Code Coverage Analysis for Detecting Malicious Android Applications

Olga Gadyatskaya

University of Luxembourg
olga.gadyatskaya@uni.lu

Thesis Details

If you are an Android user, chances are – you have got malware on your device. Security vendors, such as Kaspersky and Symantec, report on drastic surges in Android malware rates and on the ever-increasing sophistication of the discovered malicious samples. Many samples discovered in the last year exhibit complex behaviours that hinder security analysis, for example, code obfuscation, emulator detection and context-sensitivity. These techniques allow malware to evade detection by not exhibiting malicious functionalities in analysis, but only on end-user devices. Thus security analysis requires new techniques to combat with this kind of malware.

The goal of this thesis is to investigate dormant malicious functionalities in Android apps by looking at code coverage analysis results. You will select a code representation model, such as a call graph, and will design a system that will map, during app execution, elements of this model to $\{covered, not - covered\}$ labels. Then, by applying machine learning techniques, you will discover dormant functionalities in malicious Android apps.