus Rooting?

Rooting allows users to personalize their UI, remove bloatware, optimize performance, and install advanced features. Rooting is ideal for app developers needing root permissions to test apps extensively. Apps that are incompatible with the stock operating system can also be installed. Jailbreaking allows users to sideload apps, meaning they can load apps and tweaks unavailable on the App Store. The iOS interface can be customized with themes, widgets, and launchers, which gives it a personal and unique feel.

Before You Begin

Always understand the risks that both processes entail. High on this list are increased chances of bricking and voiding your warranty. Choose a safe and compatible method with your Android/iOS version. Always back up your data and current OS before proceeding with either process. Also, begin with simple tweaks and gradually escalate as you gain experience and confidence. Perform either jailbreaking or rooting ethically and responsibly.

Conclusion

You now have a solid idea of the differences between jailbreaking and rooting and these processes' potential benefits and risks. Both jailbreaking and rooting offer an opportunity to customize your device beyond manufacturer restrictions. You can make your device your own and have fun breaking through manufacturer restrictions on your smartphone. Remember to do either jailbreaking or rooting responsibly and protect yourself from any loss of data or even your device.