Journal of Information Security and Applications 40 (2018) 31–43

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Studying users' adaptation to Android's run-time fine-grained access control system

Panagiotis Andriotis[a,*], Gianluca Stringhini[b], Martina Angela Sasse[b]

[a] Department of Computer Science and Creative Technologies, University of the West of England, Frenchay Campus, Bristol, United Kingdom
[b] Department of Computer Science, University College London, London, United Kingdom

ARTICLE INFO

Article history:

Keywords:
Privacy
Android
Usability
Acceptance
Controls
Permissions

ABSTRACT

The advent of the sixth Android version brought a significant security and privacy advancement to its users. The platform's security model has changed dramatically, allowing users to grant or deny access to resources when requested by applications during run-time. This improvement changed the traditional coarse-grained permission system and it was anticipated for a long time by privacy-aware users. In this paper, we present a pilot study that aims to analyze how Android users adapted to the run-time permission model. We gathered anonymous data from 52 participants, who downloaded an application we developed and answered questions related to the run-time permission model. Their answers suggest that most of them positively accepted the new model. We also collected data that describe users' permission settings for each installed application on their devices. Our analysis shows that individuals make consistent choices regarding the resources they allow to various applications to access. In addition, the results of this pilot study showcase that on a second data collection round (occurred one month after the first phase of our experiments), 50% of the respondents did not change a single permission on their devices and only 2.26% of installed applications (on average) presented altered permission settings.

1. Introduction

When Android Developers released the Developers Preview of the Marshmallow version (v6.0) during summer 2015, a major change at the permission system was introduced; the sixth version initiated the run-time permission model. The previous versions are listing at installation time the resources that the application to be installed is going to utilize. After reviewing the requested permissions (which were presented as groups, e.g. Contacts) the user can choose to accept or deny the installation. This binary model (accept-reject) has been criticized at the past as being ineffective to provide meaningful information about the way the application to be installed will affect user's privacy [1,2]. In addition, it limits users' ability to manage the applications' accessibility to their private data. Therefore, the transition from this model to a new one, that would allow users to control the resources that applications were allowed to use (following the iOS paradigm) was anticipated for a long time.

The run-time permission model (aka ask-on-first-use (AOFU) [3]) is based on the principle of least privilege and assumes that applications will be able to function at a basic level, even if the users do not provide access to resources that might affect their privacy. Therefore, applications designed to adhere to this model must request access to sensitive resources during run-time. These actions will (in theory) keep users informed about what an application is trying to do in the background and will provide limited contextual information [4].

According to the official documentation for Android Developers,[1] there are two basic categories of permissions; *normal* and *dangerous*. The documentation notes that the system automatically grants access to resources that applications requested via *normal* permissions, because access to these resources is considered to be of low risk. On the other hand, if an application needs to access users' private information, or other sensitive data stored on the device, then the associated permissions with these actions are considered as *dangerous*. Hence, applications designed to function properly under the AOFU permission model, need to request user's permission during run-time, in order to access sensitive information. Therefore, it lies with the users' discretion if they will ac-

* Corresponding author.
E-mail address: panagiotis.andriotis@uwe.ac.uk (P. Andriotis).
URL: http://www.andrio.eu (P. Andriotis)

[1] http://bit.ly/2d4AdGH .

https://doi.org/10.1016/j.jisa.2018.02.004
2214-2126/

cept or deny access to sensitive resources. Additionally, Android users are able to revoke access to resources via the Settings application under this model. Currently, there exist nine groups of dangerous permissions: Calendar, Camera, Contacts, Location, Microphone, Phone, Sensors, SMS, Storage.

Recent research work indicated that permission requests are vital in terms of conducting resource usage risk assessment and identifying malicious behaviors [5]. Permission requests are also used to assess the app's quality and installation risk, based on patterns identified in high-reputation applications in the Android market place [6]. Therefore, app permissions play a major role in users' privacy and security. The fact that the number of decisions that smartphone users must make (regarding the acceptance of these permissions) can be unrealistically high [7], urged researchers lately to propose automated permission recommendation schemes. Some systems use crowdsourcing methods [8] and others employ machine learning models that incorporate contextual information aiming to predict users' privacy decisions [3]. In order to achieve that, Wijesekera et al. [3] used modified versions of the Android operating system to acquire application usage data and the Experience Sampling Method (ESM) [9] to collect ground truth data about users' privacy preferences. Additionally, Liu et al. [7] deployed rooted devices which were modified and enhanced with the Android permission manager "Apps Ops" [2,10]. Hence, prior work was based on experiments conducted with modified devices, specifically instrumented to gather privacy related data.

