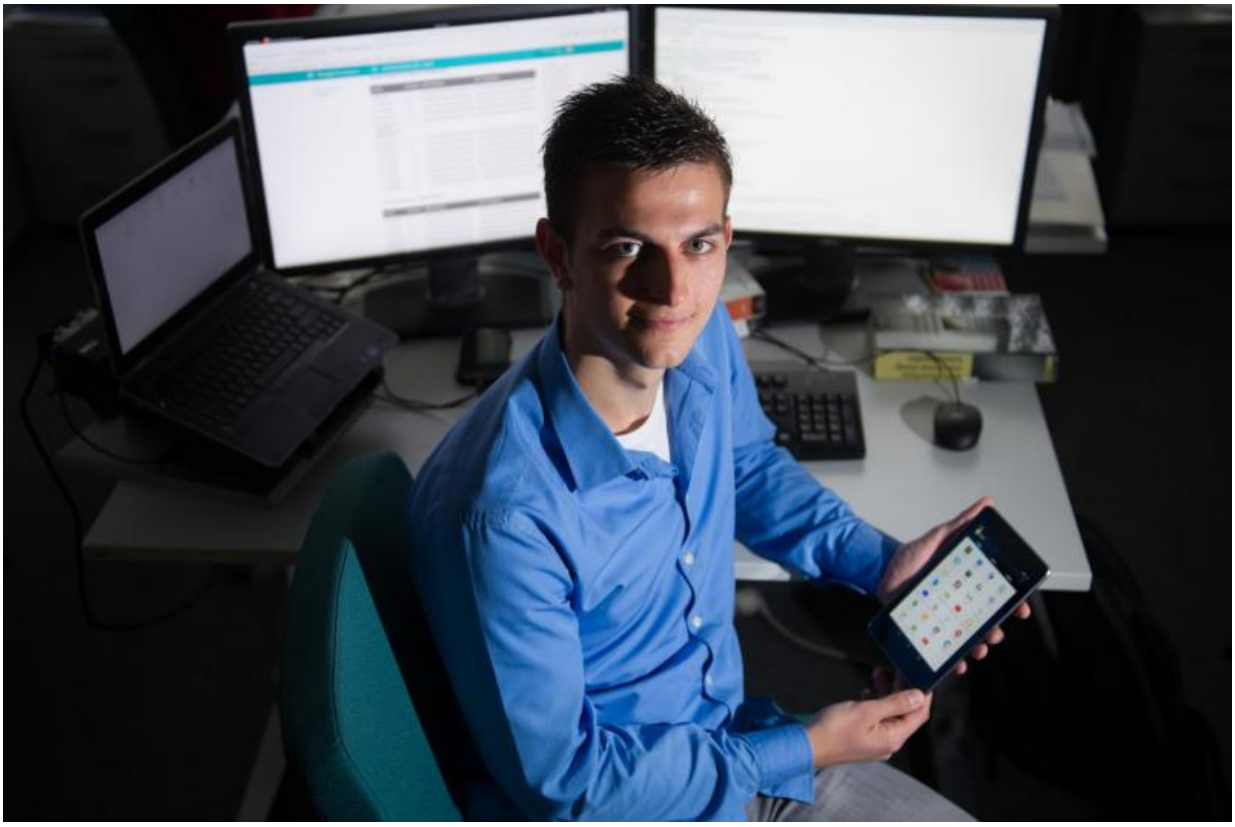
Android smartphone data spies exposed like bank robbers

March 11 2016



CISPA researcher Oliver Schranz tracks problematic information flows in smartphone apps. Credit: Oliver Dietze

When a bank is robbed, the loot will often contain a wad of manipulated banknotes. These will explode en route and release a colorful dye,

marking the money as stolen. Researchers use a similar principle to identify spyware on smartphones. Computer scientists from the Center for IT Security, Privacy and Accountability (CISPA) have now developed a matching application for the current version of the Android smartphone operating system, allowing for a more precise monitoring of malicious apps.

Android is the most widely used operating system for smartphones in the world, despite the fact that Android users are virtually blackmailed when installing new applications. Either they accept that the program will gain access to certain information, such as their personal contacts or Internet access details, or else they cannot use the app. The latest version of Android meanwhile allows users to reject some of these access requests during installation, but even so this gives a somewhat false sense of security.

"Even if an app tells me which data it would like to use, I still have no idea what it intends to do with the data," says Oliver Schranz, who completed his PhD at the Saarbrücken Graduate School of Computer Science at Saarland University. His assessment is confirmed, for instance, by a recent study conducted by the US security firm Appthority. According to their research, more than 88 percent of Android apps developed for industry use are secretly spying on user data in some way or another. At the Center for IT Security, Privacy and Accountability (CISPA), Schranz, together with Philipp von Styp-Rekowsky and Sebastian Weisgerber, developed an app that will help individual users and companies to track what is going on in suspicious apps.

The CISPA app is based on the "Taint Tracking" method, which can be compared to the colorful dye explosion triggered in a bundle of banknotes, a technique often used to track bank robbers. Hence the researchers named their app "TaintArtist". Whenever an app accesses

sensitive or privacy-relevant information, the data in question is highlighted with a kind of marker. Even if the data is altered in the process, say when new calculations are performed, the marker will remain attached even to the new results. "This lets us track the flow of information from the monitored app in more precise ways," Schranz says. Whenever the data is passed on to functions, which might then send the data out from the smartphone or display other suspicious behavior as defined in a preset corpus of rules, the pertinent markers are checked. And if the CISPA app does discover data abuse, it will set off an alarm. All that users have to do is to install the tracking app and then choose which other apps they want monitored, and what exactly should be allowed or prohibited in each of them.

Until now, this kind of information flow analysis would have made system modifications necessary, in ways that are hardly feasible for laymen. To make the same service available for all users with just a few simple steps, the Saarbruecken researchers made use of a novelty in the two most recent Android versions: In the newer versions, Android no longer executes the intermediate representation of the program code directly, but translates it into executable machine language on the device first. This allows Schranz and his team to edit the code that is needed for the markers while the translation is taking place. The code of the examined app would not have to be changed, but it would work at a slightly slower pace, according to the researchers. "Given the fact that smartphones today can handle virtually all processes within milliseconds, the increases in runtime will be hardly noticeable to users," says Schranz. This is why he is convinced that the app is also useful for businesses. "If employees use their own devices at work, with our app the company can make sure that certain data never leaves these devices," says Schranz. Whether their app will be embedded into a commercial product or will be available free of charge in future, is still open.

More information: Towards Compiler-Assisted Taint Tracking on the

Android Runtime (ART). dl.acm.org/citation.cfm?id=281 … 604&CFTOKEN=44108257

Provided by Saarland University

Citation: Android smartphone data spies exposed like bank robbers (2016, March 11) retrieved 15 May 2024 from https://phys.org/news/2016-03-android-smartphone-spies-exposed-bank.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.