Short Talk Abstract:

Certifying the Security of Android Applications with Cassandra

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

Department of Computer Science, TU Darmstadt
e-mail: ⟨lastname⟩@mais.informatik.tu-darmstadt.de

I. Introduction

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 [1], enables users of Android mobile devices to check whether applications comply with their personal privacy requirements before installing the applications.

II. Cassandra

Cassandra allows end users of mobile devices to create security policies that capture their individual privacy requirements. 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 such as “Location Data” or “Calendar & Contact Data”. Cassandra displays the flows of information in an app graphically in terms of these categories (cf. Figure 1). In case Cassandra finds a potential security violation, detailed information about the violation is provided. This allows users to make informed decisions about whether they want to install such an app nevertheless or not.

Cassandra implements a type-based information flow analysis of Dalvik bytecode. This analysis is semantically justified: The notion of security is specified as a noninterference-like security condition that is defined in terms of a formal semantics of Dalvik bytecode. We have proven that the analysis is sound, i.e., that all violations of security policies are found. To the best of our knowledge, Cassandra is the first information flow analysis tool for Android with a soundness result [1].

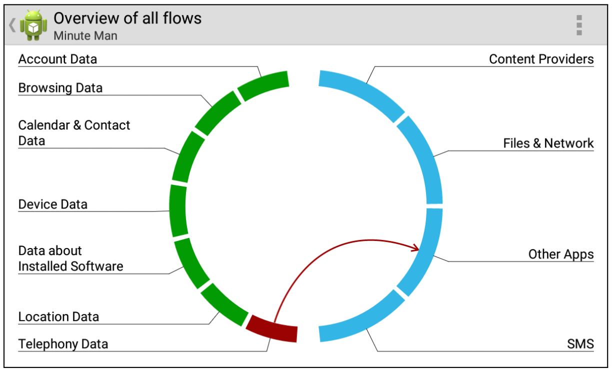

Figure 1: Visualization of information flows in an app

A user can choose whether Cassandra performs the security analysis directly on the mobile device or remotely on a server with more computation power. If the second option is chosen then Cassandra uses proof-carrying code [2] to avoid that the server becomes part of the trusted computing base. That is, the server generates a certificate that enables Cassandra to validate the security analysis efficiently on the mobile device.

There are many other solutions for analyzing Android applications w.r.t. security aspects, including information flow security. The novelty of Cassandra is that it supports user-defined security policies and that its information flow analysis has been justified w.r.t. a noninterference-like property based on an operational semantics of Dalvik bytecode.

Cassandra is available as open-source software under the MIT license and demo movies are available online.[1] We are currently evaluating Cassandra experimentally with open-source applications from the F-Droid app store. In a previous evaluation we have already shown that Cassandra is suitable for analyzing self-developed applications. The functionality of the applicatons included limiting the duration of calls to save costs, managing notes, and measuring the distance users have traveled.

Our research on Cassandra is sponsored by the German Research Foundation (DFG) within the nation-wide priority program “Reliably Secure Software Systems” (RS^3).[2]

References

[1] Steffen Lortz, Heiko Mantel, Artem Starostin, Timo Bähr, David Schneider, and Alexandra Weber. Cassandra: Towards a Certifying App Store for Android. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 93–104, 2014.

[2] George Necula. Proof-Carrying Code. In *Proceedings of the 24th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 106–119, 1997.

[1] http://www.mais.informatik.tu-darmstadt.de/cassandra.html

[2] http://www.reliably-secure-software-systems.de