Users Comprehension and Behaviour Study on Android Permissions

Normi Sham Awang Abu Bakar
Department of Computer Science
International Islamic University Malaysia
Kuala Lumpur, Malaysia
nsham@iium.edu.my

***Abstract*—**The Android Market has become the main source of applications (apps) download for Android based devices. The majority of users trust that the apps that they downloaded are safe and trustworthy. However, it is not always the case since a large numbers of apps contain several unnecessary permissions that will potentially provide threats to the users' privacy and security by stealing their important data, and also offer services that will cost money to the users. The main objective of this paper is to investigate the level of knowledge, understanding and behaviour of the users towards these permissions. The results obtained show that the awareness on these permissions among the users is still low and they need to be cautioned against the potential threats of these permissions to ensure that they can make a well informed decisions whether to install the apps or not.

***Keywords*—**Android applications; permissions; comprehension; behaviour; privacy

I. INTRODUCTION

Smart phones are becoming vital to our communication and information needs. A smart phone's ability to provide assistance our lives is directly related to the richness and quality of its mobile applications. In today's world, two main smart phone operating systems are Android and iOS. As such, the Android Play Store leads in the number of apps hosted, where, as of July 2015, the apps being hosted have reached a staggering 1.6 million, followed closely by Apple App Store with 1.5 million apps [1].

A key difference between the Android Market and the Apple App Store is that the Android Market is open, whereas the Apple App Store is gated. That is, developers self-publish to the Android Market, whereas developers must submit applications for publication to Apple, and Apple decides what gets published. Google follows an egalitarian, open model for the Android Market. Developers see this as a significant advantage that lets them control publication. So, more applications will be available to consumers because publishing them is easier. The disadvantage is that the Android Market, and therefore consumers, might be inundated with low-quality applications, making finding high-quality applications more difficult [2].

From an architectural viewpoint, Android applications are safer than iPhone applications. Each Android application runs in its own space and does not access the data from other applications without explicit user permission. iPhone applications can access many system resources by default, thereby letting the applications access user information without user permission.

Because users control which services an Android application can access, they control their own security and privacy. On the other hand, iPhone users required to believe that Apple has thoroughly evaluated each application before publishing it [2].

Although Android puts the control in the users' hands, users aren't necessarily protected from malicious applications. For example, if users download an ad-based application that sends text messages to and receives messages from friends, they must give the application access to [2]:

- personal information (to read contact data),
- all messages (to read received messages),
- network communication (to download ads from the Internet), and
- services that cost money (sending messages can incur charges).

In general, there are two steps in obtaining permissions. First, an application developer declares that his or her application requires certain permissions in a file that is packaged with the application. Second, the user must approve the permissions requested before installation. Each application has its own set of permissions that reflects its functionalities and requirements. Users can weigh the

permission against their trust of the application and personal privacy concerns [3].

The official Android Market provides every application with two installation pages. The first installation page is comprised of a description, user reviews, screenshots and an "Install" button. After pressing "Install", the user is shown a final installation page that includes the application's requested permissions, as shown in Fig. 1. Permissions are displayed as a two-layer warning: a large heading that states each permission's general category, and a small label that describes the specific permissions. If a user clicks on a permission, the detailed description will be shown. The detailed description may include examples of how malicious applications can abuse the permission, e. g., "Uses the device's location". The permission system gives users a binary choice: the user can accept all of the permissions and proceed with installation, or cancel the installation.

