Understanding and Granting Android Permissions: a User Survey

Selvakumar Ramachandran*, Andrea Dimitri⁴, Maulahikmah Galinium‡, Muhammad Tahir§, Indirajith Viji Ananth†, Christian H. Schunck†, and Maurizio Talamo¶

* University of Sunderland, Sunderland, UK; Email: firstname.lastname@sunderland.ac.uk
† Fondazione Inuit, University of Rome Tor Vergata, Rome, Italy; Email: firstname.lastname@inuitroma2.it
‡ Swiss German University, Jakarta, Indonesia; Email: firstname.lastname@sgu.ac.id
§ Sir Syed University of Engineering and Technology, Karachi, Pakistan; Email: mtahira@ssuet.edu.pk
¶ Department of Business Engineering, University of Rome Tor Vergata, Rome, Italy; Email: firstname.lastname@uniroma2.it

Abstract—Whenever users install a new application on their smart devices with an Android KitKat or Lollipop operating system they are asked to grant the application (app) provider access to features of the device, ranging from data storage to device location and from device identity to the user’s personal contacts. The implications on users’ privacy and security are significant and therefore the users’ ability to give “informed consent” is highly important. Previous work has identified low rates of user attention and comprehension to permission warnings and resulted that these fail to inform the majority of users. Here we focus on how users consider, interpret and react to differences in app permission information which is provided at three different instances of the app installation cycle: 1. Before installation in the Google Play Store 2. During the installation process 3. After installation in the Application Manager. The information provided in these instances varies considerably in its granularity and detail. For this purpose, an online survey was developed in which users were asked questions regarding the installation of a “mirror” app whose main functionality is to use the user facing camera of the phone to “mirror” the user’s face (i.e. display an image of the face) on the phone’s screen. The survey participants were shown screen shots of the app description as presented in the Google Play Store as well as of the various permission lists as they appear on the screen of the phone. The questions focused on the respondents’ perceptions and their hypothetical choices with regard to the installation of this app. Results show that the various presentations of permission information in Android versions KitKat or Lollipop cause concern and irritate a majority (51.67%) of users, especially those with some basic IT expertise. We conclude that the contextualization of app features and functionalities with the corresponding permissions needs to be improved especially for users with little IT expertise. Further user permission information should be made available at different and consistent levels of granularity.

I. INTRODUCTION

Since 2011, Android is the most widely used mobile operating systems across the world [1]. A significant factor of its success is the large availability of applications (apps) users can download and install on their devices from the Google Play Store: as of August 2017 more than 3 million Android apps are available [2]. Increasingly, mobile devices are used to implement important security functions related to payments, identification and access control [3], [4], [5], [6]. To fulfill their functional requirements apps need to get access to certain resources and data on the mobile device. Users must grant the requested permissions.

Due to the large Android user base the incentive to distribute grayware or malware is high and the number of problematic apps is constantly increasing [7] [8]. For protecting their privacy and security it is thus critical that users pay attention to permission requests. Users should be able to assess whether the requested permissions are actually aligned with the app’s key functionalities. If the requested permissions go significantly beyond what is required for the app to perform correctly this could be an important indicator that the app is grayware or malware trying to exploit and/or cause damage to the user. Since Android apps are not reviewed it is critical that users correctly assess app permissions so that they can protect their personal data.

In the most used Android operating system versions of early 2016 (KITKAT and LOLLIPOP) [9] users are requested to grant app permission at installation time. Installation can be aborted if the user does not want to grant an app the requested permissions. This procedure was changed with the introduction of the Android Marshmallow operating system where users are requested to grant permissions when an app is used for the first time and not when it is installed. At the time of this survey was conducted (March to May, 2016) [10] less than 10% of Android devices ran Marshmallow. Thus we disregard how app permissions are granted in Marshmallow for this work.

To complicate the overall situation, in Android KITKAT and LOLLIPOP app permission are displayed to users in three different forms and with inconsistent levels of granularity before, during, and after app installation.

In this work we study what factors motivate users to install apps and the ability of users to connect the description of app functionalities to required app permissions. Further we explore how the varying granularity and presentation styles of permission information provided at installation time, in the Google Play Store and in the Application Manager affect users...
and their decision making.

