Abstract

Static analysis has been used for assessing android applications for possible data leaks both known and unknown. Due to large size of applications and the libraries that they depend on, it’s expensive to perform whole program analysis which leads to either ignoring or making assumptions of the effect of the library that puts into question the soundness of the results. Missed paths are generated that lead to false alarms and missed paths that in return allow possible leaks evade detection. The study computed Android Bluetooth Library 2.1 summaries that were successful used to analyze twenty target applications and no possible data leak was detected. Exploratory approach was used to answer the research questions and lastly java-call graph suite of programs was used to construct a call graph of the library and Dexter android static tool for applications.

References


Keywords

Static Analysis, data leakages, Android Libraries