

Mobile security: Android versus Apple

October 9 2013



Credit: AI-generated image ([disclaimer](#))

Smartphones are big business, prompting fierce competition between providers. One major concern for consumers is whether a smartphone will keep their private data safe from malicious programs. To date, however, little independent research has been undertaken to compare security across different platforms.

Now, Jin Han and co-workers at the A*STAR Institute for Infocomm

Research and Singapore Management University have conducted the first systematic comparison of the two biggest operating systems in mobile software—Apple's iOS and Google's Android. The two companies take markedly different approaches to [security](#).

Apple famously maintains complete control over iOS security, promising that all applications are thoroughly screened before release and security patches are smoothly applied across all their phones. However, malicious software has appeared in the iTunes store.

Android, in contrast, displays everything that an application will need to access so that users can decide themselves whether to go ahead with an installation. Some critics argue that handing such control to unqualified users could present a security risk in itself.

To compare these two security models, Han and co-workers identified 1,300 popular applications that work identically on both iOS and Android. These applications, such as Facebook, often access code libraries on smartphones called security-sensitive application programming interfaces (SS-APIs), which provide private user data or grant control over devices such as the camera.

"We needed to establish a fair baseline for the security comparison between Android and iOS," says Han. "We achieved this goal by examining the SS-API usage of cross-platform applications."

The researchers found that 73% of iOS applications, especially advertising and analytical code, consistently accessed more SS-APIs than their counterparts on Android. Additionally, the SS-APIs invoked by iOS tended to be those providing access to sensitive resources such as user contacts.

The results imply that by allowing users to control permissions, Android

may be better at preventing stealthy [applications](#) from getting hold of private information. Notably, Android also intentionally avoids using SS-APIs if non-security-sensitive APIs can be used to achieve the same functions.

To avoid jumping to conclusions about the risk to Apple users from the iOS process, Han urges caution in interpreting the results. "Mobile platforms are constantly evolving," he says. "Our experiments were mainly conducted on iOS 5, but iOS 6 has enhanced its privacy protection so that users will be notified when an app is trying to access their contacts, calendar, photos or reminders. This may encourage developers to modify their apps so that they access less private data."

More information: Han, J., et al. Comparing mobile privacy protection through cross-platform applications. The 20th Annual Network & Distributed System Security Symposium, 26 February 2013. www.internetsociety.org/doc/colloquium/2013-02-26-comparing-mobile-privacy-protection-through-cross-platform-applications

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

Citation: Mobile security: Android versus Apple (2013, October 9) retrieved 20 March 2024 from <https://phys.org/news/2013-10-mobile-android-apple.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--