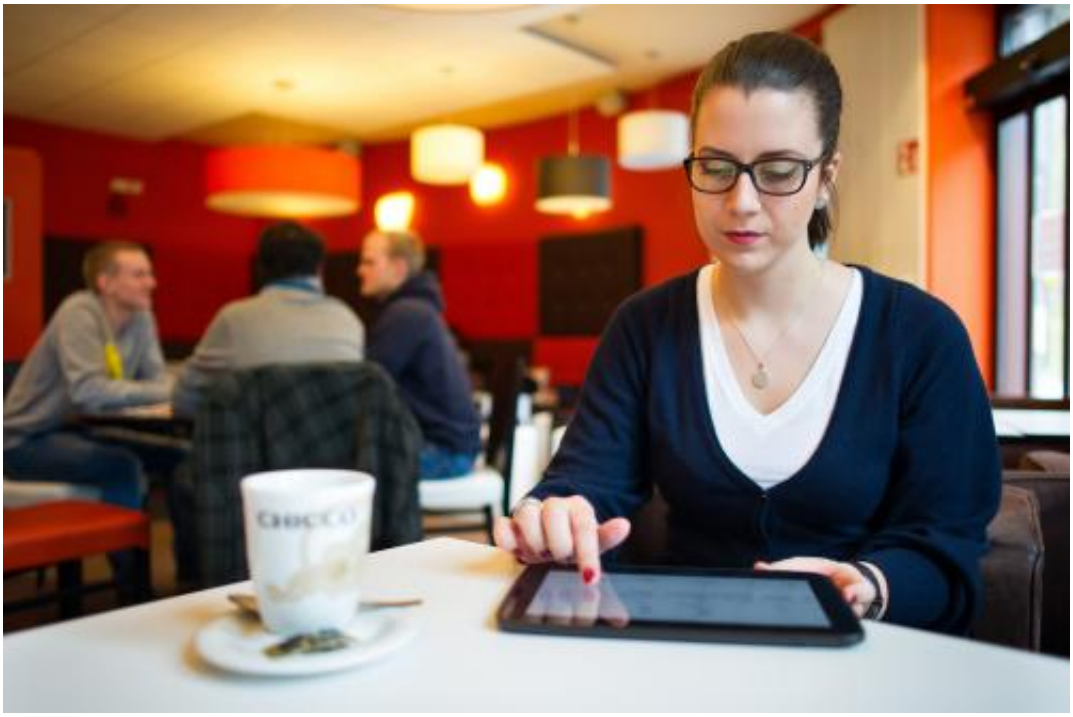
Cebit 2015: Find out what your apps are really doing

March 10 2015



The software from Saarland University uncovers data theft on mobile devices. Credit: Oliver Dietze

These tiny programs on Internet-connected mobile phones are increasingly becoming entryways for surveillance and fraud. Computer scientists from the center for IT-Security, Privacy and Privacy, CISPA, have developed a program that can show users whether the apps on their smartphone are accessing private information, and what they do with

that data. This year, the researchers will present an improved version of their system again at the CeBIT computer fair in Hanover (Hall 9, Booth E13).

RiskIQ, an IT security-software company, recently examined 350,000 apps that offer monetary transactions, and found more than 40,000 of these specialized programs to be little more than scams. Employees had downloaded the apps from around 90 recognized app store websites worldwide, and analyzed them. They discovered that a total of eleven percent of these apps contained malicious executable functions – they could read along personal messages, or remove password protections. And all this would typically take place unnoticed by the user.

Computer scientists from Saarbrücken have now developed a software system that allows users to detect malicious apps at an early stage. This is achieved by scanning the program code, with an emphasis on those parts where the respective app is accessing or transmitting personal information. The monitoring software will detect whether a data request is related to the subsequent transmission of data, and will flag the code sequence in question as suspicious accordingly. "Imagine your address book is read out, and hundreds of lines of code later, without you noticing, your phone will send your contacts to an unknown website," Erik Derr says. Derr is a PhD student at the Graduate School for Computer Science at Saarland University, and a researcher at the Saarbrücken Research Center for IT Security, CISPA. An important feature of the software he developed is its ability to monitor precisely which websites an app is accessing, or which phone number a text message was sent to.

To conclusively detect these functional relationships between the data source and the recipient, the researchers use contemporary methods of information flow analysis. They set their program up in advance with a list of suspicious code combinations that access programming interfaces,

so that it would learn to differentiate between "good" and "evil" apps, and additionally fed it with details of currently known attacks. "So it can be helpful, for instance, to know the telephone numbers of these expensive premium services. Say one of these numbers is dialed without the consent of the user, then the fraud is obvious," Derr explains. Since his method is computationally demanding and also requires a lot of memory space, the software is run on a dedicated server.

"It takes our software an average of 25 minutes per app," Derr says. So far, his research team has tested around 23,000 apps in this manner. And of course, consumers will benefit most from this approach. "The app could be analyzed on our server, and the results would be displayed on your smartphone. Or ideally, the evaluation process could be integrated directly into the app store websites," explains Derr. This is one of the reasons the Saarbrücken researchers are already discussing the issue with US online retail company Amazon. "But Google would certainly be an option as well,", says Derr.

Provided by Saarland University

Citation: Cebit 2015: Find out what your apps are really doing (2015, March 10) retrieved 14 May 2024 from https://phys.org/news/2015-03-cebit-apps.html