

Comparative Privacy Displays in App Marketplaces

Patrick Gage Kelley
Department of Computer Science
University of New Mexico
pgk@cs.unm.edu

Javier Chavez
Department of Computer Science
University of New Mexico
javiere@unm.edu

Abstract—Android applications request permissions to gain access to system operations, an OS-wide attempt to limit the access of personal information by third-party application developers. Currently, before an app is installed, the system presents these permission requests to the app consumer for approval.

However, this implementation of notice and consent is lacking in many ways. The presentation of permissions comes late in the selection process, uses jargon-heavy terms, does not show which permissions are not collected, permission “requests” are not optional, and comparisons are tedious and memory-based. Overall, this interface does not support privacy conscious decision-making.

Our work proposes a conceptual shift in the way these permission requests are displayed. We propose reducing the amount of information shown and inherently facilitating comparisons by presenting privacy information relative to other apps. Specifically, by displaying permission differences between apps within a given marketplace search we can highlight the most currently relevant information.

This focuses the user’s attention on the current action, their search, and displays the permission variance between applications that have the greatest likelihood of meeting their current goals and actually being installed. This short paper presents a new model for displaying app permissions, proposes a series of possible displays from the potential design space, and analyzes current market permissions to validate that this information is varied and rich.

I. INTRODUCTION

As of July 2013, Google reported that there are 1.5 million Android device activations each day¹ with over one billion total activations. This is up from 900,000 activations a day in June 2012,² an over 50% increase in the last year.

To truly realize the benefits of these smartphones, it is the applications, or apps, that create many of the “smart” advantages of the phones. And the Google Play store now has over 850,000 apps for users to choose from.³ But with this user choice, comes some amount of risk. Android applications are largely unregulated, with development ranging from large, high-profile companies to one-person shops. And with each application installed on a consumer’s phone or tablet, an extensive amount of data and hardware access can be granted.

As a result of Android’s widespread popularity and it’s unregulated and open development space, we continue to see reports of security concerns around Android smartphones. A July 2013 Department of Homeland Security and FBI joint

report stated that 79% of mobile malware was targeted at Android, stating Android “continues to be a primary target for malware attacks due to its market share and open source architecture” [1].

However, malware is not the only risk, many applications in the Google Play store fall into the class of adware, applications that collect excessive amounts of personal information to sell or deliver advertising content in deceptive ways. An August 2013 report that looked at 8000 applications found 22% to be classified as adware, describing common permissions requests which went past application functionality [2].

The question of which permissions an application needs to function and which are extraneous is difficult for analysis tools and experts, and thus nearly impossible for consumers to understand. Several research teams have found users unequipped to reason about permissions [3], [4], [5], let alone to decide if applications are taking more than they “need.”

For people to actually make informed decisions, they should be able to understand if what an app is requesting is appropriate and if they are personally comfortable with such a request. To facilitate this, we should provide a better interface for comparing the permissions requests of applications one is choosing between. The goal is to provide users with a display that compares relative differences between similar applications.

From here, we first describe problems with the current Android permissions display and terms. We then propose a different approach, one that comparatively displays Android permissions. We suggest a series of possible designs for that information that attempt to meet our user-centered goals. Additionally, we present a collection and analysis of data from the Google Play Store, that verifies there exist differing permissions resultant keyword searches performed on the market.

II. BACKGROUND

As of this writing Android has 134 permissions outlined for use in their documentation.⁴ These permissions are requested by applications to allow those applications OS-level privileges to use a specific piece of hardware or access a certain piece of data. The permissions each application requests is shown after a user selects the download/purchase button within the Google Play store. While the appearance varies based on device, Figure 2 shows the display on Google’s flagship tablet, the Nexus 7. This display is three touches deep in the interface, a common search shown in Figure 1 reveals no permission information, instead opting for giant icons to help users make decisions.

