Detecting and blocking leaky Android apps

May 22 2015, by David Bradley

Nine times out of ten, that Android app is connecting to multiple internet destinations without your knowledge, more than half of them require access to the sensitive, personal information on your mobile device in order to function and more than one in five data "packets" these apps send contains some of that sensitive information. That's the conclusion of Japanese researchers writing this month in the *International Journal of Space-Based and Situated Computing*.

Hiroki Kuzuno and Satoshi Tonami of Intelligent Systems Laboratory, SECOM Co., Ltd., in Tokyo, analyzed the traffic and permissions of 1,188 free Android applications that use various advertising or in-app purchase models for their monetization. They demonstrated that 93% of those applications might compromise user privacy or security in various ways. As such, the team has now devised a clustering algorithm that can analyze the internet destinations to which such apps connect and a signature-generation system that could be used to quickly alert users to a leak of personal data from their device. Such a system would once again empower the end user to take control of their mobile device and help eradicate such behavior from the Android app ecosystem.

Smart phones are almost ubiquitous and vast numbers use the Android operating system developed by Google. There are more than 1 million applications, "apps" available to users of such devices that depending on the type of app can directly access the personal information, such as location tracking data, the address book, unique device identifier (UDID) and other data. The Android system can decouple device features such as network access, the built-in cameras, and sensitive data

in order to maintain security. However, many applications request permission on installation to access such features and many users check the boxes that allow such access without recognizing how this might compromise their privacy and security.

On the whole, the information to which apps have access is most commonly used for targeting the user with advertising, but might also represent the aggregation of personal data on remote servers that might be compromised by a third party. Either way, if users were fully aware of the problems that might occur with their mobile devices leaking data in this way, they might be more wary of installing many of the apps available, even those offered by apparently legitimate and well known online companies and services.

The team tested their leaked data detection system on the 1,188 apps in their collection and used it to analyze 107,859 data packets, of which 23,309 were identified as containing sensitive information. The system proved to be 97% accurate with just 3% false positives. Of course, once developed into an end-user product, the system itself could be added to a smart phone as an app.

More information: "Detection of sensitive information leakage in Android applications using signature generation." *Int. J. of Space-Based and Situated Computing*, 2015 Vol.5, No.1, pp.53 - 62 DOI: 10.1504/IJSSC.2015.067998

Provided by Inderscience