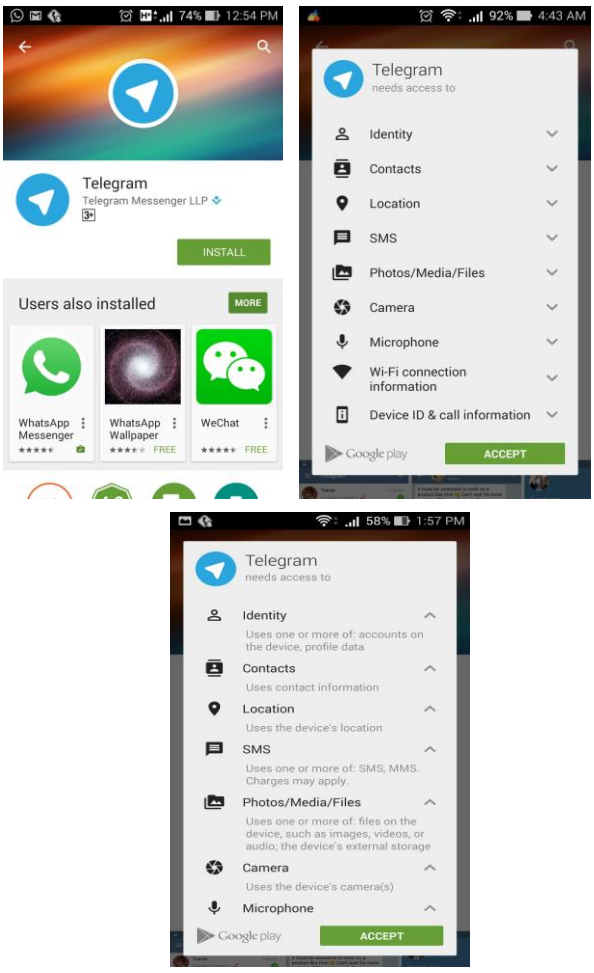

Figure 1. Top left, the Download page of an application, on the top right is the final installation page which displays the application's permission requests. At the bottom, the permission descriptions that appears if a user clicks on a permission warning.

The remaining parts of this paper are structured as follows: Section 2 discusses the prior related work, whereas Section 3 explains the Android permissions model. The research methodology is presented in Section 4, while Section 5 highlights the results of this study and finally, Section 6 concludes this paper.

II. RELATED WORK

The research on Android permissions encompasses various scopes and spectrums. The most relevant work to this research is the previous research done by Felt et. al. [3] where they examine whether the Android permission system is effective at warning users. Specifically, they evaluate whether Android users pay attention to, understand, and act on permission information during installation. They conducted two usability studies: an Internet survey of 308 Android users, and a laboratory study of 25 Android users. They found that study participants displayed low attention and comprehension rates: both the Internet survey and laboratory study found that 17% of people paid attention to permissions during installation, and only 3% of Internet survey respondents could correctly answer all three permission comprehension questions. They suggest that this indicates that current Android permission warnings do not help most users make correct security decisions.

In a similar line, Kelley et. al. [4] performed a series of semi-structured interviews in two cities to determine whether users read and understand the permissions screen, and to better understand how people perceive the implications of their decisions. Their results show that permissions displays are generally viewed and read, but not understood by Android users.

Another work by Felt et. al. discusses Stowaway, a tool for detection of overprivileges in compiled Android applications [5]. They test 940 applications and argue that one in three applications is overprivileged.

Stevens et al. [6] analyze about 10,000 free apps from popular Android markets and found that a significant sub-linear relationship between the popularity of a permission and the number of times when it is misused. Furthermore, they also study the effect of the influence of a permission (the functionality that it controls) and the interference of a permission (the number of other permissions that influence the same classes) on the occurrence of both permission misuse.

The study by Vidas et al. looks at the way permissions are managed in Android. It states that because developers do not have an easy way to determine which of the 130 application permissions their application needs, they end up specifying more permissions that they need. This results in the violations of least privileges principle [7].

Kang et al. shows that Android stores the users' sensitive information in a log file, which can be exploited by a

malicious user [8]. Security vulnerabilities also affect the user privacy. Xu et al. found security vulnerabilities in 3G smartphones, which can allow a malicious user to gain access to the user's videos [9].

From the security point of view, Sellwood and Crampton [10] analyzed the evolution of the Android permission architecture across six versions of the Android platform. They also identified a weakness in the way that the Android platform handles app permissions during platform upgrades and explain how this weakness may be exploited by a developer to produce malicious software which the average user is unlikely to detect.

Kraus et al. run a lab experiment with 48 participants and they find that users tend to choose more often the app with a lower number of permissions when statistical information with graphics were given to the participants [11].

III. ANDROID PERMISSIONS MODEL

Android applications are primarily written in Java. Unlike standard Java applications, after being compiled into Java bytecode Android applications are converted into the Dalvik Executable (DEX) format. This conversion occurs because Android applications run in the Dalvik [12] virtual machine, rather than the Java virtual machine [13].

Android applications are distributed in compressed packages called Android Packages (APKs). APKs contain everything that the application needs to run, including the code, icons, XML files specifying the UI, and application data.