Knowing that under the coarse-grained permission model, users are not allowed to intervene with the access control system (since applications can access all resources on a mobile device after the installation process), we investigate in this paper how Android users adjusted their privacy preferences under the fine-grained run-time permission model (AOFU). We consider the following questions in this pilot study. a) Which are the sensitive resources Android users allow more often to be accessed on their phones? b) Are they strict or selective when applications request access to specific sensitive data? c) Do they make consistent choices when they grant or deny access to these resources? d) Are these choices time persistent?

To this end, this paper[2] presents the results of a pilot study that assesses users' adaptation to the Android run-time permission model. For the needs of this study we developed and distributed an application at the official Android marketplace (Google Play) aiming to collect anonymous data related to the permissions that were granted (or denied) by users at that time ('Permissions snapshot'). We did not monitor users' actions for a long time because we assumed that this choice would discourage many people to voluntarily download the app and participate to the study. This is a different approach from prior work [3,4,7] as we aim to gather permission information from devices that were actually used by participants in their daily lives and were not running a modified version of the operating system. Our data collection method is not intrusive or pervasive and does not introduce biases related with asking security and privacy questions (privacy nudges). Thus, we chose to obtain snapshots of the permission settings from the participants' devices. Our application collected permission data twice (in an one-month period) and only when the users were informed and agreed to provide them, according to the ethics approval agreement. The aim of our pilot study is to examine users' perceptions of the provided security and privacy, and at the same time, to investigate how Android users adapted to the AOFU permission model. This work studies and presents security and privacy preferences of Android users of the fine-grained permission model. The contributions of this paper are the following:

- We collected data derived from devices that were running the Android Marshmallow operating system, hence the permission data came from a sample of 52 participants who were actually using these devices for a considerable period of time.[3]
- We present comparative views of users' permissions settings and other privacy preferences associated to the use of popular social media. Moreover, we showcase which sensitive resources were used from our participants more frequently.
- We demonstrate that our participants presented a consistent behavior regarding the resources they allow to be accessed by social media and communication applications. Furthermore, this pilot study shows that the granted permissions to installed applications from the same participants after a period of one month were not dramatically altered. This result verifies similar findings presented recently [7].

The rest of this paper is organized as follows. The next section discusses the methodology we used to derive data and reconstruct permission settings for each participant. Section 3 presents the acquired results focusing at the beginning on the survey answers; then it analyzes our findings from the collected permission data. In Section 4 we discuss limitations of our study, proposing at the same time directions for future work. We review related work in Section 5 and conclude this paper in Section 6.

2. Methodology

This section presents the methodology we used to collect and analyze data. Data collection was carried out in two phases using an application we developed, which was distributed via the official Android marketplace (Google Play) following the example of other recent research works [12]. The application, named "Permissions Snapshot", initially served as a survey instrument, but it also collected anonymous permission data from the devices that were using it. The participants needed to download the application on their devices, answer six multiple choice questions about their experience with the run-time permission model and then send permission data to our server. At the second phase (after a period of one month) the same participants were asked to send permission data again, as explained in more details in the following section. Before we distribute the application on Google Play and publicize it, we obtained approval to proceed with this project from the UCL Ethics Committee (Project ID Number: 8945/001).

2.1. Survey and questionnaire design

The application we developed targeted Android Marshmallow users (SDK 23+) and could not be installed on devices that run an older version of the operating system (OS). This means that the collected data came from participants who were already familiar with the sixth Android version (Marshmallow). During the data collection period (June–August 2016), the most modern version of the OS was the sixth; however, the seventh version ('Nougat') was released as a "Developers Preview" version.

Our application did not collect personal information apart from the package names of the installed applications on the device and the requested permissions. The participants were informed about this action after reading the 'Information Sheet', which was provided at the 'Description' section of the installation page on Google

[2] This is an extended version of our work [11] presented on December 2016 at the 8th IEEE International Workshop on Information Forensics and Security (WIFS) 2016.

[3] The anonymized dataset can be found online at the following address: https://doi.org/10.14324/000.ds.1520825.