¹Google Q2 2013 Earnings Call, <http://goo.gl/rHq1GB>

²Andy Rubin, <http://goo.gl/oThRzz>

³AppBrain, <http://www.appbrain.com/stats/number-of-android-apps>

⁴<http://developer.android.com/reference/android/Manifest.permission.html>

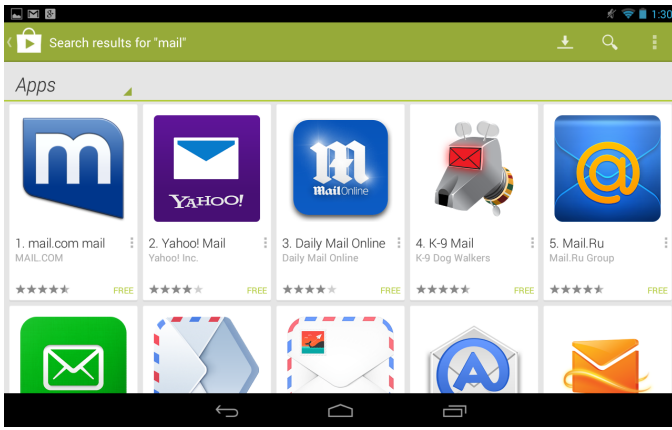


Fig. 1. Screenshot of the current application market search for the term “mail” on the Nexus 7.

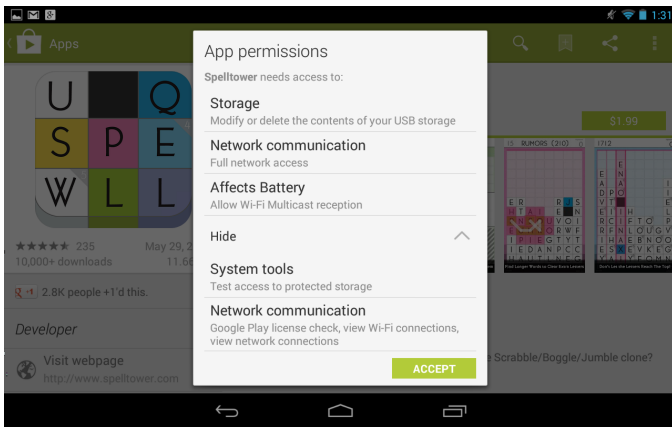


Fig. 2. Screenshot of the current application market permissions on the Nexus 7.

While Android security research now fills volumes, much of that work is focused on underlying OS level security assumptions, vulnerability analyses, and security modeling, all of which is out of scope for this paper. Researchers have explored the issue of applications requesting many permissions, with Vidas et al. finding prevalent “permissions creep,” due to “existing developer APIs [which] make it difficult for developers to align their permission requests with application functionality” [6]. Felt et al., in their Android Permissions Demystified paper, attempt to further explain permissions to developers [7].

Researchers have explored how people understand permissions, and generally consider the security of their phones. Overall, these studies have found that people largely do not pay attention to permission screens [3] though they are aware of their existence, that people do not believe they understand permissions [4], and that there are a number of widespread misconceptions regarding smartphone applications [5]. Lin et al. explored how expectations shape users’ acceptance of permissions, attempting to move towards a more crowdsourced model [8]. Kelley et al. suggest that permissions display arises too late in the decision-making process and suggest a briefer approach that can be included on the main application display [9]. However, this approach simplifies the current Android permissions beyond recognition, and still requires

users navigate into each app to make comparisons.

Research in related privacy areas including online policies and financial notices have shown that privacy-related terms, such as the Android permissions are often not well understood by consumers [10], [11]. Additionally, in their work on financial privacy notices, the Kleimann Communications Group sought to specifically create a display built for making comparisons. We will leverage their findings in our suggestions for creating comparative permissions displays.

III. COMPARATIVE PERMISSION DISPLAYS

For people to make an informed decision regarding the installation of an app, they must make a personal choice regarding how comfortable they feel letting that developer have access to the information requested. While this is different for each individual, and a number of factors including price, brand trust, need for specific functionality, reviews, and other information play into this decision, one, often missing, piece of information is how *normal* it is for a specific application to request a given set of permissions. Baselines across the entire marketplace, lead to issues surrounding the hugely different types of functionality apps can provide (compare a banking app with a flashlight app).

While much effort has gone into user understanding, focused on the clarity of terminology, reducing jargon, attempting to emphasize importance, and showing examples, little work has looked at how to provide an easy and understandable baseline for permission requests. Lin et al. provide the first steps towards the crowdsourcing of that information, but that model would require substantial human investment [8].

