Analysis of the safety level of Android operating system applications based on machine learning

Pasitxay Phimphinith

Abstract: This study presents a machine learning-based framework for analyzing the security posture of Android operating system applications. With the proliferation of mobile malware and privacy-invasive software, traditional signature-based detection methods have become insufficient against evolving threats. The proposed approach leverages supervised learning algorithms to classify applications as benign or malicious based on static and dynamic feature extraction, including permissions, API calls, network activity, and system call sequences. A comprehensive dataset comprising both legitimate and malicious Android packages was used for training and evaluation. Several classifiers, including Random Forest, Support Vector Machine, and deep neural networks, were compared for accuracy, precision, recall, and F1-score. Experimental results demonstrate that the ensemble-based model achieves over 96% detection accuracy with a low false positive rate, outperforming conventional antivirus engines. The findings underscore the efficacy of machine learning in enhancing Android security analysis, offering a scalable and adaptive solution for real-time threat detection. This research contributes to the field of mobile security by providing a robust analytical tool for assessing application safety in the Android ecosystem.

Keywords: Android security, machine learning, Android application analysis, malware detection