As companies continue to steal private data, technical solutions may be the answer

October 22 2015, by David Glance

Credit: AI-generated image (disclaimer)

Apple has removed 250 apps from its app store because they were secretly stealing Apple users' account and device identifiers to Chinese advertiser Youmi. The developers of the apps were unaware that this was happening as they were simply using Youmi's service to display ads.

It seems Apple was also not aware that this was happening because Youmi was accessing parts of Apple's software that it was not supposed to under the terms of Apple's developer agreement. Apple would normally pick up these types of abuses before listing apps in the app store, but Youmi had gone to significant lengths to hide what it was doing.

Youmi is not alone in trying to circumvent Apple's rules and access information that they are not supposed to. In an analysis of 2,019 applications from the iTunes App Store, researchers from Purdue University found that 7% of them were accessing "private APIs", making them a security risk for anyone installing and using the apps.

There are other reasons that developers resort to accessing functionality in the system that they are not supposed to. Sometimes this is to get around a limitation in functionality of the system that Apple simply hasn't chosen to make available to anyone other than its own developers. In these cases however, developers are usually aware of the risks of having the app rejected by Apple during the app approval process during the submission to the app store. Deliberately hiding the fact that an app is using functionality it is not supposed to, clearly signals a darker purpose.

Even without these types of covert actions, users of apps necessarily have to trust developers not to misuse personal and private information that may be collected as part of the normal use of an app. This becomes more problematic with apps that deal with particularly sensitive data like a person's health or finances.

Technically, it is possible to adopt approaches to how personal data is stored on a mobile phone that makes it much harder for the application developer, or anyone else, to get access to that data without a user's explicit permission.

Apple itself has adopted some of these practices with the storage of data from its HomeKit and HealthKit services. A user's health data in HealthKit is stored only on the iPhone, and if backed up to the cloud, or even another machine, it has to be first encrypted by the data's owner. Any other app trying to get access to HealthKit data can only do so when the user has given explicit permission and has the screen unlocked. Of course, once the user has given permission, it is possible for an app to read and save the data elsewhere and once again, the user is at the mercy of whoever developed the app.

Unfortunately, there are few ways around this problem although one possibility may lie in a technology that allows the data to always remain encrypted when accessed by other applications.

One way to protect against the possibility of badly behaved applications from "leaking" potentially secure data and then storing it elsewhere is to use a technique that is called "homomorphic encryption". This is a system that allows for the data to be encrypted and still allow access by way of queries that are also encrypted. In this way, anything asking questions of the data can get an answer but at the same time, be prevented from knowing the data that went into forming the answer.

This was thought to be completely impractical to implement until Craig Gentry), a research scientist working at IBM described how it could be done.

Homomorphic encryption may provide part of the answer to protecting personal data whilst still allowing other connected applications from getting answers to questions about the data. It is not the complete solution however as it is necessarily limited in what sort of interactions it allows.

Chinese advertising company Youmi has now apologised for its

"snooping" on users' private data. It is not clear how sincere this apology actually is and certainly the fact that there is little consequence for these actions will not dissuade it, or others, from doing the same again. A technological solution that enforces good behaviour on companies to whom we entrust our data may be the only way this data will stay protected and under our control.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation