INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

NORVISDROID

A Novel Malicious Android Application Detection Scheme

A dissertation by

Mr. Maturankan Krishnamohan

W1790145 / 2019618

Supervised by:

Mr. Rathesan Sivagnanalingam

This document includes partial fulfillment of the requirements for the BEng Software Engineering degree at the University of Westminster.

May 2023

ABSTRACT

Detection of malicious Android applications remains a challenging task, despite various schemes and frameworks proposed by researchers that combine different analysis methods and detection models using various algorithms. The existing methods have been developed and tested on specific malware datasets from a specific time period lacking the generalization ability and not very effective against zero-day Android malware. Traditional malware analysis techniques face difficulties with feature selection and representation due to complexity and multicollinearity issues. Additionally, they are not effective against recent malware advancements such as obfuscation and evasive mechanisms.

This research aimed to examine the effectiveness of image-based analysis in normality-based detection of malicious Android applications. The system was built to detect zero-day Android malware, independent of known malware patterns and datasets, and free from feature-related issues. The hypothesis was that each category of benign Android applications would have a common set of features that distinguished it from malicious applications in the same category. Image-based analysis, instead of traditional analysis methods, was employed to overcome the challenges posed by malware obfuscation and evasion techniques as well as feature related issues.

The system was evaluated using sets of benign and malicious apps including obfuscated malware apps to validate its effectiveness. 125 different combinations of feature extractors and novelty detection algorithms were experimented alongside category-based models and category-less model. Image fusion techniques were also studied and experimented. The proposed system was able to produce promising results during the testing and evaluation phase. This research project serves as a valuable contribution to the Android malware detection field and opens up new avenues for future research and development.

Keywords: Android, Anomaly Detection, Binary Data, Cybersecurity, Image Analysis, Machine Learning, Malware Detection, Novelty Detection, One Class Classification, Transfer Learning.

Subject Descriptors:

- Security and privacy → Intrusion/anomaly detection and malware mitigation → Malware and its mitigation