PrivacyInformer: An Automated Privacy Description Generator for the MIT App Inventor

Daniela Miao
Computer Science and Artificial Intelligence Laboratory
MIT
Stata Center, 32 Vassar St.
Cambridge MA USA

dmiao@csail.mit.edu

Lalana Kagal
Computer Science and Artificial Intelligence Laboratory
MIT
Stata Center, 32 Vassar
Cambridge MA USA

lkagal@casil.mit.edu

Abstract

With advancements in mobile communication technology, mobile privacy is rapidly emerging as a field of concern for mobile developers, industry leaders and the public. Privacy issues in the mobile applications market could compromise the well-being of smartphone consumers, yet developers continue to struggle with producing appropriate privacy documents. As a part of my research work, I have developed a technical solution named PrivacyInformer, as an add-on to the MIT App Inventor. During my presentation I will show how PrivacyInformer can automatically produce privacy descriptions in both human-readable and machine-readable format, by simply analyzing the source code of the App Inventor project. This serves as an enabling mechanism for better visual representation of privacy-related information and smart matching of users' privacy preferences with mobile applications.

1. Introduction

In this age of technology, users leave a staggering number of sensitive, personally identifiable information on their phones -- a reality that both drives and results from the networking era. Recent events surrounding privacy breaches have prompted many users to grow wary over potential privacy risks imposed by their mobile apps. Unfortunately, when choosing which mobile app to install, users are generally provided with no information on privacy implications of the application. The Android permission system seeks to address this need, but the description it provides are excessively broad and offers little meaningful information to users. Hence, there remains a compelling need for a mechanism that allows users to better understand privacy-related behaviors of mobile apps.

For the average mobile app developer, writing documentation for the app is a time-consuming and mundane process. This is especially true for App Inventor developers, who often come from a non-technical background and lack full understanding of the app

behaviors themselves. Given the burden of work, privacy documentation is often neglected.

This talk introduces a privacy description generation tool, named PrivacyInformer that focuses on resolving privacy concerns in the mobile applications market. MIT App Inventor was chosen as the base platform because it provides a controlled development environment where all project components are released and maintained by the App Inventor team. This allows PrivacyInformer to accurately analyze project source code of App Inventor applications. Finally, App Inventor tools are exposed to everyone regardless of technical background. This means as privacy enhancements are released via App Inventor, privacy awareness is raised at a global scale.

2. Overview of PrivacyInformer

Upon starting an App Inventor project, the user will have the option of enabling the automatic privacy description generation feature provided by PrivacyInformer (see Figure 1), which will automatically package a privacy description with the compiled application. The system is designed such that, at the time of compilation, PrivacyInformer statically analyzes the source code of the App Inventor project, and gains an understanding of how components are used within the application.