Each Android application contains an important XML file called a manifest. The manifest file informs the Android framework of the application components and how to route Intents between components. It declares which permissions the application must have in order to access protected parts of the API and interact with other applications. It also declares the permissions that others are required to have in order to interact with the application's components [14].

A *permission* is a restriction limiting access to a part of the code or to data on the device. The limitation is imposed to protect critical data and code that could be misused to distort or damage the user experience. Each permission is identified by a unique label. Often the label indicates the action that's restricted. For example, here are some permissions defined by Android [14]:

android.permission.CALL_EMERGENCY_NUMBERS
android.permission.READ_OWNER_DATA
android.permission.SET_WALLPAPER
android.permission.DEVICE_POWER

A feature can be protected by one permission. If an application needs access to a feature protected by a permission, it must declare that it requires that permission with a <uses-permission> element in the manifest. Then, when the application is installed on the device, the installer determines whether or not to grant the requested permission by checking the authorities that signed the application's certificates and, in some cases, asking the user. If the permission is granted, the application is able to use the protected features. If not, its attempts to access those features will simply fail without any notification to the user [14].

IV. RESEARCH METHODOLOGY

This study was conducted to investigate on the users' comprehension and influence on user behavior of Android apps permissions. The methodology used in this study is using Internet survey where participants are requested to answer a set of comprehension and behavior questions to test whether they pay attention to the apps permissions during the installation process.

A. Procedure

Participants were first given several demographic questions related to their general background. Later, they are required to answer a series of questions on permissions comprehension and their actions towards application installations.

With regard to the selection of participants, only those who stated that they use Android operating system for their smartphones were chosen in the experiment. The survey ran for 2 weeks and at the end of the period, the results were compiled and analysed.

B. Participants

Participants for this study were recruited using Facebook call for participation. The participation is on voluntary basis, and the participants were given a gift for their participation. The recruitment drive managed to get 117 participants. The distribution of the participants' gender is 55% male and 45% female. The age distribution of the participants was: 27% from Below 18 years old group, 55% between the ages of 18 and 25, 8% between the ages of 26 and 30 years, 10% from 31 years and above. Next, the participants were asked to indicate whether they pay attention to permission given during an installation, and 40% of them indicate that they paid attention while 60% are completely unaware of permissions.

V. RESULTS AND ANALYSIS

First, we ask the knowledge related questions to the participants to know the level of their knowledge on the matters surrounding the Android permissions.

A. Knowledge related questions

1) The participants are asked to rate their knowledge on the Android application security concept. They are given

five choices: "1-Very knowlegable", "2-Knowlegable", "3-Not sure", "4-Some knowledge", "5-No knowledge". The results are presented in Table 1.

TABLE I. ANDROID SECURITY KNOWLEDGE

Knowledge Level	Participants' Percentage
Very knowledgeable	5%
Knowledgeable	21%
Not sure	37%
Some knowledge	19%
No knowledge	18%

2) The next knowledge question is: "Do you know at which point application access rights are granted?". About 36% of the participants answered "After installation of the application", 40% of them answered "At application installation", and 39% answered "I don't know". The right answer is "At application installation" and it seems that only 40% managed to answer the question correctly.

3) Later, the participants were asked whether they know that the applications released in Android Market are subject to a security vetting process. The results show that 32% of the participants reported that they think all applications would go through the vetting process, while 20% think the applications do not go through any vetting and 48% answered that they are not sure. The correct answer is the applications do not go through any vetting process by the Android market.

These results shows that the level of knowledge for the users are still low and this fact indicates that more awareness need to be instilled in the user to make them understand the implications of the Android permissions on their privacy once they choose to install the relevant applications.

B. Comprehension related questions

Another set of questions were asked to gain some insight on the participants' comprehension of the security and privacy impacts of the different types of permissions.

1) The first question asked is related to INTERNET permission. The results obtained are shown in Table 2.

TABLE II. INTERNET RELATED PERMISSION

Permission	Options	Responses
INTERNET Category: Network communication Label: Full Internet access	✓Sends information to the application server ✓Load advertisements X Read your list of phone contacts X Read your text messages X None of the above I don't know	48.2% 43% 12.3% 7.9% 7% 24.6%

2) The next question is related to the READ_PHONE_STATE permission and the results are depicted in Table 3.

