Detecting Android Malicious Applications Using Static and Dynamic Analysis Techniques

This dissertation introduces DDefender, a hybrid and an automated detection system that detects malicious applications on Android devices. DDefender extracts a diverse set of features by integrating static and dynamic analysis techniques, and then applies machine learning algorithms to effectively detect malicious applications. Specifically, DDefender uses dynamic analysis to extract system calls, system information, network traffic, and requested permissions of an inspected application. Then, it utilizes static analysis to extract features from the inspected application such as components, activities, and services. By applying several machine learning algorithms, DDefender was evaluated on a dataset of 24,100 applications, and successfully achieved up to 99% detection accuracy.

In addition, this dissertation presents a web service tool, called DDefender web service, that allows users to analyze Android applications before installation. DDefender classifies malicious applications efficiently with a minimal impact on battery life and performance of the device.

The Oakland University and School of Engineering and Computer Science communities are invited to attend Hani Alshahrani’s defense of his Ph.D. dissertation. Seating is limited. RSVP with Katie Loodeen at loodeen@oakland.edu.