Our approach is to automatically to display only the most salient privacy information for each specific application-selection decision. Accepting that applications of different types require different permissions to provide a set of functionality, we seek to understand what those base permissions are, and which permissions requested are *additional*. To do this, we approximate apps of similar functionality by relying on the results provided by the marketplace search. While a single search term can obviously return many different types of apps, we will later show that for common searches we do see trends in the types of applications returned. Additionally, as most users are only going to consider installing apps from the list of search results, this has the benefit of comparing the permissions of the apps that will most likely be downloaded.

IV. DESIGN POSSIBILITIES

Revisiting Figure 1, we see that a consumer is given almost no relevant information when first performing a search, rather being forced to browse each application and compare by memory. While earlier work has already found users would prefer more comparison-based interfaces [9], the permissions data we have shown provides an obvious way to compare applications based on privacy.

We believe there are two ways to leverage comparative permissions displays in the Google Play store. First, after a search is performed a small privacy-display can be presented above the search results. This display can highlight the permissions variability across the search and list common permissions

that these apps request. Second, when a user views a specific application’s permission display, the display can be updated based on the search that had been performed, to indicate the commonality of each requested permission, highlighting permissions which are rare or unique.

Future work should include designing and testing these variants and others, based on the data and approach we have described here.

Our approach does not solve all the display issues that have been identified regarding the design of privacy labels [10], specifically lacking the following:

- All of the permissions an application uses will not be displayed (by default).
- All of the permissions an application doesn’t use will not be displayed.
- Good definitions and terms must still be used for users to understand the differences.

Some of these issues can be addressed through a layered approach, i.e. showing more information for advanced users who seek it, and also through refining terms and using a layout that is successfully tested. However, our approach inherently:

- Shows only a small number of relevant permissions (minimize information overload).
- Allows direct comparisons on privacy with related applications.
- Highlights a series of expected privacy norms for a specific type of application.

V. PERMISSIONS ANALYSIS

For our approach to be successful, it hinges on applications with similar functionality often requiring permissions which are not completely divergent, as well as different types of applications needing different permissions. To test this we needed to collect and analyze permission requests from the Google Play store.

Currently, Google does not release any information on common searches which are performed within the Play Store. To approximate something similar to common searches we used a list of 100 keywords as reported by Chomp, an application search engine.⁵

These keywords are intended to help users find applications, written to capture popular searches, and we believe this list is a reasonable approximation, without a direct list of common searches. We understand that using this substitute keyword list is a limitation of this work, but we believe it to be reasonable, and have listed all of the keywords in Figure 3.

For each keyword we collected the permissions of the top 48 applications that a Google Play search returns. Across the 4782 application results we had 3743 unique applications with 95 unique permissions requested across a total of 29910 permission requests.

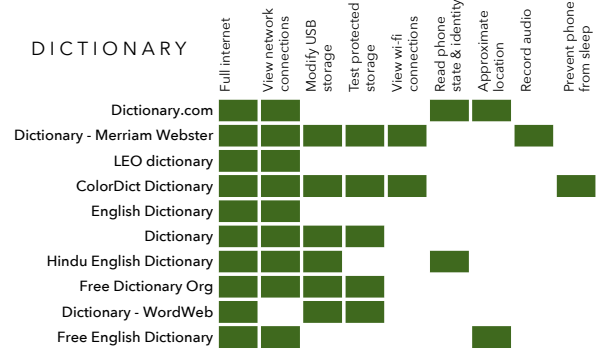


Fig. 4. The top ten results for the search term dictionary, and the permissions they request.

For each keyword we sought to understand the amount of variability in the permission requests of the applications returned. To measure this we created a binary vector for each application, which describes the permissions each application requests. We then compared the permission vectors for each application using a Hamming distance calculation. The average distance across all pairwise comparisons for a keyword is shown in Figure 3. This was done for all 48 applications returned for a keyword, as well as for only the top 10 applications.

