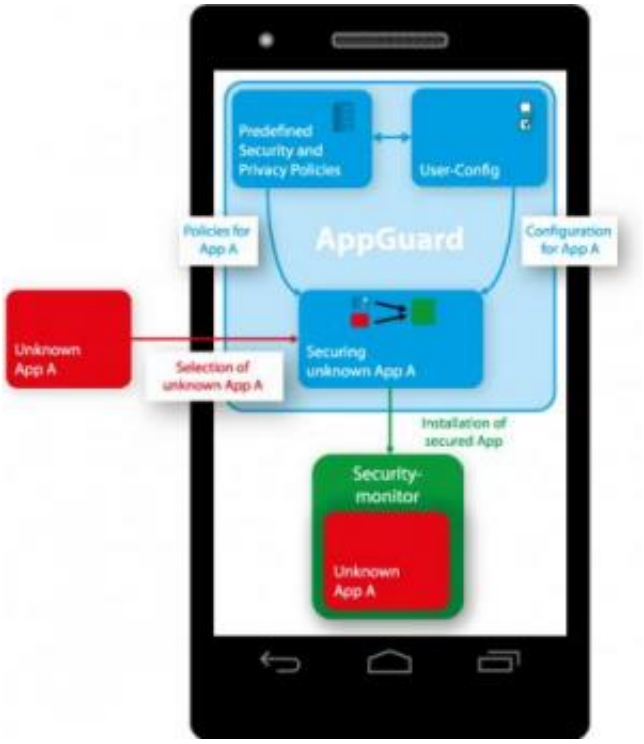
Computer scientists prevent data theft on smartphones and tablet computers

February 27 2013



Some mobile applications on web-enabled mobile phones and tablet computers spy on personal data. Computer scientists from Saarbrücken prevent this through a new approach. The freely available app attacks the program code of the digital spies. Credit: Bellhäuser - das bilderwerk

Some mobile applications on web-enabled mobile phones and tablet computers spy on personal data. Computer scientists from Saarbrücken prevent this through a new approach. Its chief attraction: For the

protection to work, it is not necessary to identify the suspicious programs in advance, nor must the operating system be changed. Instead, the freely available app attacks the program code of the digital spies. The researchers present the app at Cebit 2013 in Hanover.

"Malicious Android apps are becoming a mass plague" is the headline of a study published by a German software company for anti-virus programs in recent days. That this is not just a sales pitch is confirmed by the analysis of the governmental supported "Stiftung Warentest" consumer survey. In May last year, it categorized 37 popular apps as "critical" for the user's privacy.

"I am not surprised. My smartphone knows everything about me, starting with my name, my phone number, my e-mail address, my interests, up to my current location," explains computer science professor Michael Backes, who manages the Center for IT-Security, Privacy and Accountability at Saarland University.

To prevent smartphones and tablets turning into digital spies the researchers have developed a new method which works for the Android operating system. "Similar to a screening line, the method scans every selected app installed on the smartphone and indicates its real behavior: Accessing your private contacts, establishing a connection to the internet and checking your position", Backes explains. The user can now revoke or grant privileges to the respective app at any time. A company founded by Backes used the published method to develop an app named "SRT Appguard". It runs problem-free on Android 2.0 and higher. It is also now guaranteed that the guarded apps receive updates from the Google Play Store.

For their approach, the Saarbrücken researchers use the fact that the Android apps, written in the programming language Java, run in a so-called virtual machine. Compared to other smartphone operating

systems, a running app can access the storage of Android's virtual machine. That's when SRT Appguard comes into play. Before the suspicious app starts, Appguard scans the storage of the virtual machine to detect security-critical functions – identified by the IT-security experts from Saarbrücken. It does not manipulate the bytecode anymore. Instead, it directs the function call within the virtual machine to the security monitor, which observes the suspicious method calls and can even block them.

More information: Michael Backes, Sebastian Gerling, Christian Hammer, Matteo Maffei and Philipp von Styp-Rekowsky: The Android Monitor – Real-time policy enforcement for third-party applications www.infsec.cs.uni-saarland.de/ … /android-monitor.pdf

Download of SRT Appguard from the software register Heise.de www.heise.de/download/srt-appguard-1187469.html

Provided by Saarland University