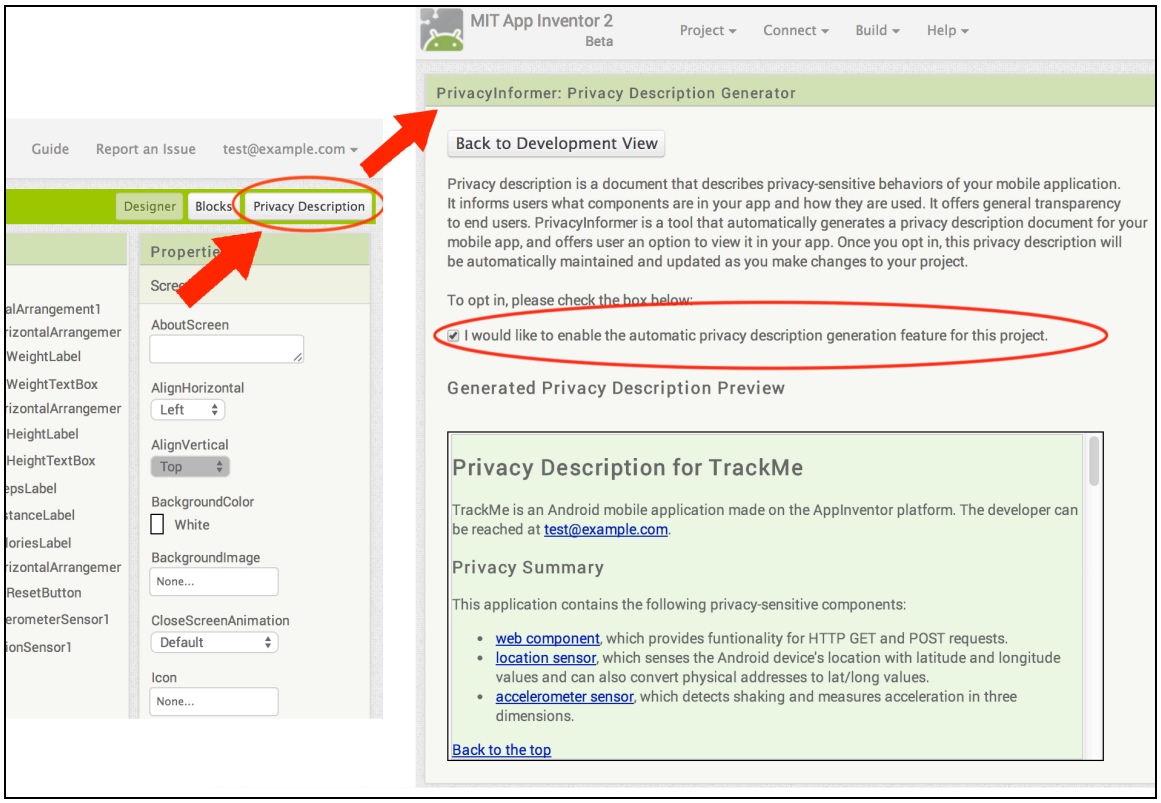

Figure 1: PrivacyInformer view that allows users to enable the automatic privacy description generation feature

The following analyses are done by PrivacyInformer in order to generate the privacy description:

- Identifies privacy-sensitive components in the application and imports pre-generated privacy templates corresponding to these components. For instance, if a mobile app uses the Web component and its corresponding privacy template states the application's ability to transfer data to the Internet, then the privacy description will contain the same statement (directly copied from the Web component's privacy template).
- Analyzes methods and values used in the components. For each method of each component, find privacy-relevant interactions with other methods or components and include them in the privacy description. For instance, identify that location information is being collected by the Location sensor and sent externally off the phone using the Web component.
- The privacy description is inserted into the application (included as part of the apk), so that the human-readable version is accessible via the mobile application's Android menu options.

A machine-readable version of the privacy description is generated in Linked Data format and attached to the meta-data of the compiled apk, because this allows more flexibility for data manipulation later. This file can be used in the future to enable further reasoning and user privacy preference matching.

3. Future Work and Conclusion

As mentioned previously, PrivacyInformer opens the door for much research in the area of increasing privacy accountability of mobile applications. It acts as an enabling mechanism for users to select apps based on their customized preferences. Given the privacy description attached with each App Inventor app is in Linked Data format, one can easily reason over it and produce a matching algorithm to present users applications that fit their privacy preferences. Furthermore, this document can be extracted and processed to generate corresponding rules that enforce data access. For instance, a system like the Open Mustard Seed (OMS) trust framework could use such rules when third-party applications request data from the end-user's personal store.

In summary, during this talk we attempt to alleviate the current privacy issues in the mobile applications market. We introduced a tool as a part of the MIT App Inventor named "PrivacyInformer". It seeks to provide a quick and automatic way to help developers produce privacy descriptions for their mobile apps. By analyzing the source code of the application at compilation time, we are able to produce an accurate description of privacy-relate behaviors of the application to mobile app users. We do so in both human-readable and machine-readable formats, hence opening up many future research opportunities to improve the outlook of mobile privacy, both in areas of enhancing visualization of privacy information and matching user preferences against appropriate mobile apps.