Privacy Friendly Apps - Making Developers Aware of Privacy Violations

Karola Marky* Andreas Gutmann* Philipp Rack* Melanie Volkamer*‡

*Technische Universität Darmstadt, Darmstadt, Germany
name.surname@secuso.org
‡Karlstad University, Karlstad, Sweden

Abstract

Android devices are widely used on a daily basis. As those devices can open doors for attackers and companies to privacy sensitive data, developers have to be aware of potential risks. We introduce the project of *Privacy Friendly Apps*, explain its design principles and describe some of its resulted apps. The long-term goal of this project is twofold: (1) raise awareness of developers regarding potential privacy violations posed through unnecessarily overprivileged apps; (2) compile a list of common errors and mistakes that lead to unintended privacy violations.

1 Introduction

In the past years, mobile devices have become widely adopted products. Their omnipresence in people's daily routines and their frequent interconnection with other personal devices provide them potential access to a plethora of (privacy sensitive) data.

With roughly 80% market share in 2015, Android is the most frequently used mobile operation system [Int15]. Its API contains a set of routines, protocols, and tools for developers to build software applications (apps) and thus is a gateway to potential misuse and privacy violations. In order to protect privacy sensitive data, Android defines a *permission* system as security model: Before an app is permitted to access functionality or data, a permission has to be granted by the user. This approval takes place before the app installation (until Android 6.0 "Marshmallow"[1]) and the user grants all permissions at once. If the permissions are not granted the installation process is canceled. These permissions are categorized, e.g. the camera permission is required to operate the LED light.

Even if no privacy violation is intended, developers might include more permissions than an app requires for its functionality. Such overprivileged applications bear two risks: (1) Android's permission request system can be less effective and (2) the impact of bugs and vulnerabilities increases [Fel11]. Hence, the application's permissions could be misused by another application [Ort11]. Also granting more permissions than required for the functionality might lead to the mistrust of users.

A few app rating mechanisms, e.g. as proposed by Jialiu *et al.* [Jia14], determine whether a permission is required for an app's functionality. It is estimated that at least one third of Android applications request more permissions than necessary [Fel11]. Hence, raising the awareness of developers regarding potential privacy and security violations introduced by unnecessary permissions can contribute to mitigating related problems, e.g. by addressing BYOD (bring your own device) concerns [Mil12].

Research orthogonal to ours explores how user can be guided to more privacy aware app choices and installation decisions. This includes research on user's decision making and the derivation of guidelines for privacy aware app decisions [Kul16] as well as on the actual presentation of the permission granting screen in the Google Play Store [Ger15]. Progress in these research directions is likely to shift market demand towards more privacy friendly apps, which requires corresponding knowledge and awareness of developers.

[1] In Android 6 (released in Oct. 2015) and thereafter, permissions are granted during run-time, which could also lead to privacy violations.

In: D. Aspinall, L. Cavallaro, M. N. Seghir, M. Volkamer (eds.): Proceedings of the Workshop on Innovations in Mobile Privacy and Security IMPS at ESSoS'16, London, UK, 06-April-2016, published at http://ceur-ws.org

Our contribution is a set of guidelines for Android application development to make developers aware of potential privacy violations. To test this set university students will develop apps during their programming lab. The results are compared in terms of their potential privacy violations to similar applications in the Google Play Store. As a positive side effect, we contribute privacy friendly apps to society. We further hope that the approach of developing privacy friendly apps within student's programming labs will be adopted by other educational institutions.

2 Privacy Friendly Apps

The Privacy Friendly Apps project is based on few principles, as described in this section. They are applied to evaluate common mistakes and violations regarding privacy violations. Based on Android's security model for data, we identified permissions as the biggest threat to privacy sensitive data. Each Privacy Friendly App complies with the following principles:

Minimal Permissions. Each app uses only those permissions actually needed by the app to implement its functionality. Every use of a permission has to be justified by the developers. This justification should lead developers to reflect about the use of permissions.

Open Source Licence. The source code is licenced under an open source licence (typically GPLv3[2]) and published on the open source platform Github[3]. This procedure guarantees that other persons familiar with programming can review the code. Publishing the source code furthermore builds trust as privacy violations could be discovered by anyone who inspects the code.

No Advertisement or Tracking. Privacy Friendly Apps refrain from tracking or advertisement. Advertisement and tracking might result in a privacy violation and it's not intended to encourage students to integrate these features gratuitously into a privacy friendly app.

In addition to the Google Play Store and Github we try to publish[4] resulting apps in the alternative app store F-Droid. This store exclusively contains open source apps and compiles these directly from the source code. Thus, it is assured that the resulting app matches to the published source code. During this procedure F-Droid examines the app regarding security and privacy issues.

[2]http://www.gnu.org/licenses/quick-guide-gplv3.en.html

[3]https://github.com/

[4]We referred to "try to publish" because F-Droid carefully reviews submitted apps.

Publishing in F-Droid offered a good access to the open source community. We have received feature requests, issues and comments on Github's issue tracker regarding some apps. Regarding one application we received recommendations to provide additional privacy. This recommendation leaded us to carefully review the camera permission which is required to control a phone's LED. So adding the apps to this store supports us identifying privacy risks by utilising collective knowledge.

