Advancing the Understanding of Android Unlocking and Usage

Lina Qiu
University of British Columbia
Department of Electrical and Computer Engineering
lqiu@ece.ubc.ca

Ildar Muslukhov
University of British Columbia
Department of Electrical and Computer Engineering
ildarm@ece.ubc.ca

Konstantin Beznosov
University of British Columbia
Department of Electrical and Computer Engineering
beznosov@ece.ubc.ca

1. PROBLEM MOTIVATION

Given the fact that personal mobile devices provide access to and/or store a great deal of personal and sensitive data, including passwords, contacts, files, emails, etc., it is not surprising that unauthorized access to the device is one of the highest security risks for smartphone users. To protect such data and services from unauthorized access, some smartphone users lock their phones using PIN, password, biometrics and DAP ("draw a pattern"). Yet, others don't, risking the data and online services accessible through their devices, mainly because of the inconvenience of unlocking, lack of motivation and awareness. One way to improve user behaviour is to offer them more usable unlocking mechanisms, without sacrificing the security. It remains an open problem, however, how to optimize both security and usability for smartphone unlocking mechanisms. Thus, it is important for researchers to understand the interplay between security and usability of unlocking mechanisms in situ. To this end, we are preparing a longitudinal field study, in the course of which our monitoring app installed on the participants' Android smartphones will collect detailed relevant data.

2. OUR APPROACH

By conducting a two-month long field study with a diverse sample of user, we will obtain empirical data about them unlocking their Android smartphones and interacting with the apps. The collected data will include the length of unlocking and interaction sessions with the devices, outcomes (failed/succeeded) of the unlocking attempts, the unlocking mechanisms employed on participants' devices, whether the device is locked manually or through auto-lock, foreground applications and their sensitivities from participants' point of view, participants' attitudes of sharing their devices with other people, device locations and accelerator data, the model of the device and its screen size.

We decide to recruit participants from one region, US specifically, to avoid the influence of multi-nationalities. To recruit a representative sample of about 100 participants from US, we plan to advertise our study on Facebook. We are looking for additional options of recruitment.

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

3. RELATED WORK

In the preliminary work[1] by our research group, we examined authentication time, error-rates, and how users' choices of the unlocking mechanisms are linked to the different patterns of smartphone usage, offering insights into improving Android unlocking mechanisms and related user experience. Compared with that study, our new study will collect more diverse data and have a more representative sample of users. Specifically, our app will log proximity/accelerometer/gyroscope sensor data, to help us identify incoming/outgoing calls, whether participants remain at rest or moving while unlocking, and their locations. We will collect participants' subjective opinions on device sharing and apps' sensitivities; and the screen size of participants' devices will be recorded to help us measure how it correlates with the performance of authentication systems. While in the preliminary study, we used UBC mailing lists as one of the advertising tools, most of the participants ended up being students, resulting in a skewed sample. In the new study, we are aiming to get a more representative sample.

Hintze et al.[2] investigated the number of interactions per day, the average interaction duration and the total daily device usage time by using a state machine based on screen-on/off events, to analyze mobile device data logs of 1,960 Android smartphones, which were collected by the Device Analyzer project. Our study differs with it in several aspects. First, the data logs they used did not explicitly indicate the failed unlocking attempts, which will be recorded directly in our study. Another difference is that we will collect precise timing about foreground applications, in order to analyze the patterns of user sessions.

Harbach et al.[3] conducted a global-scaled survey on Google Consumer Surveys (GCS), with 8,286 participants from 8 countries, to investigate whether people's attitudes towards smartphone unlocking differ in national cultures. Instead of analyzing users' unlocking behavior and attitudes on a global scale, we are interested in how US subscribers use smartphones, and how their choices of unlocking mechanisms correlate with their smartphone usage patterns. Moreover, we focus on investigating the performance of different unlocking mechanisms (PIN, password and DAP) in situ, while they only studied whether participants employed any unlocking mechanisms on their devices or not. Also, their data was self-reported, whereas most of our data will be collected automatically, avoiding the bias due to self-reporting.

In another study by Harbach et al.[4], through a month-long field study, they collected data from a panel of PhoneLab users (all affiliated with a local university) with instrumented smartphones (a modified LG Nexus 5), to check the in situ performance of Android unlocking mechanisms. In contrast to their study, (1) we will conduct a longer field study (two months); (2) we do not require participants to use the same type of Android device while participating in the study, and (3) we will recruit a more representative sample of participants.

