Improving Android Permissions Models for Increased User Awareness and Security

Jeffrey Palmerino
Rochester Institute of Technology
1 Lomb Memorial Dr
Rochester, New York
jrp3143@rit.edu

ABSTRACT

Determining how to make users more aware of the permissions used in their favorite apps is one of the largest challenges facing mobile developers today. Research has shown that the less aware a user is, the less secure they feel while using the app. Unfortunately, this same research has shown that users are not well informed of the permissions their apps use, leading to many users feeling insecure. This makes us ask, how can users become more informed about the permissions their apps use so they can feel more secure?

To better understand this question, we examined the effects of the previous and current Android permissions models, as well as our proposed permissions model through an in person study. Our primary findings were I) Our proposed permissions model makes users significantly more secure than both Android models. II) Runtime based permissions models make users significantly more informed than install-time based models.

CCS CONCEPTS

•**Security and privacy** → *Mobile platform security; Software security engineering; Privacy protections;*

KEYWORDS

Mobile Permissions, Mobile Privacy, Mobile Security

ACM Reference format:
Jeffrey Palmerino. 2018. Improving Android Permissions Models for Increased User Awareness and Security. In *Proceedings of MOBILESoft '18: 5th IEEE/ACM International Conference on Mobile Software Engineering and Systems , Gothenburg, Sweden, May 27–28, 2018 (MOBILESoft '18),* 2 pages.
DOI: 10.1145/3197231.3198446

1 INTRODUCTION

With an incredibly diverse set of functionality within applications on our mobile devices, users are capable of performing a variety of tasks with the tap of a button. However, in order to perform many of these tasks, apps need to request access to certain types of information from their users. For example, if an application needs access to the user's photo library in order to provide some kind of functionality (like Instagram), the app needs to explicitly ask the user for this granted access. Therefore, these 'permissions requests' play an integral role in the user's ability to keep information on their phones private as they see fit, which in turn effects how secure users feel while using the app.

Until 2015, Android's permissions model was install-time based. Meaning, the user had to either accept or deny all permissions the app requested at the time of installation [1, 2]. This left users with only one option in order to use the desired application, accept all permissions. Research would eventually prove that the install-time model made users highly uninformed about the permissions their apps were using [3], leading to the release of a different permissions model that users are still using today, Android 6.0. This new and improved model, which is run-time based, gave users more control over the permissions the app had access to, hoping to combat the issues seen with the install-time model [1, 2].

Our work examined the effectiveness of the upgrade from Android 5.0 to Android 6.0, while providing a proposed permissions model that is run-time based. In order to compare these models effectively, we conducted an in person study consisting of 185 participants. Users were asked to complete a pre-study survey, play a simple tic-tac-toe game on a laptop provided to them, and complete a post-study survey that allowed us to measure their experience with the permissions used in the game.

2 STUDY DESIGN

Our study consisted of the following three phases:

(1) **Pre-study survey:** Collect user demographic data and information about smartphone usage and Android experience. This allowed us to ensure we didn't end up with a sample of only one type of user, i.e. tech-savvy, non-tech savvy, no experience etc..
(2) **Play game:** User plays tic-tac-toe and is instructed to act like they are using their own device. This allowed us to emulate a realistic scenario of a user using an app on their own device, without asking them to download the app on their phone directly.
(3) **Post-study survey:** Collect feedback from users on their experience with the study and measure how well they knew the meanings of requested permissions, how well they could remember what permissions were requested, and how secure they felt using the app.

We recruited participants for our study by conducting it at a local event that brings together thousands of community members to a single location. Visitors were asked if they wanted to play the

MOBILESoft '18, Gothenburg, Sweden

DOI: 10.1145/3197231.3198446

tic-tac-toe game we had created, but were only informed they were participating in our study if they asked. Due to our study involving humans, an approved IRB was obtained that covered participants who were at least 18 years of age.

