Poster: A Large Scale Investigation of Obfuscation Use in Google Play

Abstract

Android applications are frequently plagiarized or repackaged, and software obfuscation is a recommended protection against these practices. However, there is very little data on the overall rates of app obfuscation, the techniques used, or factors that lead to developers to choose to obfuscate their apps. In this paper, we present the first comprehensive analysis of the use of and challenges to software obfuscation in Android applications. We analyzed 1.7 million free Android apps from Google Play to detect various obfuscation techniques, finding that only 24.92% of apps are obfuscated by the developer. To better understand this rate of obfuscation, we surveyed 308 Google Play developers about their experiences and attitudes about obfuscation. We found that while developers feel that apps in general are at risk of plagiarism, they do not fear theft of their own apps. Developers also report difficulties obfuscating their own apps. To better understand, we conducted a follow-up study where the vast majority of 70 participants failed to obfuscate a realistic sample app even while many mistakenly believed they had been successful. These findings have broad implications both for improving the security of Android apps and for all tools that aim to help developers write more secure software.

PUBLISHED PAPER

Title:
A Large Scale Investigation of Obfuscation Use in Google Play

Authors:
Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl

Date:
December 03-07, 2018

Venue:
Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC ’18)

DOI:
10.1145/3274694.3274726

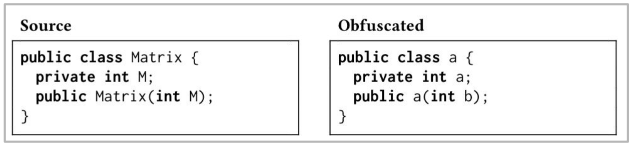
PDF:
https://saschafahl.de/static/paper/androidobfuscation2018.pdf

A Large Scale Investigation of Obfuscation Use in Google Play

Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl

Motivation

Software obfuscation is a possible protection against plagiarism and repackaging of apps.



Source

```
public class Matrix {
  private int M;
  public Matrix(int M);
}
```

Obfuscated

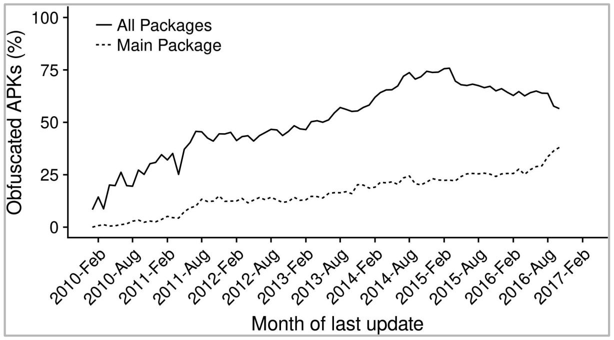
```
public class a {
  private int a;
  public a(int b);
}
```

Yet the current state of software obfuscation in the Android app environment is mostly unknown.

We performed 3 experiments to investigate the use of obfuscation.

Exp 1: Large Scale Analysis

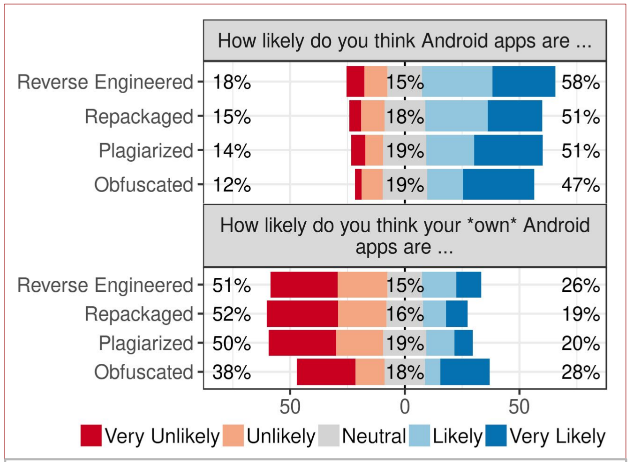
- Static analysis of 1.7 million free apps on the Google Play Store
- Detection of both common and more tool specific obfuscation patterns in apps



Result: roughly 25% of apps appear to be obfuscated, the majority by using ProGuard.

Exp 2: Developer Survey

- Survey of 308 Google Play developers
- Questions about experiences and perceptions of obfuscation



Skewed threat perception for Android apps overall compared to the developer's own apps.

Result: developers are overall aware of general threats and the possible benefits of obfuscation, but perceive negligible personal impact

Exp 3: Obfuscation Experiment

- In the survey, 35% described problems using ProGuard
- We asked 70 developers to obfuscate two small sample apps using ProGuard

Result: most developers succeeded in obfuscating a basic example app, but 78% failed to obfuscate a more complex and realistic app example

Discussion

We found two major themes in our experiments:

- *"Security through insignificance?"* Developers downplay risks for their apps compared to their perception of the whole app ecosystem
- *"Optional obfuscation"* Usability problems with obfuscation tools further decrease motivation for obfuscation

Acknowledgments

This work was supported in part by the National Science FOundation under grant numbers CNS-1526718 and CNS-1562485.