

How Secure are iPhone and Android Apps

April 1 2010, by John Messina



The Android smartphone and iPhone handle application security radically different.

(PhysOrg.com) -- Today's smartphones are pocket size computers that can be customized by downloading applications. This is what makes a smartphone vulnerable to cybercriminals. In this article we will examine how an iPhone and Android phone handles security. Both phones handle security radically different.

In order for iPhone application to get listed in [Apple's App Store](#), developers must create an account and pay an annual fee. All applications are evaluated by a team at Apple and approve each version of the software before it's made available in Apple's App Store. Apple roughly disapproves about 10% of all applications submitted to the App Store because the applications would steal [personal information](#) or pose a threat in some other way to the user.

In Android's Marketplace, applications are not evaluated by [Google](#). Android users are protected in a completely different way by using a security model based on "capabilities". Each Android app that is installed must tell the phone's OS what capabilities it requires.

When an application is installed, the Android OS lists all the "capabilities" that is required in order for the application to run. This allows the capabilities-based system to be governed by the OS and preventing the application from doing more than what it's supposed to.

The capabilities-based system has its flaws. For instance, there is no way of knowing that the application will act the way it's supposed to with the trust that it's given. This system also can't tell the difference if the privileges it grants the application is for legitimate use or not. For example, some applications will ask for a user name and password to communicate over the internet with a remote host.

Other security features for the iPhone and Android phones is that they both can be set to lock after a length of inactivity; a password is then required to unlock the phone. The iPhone however has an additional security feature where 10 failed password attempts can erase all data on your phone. The iPhone also supports remote wipe. The Android OS has neither of these features making it less secure.

No matter what security features are deployed in the [iPhone](#) or Android smartphones there are other ways of obtaining personal information from smartphones. Manufactures can only try to make it harder for cybercriminals obtaining your personal information.

More information: Via: [TechnologyReview](#)

Citation: How Secure are iPhone and Android Apps (2010, April 1) retrieved 24 April 2024 from <https://phys.org/news/2010-04-iphone-android-apps.html>

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.