What is the price of free?

March 6 2012

Android. Credit: University of Cambridge

Scientists from the Computer Laboratory at Cambridge University have designed a method to improve privacy control in the Android apps market. The method reaches a balance between the need for developer's revenue and the need for user's privacy.

As the market expands, it has become a question of freedom versus control in the Android app market. Security is playing catch-up, as the breaching of personal privacy increases due to a deluge of malicious software being released into the marketplace.

In a recent case, the social network Path found itself at the centre of fierce controversy, after accessing and uploading iPhone users' contact databases without their permission.

Smartphone apps provide useful services. However, there is a hidden

cost, often unknown to the user – developers collect information about the user without their full knowledge. Apps can access your contact numbers, track your current location, view your web history and then share this data with mobile ad networks.

As a result of growing concerns about users' data privacy, the United States White House has released a first draft of a Consumer Privacy Bill of Rights which aims to give consumers the right to exercise control over what personal data companies can collect and how they use it.

To understand the privacy implications of mobile applications, the Cambridge team wrote a programme that was able to collect and analyse the metadata of 251,342 applications available on the online market.

The Android market consists mainly of free applications (73%). The analysis revealed that 80% of those are supported by targeted advertisements. Furthermore, free applications are far more popular in terms of downloads as only 20% of paid apps get more than 100 downloads and only 0.2% of paid apps have more than 10,000 downloads (compared to 20% of free apps).

At the same time, based on the results of this study, free apps request significantly more permissions to access sensitive information such as the user's location, messages (e-mail/sms), contacts, calendar, phone number and IMEI. This includes, for example, 35% of free applications in the "comics" category that request access to the user's location, or games asking for the user's phone number and contacts (just to name a few).

In fact, more than 70% of free apps request one such "dangerous" permissions compared to just 40% of paid applications. Although the Android market raises alerts for applications that require dangerous permissions, this analysis revealed that these alerts have no impact on the

decision of users to download applications. Indeed, the number of downloads for a given application appears to not be correlated to the number of dangerous permissions they request.

Free applications request additional information merely to support their own revenue as mobile advertisements typically capture personal information in order to profile the mobile phone user and deliver relevant advertisements to the mobile phone. However, as the media stories have revealed, not all of the 52,680 developers can be trusted. The problem with the current app model is that the developer is responsible for collecting as much information as possible and forwarding it to the advertising networks in order to display these targeted advertisements.

Dr. Ilias Leontiadis and Dr. Christos Efstratiou, from the Computer Laboratory at the University of Cambridge, said: “Various researchers have proposed ways of protecting privacy in the past, by either blocking information or giving fake information to the mobile application. However, if we follow this paradigm this would significantly reduce the number of free ad-supported applications that are available today. In our work we have tried to design a new approach that can reach a balance between the need for developer’s revenue and the need for user’s privacy.”

The new model is based on applying a more sensitive approach to privacy control. The process focuses on ‘decoupling’ (separating) privacy control between the application and the advertisement support component, where two separate flows of information are allowed: one towards the application/developer and one towards the ad-networks.

The ‘decoupling’ allows the specification of distinct privacy requirements for the two entities. For the application, this allows the specification of privacy requirements that are directly related to the

actual service offered by the application. For the ad-network component, the distinct flow of private information can allow the implementation of privacy control techniques specifically designed to support an ad-driven market.

Dr. Ilias Leontiadis, said: “We’ve developed a method that can control how much personal information is released to advertisers depending on the revenue that a developer receives. This means that if a developer gets enough money for their ad-supported applications, then private information can be selectively blocked to protect users.”

Provided by University of Cambridge