TABLE III. READ_PHONE_STATE RELATED PERMISSION

Permission	Options	Responses
READ_PHONE_STATE Category: Phone calls Label: Read phone state and identity	✓Read your phone number X See who you have called ✓Track you across applications X Load advertisements X None of the above I don't know	50.9% 32.5% 45.6% 13.2% 6.2% 21.1%

3) Another comprehension question is regarding the WRITE_EXTERNAL_STORAGE permission. The answers are shown in Table 4.

TABLE IV. WRITE_EXTERNAL_STORAGE RELATED PERMISSION

Permission	Options	Responses
WRITE_EXTERNAL_STORAGE Category: Storage Label: Modify/delete SD card contents	✓Read other applications' files on the SD card ✓Change other applications' files on the SD card X See who you have made phone calls to X None of the above I don't know	33% 23% 10% 5% 29%

4) The fourth comprehension question is on the WAKE_LOCK permission, as shown in Table 5.

TABLE V. WAKE_LOCK RELATED PERMISSION

Permission	Options	Responses
WAKE_LOCK Category: System tools Label: Prevent phone from sleeping	✓Keep your phone's screen on all the time ✓Drain your phone's battery X Send text messages X Delete your contact list X None of these I don't know	20% 38% 7% 6% 7% 20%

5) The next comprehension question is on the CHANGE_NETWORK_STATE, and the results are shown in Table 6.

TABLE VI. CHANGE_NETWORK_STATE RELATED PERMISSION

Permission	Options	Responses
CHANGE_NETWORK_STATE Category: System tools Label: Change network connectivity	✓Turn your WiFi on or off X Send information to the application's server X Read your calendar X See who you have made calls to X None of these I don't know	30% 28% 8% 4% 6% 24%

C. Behaviour related questions

In order to investigate whether the number and type of permission will influence the users' installation decisions, they are required to answer a set of behaviour related questions. In Android Market, users are shown the list of permissions on the final installation page. If the users dislike the requested permission, they can refrain from downloading the application.

1) The respondents were asked "Have you ever not installed an app because of permissions?". The responses are shown in Fig. 2.

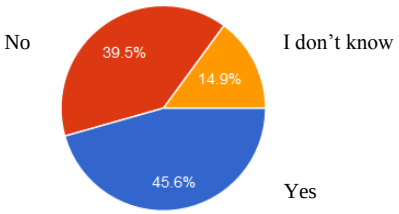

Fig. 2 Application Installation Decision

2) The second behaviour related permissions question is: "What would you do if you are warned that an application requires permissions that are potentially harmful?". Their answers are recorded in Table 8.

TABLE VII. BEHAVIOUR ON HARMFUL PERMISSIONS

Behaviour on harmful permissions	Participants' Percentage
I will delete the application	28%
I will ignore the warning	11%
I will not install the application and search for an alternative	47%
I will not take any action	21%

3) Next, they were asked whether they refer to other resources before they download the Android applications. Their answers are presented in Table 9.

TABLE VIII. OTHER REFERENCES

Other references	Participants' Percentage
Market reviews	48%
Internet reviews	27%
Screenshots	13%
Permissions	11%

4) Lastly, the respondents were asked the most important question: "If you are to choose between a free app with harmful permissions, and an app which you have to pay for but with zero permission, which one will you choose?". Fig. 3 highlights the results. The results show that about 72% of the respondents inform that they prefer to download and install free applications even though there are possibilities that they contain harmful permissions.

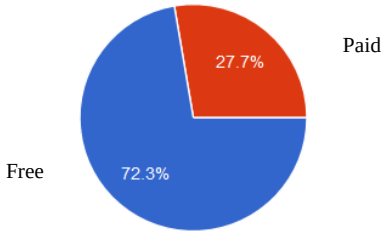

Fig. 3 App choices

VI. RESULTS DISCUSSION AND RECOMMENDATIONS

Based on the results presented in Section V, we can make several conclusions regarding the Android users' comprehension level on the permissions and also how users' react to the permissions when they are warned about the potential security risks of using the apps.

A. Impact of permissions

The responses from the users show that the majority of Android users do not pay attention to permissions or understand permission warnings. According to Felt et al [3], attention and comprehension are prerequisites for informed security decisions. The results in this study demonstrate that most users have difficulties in understanding the impact of app permissions on their privacy and security.

In the knowledge related questions, most respondents either answer the wrong questions or simply state "I don't know". This shows that the level of knowledge on Android permissions is still low and awareness campaigns should be increased to make the public to become more aware of the risks of Android permissions.