We find a large variability in the average distance between permissions for a keyword. At the low end, “dictionary” has an average distance of only 2.2, whereas terms like “video chat,” “text free,” and “yahoo mail” all score over 11. While this may be a result of certain types of applications having more requests, we also see that as these requests increase there is a wider variability.

Looking at a few specific terms provides insight into the amount of variability that we hope to leverage. In Figure 4 we see the top ten applications for a search for “dict.” Here, nearly every applications uses network data and can view network connections. Many use storage. More interestingly, we see two dictionary applications that request access to a user’s IDs and phone state, two that request location, and one that requests the ability to prevent the phone from sleeping. It is these requests that are the most salient when making a privacy preserving-decision. This information might sway a privacy-conscious individual’s decision when downloading a dictionary application.

In Figure 5 we see a similar chart for the top ten applications for the search “free music.” Here we see both a larger core permissions set, as well as a much longer tail of requests.

This variability in permissions is something that we can leverage to show users’ information that assists with comparisons, and takes advantage of the knowledge that different types of apps will need different or more permissions to function.

VI. CONCLUSION

We have proposed reducing the amount of information that is shown by presenting privacy information in a relative way, re-assessed with every user search. By displaying comparative

⁵<http://searchengineland.com/the-most-popular-appstore-keywords-from-chomp-googleplay-135744>

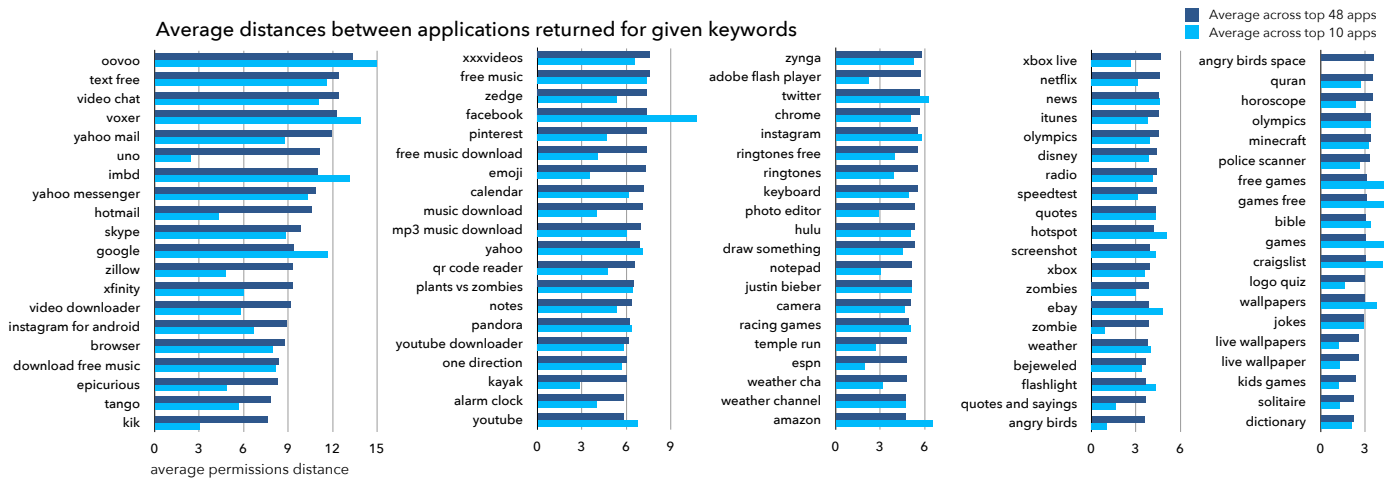


Fig. 3. The average distances across applications for both the top 48 and top 10 applications returned by each keyword search.