3 PROPOSED PERMISSIONS MODEL

In order to know if the current Android 6.0 model could be improved upon, we created a run-time based permissions model to see if we could further enhance user feelings of security and levels of awareness. Our proposed model emulated what users would typically experience with Android 6.0, however, we made two important modifications.

The first modification we made in our proposed permissions model was through the use of custom messages. These custom messages portrayed information to the user whenever a permission request occurred in a way that was non-technical, which made it quite clear to the user what the app was asking to do.

Our second modification dealt with other apps that use the requested permission. For example, if an app requests permission to the user's photos, the message displayed on the screen would say something related to, *"Other apps using this permission: Facebook, Twitter"*. An example of this notification is shown in Figure 1.

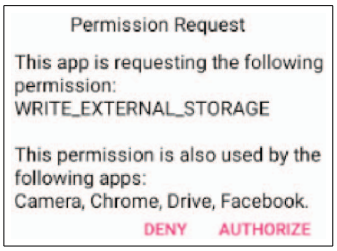

Figure 1: Permissions Requested in Other Apps

By giving users the ability to see other apps that use the requested permission, especially ones they are familiar with, we provided more comfort to the user while they completed our study.

4 RESULTS

To compare the results from our study, we used the Mann-Whitney U (MWU) test for statistical analysis. We chose MWU because we found our data to be significantly non-normal in nature, and the MWU test is specifically fit for those kinds of data distributions. The second was because our survey consisted of questions that had Likert Scale questions, which meant ordinal data responses, and the MWU test is more appropriate for analyzing ordinal data.

After the initial analysis of our proposed model compared to the current and previous Android models, we found that our proposed model not only made users feel significantly more secure than the install-time model, but it also made them feel significantly more secure than the current run-time model. These results were based off MWU tests that compared the differences in Likert Scale responses to a question in our post-study survey that asked, *"How much do you agree with the statement, 'I felt secure using this application'?"* Table 1 shows the detailed results from our MWU tests, and the resulting p-values of <0.05 that indicate statistical significance.

Table 1: MWU Results

Group 1	Group 2	p-value
Install-time	Proposed Model	0.0131
Runtime	Proposed Model	0.0387

While conducting our initial analysis we also found that the current run-time model did not make users feel significantly more secure than the old install-time model. These results came as a surprise, seeing as one of the main goals of upgrading Android 5.0 to Android 6.0 was to help make users feel more secure about the apps they use, and their associated permissions. The results from the MWU test, which compared the average Likert Scale responses, are shown in Table 2.

Table 2: How Secure Users Feel

Install-Time (5.0)	Runtime (6.0)	p-value
4.41	4.55	0.7618

Improving how secure users feel was not the only goal of our proposed model, as we also focused on improving how informed users are. After conducting further MWU tests, we found that our proposed model did not significantly increase how informed users were about the permissions the app was using. However, we did find a statistically significant difference in how informed users were in both run-time models compared to the old install-time model. These results demonstrate that moving to a run-time based permissions model from an install-time based model helped make users significantly more informed.

5 THREATS AND FUTURE WORK

Although our study consisted of a large group of people, the convenience in which our data was collected effects the generalizability of our results. By taking advantage of the large community event, the users who participated may not properly represent the true population of end-users. Therefore, future studies conducted should focus on more random samples of participants.

Another threat to our study is the use of only a gaming application. Had we used a more sensible category like finance or medical, our results could have differed greatly. Future work could be done to apply our proposed model to other categories to see if the results are similar. If they are not, that may imply that users care differently about how secure they feel when functionalities and expectations of the app change.

REFERENCES

[1] Get ready for the sweet taste of android 6.0 marshmallow. https://android.googleblog.com/2015/10/get-ready-for-sweet-taste-of-android-60.html.
[2] Requesting permissions at run time. https://developer.android.com/training/permissions/requesting.html.
[3] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 3:1–3:14, New York, NY, USA, 2012. ACM.