22. CLEMENT SUNNY

Machine Learning-Based Malicious Application Detection of Android

Abstract

In this seminar, a machine learning-based approach which is used to detect malicious mobile malware in Android applications is presented. This system is able to capture instantaneous attacks that cannot be effectively detected in the past work. Based on this approach, this method implements a malicious app detection tool, named Androidetect. First, the system analyses the relationship between system functions, sensitive permissions, and sensitive application programming interfaces. The combination of system functions has been used to describe the application behaviours and construct eigenvectors. Subsequently, based on the eigenvectors, the methodologies of naive Bayesian, J48 decision tree, are compared regarding effective detection of malicious Android applications. Androidetect is then applied to test sample programs and real-world applications. The experimental results prove that Androidetect can better detect malicious applications of Android by using a combination of system functions compared with the previous work.