4. DESIGN OF THE DATA COLLECTION FRAMEWORK

Our data collection framework contains three main parts: Installation, Data Collection and Data Uploading. And each part contains several modules. See Figure 1 for the overall structure. We'll collect four categories of data: demographics, authentication session's data (e.g., unlocking length, unlocking mechanisms, outcomes of unlocking attempts), user session's data (e.g., the length of interaction sessions with the devices, foreground applications), and survey results (e.g., participants' attitudes of sharing devices and apps' sensitivities).

We'll collect participants' demographics data and record it into a user profile text file right after they install our app on their Android devices. Our app will also ask participants to grant certain permissions, namely, device administration permission and usage access permission to our app after installation, in order to enable it to work properly.

The main data collection part will be done by a separate Android process; designed to run as a background service to observe the screen status and to record all interesting events transparently. The data we are interested in includes screen on/off events and incoming/outgoing phone calls, which will be used to help discard short sessions that only contain phone calls. We are implementing relevant receivers and listeners to listen to these events, and then trigger the background service to log the corresponding data into two pre-created files (authentication sessions and user sessions). The background service will also record the outcomes of the device unlocking attempts, including both successful and failed attempts, along with participants' current accelerometer and location data. After participants successfully unlock their devices, a user interaction session will begin and the data collection process will start to run in background and check the list of all running apps every 500 milliseconds to identify and collect the foreground app information. In particular, the process will record when each application is launched and closed.

Furthermore, the main data collection process will also collect participants' perceptions of the sensitivities of apps on their devices, and their attitudes towards device sharing. The background service will randomly present to participants mini-questionnaires with a short list of apps when the device was unlocked, to ask participants' opinions on how sensitive they feel these apps are in the current situation. In order to not overwhelm participants, the questionnaire will be displayed right after the device is unlocked randomly, with a certain probability. Participants' attitudes towards device sharing will be recorded weekly with a questionnaire. The participants will be allowed to dismiss any questionnaires during the data collection, in order to quickly access their devices if necessary.

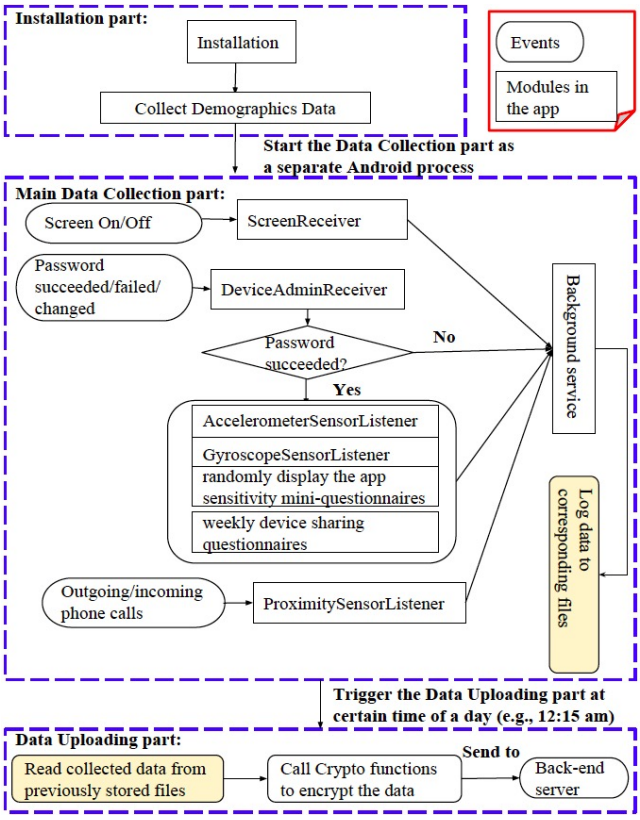

Figure 1: Data flow of the Data Collection Framework.

To improve the quality of the collected data, we will record password change events into the authentication session data file. Once a password change event is received, the app will pop up a question to ask participants what kind of changes they have made. Data Uploading is the last part of our app. After all data is collected, our app will encrypt it with a pre-installed public key, and then upload it to our back-end server on a daily basis.

5. REFERENCES

[1] A. Mahfouz, I. Muslukhov, and K. Beznosov. Android users in the wild: Their authentication and usage behavior. Under review.

[2] D. Hintze, R.D. Findling, M. Muaaz, S. Scholz, and R. Mayrhofer. Diversity in locked and unlocked mobile device usage. *ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2014.

[3] M. Harbach, A. De Luca, N. Malkin, and S. Egelman. Keep on lockin' in the free world: A multi-national comparison of smartphone locking. San Jose, CA, USA, 2016.

[4] M. Harbach, A. De Luca, and S. Egelman. The anatomy of smartphone unlocking a field study of android lock screens. San Jose, CA, USA, 2016.