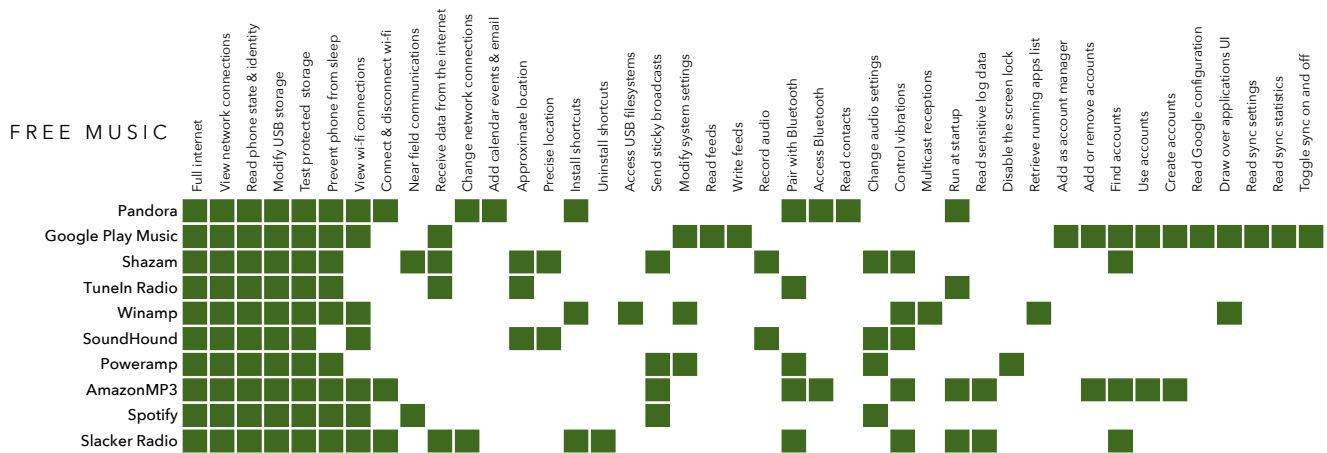


Fig. 5. The top ten results for the search term “free music,” and the permissions they request.

privacy information relative to apps a user is likely to download, we can focus a user’s attention on the most relevant data: the permission variance between applications that have the greatest likelihood of meeting their current functionality needs and being downloaded. This short paper has shown that permission requests are varied and rich, and interesting differences are found in common keyword searches. We have proposed high-level ways to incorporate this information into a better marketplace search experience, that helps users compare applications and protect their privacy.

REFERENCES

- [1] Department of Homeland Security, “Threats to Mobile Devices Using the Android Operating System,” <http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf>.
- [2] ZScale, “Gap between Google Play and AV vendors on adware classification,” http://research.zscaler.com/2013/08/normal-0-false-false-false-en-us-x-none_8.html.
- [3] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, “Android permissions: User attention, comprehension, and behavior,” in *Symposium on Usable Privacy and Security (SOUPS) 2012*, 2012. [Online]. Available: <http://www.cs.berkeley.edu/~afelt/felt-androidpermissions-soups.pdf>
- [4] P. Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, and D. Wetherall, “A conundrum of permissions: Installing applications on an android smartphone,” in *Financial Cryptography and Data Security*, 2012, vol. 7398, pp. 68–79. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-34638-5_6
- [5] J. King, ““How come i’m allowing strangers to go through my phone?”- Smartphones and privacy expectations,” 2013, <http://jenking.net/mobile/>.
- [6] T. Vidas, N. Christin, and L. F. Cranor, “Curbing android permission creep,” in *W2SP 2011*, 2011.
- [7] A. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, “Android permissions demystified,” in *In Proceedings of the 18th ACM conference on Computer and communications security (CCS ’11)*, 2011.
- [8] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, “Expectation and purpose: understanding users’ mental models of mobile app privacy through crowdsourcing,” in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, ser. UbiComp ’12. New York, NY, USA: ACM, 2012, pp. 501–510. [Online]. Available: <http://doi.acm.org/10.1145/2370216.2370290>
- [9] P. G. Kelley, L. F. Cranor, and N. Sadeh, “Privacy as part of the app decision-making process,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI ’13. New York, NY, USA: ACM, 2013, pp. 3393–3402. [Online]. Available: <http://doi.acm.org/10.1145/2470654.2466466>
- [10] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, “A “Nutrition Label” for Privacy,” in *Proceedings of the 2009 Symposium On Usable Privacy and Security (SOUPS)*, 2009.

[11] Kleimann Communication Group Inc., “Evolution of a prototype financial privacy notice.” February 2006., <http://www.ftc.gov/privacy/>

[privacyinitiatives/ftcfinalreport060228.pdf](#).