Detecting Privacy Violations in Children's Apps Using HPCs

Hussain, Suha (School: Queens High School for the Sciences at York College)

The recent surge in children's apps reflects the proliferation of new avenues for education and entertainment globally. However, more than half of all children's apps on the Android platform violate the Children's Online Privacy Protection Act (COPPA), indicating an invasion of user data privacy that threatens the safety of millions. Previous research on detecting COPPA violations rely upon an analysis of the system binary, which is neither scalable nor reliable. To overcome these challenges, hardware performance counters (HPCs) were utilized to detect COPPA violations. A novel dataset was established after the profiling of a number of COPPA-compliant and COPPA-violating Android apps. Based upon this dataset, two methods, a general COPPA violation detector and a series of specialized COPPA violation detectors, were formulated. The former detects the existence of any possible COPPA violation. Supervised learning algorithms were applied to the whole dataset and, to address HPC measurement constraints, to feature-reduced data. The latter detects the existence of a specific COPPA violation. Thus, several specific COPPA violation detectors trained upon feature-reduced data were developed. In addition to yielding high accuracies and low misclassification rates, these classifiers are secure, efficient, and adaptable due to the nature of HPCs. Moreover, this software can be incorporated within multiple points in the architecture of the mobile phone and the supply chain as a whole.

Awards Won:
National Security Agency Research Directorate : First Place Award "Science of Security" of $3,000
Association for Computing Machinery: Second Award of $3,000