II. BACKGROUND AND RELATED WORK

Android’s permission system is intended to inform users about what features of the phone (in terms of sensors and data) the app requests to access. This information is indicative of the potential privacy and security risks users accept when installing an app. At the time a user installs an app, he or she has the opportunity to review the application’s permission requests and to cancel the installation if these are found to be unacceptable.

For improving the security and privacy comprehension of end users, permission requests and textual descriptions are provided by Android apps. These have been found to be hard to comprehend for users but also to be in part misleading with regard to privacy protections [11] [12] [13].

Felt et al [14] discuss the effectiveness of Android permissions by studying both user attention and comprehension. The study finds that both attention and comprehension is low. In fact, only 3% of respondents were actually able to answer all permission comprehension questions they received correctly. This is a very low percentile, however permissions can relate to relatively intricate aspects of accessing data and sensors. Answering the related questions correctly is thus not always straightforward even for users with IT expertise.

Kelley et al. [15] find through 20 semi-structured interviews that users are often unaware of the security risks associated with mobile apps and falsely believe that apps are tested and questionable apps are rejected before they become available in the Google Play Store.

Several tools have been developed for avoiding privacy violations mostly by identifying malevolent behavior of apps [16] [17] [18] [19] [8] [20]. Ref. [21] introduces a sensor-access widget, a graphical user interface element which resides within an application’s display and which provides an animated representation of the personal data being collected by its corresponding sensor, calling attention to an application’s attempt to collect data. However, it is not clear to what extent users with little IT background are aware of such tools and what fraction of these users would actually see a need to install them.

Android KITKAT and LOLLIPOP users can review individual app permissions in three ways:

- Permission list of the latest version of an app as available in the Google Play Store
- Permission list displayed to the user at installation time (i.e. when the user is requested to grant the permissions)
- List of permissions previously granted to an installed app made available via the application manager

An example of such different permission list is shown in figure 1 (for the “mirror app” referred to in the survey). As can be seen from this example app permissions are actually displayed and commented differently in each presentation mode.

A central aspect of this work - which has so far not been addressed - is to study how users perceive the differences between these three representations of permission information. We aim to understand whether users actually care about these differences and how users feel affected by them. Evaluating differences in permission representation becomes very intricate if apps require a complex set of permissions. To reduce complexity we thus focus - in contrast to some studies mentioned before - on a simple app which strictly requires just one permission to provide its basic functionality. This procedure allows us to obtain a realistic picture of what fraction of users is actually able (both in terms of attention and comprehension) to correctly identify a strictly required app permission in a simple and straightforward context.

III. METHODOLOGY

The Internet based survey (in two slightly different variants) was promoted via social media during the period of March 18, 2016 to May 2, 2016. Respondents were recruited via several Facebook profiles including two popular Facebook users from India, with more than 20,000 followers each. Any statements and opinions provided as comments in the social media were promptly deleted by the promoters in order to reduce bias. A total of 510 completed Android users surveys were obtained.

The survey is intended to focus on Android users only. Therefore, the first question in the survey was chosen to be “Have you ever installed an App on an Android device?”.

For respondents who answered “no” the survey ended at this point (leading to the exclusion of 31 responses). One response included inappropriate comments and was excluded for that reason. The total number of responses analyzed is 478.

A. Survey structure

The survey consists of 13 technical and 6 demographic questions regarding gender, age, occupation, country of residence, self declared IT expertise, and the android device type/model used. Optionally, users could provide an email address and leave a final comment.

To reduce the level of abstraction, many questions of the survey were centered around a simple example app available in the Android store, providing a single core functionality. The chosen app is a “mirror app”. This kind of app provides a mirror functionality, i.e. it displays objects much like a simple, hand held mirror would do. In principle a user could obtain this basic functionality without using any dedicated app just by operating their phone’s camera in front mode operation, i.e. in “selfie mode”. It is fairly obvious that a permission to use the phone’s camera is required for such an app to work. Given the simplicity of the idea behind this type of application there are many “mirror” apps available in the Google Play Store. For the survey an application was chosen which requests several additional permissions along with the permission for camera access. This choice allows us to study 1) whether users can correctly identify camera access as a required permission and 2) whether users differentiate between such strictly required permissions and other - not strictly required permissions - that may be requested by such an app.
Fig. 1. Permission list shown to the user. (Left - Android Store; Center - At Installation; Right - Application Manager)

Fig. 2 shows a screen shot of this mirror app as presented in the Android store. Note that the description of the app explicitly states that the app “uses the front facing camera to function as a mirror”. From the further app description “offers a selfie camera, freeze frame feature and some other great settings” one can conclude that the “Photo/Media/Files” permission is required as well in order to be able to store photos. To further reduce the level of abstraction it was decided not to show all three ways of representing app permissions in each survey. Therefore two variants of the survey were created which differ in the permission list shown in the context of question 8:

- “Assuming that you would like to have such a Mirror App on your device, how comfortable are you with the requested permissions shown above?”

