3-2019

Functionality & privacy in mobile applications - who's going to win the game

Debin Gao
Singapore Management University, dbgao@smu.edu.sg

FUNCTIONALITY & PRIVACY IN MOBILE APPLICATIONS – WHO'S GOING TO WIN THE GAME?

GAO DEBIN

ASSOCIATE PROFESSOR OF INFORMATION SYSTEMS
FACULTY MANAGER, SMU BSC (IS)-CMU FAST-TRACK PROGRAMME

"WHEN IT COMES TO MOBILE APPS, DEFENCE AND ATTACK ARE IN PERPETUAL ARM-WRESTLE"

MOBILE APPS have brought so much convenience and fun into our lives. From route planning to grocery shopping, reserving flights and hiring bicycles, to the action games we play to pass the time on public transport.

But have we become so seduced with the seemingly limitless functionality of mobile apps that we're overlooking their fundamental downside – the potential compromise of our security and privacy?

Security issues can arise as a result of vulnerabilities embedded inside an app, typically unintentionally, during the development stage, which can then be exploited by malicious hackers. Privacy concerns come from the intentional leaking of private user information to third parties without the user's knowledge.

Some users choose to ignore such concerns because they find the functionality gained from the apps - many of which are free of charge - outweighs the security and privacy risks. And on the other side, developers actively invest time and money to reap the potential gain from the collection of behavioural data – through a heavily subsidised bicycle rental app for example. So will mobile apps ever offer functionality as well as privacy and security?

In general, developers are (slowly) producing more secure applications. That said, no matter how much technology advances, and how much better we understand security, developers are human beings and humans do make mistakes. Also, the economics of the app market sets a

low bar for security in order to encourage individual developers, and those who are less experienced, to publish their apps. And of course, as more and more of us use apps, so the market for malicious activity expands.

Unlike many other products, there is no universally agreed security standard for mobile apps and, despite the research community's best efforts, testing for security is fraught with challenges for three key reasons:

First - there remains a lack of reliable yet simple-to-use technology to check security with high precision and efficiency - not to mention obfuscation techniques employed by some app developers to make the task even more challenging.

Second, it may be hard to draw the line between the legitimate and the illegitimate when evaluating some specific operations of an app. For example, a currency-converting app may collect geo-location to infer the local currency, but it's arguable whether this is necessary especially if fine-grained geo-location data is captured and sent back to the developer.

And third, the application of strict screening rules may not be in the economic interests of the app markets themselves. The security standards that do exist currently are set by the two dominant market players Google Play and the iOS App Store – both perform quality control via a review process, where the developers submit their app for review before they can be published on the market.

Interestingly, besides providing some guidelines in developing good applications, the review process of neither market is transparent. This makes it challenging to establish a universal standard – although equally it can be argued that this opacity also makes it harder for malicious apps (especially those intentionally-made ones) to go undetected.

However, many also feel that the key barrier to ensuring security and privacy is the human factor. When presented with new and exciting functionality and features, users tend to forget about security and privacy concerns. Many even make an informed decision and opt for using insecure software as long as the gain in functionality is good enough. This behaviour is also observed at corporate level where companies frequently opt to invest more on software functionality but much less on software security.

When it comes to mobile apps, defence and attack are in a perpetual arm-wrestle – and there is no simple solution. Ultimately however, it is possible for app functionality and privacy to coexist. Modern mobile operating systems are privacy-aware, and have matured systems which can handle private information properly and it's not difficult for app developers to take necessary steps in using and securely managing this private information.

And as end user awareness of security and privacy grows, it's likely those engaged in the malicious, misuse of the technology will find it harder and harder to bring their efforts into the marketplace.