Visualizing Risk by Example: Demonstrating Threats Arising From Android Apps

M. Hettig, E. Kiss, J.-F. Kassel, S. Weber, M. Harbach, M. Smith
Distributed Computing and Security Group, Leibniz University Hannover, Germany
{hettig, kiss, jan-frederik.kassel, suey}@stud.uni-hannover.de,
{harbach,smith}@dcsec.uni-hannover.de

1. INTRODUCTION AND BACKGROUND

Previous research has shown that only 17 % of Android smartphone users are consciously aware of the specific permissions an app demands during installation [2]. While this result is hardly surprising, it still puts the majority of smartphone users at risk.

Kelley et al. recently argued that since permissions are not shown until after the installation button has already been pressed, the risks potentially arising from excessive app privileges are not part of the user's decision process anymore [3]. They introduced a modified app information screen and showed that users became more reluctant to install apps requesting too many permissions. While they were able to increase the awareness of requested permissions, participants still reported that they were unsure about the threats arising from apps requesting too many permissions.

We can conclude that users currently show limited awareness of threats and risks during the selection and installation of a new app and that the safety of their personal data is at stake. We believe that this situation can be improved by emphasizing the risks associated with an app's installation. Thus, we evaluated a novel presentation of app permissions: our prototype illustrates risks arising from app permissions in the form of worst-case examples to demonstrate potential attack scenarios resulting from the malicious use of the requested permissions. In related work, Rader et al. [4] showed that many users learn about security from informal stories told by family and friends. Hence, in the terms of their work, we try to let the app market tell the user small stories about how private information may be at risk.

In this position paper, we suggest to assist users in understanding permissions by using examples to communicate risk. We present results from a pilot study that evaluate the effectiveness of this approach. We compare app installation counts of the original Android market with our improved display.[1] Our results show that making threats graspable using the user's actual personal information on the phone demonstrate the possible severity of permission abuse.

[1]The work of Kelley et al. was not published at the time of running this study.

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

2. METHOD

The Android OS defines a large number of permissions of which many are rarely used [1]. To test the efficacy of our alternative permissions display, we selected eight permissions commonly used by popular apps, since the market generally displays only a limited number of permissions. To find the most common permissions, we crawled 34,875 most popular apps on the Android Play Store in early 2013. From this set, we picked eight common permissions (see Table 1) that lend themselves well to visualization. An analysis of which permissions cannot be visualized by examples is subject of future work, as this exploration intends to show the best-case effects of our approach.

Permission	Requested By
full network access	82%
modify external storage	56%
read phone status and identity	42%
precise location	23%
use accounts on the device	16%
take pictures and videos	8%
read contacts	7%
read call log	6%

Table 1: The permissions selected for our evaluation and how many of the 34,875 apps requested them.

Based on our findings, we implemented a mockup of the Market application (now Play Store[2]). In addition to the conventional representation of permissions as text, a more vivid representation of the aforementioned permissions was implemented (cf. Figure 1). Before being able to install an app, the user would be presented with examples of worst-case scenarios using the capabilities the app will have after installation. For example, for an app requesting the "*take pictures and videos*" permission, the market would show a live capture of the phone's camera, the phone's current position on a map for the "*precise location*" permission, and a slide show of personal pictures stored on the SD card with a superimposed trash can for the "*modify external storage*" permission.

[2]We used the Android 2.3 market for this pilot study since more participants from our subject pool indicated to use Android 2.3.

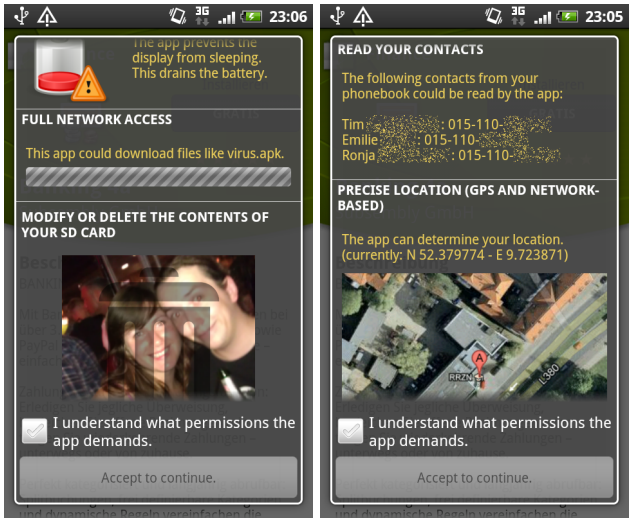

Figure 1: Some examples of visualizations of Android permissions.