In one variant a screenshot of the permission list of the mirror app as displayed in the Android store is shown in the context of this question (see panel 1 of fig. 1). In the other variant a screenshot of the permission list displayed at the time of installation (panel 1 of fig. 1) is shown instead.

The full survey questionnaires are accessible via the links provided in references [22] and [23]. From the 478 analyzed surveys 171 were based on variant 1 and 307 were based on variant 2.

B. Survey content

The survey set out with three questions focused on gaining a better understanding of some of the criteria which might influence a user’s decision to install a certain app.

- Are the expected features of an app a criterion for installing it?
- Are endorsements from friends and relatives a criterion for installing an app?
- Is the popularity of an app a criterion for installing it?

The more technical questions focused on the following aspects:
• User’s carefulness while reading a permission list.
• Attention to and comprehension of required permissions when installing an app.
• Select the permissions required by the mirror app to provide the functionalities described in the Android store from the full list of possible permissions.
• Assess level of comfort with permissions in fact requested by the “mirror app”.
• Assess knowledge about the possibility to check app permissions after installation.
• Impact of discrepancies in displayed permission information between the Android store/at installation time and the permissions displayed in the application manager.
• Identification of not strictly required permissions.

C. Data Analysis

The variables associated with the survey were grouped in three classes: general or social variables, profiling users in general; technological variables related to technical knowledge and awareness; action variables, indicating effective and practical user behavior. Statistical logistic regression was carried out to explore the relationships between these three classes in order to gain a deeper understanding of different user types, their choices and how these users feel affected by the different app permission representations.

To measure the influence of the expertise level of a single answer in a question we used a logistic regression model [24] where every level of expertise is a candidate predictor and the dichotomic dependent variable is the answer (the probability to choose or not to chose a specific answer in the set of all available answers associated to a question). For every couple (X,Y) where X is an expertise level and Y is an answer (for the specific question) we calculate the beta (correlation) parameter and we verify its significance using the Wald test [25].

To analyze categorical data cross-tabulation [26], also known as contingency table analysis was carried out. Cross tabulation is a two or more dimensional table with frequency of respondents that have specific characteristics described in the cells of the table. To measure the strength of the relationship between the variables, chi-square statistic was used.

Our results are presented by quoting the beta parameter (correlation) and Wald test values. The Wald test value has to be evaluated considering that the significance threshold for a $p$ value of 0.05 (0.01) corresponds to 3.84 (6.64). Higher values of the test value imply higher confidence in the validity and significance of the beta parameter value.

IV. RESPONDENTS

The surveys received responses predominantly from India, Pakistan, Indonesia, Europe and North America (see fig. 3). 13% of the respondents were female and 80% male. 97% of respondents were below the age of 45 years (see figure 4). 31% of respondents responded “yes” to the question “Are you an IT expert?”, while 69% responded “no” or “not sure”. A large fraction (41%) of the respondents were students, 31% stated that they are working in the IT sector and 20% stated to be working outside the IT sector (see fig. 5).

V. SURVEY RESULTS

A. Criteria for selecting Apps

The expected features of an app matter for a majority of respondents (70.5% chose 4 or 5 out of a scale of 1-5), followed by popularity (62% chose 4 or 5 out of a scale of 1-5). An endorsement by friends and relatives matters only for a minority (42% chose 4 or 5 out of a scale of 1-5) of respondents. However, for those respondents who identified
themselves as IT experts endorsements are significantly more likely to matter highly (beta 0.639, test 7.1).

B. Attention to and comprehension of permissions

Respondents were shown a typical permission list of a very popular app (installation perspective) and were asked

- “How carefully do you usually read the list of permissions when you are about to install an Android App from Google Play Store?”

23% of respondents answered 5 on a scale from 0 (not at all) to 5 (very carefully). However, about 63% of respondents chose an answer between 1 and 3 (about equally distributed between 1 and 3). We find a significant correlation between users claiming to be an IT expert and their claim to read app permissions “very carefully” (beta 0.896, test 15.8).

