P-Lint: A Permission Smell Detector for Android Applications

Abstract:

Android is built upon a permission-based structure, where apps require access to specific permissions in order to carry out specific functionalities. While Android has provided a set of best practices intended to aid the developer in properly defining and manipulating these permissions on their source code, developers do not always adhere to these guidelines. Although some of the resulting issues may be minor and lead to slight user confusion, other mistakes may create more serious privacy and security related issues. We've defined improper usage of these permission best practices to be permission smells to indicate possible permissions related syntactic issues and have created a tool P-Lint to assist in the identification of these smells on the source code. P-Lint's goal is to not only help developers create better, more secure apps by providing guidance on properly using permissions, but also in allowing researchers to better understand the common permission smells through empirical analysis on existing apps. P-Lint is publicly available on the project website: https://p-lint.github.io

Introduction:

Beginning with Android Marshmallow (API 23), developers may now ask users to request permissions at run-time, and users may choose to grant only some of the app's requested permissions. This significantly differs from previous versions of Android where developers would only be allowed to ask for permissions upon the installation of the app, and users would have to accept the permissions in an all-or-nothing fashion. Android introduced several permission 'best practices' for using this new permissions model. Not adhering to some of these rules can have more profound effects in comparison with other rules. A 'code smell' is a symptom of a bad programming practice, and not a syntactic error, i. e., not that an issue necessarily exists. Similarly, we define permission smells, as an indication of a permission-related bad programming practice. Some examples of permission smells include not adhering to Google's permission best practices guideline and misusing the checkSelfPermission(), requesting permissions when Intents are advised to be used, or possible misuse of custom permissions. We have designed and implemented P-Lint1 (Permission-Lint) to detect permission smells. The primary contributions of P-Lint are:

• Assist developers with developing better permissionrelated statements and methods, and help them adhere to defined standards.

• Provide a tool for researchers to analyze a large number of existing apps for permissions related bad practices, which may have led to potential privacy or security vulnerabilities. To our knowledge, this is the first tool that analyzes Android apps for proper permissions usage from a standards perspective. P-Lint differs from tools such as PScout and Stowaway since it does not focus on merely identifying the permission-gap, but in performing permissions checks based on best practices.