The list of comprehension related questions were introduced to find out how far the participants understand the true meanings of the permissions. Participants are allowed to choose more than one answer, and the results show that only half of the participants have the ability to relate the permission name with the possible security risks. The possible solution to this problem is to have the Android Market to impose the requirement to include permission warnings that focus fully on risks, for example, instead of displaying "Prevent phone from sleeping", this label should be used "Drain you phone's battery". This would give the users more information on permissions to aid them in making the right decision.

The behaviour related questions aim to understand the users' actions after they were informed on the risks or impacts of the permissions to their devices. For the question that asks the respondents whether they would not install the apps with harmful permissions, almost half of them answered that they will not install the application and will look for alternatives (Table 8). This shows that the users are concerned about their privacy and security, however, if the choices of applications are limited, they still have no choice but to agree with the installation.

B. Users' choice

The next important question is whether the users would choose between free apps with harmful permissions and paid apps with zero permission. About 72% of the respondents stated that they would still download free apps even though they contain harmful permissions. The possible explanation would be, due to the lack of knowledge and comprehension regarding the app permissions, users would make choices that could potentially be harmful to their devices.

VII. CONCLUSIONS

Android app permissions are essential in ensuring any individual app to function properly. However, if an app contains too much permission required, especially the ones that cost money, and also steal important information from the users, it has become a potential threat to the privacy and security of the users. This research aims to investigate the comprehension and behaviour of the users when faced with choices regarding the app permissions. Largely, our results show that the general knowledge and comprehension levels are quite low, and users need to be warned about some types of permissions that could potentially harm them in relation to the compromised private information and loss of money. Several recommendations were given to help to lessen the impact of the data and financial loss. However, at the end of the day, it is up to the users to decide whether to continue to install the apps or not.

References

[1] http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[2] M. Butler, "Android: Changing the Mobile Landscape", in Pervasive Computing, January-March 2011, pp. 4-7.

[3] A. Felt, E. Ha, S. Egelman, A. Hanet, E. Chin and D. Wagner, "Android permissions: User attention, comprehension and behaviour", Technical Report No. UCB/EECS-2012-26, 2012. University of California at Berkeley.

[4] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, D. Wetherall, "A conundrum of permissions: Installing applications on an Android smartphone", LC 2012 Workshops, LNCS 7398, pp. 68-79, 2012.

[5] A. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. "Android permissions demystified". In CCS '11, pages 627-638, New York, NY, USA, 2011.

[6] R. Stevens, J. Ganz, V. Filkov, P. Devanbu and H. Chen, "Asking for (and about) permissions used by Android apps", in Mining Software Repositories (MSR) 2013, San Francisco, California, May 2013.

[7] T. Vidas, N. Christin and L. F. Cranor, "Curbing Android permission creep", in Proccedings of the 2011 Web 2.0 Security and Privacy Workshop. Pp. 20-25, Oakland, California, May 2011.

[8] J.Kang, S.Seo, J.W.-K Hong, "Usage pattern analysis of smartphones," Network Operations and Management Symposium (APNOMS), 2011 13th Asia-Pacific, pp.1-8, 21-23 Sept. 2011.

[9] N. Xu, F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng, "Stealthy video capturer: a new video-based spyware in 3G smartphones." In Proceedings of the second ACM conference on Wireless network security (WiSec '09). ACM, pp. 69-78, New York, NY, USA, 2009.

[10] J. Sellwood and J. Crampton, "Sleeping Android: The Danger of Dormant Permissions", in 2013 Workshop on Security and Privacy in Smartphones and Mobile Devices (*SPSM'13*), *pp.* 55-66, Berlin, Germany, November 8, 2013.

[11] L. Kraus, I. Wechsung and S. Möller, "Using Statistical Information to Communicate Android Permission Risks to Users", 4th Workshop on Socio-Technical Aspects in Security and Trust, pp. 49-55, Vienna, Austria, 2014.

[12] D. Bornstein, Dalvik vm internals (2008), http://goo.gl/knN9n (accessed May 25, 2016)

[13] C. Gibler, J. Crussell, J. Erickson and H. Chen, "AndroidLeaks: Automatically Detecting Potential Privacy Leaks in Android Applications on a Large Scale", TRUST 2012, LNCS 7344, pp. 291-307, 2012.

[14] Android developer reference, http://d.android.com/ (accessed April 10, 2016)