Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns

Gökhan Bal [a,*], Kai Rannenberg [a], Jason I. Hong [b]

[a] Goethe University Frankfurt, Chair of Mobile Business & Multilateral Security, Theodor-W.-Adorno-Platz 4, 60629 Frankfurt am Main, Germany

[b] Carnegie Mellon University, School of Computer Science, Human-Computer Interaction Institute, 5000 Forbes Ave, Pittsburgh, PA 15213, USA

ARTICLE INFO

Article history:
Received 20 December 2014
Received in revised form
24 March 2015
Accepted 12 April 2015
Available online 22 April 2015

Keywords:
Smartphone privacy
Privacy risk communication
Privacy behavior
Human factors
Experimental research
Information-flow monitoring

ABSTRACT

Modern smartphone platforms offer a multitude of useful features to their users but at the same time they are highly privacy affecting. However, smartphone platforms are not effective in properly communicating privacy risks to their users. Furthermore, common privacy risk communication approaches in smartphone app ecosystems do not consider the actual data-access behavior of individual apps in their risk assessments. Beyond privacy risks such as the leakage of single information (first-order privacy risk), we argue that privacy risk assessments and risk communication should also consider threats to user privacy coming from user-profiling and data-mining capabilities based on the long-term data-access behavior of apps (second-order privacy risk). In this paper, we introduce Styx, a novel privacy risk communication system for Android that provides users with privacy risk information based on the second-order privacy risk perspective. We discuss results from an experimental evaluation of Styx regarding its effectiveness in risk communication and its effects on user perceptions such as privacy concerns and the trustworthiness of a smartphone. Our results suggest that privacy risk information provided by Styx improves the comprehensibility of privacy risk information and helps the users in comparing different apps regarding their privacy properties. The results further suggest that an improved privacy risk communication on smartphones can increase trust towards a smartphone and reduce privacy concern.

1. Introduction

Modern smartphone platforms have unique properties that make them highly privacy-affecting: they are always on, they are connected to the Internet, they follow their users in space and time, they are open to third-party applications (also known as "apps"), and they provide those apps with access to a multiplicity of sensitive resources and information such as location, contacts, call log, or browsing history. Real-world privacy incidents related to smartphone apps such as the "Path" (Thampi, 2012) and "Brightest Flashlight" (Federal

* Corresponding author. Tel.: +49 (69) 798 34702.
E-mail addresses: goekhan.bal@m-chair.de (G. Bal), kai.rannenberg@m-chair.de (K. Rannenberg), jasonh@cs.cmu.edu (J.I. Hong).
http://dx.doi.org/10.1016/j.cose.2015.04.004

Trade Commission, 2013a) cases, where apps transmit highly privacy-sensitive information to their own or to third-party servers without explicitly asking their users for permission, demonstrate the existence of a real threat to user privacy. The presence of such privacy risks notwithstanding, existing privacy notices in smartphone app ecosystems are in most cases not successful in informing users appropriately about potential and actual privacy risks of services. One key explanation for failing in privacy risk communication is that often the underlying conceptualizations of privacy risks are limited to access-control information, such as granting an application access to some resources (e.g. "Application A wants to access your location"). However, such information does not inform users about the risks associated with granting access and, especially in the context of smartphone app usage, relevant factors such as the type of data that is processed, the frequency of access, the destination of sensitive information flows, or the usage of third-party libraries such as ad networks or analytics tools are not considered in risk assessments. We argue that privacy risk assessments of apps should also consider the long-term access behavior of apps, moving from just providing access-control information to also providing privacy-impact information. These kinds of mechanisms should help end-users reason about multiple information flows that happen over time and help them understand the potential and actual impact an app may have on privacy.

In this paper we propose Styx,[1] a privacy-awareness and privacy risk communication system for smartphone platforms. We use privacy-impacting behavioral patterns (PIBP) as the conceptual basis for our system (Bal, 2012). PIBPs are useful for modeling long-term data-access behavior of apps associated with specific threats to user privacy. Thus, the PIBP concept bridges the gap between sensitive information flows and how they impact user privacy. We developed and evaluated a proof-of-concept implementation of Styx to investigate its effectiveness regarding privacy risk communication. We present the results from an experimental evaluation with 50 participants. With our work, we contribute to the knowledge base of information privacy technology design, particularly regarding privacy risk communication methods. More specifically, the contributions of this paper are as follows:

1. We introduce a new perspective and conceptualization for long-term privacy risks of smartphone app usage, that is the *second-order privacy risk* perspective. This second-order privacy risk perspective reflects the potential impact of user-profiling and data-mining on users' privacy.
2. We introduce Styx, a real-time privacy risk communication system for the Android platform that employs the second-order privacy risk perspective.
3. We present results from an experimental evaluation of a proof-of-concept implementation of the user-faced components of Styx to demonstrate its utility, focusing on its effectiveness regarding privacy risk communication.

The paper is structured as follows. Section 2 provides background knowledge by discussing concepts and theories from relevant literature. In Section 3, we discuss our design and evaluation approach in detail. We first present our design principles that we derived from literature on usability aspects of privacy technology. Next, we present the results from the conceptual work behind Styx, i.e. we introduce the central concept and the high-level conceptual architecture of Styx. Following that, we provide details about the design process of the proof-of-concept implementation of Styx, and finally, we provide details and results from the experimental user study that we conducted to investigate on the effectiveness of Styx regarding privacy risk communication. The results of the user study are presented in Section 4. Section 5 first discusses the results of the user study and then discusses potential implications and limitations of our results. Section 6 concludes this article.

2. Theoretical background and related work

In this section, we first emphasize the importance of privacy transparency in privacy protection and provide motivation for focusing on this aspect in the context of smartphone app ecosystems. Next, we discuss the nature of privacy risks in smartphone app usage. We propose a new perspective and conceptualization of privacy risks in the context of smartphone apps and also discuss the causes of these risks. Following that, we discuss existing privacy risk indicators in smartphone app ecosystems and elaborate on their effectiveness. Alternative approaches of privacy risk indicators proposed by other researchers will be discussed subsequently. Finally, we discuss approaches complementary to privacy risk communication systems such as information-flow analyzers and mechanisms that are intended to give users more control over the flow of their personal data.

2.1. *Privacy transparency*

Over the last decades, several international organizations developed basic principles on data protection and codes for fair information processing to foster and guide the protection of individuals' information privacy (European Parliament and Council, 1995; ISO, 2011; OECD, 1980; U.S. Department of Health Education and Welfare, (1973); United States Congress, 1974). Amongst other principles, they all emphasize the importance of transparency (individuals should have a right to view all information that is collected about them). Beyond the general principles for data protection, privacy protection or privacy management can also be described as a process. Derived from Bruce Schneier's (2000) definition of information security as a process, Brunk (2005) proposed the "Privacy Space Framework" that consists of the stages awareness, detection, prevention, response, and recovery. This view on privacy management suggests that privacy management has to start with awareness of privacy-related issues and that without awareness and detection of privacy issues no privacy

[1] Inspired by the river "Styx" in Greek mythology, which formed a boundary between the world of the living and the underworld, around which it flows seven times (The Theoi Project 2014). We use this as a metaphor for our privacy-awareness system that brings sensitive-information flows from the hidden, "dark side" of the smartphone device to the user's "realm".