Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität ulm

Security Analysis of an Android App

Master's Thesis

30 CP

The majority of adults have cell phones that are used for many different tasks, and for each task there are different apps, resulting in 2.8 million apps in the Google Play Store. Using apps always requires a certain level of trust, as most of them require at least an Internet connection and access to storage. However, such permissions open the door to vulnerabilities that can be exploited. Especially apps for older Android versions that are no longer patched may have known vulnerabilities. Furthermore, these permissions can be abused to collect user information which are sent it to backend servers.

In this thesis, you first have to consider which app of the Google Play Store is most likely to have a vulnerability and justify this decision. Then compare existing methods for finding vulnerabilities in APKs and either choose one or create a new methodology that is more appropriate for your use case.Then you must reverse engineer the app and analyze it for vulnerabilities. As an additional optional task, you can also look for security and privacy v breaches in the app itself.

Suitable for all students who are interested in app reverse engineering and at least have flashed a custom rom.

Michael Wolf | michael.wolf@uni-ulm.de| O27-3210

If your are interested or you need additional details, feel free to contact me or drop by for a non-binding chat.