

Accepted Manuscript

Title: The performance cost of software obfuscation for android applications

Author: Yan Zhuang

PII: S0167-4048(17)30209-2

DOI: <https://doi.org/doi:10.1016/j.cose.2017.10.004>

Reference: COSE 1216

To appear in: *Computers & Security*

Received date: 8-2-2017

Revised date: 3-9-2017

Accepted date: 5-10-2017



Please cite this article as: Yan Zhuang, The performance cost of software obfuscation for android applications, *Computers & Security* (2017), <https://doi.org/doi:10.1016/j.cose.2017.10.004>.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

The Performance Cost of Software Obfuscation for Android Applications

Yan Zhuang

Department of Computer Science, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU),
D-91054 Erlangen, Germany

E-mail: yan.zhuang@cs.fau.de

Abstract

Software security of Android applications is especially susceptible (vulnerable) to malicious reverse engineer than the native code based software, because its Java bytecode is easier to decompile and to reconstruct the original Java source code. Therefore obfuscation is an essential criterion for the protection of Android applications. Meanwhile, the unpredicted performance loss will be caused by the obfuscation, which might seriously influence the user experience of the software. Therefore the obfuscation degree and the performance cost out of it require being optimized. In this paper, we are working on the problem that: to obfuscate an Android application to a target level of “difficulty” degree, while not substantially “slowing it down”. We measure “difficulty” by utilizing software complexity metrics and the “slow” in CPU cycles. Within the framework designed for obfuscating Android applications, we implement the “Naïve Bayesian Classifier” algorithm for the optimized obfuscation of the software complexity and the performance, and show that it outperforms the algorithm whose predictions rely on mean values. We furthermore investigate the performance penalty imposed by obfuscation process when framework targets different complexity values and metrics. We show that some obfuscation methods are more performance costly than others to achieve the same metric value increase. Our result shows that, for any given software complexity, the required performance benefits can be achieved if the right obfuscation techniques are used.

Keywords:

software complexity metric, obfuscation, software quality, performance measurement, optimized obfuscation, Android applications

Download English Version:

<https://daneshyari.com/en/article/6884027>

Download Persian Version:

<https://daneshyari.com/article/6884027>

[Daneshyari.com](https://daneshyari.com)