21 December 2021 Study · Mobile Security

On-Device Patching Framework for Android 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 This content is no longer updated.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 2021-12-13
Source https://technology2.a-sit.at/en/publications/on-device-patching-framework-for-android-applications/

Patching existing Android packages has a broad range of applications, ranging from fixing security vulnerabilities to instrumenting potential malware, or extending some software's functionality.

However, existing solutions support solely patching an applications's program code, which only represents one part of an Android app. Additionally, patch developers are usually only enabled to patch concrete applications, or at least concrete classes known at the time of patch development. These limitations counteract the frequent need to modify classes based on their inheritance tree, or go beyond manipulation of the control flow, e.g. by adding resources or altering a package's manifest file.

This project saw the development of a fully-functional patching framework consisting of a development kit for the convenient creation of application-agnostic patches, as well as a complete deployment pipeline that is performant enough for integration into mobile applications.