Android Firmware Image Analysis

Advisor: **Florian Draschbacher**

Motivation

When analysing the security of Android firmware images, a critical undertaking is understanding the relations between different system components. While the source code can help this process in some parts, other parts are usually proprietary to specific device vendors and closed-source. Reconstructing the interdependencies between different components (i.e., user space software and device drivers) is particularly obfuscated by hardware abstraction layers (HAL) and inter-process communication (IPC) mechanisms. In this project, you design and develop a tool that helps researchers uncover the dependencies between different components of Android firmware images. From a given firmware image, this tool will generate a navigable visual map of key system components and their interactions.

Goals and Tasks

- Get an understanding of Android firmware image structure and key system components
- Identify involved file types and suitable static analysis techniques
- Implement a program for resolving and visualising interdependencies
- Apply it to construct case studies on real-world Android firmware images

Literature

- T. Sutter and B. Tellenbach
  FirmwareDroid: Towards Automated Static Analysis of Pre-Installed Android Apps
  2023 IEEE/ACM 10th International Conference on Mobile Software Engineering and Systems (MOBILESoft)

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
+ DiplomandInnenseminar (CS)
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Basic knowledge of Android OS fundamentals
- Experience in C/C++
- Experience with (embedded) Linux

Advisor Contact

florian.draschbacher@isec.tugraz.at