New approach uncovers data abuse on mobile end devices

July 5 2012

Increasingly often, mobile applications on web-enabled mobile phones and tablet computers do more than they appear to.

In secrecy, the "apps" forward private data to a third party. Computer scientists from Saarbrücken have developed a new approach to prevent this data abuse. They can put a stop to the data theft through the app "SRT AppGuard". The 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.

"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. "It even knows my friends quite well, as it saves their contact details, too," says Backes. Therefore he is not surprised that several mobile applications, also known as apps, display simple functionality up front, while in the background, they send the identification number of the device, the personal whereabouts of the user, or even the contact details of friends, colleagues and customers to a server somewhere in the internet.

The producers of anti-virus software have been making vivid predictions of such scenarios for some time now; in the meantime, scientific studies also prove the threat. A study from the University of California in Santa

Barbara (US) concluded that among 825 examined apps for the iPhone and its operating system iOS, 21 percent forward the ID number, four percent the current position, and 0.5 percent even copy the address book.

Michael Backes and his team of researchers now bring this abuse to an end. Their approach focuses on Android. It is the most common operating system for smartphones and tablet computers. Developed by the Google software group, this freely available operating system is used by several mobile phone manufacturers, and since November 2011 is activated daily on more than 700,000 devices.

However, Android is known for its rigorous policy on assignment of privileges. If a user wants to install a downloaded app, he learns via a list which access rights to data (location, contacts, photos) and functions (Internet, locating) will be claimed by that app. Now he has two options: Either he accepts all conditions, or the app will not be installed. After the installation, the privileges cannot be revoked. "Moreover, many developers generally claim all rights for their app because the concept of privileges of Android is misleading, but they want to ensure the smooth functioning of their app nevertheless," explains Philipp von Styp-Rekowsky, PhD student at the chair in IT security and cryptography.

This "sink-or-swim" strategy is put to rest by the researcher from Saarbrücken. The app "SRT AppGuard" based on their approach determines, for every application installed on a smartphone, what it accesses, and shows this information to the user. Privileges can now be revoked or granted to the respective app at any time. The researchers have already published the app on the platform "Google Play". It can be downloaded there for free. It runs problem-free on Android 3.x.x and higher. The development of the app has been taken on by the enterprise Backes SRT, which was founded by Backes in 2010. It is also located on the campus in Saarbrücken.

Technical background

For their approach, the Saarbrücken researchers use the fact that the Android apps work in a so-called virtual machine, which is written in the computer language Java. Therefore the apps are saved on the smartphone as executable "bytecode" after installation. That's when SRT AppGuard comes into play. While the suspicious app is running, it is checking its bytecode for the security-sensitive instructions, which it had been programmed to do by the experts from Saarbrücken. It adds a special control code in front of the suspect comment or procedure. This is only necessary once, as the secured bytecode replaces the original one afterwards. This overwriting process usually only takes a few seconds and a small number of lines of additional code. The computer scientists have reviewed 13 apps, among them the popular game "Angry Birds", the music identifying app "Shazam" and the social-media apps "Facebook" and "What's app". For the app belonging to the microblogging service Twitter, for example, it needs 16.7 seconds and 48 additional lines of code. "It is just as in an art museum ," explains Styp-Rekoswky, "Instead of checking every visitor, you only provide the most valuable paintings with an invisible alarm function."

But the Saarbrücken app can do even more than just providing alerts. It is also able to block suspicious requests or change them so they cannot do any harm. "Thus, we can also prevent the use of known security vulnerabilities of the respective apps or Android operating system," adds Professor Michael Backes. This possibility is very important if the manufacturer cannot provide security fixes in time," says the professor.

More information: The App on Google Play Store
play.google.com/store/apps/det … .srt.appguard.mobile

Provided by Saarland University