Study on User's Attitude and Behavior towards Android Application Update Notification

Yuan Tian, Bin Liu, Weisi Dai, Lorrie Faith Cranor, Blase Ur
Carnegie Mellon University
yt@cmu.edu, bliu1@cs.cmu.edu, weisi@cmu.edu, lorrie@cs.cmu.edu, bur@cmu.edu

1. INTRODUCTION

App updates on smartphones are critical to users' security and privacy. While new versions of the apps could fix important security bugs, users are not always comfortable with them for various reasons such as changed privacy invasiveness. Therefore, making update decisions is a non-trivial task for users.

In this project, to understand users' behavior and attitude on app updates, we conducted two studies: an online survey to study users' update behavior and attitudes, and a user experiment to evaluate our proposed new notification message for app updating. From the survey responses, we learned that only around half of participants left the app updates fully automatic. And they reported that privacy invasiveness and permission-related concerns are among top-mentioned reasons of not updating an app. And from the experiment, we found several significant effects that our proposed review-based update notification can better alert users to avoid privacy invasive app updates, especially for apps with less trust from the users, comparing to notifications with permission descriptions only.

2. RELATED WORK

The update behavior of Android apps has been first studied by Moeller et al.[5] by analyzing the updates of apps on Google Play quantitatively. An attack of the android system called App Update Attack is studied by Tenenboim et al.[4]. App updates might be a potential way to implant new security vulnerability and privacy data leaks to the users' phones. Chin et al.[1] studied users' confidence in security and privacy on Android. Their found that users reported various concerns because of some misconceptions or misunderstandings. Android permissions provide a mechanism for users to manage the access control of apps, especially when fine-grained controls are granted [3]. Kelley et al. [2] proposed a novel framework that introduces permission information into the process of app installations, which can help participants to choose less over-privileged apps.

3. METHODOLOGY

We first conducted a survey on Amazon MTurk ("MTurk"). In this survey, we recruited participants who satisfy the criteria: Located in the U.S., MTurk HIT approval rate $\geqslant$ 95%, 18 years old or above, literate in English and having used Android device for at least 1 month and installed some app(s) on it using Google Play. On average, each assignment requires 9–10 minutes to finish. We paid $0.20 to each HIT as compensation. In the survey, we ask the participants about people's behavior regarding application updates.

We then did a user study to test if our proposed app update notification can better nudge users to make decisions that provide more privacy. In this study, we hired participants from MTurk to install an app we developed. In the screening survey, we claimed that we are doing a study on battery usage of Candy Crush Saga which is a popular game, and the app monitors the battery usage. The compensation for finishing the screen survey is $0.10.

After 12 hours of the installation, the app pushes a notification to the notification area of their device. Clicking on the notification opens a dialog that similates the update notification dialog from Google Play, but with different messages. We chose two popular Android apps, namely Google Maps and Candy Crush Saga, as the app which need to be updated (each participant only sees one of them).

We want to know if presenting the users with negative reviews on privacy about the updated app would help users make a better decision, so in the dialog the app displays either regular new permission requests or a review text.

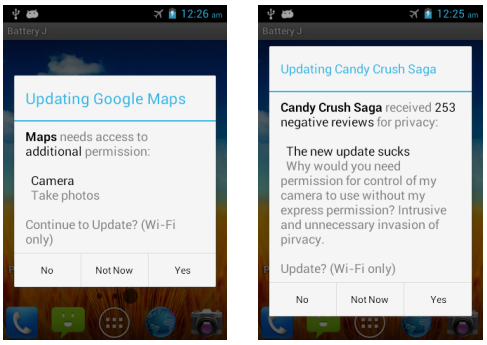

Figure 1: Sample Dialogs of the Update Notification

In the dialog the user can choose to update immediately ("Yes"), or refuse to update ("No"), or make a decision later ("Not now"). The notification would appear again after 3 hours if the user clicked on "Not now" to give user up to 3 more chances to make a decision. The app reports the user's interactions to our secure server. Each participant is awarded $3.00 for completing this part.

We designed this experiment as a between-group study with 4 conditions: (1) Google Maps, permission requests (see Figure 1 left), (2) Google Maps, negative reviews, (3) Candy Crush Saga, permission requests, and (4) Candy Crush Saga, negative reviews (See Figure 1 right). Thus in the conditions

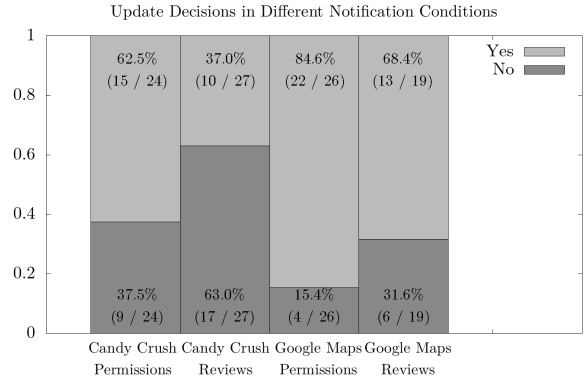

Figure 2: Distribution of decisions in conditions

above, we may examine the effect of negative reviews under different apps, which are expected to have different levels of trust from the user.

