22 December 2016 Study · Mobile Security · Privacy & Crypto

Static Analysis of iOS Applications

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/static-analysis-of-ios-applications/

The behavioral analysis of mobile applications for Apple iOS is still a very challenging procedure, both in terms of time and resources required. In the end, it is usually not clear which measures an application provides to protect sensitive data. Similarly, it is difficult to determine whether apps violate established security principles, such as when cryptographic functions are used, and thus facilitate attacks on critical data.

Within the scope of this project, a solution was sought in order to be able to subject iOS applications to an automated static analysis. It should provide concrete statements on safety-relevant properties. Specifically the goal was to determine whether apps use cryptographic functions in a secure way. Since the static analysis of iOS applications is a comparatively little explored topic, the first step of this project involved the development of a knowledge base on all the components involved. The main findings will be explained in this report. In the second step, an analysis environment was designed to enable a fully automatic analysis of iOS applications. The suitability of the propagated solution could be proven within the scope of an implementation and the test with real applications. In addition to insights into implementation weaknesses in apps, this practical test has also highlighted limitations to the solution, which can hinder a consistent analysis.

The proposed concept as well as the practical implementation show that the static analysis of iOS applications can be carried out in a targeted manner. The large number of available iOS applications with security-relevant functionality also impels the need to implement even more specific researches of individual apps in the future.