Certifying the Security of Android Applications with Cassandra

Work-in-Progress Report

David Schneider

Technische Universität Darmstadt

joint work with:

Steffen Lortz, Heiko Mantel, Artem Starostin,
Alexandra Weber, Timo Bähr

August 8, 2016

Abstract

Modern mobile devices store and process an abundance of data. Although many users consider some of this data to be private, they do not yet obtain satisfactory support for controlling what applications might do with their data. In fact, many Android applications reveal private data of users to untrusted third parties without their consent.

Our Certifying App Store for Android, Cassandra, enables users of Android mobile devices to check whether applications comply with their personal privacy requirements before installing the applications. To make this possible also for non-experts, Cassandra provides a policy editor that allows users to create security policies in terms of intuitively comprehensible categories of data. Cassandra displays the flows of information in an application graphically in terms of these categories. This allows users to make informed decisions about whether they want to install an application or not. Cassandra implements a type-based information-flow analysis. This analysis is semantically justified: It has been proven to be sound with respect to a formal operational semantics of Dalvik bytecode and a formal noninterference security condition. To our knowledge, Cassandra is the first static information-flow analysis tool for Android with a soundness result. We have applied Cassandra to self-developed case studies as well as to selected open-source applications from the F-Droid app store. Recently, a new analysis algorithm has been implemented that has increased the performance of Cassandra significantly. Currently, we are working on providing security guarantees for a wider range of third-party applications.