Our mockup contained four different app categories with four apps per category, requesting the following permissions: *Office* apps required a reasonable set of permissions (network, phone status and identity, modify external storage), *Finance* apps a slightly unreasonable set (seven permissions including take pictures and video as well as precise location), *Weather* apps an obviously unreasonable set (five permissions including modify external storage and taking pictures) and *Games* apps required no permissions at all. All apps in one category requested the same subset of permissions. We chose to vary permissions between categories instead of between apps to remove the influence of non-security or -privacy factors (such as ratings, comments or pretty screenshots) on the installation decision.

Our study used limited deception to prevent bias: participants were invited to a usability test of an alternative app store implementation. First, participants were presented with a questionnaire including questions on their general behavior during app installation and corresponding worries about security. The questionnaire also contained dummy questions to distract from the study's true aim. After obtaining consent, we installed our mockup store on each participant's personal device and then asked them to role play as if they wanted to install one app from each of the above categories. They were asked to think-aloud while completing the task and told that not installing an app is also a valid option. During the entire introduction, we never explicitly mentioned permissions. After finishing the tasks, participants completed another questionnaire, were debriefed and had the opportunity to ask any questions. The study used a within-subjects design on the original and modified versions of the permissions display. We counterbalanced for effects of learning and fatigue by randomizing which version of the permissions display was presented first.

3. STUDY RESULTS

We recruited a convenience sample of 11 participants, including 2 women and 7 participants with a background in IT or computer science. We did not find any significant differences in our data based on demographics or task order.

The number of apps installed per user was statistically significant between the two versions of the Android market (paired-samples t-test, $t = 3.99$, $p = .003$). In the unmodified mockup of the market app, participants installed 2.9 apps on average while they only installed 1.7 after seeing examples of threats in our improved version. Moreover, the installation of apps requiring unnecessary permissions decreased significantly from 50 % to 13.6 % of possible app installs in the over-requesting finance and weather categories ($t = 3.07$, $p = .012$).

The participants' reactions to our approach were very encouraging: Displaying examples made participants see the possible threats. One participant stated: "Oh, I just found out that some apps can actually read my data, which I didn't realize before." Another participant also pointed out after seeing our improved permissions display in contrast to the original market that realizing the threat will influence his behavior: "Right now i realize the impact of the permissions [...] I don't want to install this app."

Finally 36.4 % of participants indicated that they worry about their security during app installation before they tested our permissions display, while, in the last part of the study, 65.3 % mentioned that they will be more mindful of their security and privacy in the future.

4. CONCLUSION AND FUTURE WORK

In this position paper, we argue that demonstrating potential IT security or privacy risks using concrete examples is a more effective way of warning users compared to the traditional approach. We presented a pilot study that tested the efficacy of visualizing Android app permissions using, for example, actual private photos, the current location and text messages sent in near past. We found encouraging results suggesting that using our system made users more aware of possible risks arising due to the installation of smartphone apps.

In future work, we intend to extend our study to confirm our results for a broader audience. We would also like to examine which Android permissions and general use cases can or cannot benefit from this approach. We also intend to extend this concept beyond permissions. For example, internet browsers could display form data that a user is going to send over an insecure channel to warn about not using SSL. Additionally, the efficacy of a retrospective use of the example approach may be of interest: After reading emails over an unencrypted connection, the user could be warned that this content may have been read by several other parties.

5. REFERENCES

[1] A. P. Felt, E. Chin, S. Hanna, and D. Wagner. Android permissions demystified. In *Proc. CCS*. ACM, 2011.

[2] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android Permissions: User Attention, Comprehension, and Behavior. In *Proc. SOUPS*. ACM, 2012.

[3] P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy as Part of the App Decision-Making Process. In *Proc. CHI*. ACM, 2013.

[4] E. Rader, R. Wash, and B. Brooks. Stories as Informal Lessons About Security. In *Proc. SOUPS*. ACM, 2012.