App security testing tool

July 22 2013

"Please contact the administrator." This error message usually flashes up on the monitor when employees want to install new software on their office computer. The reason is simple. Companies want to protect themselves and their computers against viruses and other malware, and make sure that confidential business information does not go astray. What is standard practice with fixed desktop computers is rather more difficult to implement with mobile smartphones.

It is almost impossible to stop employees installing a range of apps on their smartphones, particularly when the handsets belong to them, but operate on the business network. But just how trustworthy are those apps? Are they carrying malware that can steal documents and passwords, or damage machines and servers? What about security? Is important information being transferred without encryption? How are business documents saved? Can unintended viewers get hold of them if somebody happens to lose their smartphone?

Individual test reports

In the future the Appicaptor test framework, developed by researchers at the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt, will provide answers to these questions. The system provides companies with individual reports for every app and operating system. "Our Appicaptor framework consists of different analytic methods and tools," says Dr. Jens Heider, Head of Department at the SIT's Testlab Mobile Security. "It can analyze apps working on both Android and iOS-based smartphones, so it's able to work regardless of platform. It can also be built on to suit special requirements." Appicaptor screens for security gaps and malware automatically, and displays a warning if it finds anything. But a clean bill of health after one scan does not mean everything is fine for the long haul, so the software scans at regular intervals, as apps are modified and reconfigured frequently. Using Appicaptor, companies can put together an app-whitelist - a list of apps that employees are free to install on their smartphones. Or they can draw up a blacklist of apps that are dangerous and that employees must avoid at all costs.

"Appicaptor is not a piece of test software, but a flexible testing platform that brings together different testing tools," Heider says. The scientists put a lot of development work into making results intelligible. At first, only IT specialists were able to interpret Appicaptor's output. Now the software generates warnings that lay users can act on, such as "Security risk: This app is saving data without encryption." Another hurdle the researchers had to overcome was the impenetrability of iOS. Apple is very secretive about the structure of the system. This meant that the scientists had to delve deep to find out how it worked and decide which threats to the platform to screen for.

The framework is already in operation, but it is in constant development and being adapted to work with new operating systems. Researchers are currently testing and optimizing it with industry partners. This testing phase will continue until fall of this year. One result so far is that businesses often want a bespoke test case. Another requirement is that the system must be compatible with companies' own app stores and mobile device management systems. As a result, the SIT is only offering Appicaptor as a business services product. In spite of this, private users will probably benefit from the results gleaned. "We anticipate that apps will become better as a result of increasing checks, and security gaps will be less and less of a problem."

Provided by Fraunhofer-Gesellschaft

Citation: App security testing tool (2013, July 22) retrieved 20 March 2024 from https://phys.org/news/2013-07-app-tool.html