Android Permissions

As mobile technology advances we have seen a massive rise in mobile gaming and an exponential growth of content available for download. Most apps require some permissions to access data on the mobile device. Some of these permissions are necessary for the normal running of the app, some of them are extras that are useful but not integral, and some can be considered totally unneeded and invasive. I will explore various studies and compare findings to determine attitudes towards permissions and how well informed people are of what they are agreeing to.

In 2014 Olmstead and Atkinson of Pew Research Center (a US based tech and science information website) conducted a study into android app permissions and the nature of said permissions. In total 235 unique permissions were identified. 165 of these dealt with access to hardware and the remaining 70 related to user data. Only a handful of these permissions are commonly used and all developers are forced to use the same generic permission descriptions which can be misleading.

One of the most commonly used permissions is ‘Modify or delete the contents of your usb storage’ This permission allows an app to access an installed SD card or internal memory. This can be used for something as simple as saving data for progression in a game. Or can be used with malicious intent to access and steal images or sensitive data stored on the device. ‘Ultimately, this permission could certainly give an app access to user information — but this potential is highly dependent on each user’s individual situation and device.’ (Olmstead & Atkinson, 2015).

Also in 2014 Kang et al. published a paper looking at android app permissions and user attitudes towards them. In their study, they asked university students to answer a series of questions about apps and their permissions and a preliminary questionnaire about their knowledge and familiarity of permissions.

The responses to the preliminary questions show some interesting statistics. Slightly less than 57% of users said that they understood what is meant by app permissions and only 25% of participants said they pay attention to permissions. The demographic used to obtain these figures may mean the wider world may be even more shocking. ‘our sample of users, on average, are younger (97.98% of them were aged between 18 and 29) and have higher education’ (Kang, Kim, Kim, & Huh, 2014). This leads me to believe that with a wider demographic far less than 25% of users will consider permissions before accepting.

Both papers also explore the number of permissions in a new app vs an established app. New apps tend to have less permissions and only include those necessary for the running of the app. New permissions are then added in new updates and users may accept these without considering if they are necessary. In this fashion, more and more permissions are added to the point an established app could have almost total control of your device hardware and its contents, far beyond what is needed for the core functionality of the app.

Due to this growing concern of app permissions in 2013 the Guardian published an article about their own mobile app and a detailed breakdown of permissions and why each was needed. One of these permissions is also very popular with mobile and even web apps, ‘find accounts on device’. This permission allows the app to access your social media accounts and use your details for a secure login. While this saves the user time in having to fill out their details and sign up for yet another account, it also gives the app complete control over your social media app. While you can trust reputable apps to an extent, ‘We never use or post content to any social networks without asking you first.’ (Grinsted, 2013) malicious apps are able to use this permission to post to your social media without your knowing.