4. RESULTS

4.1 Result for the Online Survey

In the survey, we asked the participants to report their strategies updating their apps on Android devices. According to the responses of 300 participants, a little bit surprisingly: 47.7% of them updated apps automatically; 25.0% of them updated apps manually; 25.0% reported that they have used both strategies.

We asked participants to recall their experience regarding not updating an app. Around 59.3% of participants reported that they have experienced choosing not to update an app. And around 42.7% of all participants have regretted some app update(s). We also asked a follow-up open question on reporting reasons of not updating or regretting on updates. From the responses coded by two research with 87.5% agreement, we found that privacy and permission-related concerns are one of the two most-frequently-mentioned reasons, together with functionality / experience changes. Another interesting finding is that a considerable amount of responses mentioned considering negative reviews from other people either from online or offline sources.

4.2 Result for the Update Notification Study

We recruited participants on MTurk to install our apps. We got 736 valid responses from the screening survey and 96 participants finished all the steps. Around 62.5% of them are male.

We have the following observations from the experiments:

- Negative reviews are better at alarming the users about the privacy violations in app update.
- The trust to an app is very important to users when they make the update decisions, which is different from the self-reported about the decision factors in the online survey.
- People who read the update notification longer usually make better decision for privacy. Participants stay longer in the notification for the negative reviews than for the new permission.

As illustrated in Figure 2, 63.0% of people refuse to update Candy Crush Saga when they are shown negative reviews, while only around 37.5% of the users who are notified by new permissions avoided the privacy invasive update. Similarly, though users tend to update Google Maps more, the percentage of them to not update in the negative reviews condition (31.6%) is still around twice as these who don't update in the sensitive permissions condition (15.4%). A χ^2 test indicated a p value of 0.0148.

We collected, coded and analyzed users' reasons of making that specific decision in the study. We find that the leading reason for users to choose *not* to update is that users read the negative reviews for privacy (52.7%) about the update, while other factors such as sensitive permissions(25.0%) and phone limits(22.2%) exist much less frequently. On the other hand, when people choose to update, the major reasons are that users always keep apps up-to-date (69.4%) and they trust Google Maps (24.5%).

From the logs collected, we discover that users stay for longer time on the interface screen if they choose not to update. The average stay time of choosing not to update is 152% higher than that of updating the app (t-test, $p = 0.03$).

When participants are tested about Candy Crush updates, people who get the negative review notifications read longer (average time is 20.0 s) than those who get the new permission notifications (average time is 5.9 s) using t-test ($p = 0.0286$).

We analyzed the numbers of users' clicks on the "not now" options and found that most of the users make their update decision right away (76.5%). This result provides an insight for designing app update notifications: reviews from other people can better help users identify the privacy invasive behaviors.

5. REFERENCES

[1] E. Chin, A. P. Felt, V. Sekar, and D. Wagner. Measuring User Confidence in Smartphone Security and Privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 1:1–1:16, New York, NY, USA, 2012. ACM.

[2] P. Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, and D. Wetherall. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In J. Blyth, S. Dietrich, and L. Camp, editors, *Financial Cryptography and Data Security*, volume 7398 of *Lecture Notes in Computer Science*, pages 68–79. Springer Berlin Heidelberg, 2012.

[3] B. Liu, J. Lin, and N. Sadeh. Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help? In *Proceedings of the 23rd International Conference on World Wide Web*, WWW '14, pages 201–212, 2014.

[4] L.Tenenboim-Chekina, O. Barad, A. Shabtai, D. Mimran, L.Rokach, B. Shapira, and Y. Elovici. Detecting Application Update Attack on Mobile Devices through Network Features. In *Workshop paper of The 32nd IEEE International Conference on Computer Communications*, 2013.

[5] A. Möller, F. Michahelles, S. Diewald, L. Roalter, and M. Kranz. Update Behavior in App Markets and Security Implications: A Case Study in Google Play. In *Proc. of the 3rd Intl. Workshop on Research in the Large. Held in Conjunction with Mobile HCI*, pages 3–6, 2012.