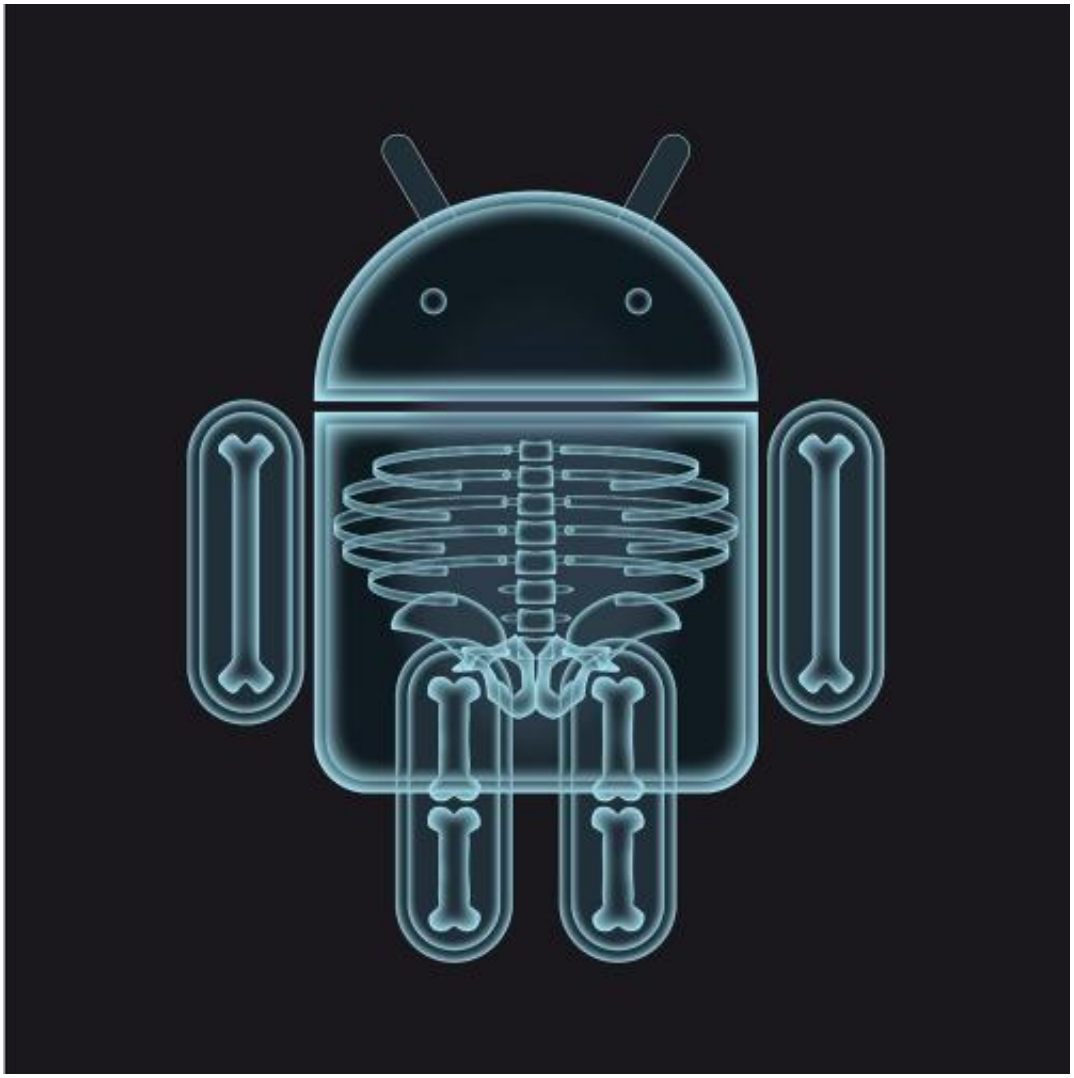
More secure app store for Android

November 4 2013



Apps. Everyone has them and everyone uses them. These small

computer programs installed on our smartphones and tablet computers make work and play easier. With just the tip of a finger on the square icons, we know where and when the next rain clouds are expected, we can book train tickets while traveling, start gaming while mobile, or listen to our favorite music. For most of us, these little mobile helpers have become indispensible. A total of almost two million of them are already available today on the platforms of the two largest providers, Apple and Google. And the trend is rising.

Privacy risks and commercial harms

However, the miniprograms are not always benevolent. "The business model for free apps often goes like this: You need pay nothing for my services, but in exchange I'm grabbing your data," reflects Dr. Julian Schütte of the Fraunhofer-Research Centre for Applied and Integrated Security AISEC in Garching near Munich. The apps pick up the data usually without the knowledge of the user. The theft runs from address data, to emails and locations, right through to identification numbers of the user devices. The app developers pass the data to third parties for geographical and personal advertising. "A fact that perhaps is viewed less critically or even as being useful, if the apps are used privately. For companies, by contrast, they conceal big risks. If email with commercially sensitive content, geographical information on employees, or confidential contact information is passed without knowledge, it is not just problematic for technical reasons of data privacy protection. It can also do commercial harm," warns Schütte.

To protect against this danger, corporate IT departments are increasing their monitoring of apps used by employees. "With an established mobile operating system like iOS, mobile device managers – IT Department employees who administrate the pool of corporate cellphones – already have quite good control over the software stored upon the devices. However, for latecomer and now market-leader

Android, there is currently no tool with which corporate IT can prevent downloading of wild apps, to our knowledge," says Schütte.

Scientists at AISEC have now closed this loophole. Their new app store filters out problematic Android apps automatically and offers employees only mobile applications that conform to a corporation's own guidelines on IT security. "Administrators and mobile device managers are able to determine themselves which apps are permitted to be installed and which ones are not," says Schütte.

Additional advantages of the AISEC solution: the analysis of the apps is flexible and can be adapted to a wide range of company directives. In addition, the IT department can also stipulate that apps are only permitted to communicate through encryption. "That is no small feature during these times of NSA spying scandals," according to Schütte. And finally, the software does not just work for apps offered today. "With the aid of our app-store, companies are able to build markets with their own apps that are clean from a security point of view," Schütte adds.

The security filter for Android apps consists of an app installed on the user device that is directly connected to the IT architecture of the corporation through the analysis system called App Ray running in the back end. Searching for and downloading apps takes place exclusively through App Ray. "Employees are automatically presented only with safe applications," explains Schütte. That is guaranteed by the centerpiece of the store – the Backend Analysis Tool. It puts apps through their paces automatically and then authorizes them for release or not. "With the help of App Ray, we know where data flow to and from within an App, can investigate the files and source text they contain, chase down the technical details of all the data flows, run the app within a test environment and observe its behavior there. This creates a total security picture of every single mobile application available," as Schütte describes the MO. The AISEC solution works as a framework that

integrates existing security features, such as an analysis tool that investigates the Apps using forty different virus scanners simultaneously.

Provided by Fraunhofer-Gesellschaft