Available online at www.sciencedirect.com

ScienceDirect

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

ELSEVIER

Signalling over-privileged mobile applications using passive security indicators

Luigi Lo Iacono [a,*], *Peter Leo Gorski* [a], *Josephine Grosse* [a], *Nils Gruschka* [b]

[a] *Data and Application Security Group, University of Applied Sciences, Cologne, Germany*
[b] *University of Applied Sciences, Kiel, Germany*

ARTICLE INFO

Article history:
Available online

Keywords:
Over-privilege
Mobile applications
Application store
Usable security
Privacy
Android

ABSTRACT

As mobile devices have evolved from simple phones to rich computing systems, the data stored on these multi-taskers have consequently become more sensitive and private. Due to this, modern mobile operating systems include sophisticated permission systems for restricting the access to this device for the mobile applications. However, many applications acquire more permissions than required. These over-privileged applications can affect data security and user privacy. All application permissions are indicated to the user, but these notifications have been shown to be ignored or not understood. Thus, other mechanisms need to be improved.

This paper presents design approaches to communicate the degree of over-privilege in mobile applications. It uses an additional rating system in application stores to inform users before making the decision of installing a specific application. The approaches have been evaluated in a usability study based on distinct prototype Android application stores. The findings show that passive security indicators can be applied to influence the decision-making process of users before downloading and installing an application.

1. Introduction

Mobile devices like smartphones or tablets have become essential companions for the majority of people. However, the combination of very sensitive data (like address book, current location, emails or even health information) and many applications from different sources creates severe security and privacy risks. Informing users of mobile devices effectively has turned out to be a challenging task.

Research has identified over-privileged applications as one cause leading to potential security and privacy risks (Felt et al., 2011). From a technical perspective the term over-privilege is used for programs, which claim more access rights than the offered functionality actually requires. This is the case for one third (Felt et al., 2011; Wang et al., 2013) of the applications offered in the Google Play Store (Google, 2016). This can be conditioned by the expressiveness and granularity determined by an operating system (Barrera et al., 2010) or may be caused by developer errors (Felt et al., 2011) even partially induced by usability issues of Security APIs (Felt et al., 2011; Gorski and Lo Iacono, 2016). With a global market share of more than 80% (IDC Research Inc., 2015) Android is the most used operating system for smartphones and tablets around the world.

[*] *Corresponding author.* Cologne University of Applied Sciences, F07/IMP, Betzdorfer Str. 2, Cologne, Germany
E-mail addresses: luigi.lo_iacono@th-koeln.de (L. Lo Iacono), peter.gorski@th-koeln.de (P.L. Gorski), grosse_j@hotmail.com (J. Grosse), nils.gruschka@fh-kiel.de (N. Gruschka).

http://dx.doi.org/10.1016/j.jisa.2016.11.006
2214-2126/© 2016 Published by Elsevier Ltd.

Consequently, there is potentially a high risk for users to choose and install over-privileged apps unknowingly and perhaps even unwittingly. From an implementation perspective over-privilege may have a different meaning. The question in this context is which range of functions is appropriate for a specific application, e.g. why should a calculator application have access to sensitive personal data? The answer will likely be different for economic and privacy arguments.

The popularity of mobile devices has led to a large selection of downloadable software in application stores and many applications actually offer quite similar functionalities. Therefore application stores offer metrics like download counts, pricing, screen shots and user ratings for helping users to choose from the extensive application range. This provided information influences the decision-making process before installing a particular application. Unfortunately privacy notices are not displayed until the definite decision to install an application has already been made.

The Android permission system was originally designed to alert the user to the permissions and privileges a particular application has at its disposal. Up until Android 6.0, when installing an application from the Google Play Store, the user gets presented with a list of all claimed permissions and can then either accept all or none. This method of displaying permissions at the time of installation includes the drawback that the users have already decided to install the application in question, even before the permission-notification shows. Agreeing to the requested permissions without having even read them has quickly become an automated process for many users (Felt et al., 2012; Kelley et al., 2012). When users pay attention to claimed permissions, they often do not understand their meaning (Kelley et al., 2012).

With Android 6.0 the permission management has changed. Much like with iOS (Apple Inc., 2016), the user is now asked to grant access to specific information or resources when the used feature is accessed for the first time by the application. This makes it easier for a user to see the use of certain permissions. However, also here users do not understand or tend to ignore the permissions that an application requests. Thus, the question arises if a visual security indicator integrated side-by-side with the rating system in application stores is able to inform the users' decision-making process in terms of over-privileged applications.

In this paper a passive security notification scheme is introduced for communicating the level of over-privilege of mobile applications. Most importantly, it is deployed as source of information for the user as early as possible in the application selection process. In order to evaluate the acceptance and effectiveness of the introduced approach a usability study has been conducted, supposed to answer the following research questions:

1. What kind of symbolism is suitable for communicating the level of over-privilege?
2. Where to best place and visualize the passive notification system in the application selection process?
3. Would users find a notification system communicating the degree of over-privilege of an application helpful?
4. Would it effectively influence a user's decision to select and install a specific application?

As a prerequisite to evaluate the usability of a notification scheme for over-privilege, models need to be designed as well as their integration in an application store has to be elaborated first (see Section 3). Therefore, existing work should also be discussed.

2. Related work

The issue of passive security indicators to indicate over-privileged mobile applications is a branch of the thematic area of privacy notices. An important and intended characteristic of such notices is to effectively communicate privacy relevant information. A design space for effective privacy notices has recently been proposed by Schaub et al. (2015) based on a comprehensive literature review. When placing over-privileged notification systems in the general context of privacy notices it gets clear that this constitutes just one important part of a holistic privacy notice concept. In respect to the design space introduced by Schaub et al. (2015), the classification of an over-privileged notification system can be outlined as follows:

- **Timing:** To inform and positively affect a user's decision to select, download and install an application on a mobile device, a notice has to take effect in the decision-making process that is typically before selecting an application from a list of presented applications and subsequently pressing the install button.
- **Channel:** An over-privileged notification system can be applied by an appropriate integration into digital marketplaces, either accessed by store applications on mobile devices or via browsers.
- **Modality:** In the context of this work a visual notification system is tested which uses symbols as well as textual elements for interaction.
- **Control:** An over-privileged notification system does not provide privacy controls. It is meant to inform the user's decision-making process to foster a more security and privacy aware selection of mobile applications.

These four dimensions characterize a specific field of research for privacy notices, which also has been addressed by existing studies. These distinctly differ in their visual concepts. Kelley et al. (2013) have proposed a "privacy facts" checklist as part of the main screen and "listing" view in Google Play Store respectively. The checklist can be described as "privacy summary" consisting of ten data items an application will either collect or use, e.g. photos, locators or advertising. This approach only uses textual elements and renounces of symbols. The results of a lab study as well as of an online study showed that the "privacy facts" display can positively affect the application selection process directly compared to the standard Android design but is not generally the decisive selection criterion between competing applications (Kelley et al., 2013). Factors like popularity or rating can strongly influence users' decisions. This approach does not propose a rating, which could allow the user to quickly form an opinion at a glance. Thus, users would have to assess potential security or privacy risks by themselves. This is also the case for the "privacy notice"