

# Abstract

Stefan Dimitrov  
Mentor: Ming Chow

October 17, 2013

The traditional software distribution channel on the iOS platform is Apple's own AppStore, which is known for its stringent app approval policies and quality control. One of the aims of Apple's approval process is to prevent malicious software from reaching its customer base. This preemptive strategy has proven to be relatively successful, but has been criticized for rejecting benign apps that replace or enhance core services. Jailbreaking has opened an alternative outlet for this niche of software offerings by letting users install apps from third party software repositories outside of Apple's regulation, however, this lack of security audit theoretically enables the unhindered distribution of potentially malicious code. Moreover, because jailbreaks exploit a security vulnerabilities within iOS in order to grant apps root privileges and unrestricted filesystem access, they effectively disable several security features in iOS. However, jailbreaking also allows the installation of third-party patches targeting those very vulnerabilities. In addition, jailbreak tweaks that improve privacy control have surfaced in response to controversial AppStore apps that misuse user information, yet pass the approval process. These subtle, but significant differences between the stock and jailbroken flavors of iOS motivate this paper in an attempt to explore the pros and cons of jailbreaking regarding security and privacy.