3 Developed Apps

Several Android apps[5] have been or are currently developed by students during programming labs. This section summarizes four representative apps with regard to their functionality, required permissions and the average amount of permissions needed by the top ten of similar apps[6] as displayed in the Google Play Store.

Dicer can be used to roll six-sided dice.
Amount of permissions: 1
Average permissions (Play Store): 2.9

QR Scanner decodes several QR Code formats as well as barcodes and supports the user in detecting malicious links embedded in QR Codes.
Amount of permissions: 2
Average permissions (Play Store): 10.7

Torchlight uses the LED camera flash light to provide the smart phone with a torchlight.
Amount of permissions: 1
Average permissions (Play Store): 6.9

Sudoku Game.
Amount of permissions: 0
Average permissions (Play Store): 4.5

4 Considerations and Early Findings

We plan to evaluate the development process of Privacy Friendly Apps based on the three principles. We intend to learn which guidelines and which type of knowledge is useful to raise developers' awareness. Therefore, we have designed two questionnaires for programmers to evaluate their awareness level and learning curve. In the future, the developers will therein report their software development skills in general and particularly regarding the Android platform. From this self-reported data we hope to gain further insights.

[5]Corresponding source code can be found at https://github.com/SecUSo

[6]If available and after manual inspection to ensure similarity.

Spreading the idea of letting students of other educational institutions develop Privacy Friendly App is another aspect of considerations. As computer science students typically have to participate in a programming lab they could contribute their results to society e.g. in form of a Privacy Friendly App based on the principles listed in Section 2.

We would like to note that we don't want to badmouth intended privacy violations if there are justifiable reasons, such as to provide a free app based on financing by advertisement. Alternative financing methods like "flattering" or donations are out of this work's scope.

An early example of knowledge which we plan in integrate into our guidelines is the result of an analysis of the development process of a Sudoku application. In order to play this game without interruptions from the screen turning off, the phone has to be prevented from sleeping. Therefore, a specific permission can be included to receive the intended effect. This permission, however, can be circumvented by adding a flag in a specific part of the code. This circumvention is a part of the official Android documentation but frequently overseen by developers. The frequent use of the "prevent phone from sleep" permission might be based on insufficient or missing documentation on online platforms. Therefore we assume that many current and future developers are not aware thereof and thus we want to include this information it in our upcoming guidelines.

5 Conclusion and Future Work

In this paper, we have listed few principles for Privacy Friendly Apps and roughly described how we let students develop apps based on them. Our Privacy Friendly Apps developed in compliance with them require less permissions than the corresponding Google Play Store's top ten similar apps (see Table 1).

Table 1: Required permissions and the average amount of permissions from Play Store's top ten needed for each app.

Application	Amount of permissions	Average permissions
Dicer	1	2.9
QR Scanner	2	10.7
Torchlight	1	6.9
Sudoku	0	4.5

Suggested future work is to derive further principles and provide guidance for privacy aware Android development. We plan to analyse data from Github (source code, issues and comments)[7] to identify additional principles, common mistakes and knowledge gaps. Therefore we also plan to evaluate the student's learning curve. The goal is to provide a procedure of training developers in awareness, e.g. a guide, flyer or similar as well as a list of privacy-related problems experienced by developers while developing an Android app.

Additionally, the approach of developing Android apps based on our principles could spread to other educational facilities. Computer science students are often required to participate in programming labs. By developing a privacy friendly application they furthermore contribute to society.

[7] Including applications not developed in cooperation with us.

References

[Fel11] A. P. Felt, E. Chin, S. Hanna, D. Song, D. Wagner. Android permissions demystified. *Proceedings of the 18th ACM conference on Computer and communications security*, 627–638, 2011. ACM.

[Ger15] P. Gerber, M. Volkamer, K. Renaud. Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy. *ACM SIGCAS Computers and Society, 45(1)*, 16–21, 2015. ACM.

[Int15] International Data Corporation. Smartphone OS Market Share, 2015 Q2. *http://www.idc.com/prodserv/smartphone-os-market-share.jsp*, 2015. Accessed 28-01-16.

[Jia14] L. Jialiu, B. Liu, N. Sadeh, J. Hong. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. *Symposium On Usable Privacy and Security (SOUPS 2014)*, 199–212, 2014.

[Kul16] O. Kulyk, P. Gerber, M. El Hanafi, B. Reinheimer, K. Renaud, M. Volkamer. Encouraging Privacy-Aware Smartphone App Installation: Finding out what the Technically-Adept Do? *NDSS Workshop on Usable Security (USEC)*, 2016.

[Mil12] K. W. Miller, J. Voas, and G. F. Hurlburt. BYOD: Security and privacy considerations. *It Professional (5)*, 53-55, 2012.

[Ort11] C. Orthacker, P. Teufl, S. Kraxberger, G. Lackner, M. Gissing, A. Marsalek, J. Leibetseder, O. Prevenhueber. Android security permissions–can we trust them? *Security and Privacy in Mobile Information and Communication Systems*, 40–51, 2011. Springer.