Announcement: Student job in cooperation with Fraunhofer AISEC, Garching

Automated Reverse Engineering of Mobile Apps

Motivation and Topic

Manual reverse engineering of binaries is a time-consuming process and its results depend on the knowledge and experience of the pentester. Fraunhofer AISEC is conducting research on automating this process as far as possible with a focus on mobile applications.

The subject of this research is thus to reconstruct the semantics of an application or native library in a high-level representation that can then be analyzed for vulnerabilities. Existing tools like McSema, IDA Pro, radare2 and angr already provide good starting points, but they are tailored to manual reverse engineering and do not provide the level of abstraction that is required for automated vulnerability detection.

If you enjoy self-driven research and development in this area, we currently have an opening for a research assistant position.

Your goal would thus be to start out by exploring the hacking and research communities for reverse engineering tools and to evaluate their capabilities for Mach-O (iOS) and ELF (Android) ARM binaries. Then, you will work on implementing a solution for the reconstruction of the program semantics of iOS apps and Android native libraries, whereas you can build upon extensive existing work by Fraunhofer AISEC.

The monthly working time is 40 hours, but can be de-/increased on request.

Requirements

- Experience in programming in Java and/or Python and/or C/C++
- Interest in reverse engineering and wading through some ARM (dis-) assembly
- Experience or at least interest in learning about static code analysis, different intermediate representations, and reverse engineering tools
- Fluency in German or English

Contact

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Julian Schütte
Email: julian.schuette@aisec.fraunhofer.de
Phone: +49 89 322-9986-173