18 October 2017 Study · Mobile Security · Privacy & Crypto

Fingerprinting Code of Mobile 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 This content is no longer updated.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.

Version 2017-10-05
Source https://technology2.a-sit.at/en/publications/fingerprinting-code-of-mobile-applications/

The analysis of applications for mobile platforms (Android, iOS) has shown that security-relevant problems are often not to be found in the application code itself, but are introduced by components of third-party software. Often, these problematic code parts are made freely available and are thus found in many applications. If the program code is obfuscated by the manufacturer, it becomes very difficult to find precarious code parts.

The aim of this project was to develop a strategy to find already known code fragments which are regarded as problematic or potentially dangerous in the security context by automated means. The approach thus designed can help to reduce the effort required for manual inspection of applications and sometimes significantly facilitate the rapid detection of security-relevant errors despite code obfuscation.