To Improve smartphone privacy, control access to third-party libraries

September 12 2017

Credit: CC0 Public Domain

Smartphone apps that share users' locations, contacts and other sensitive information with third parties often do so through a relative handful of services called third-party libraries, suggesting a new strategy for

protecting privacy, Carnegie Mellon University researchers say.

Controlling access to these third-party libraries, which help app developers make money by targeting people with ads or compiling marketing profiles, promises to be an effective way of limiting the unwanted release of personal information. The research team developed an app for rooted Android phones that manages interactions with these libraries and informs the user of how each library uses the data.

"Each of these libraries may be used by multiple apps on your smartphone," said Yuvraj Agarwal, assistant professor of computer science in the Institute for Software Research. "Making decisions about what information to share with each library, rather than just what each app should share, dramatically reduces the number of decisions a user has to make to protect privacy.

"It's also more effective because if a user allows even one app on their device to provide a particular library with access to their sensitive information, that's really all the library needs," Agarawal said.

In a new study, the CMU team analyzed how 1,300 people used 11,000 popular Android apps and found that the top 100 third-party libraries account for more than 70 percent of instances when private data was shared. In fact, just the top 30 libraries account for more than half of those occurrences.

The researchers will present their findings and their latest privacy management app at Ubicomp 2017, the ACM International Joint Conference on Pervasive and Ubiquitous Computing, Sept. 13-15 in Maui, Hawaii.

Third-party libraries are used by app developers to add functionality to apps, such as using Facebook libraries for authentication. They also

enable developers of free apps to make money by linking their app to them; the Google AdMob library, for instance, might access a user's location to target the user with ads, while the Flurry analytics library might gather user information for a marketing profile.

Recent versions of Android and Apple's iOS require users to make individual decisions on whether an app can access sensitive information. But users do not know why the app needs that access or whether it is related to functionality or simply for advertising.

"Users are often overwhelmed by the number of decisions they need to make," said Agarwal, who is affiliated with ISR's Societal Computing program.

The Protect My Privacy (PmP) for Android app the CMU researchers developed allows users to make decisions based on whether the app itself, or one or more included third-party libraries in the app, are responsible for access to their sensitive data. This gives the user more context for making privacy decisions. Testing showed that targeting libraries reduces the number of decisions users need to make by 25 percent.

The PmP app does not require users to make a yes or no decision about a library; it also offers the option of sharing only some information with certain libraries. In that way, users who appreciate free apps can still help support the app developer. For instance, if a user does not mind that a library knows what city the user is in, but doesn't want to share an exact address, the app can send suitably anonymized location information to the app.

"If I tell the library that I'm in Pittsburgh, it can still send me relevant ads, the developer can still make money, but I don't have to give my home address or my detailed whereabouts," Agarwal said.

The PmP app is available on Google Play, but only works on rooted Android phones—smartphones modified to give users complete access to the operating system. Most users choose not to root their phones; it can void warranties. But Agarwal said there is no reason why PmP's useful features could not be added by Google to the Android software, or by Apple to the iPhone's iOS. (An earlier version of PmP for jailbroken iPhones used by about 250,000 people does not yet include the library-based approach.)

"We're hoping our work will influence Google and Apple," Agarwal said. Google, in fact, provided some of the support for this study, as did the Air Force Research Laboratory and the National Science Foundation.

In addition to Agarwal, the research team included Jason Hong, associate professor in the Human-Computer Interaction Institute, Saksham Chitkara and Suhas Harish, both master's degree students in the Information Networking Institute, and Nishad Gothoskar, a senior majoring in computer science and mathematical sciences.

Provided by Carnegie Mellon University