The respondents were then introduced to the “mirror app” and - based on that description as shown in fig. 2 - were asked to select permissions that “should in your opinion be requested by the app for providing the promised functionalities”. 65% of the respondents correctly concluded that the “mirror app” requires camera access (even though this was explicitly pointed out in the app description shown to the survey participants). This implies that - even in this simple and highly contextualized example - 35% of respondents did not pay the required attention and/or did not have a sufficient level of comprehension to correctly identify the camera permission as a required one (see fig. 6). Respondents who correctly identified the camera permission as required were found to be significantly more likely to claim that in the app selection process the “expected features highly matter” (beta 0.875, test 19.9) underlining that a certain level of attention and comprehension is the basis for developing some degree of selectivity with regard to app features. Further, respondents who characterized themselves as IT experts were found to have a significantly higher probability to correctly identify the camera permission as required (beta 0.535, test 6.09).

The respondents were then confronted with the actual permissions requested either as displayed in the Android store (variant 1) or as displayed at installation time (variant 2). First, we do not find any evidence that differences between the permission view at installation time and at the Android store significantly influence the responses to any survey questions. As can be seen in fig. 2 the app requests some permissions (like “location”) that cannot be readily justified by the app’s main feature. The respondents were asked

- “Assuming that you would like to have to such a Mirror App on your device, how comfortable are you with the requested permissions shown above?”

The results are shown in the second panel of fig. 6. We find a significant correlation between respondents having correctly identified the camera as a required app permission and their choice of being “not comfortable - will not install this mirror app” (beta 0.807, test 11.5). On the other hand users that have not chosen the camera tend to the decision “very comfortable - will install the mirror app” (beta 0.764, test 10.7).

C. Perception of permission list in application manager

The final technical questions of the survey were devoted to understand whether the differences between the permission information displayed before (Android Store) or during installation versus after the installation (in the application manager) is causing concerns or is not perceived as relevant. About 66% of respondents correctly believe that it is possible to check app permission after installation and about 45% claim to have already done so.

Survey respondents were shown a screenshot of the permission list in the application manager (see panel 3 of fig. 1). When asked

- “In your opinion, are the permissions given in the list above (as shown in the application manager after installation) consistent with the permissions you have granted at the time of installation?”

a total of 247 respondents (51.67%) answered that there are discrepancies out of which 121 found these to be “major” and 126 “minor”, see fig 7. Those respondents who correctly included the camera as a required app permission were significantly more likely (beta 1.36, test 25) to perceive discrepancies whereas respondents who did not identify the camera as required were significantly less likely to perceive discrepancies (beta 0.727, test 11.3). This result clearly indicates that the sensitivity to differences in app permissions critically depends on a basic level of comprehension and
attention which a significant number of respondents do not demonstrate even in this fairly straightforward scenario.

VI. CONCLUSION

Respondents who demonstrate a low degree of attention and comprehension appear to feel comfortable with the requested app permissions even if these cannot be justified by the primary app functionalities. Such users also show little discernment for differences in how app permission are presented. Compared to other work, a relatively large fraction of users (65\%) actually correctly identifies a critically required app permission. We believe that this is related to the provided example which supports contextualization.

Therefore any requested app permissions should be contextualized to the largest degree possible so that users may understand more easily in what context and for what app functionalities certain permissions are required. Newer versions of Android have made progress in that regard by not requesting permissions up-front at installation time, but at the time an app is attempting to access data, sensors or features that require a user permission. However, more work is required to assess the actual impact of this change especially on users with no or little IT expertise.

The different presentations of app permissions caused significant concern among those users who demonstrated a sufficient understanding of what permissions are required. In current Android versions an editable overview of app permissions is provided in the application manager. This avoids the confusion created by providing several perspectives. However, this has been achieved at the expense of significantly reducing the granularity of permission information. It might be desirable to provide a layered view with different and consistent levels of granularity instead. This would provide a short, informative overview for less experienced users but allow - at the same time - a more differentiated assessment by the more experienced and concerned users.

The finding of this work are particularly important if applied to sensitive health-care apps and will be taken into account for more experienced and concerned users. The more experienced and concerned users.

This work has received funding in part from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 689209.

ACKNOWLEDGMENTS

This work has received funding in part from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 689209.

REFERENCES


