

Android vulnerability neutralised

May 24 2012



©Shutterstock

Smart phones and tablet computers - once the latest must-have devices for technology geeks - are becoming increasingly more popular with the mainstream. The Android platform is now one of the most popular platforms with over 300 million Android devices in use since February and 700 000 devices being activated with each passing day. One of its main attractions is the open source software that allows a huge community of program developers to write applications. But with so many people contributing to this innovation, the operating system is open to bugs and security holes. In a new study, however, researchers in Italy may have neutralised any potential problems.

Researchers from the Bruno Kessler Foundation, the University of Genoa, Telematic University E-Campus and the University of Padua in

Italy embarked on their project with one idea in mind: to revolutionise the way ICT systems and applications are designed, implemented, deployed and consumed. They foresee an Internet of Services (IoS) whereby business functionalities are designed and implemented by producers, deployed by providers, aggregated by [intermediaries](#) and used by consumers. This, they say represents a major mind shift in the way programs and applications are traditionally developed; these would be built by composing services that are distributed over the network and aggregated and consumed at run-time in a demand-driven, flexible way.

In applying and developing their new methodology the researchers discovered a major susceptibility present in all versions of Android, a popular operating system developed by Google - famous for its search engine, specifically for [smart phones](#) and tablet computers. This, they say, could very well have been exploited by [malicious software](#) applications. Some malicious software (malware) have the ability the ability to "brick" devices, what experts describe as a device that can no longer be used and is about as useful as a brick.

Once the weakness in the platform was found the researchers immediately reported it to [Google](#) and to the Android security team as well as providing them with a detailed analysis of related risks. Once they made their report they then went one step further and designed a solution to the risk which was then verified by the security team of Android. The researchers hope that once its effectiveness is proven it will then be adopted in a future operating system update.

If the team had not acted as they did, the weakness could have allowed malicious application software to saturate the physical resources of the device, leading to complete blockage of both Android-based smart phones and [tablet computers](#). The problem with malware is its insidiousness because these applications do not require any authorisation during installation and would appear harmless to the user until it is too

late.

The result compiled by the Italian research team will be published during the proceedings of the 27th IFIP International Information Security and Privacy Conference - SEC 2012, which will be held in Heraklion, Crete, Greece, on June 4-6, 2012.

More information: www.spacios.eu/

Provided by CORDIS

Citation: Android vulnerability neutralised (2012, May 24) retrieved 25 June 2024 from <https://phys.org/news/2012-05-android-vulnerability-neutralised.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.