Analysis and Evaluation of SafeDroid v2.0, a Framework for Detecting Malicious Android Applications

Android smartphones have become a vital component of the daily routine of millions of people, running a plethora of applications available in the official and alternative marketplaces. Although there are many security mechanisms to scan and filter malicious applications, malware is still able to reach the devices of many end-users. In this paper, we introduce the SafeDroid v2.0 framework, that is a flexible, robust, and versatile open-source solution for statically analysing Android applications, based on machine learning techniques. The main goal of our work, besides the automated production of fully sufficient prediction and classification models in terms of maximum accuracy scores and minimum negative errors, is to offer an out-of-the-box framework that can be employed by the Android security researchers to efficiently experiment to find effective solutions: the SafeDroid v2.0 framework makes it possible to test many different combinations of machine learning classifiers, with a high degree of freedom and flexibility in the choice of features to consider, such as dataset balance and dataset selection. The framework also provides a server, for generating experiment reports, and an Android application, for the verification of the produced models in real-life scenarios. An extensive campaign of experiments is also presented to show how it is possible to efficiently find competitive solutions: the results of our experiments confirm that SafeDroid v2.0 can reach very good performances, even with highly unbalanced dataset inputs and always with a very limited overhead.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Sapienza - Università di Roma, Technical University of Denmark
Corresponding author: Spognardi, A.
Contributors: Argyriou, M., Dragoni, N., Spognardi, A.
Number of pages: 15
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: Security and Communication Networks
Volume: 2018
Article number: 4672072
ISSN (Print): 1939-0114
Ratings:
Scopus rating (2018): CiteScore 1.81 SJR 0.311 SNIP 0.862
Web of Science (2018): Impact factor 1.376
Web of Science (2018): Indexed yes
Original language: English
Electronic versions:
4672072.pdf
DOIs:
10.1155/2018/4672072
Source: FindIt
Source ID: 2438890818
Research output: Contribution to journal › Journal article – Annual report year: 2018 › Research › peer-review