Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Announcement: Student job in cooperation with Fraunhofer AISEC, Garching

Finding Vulnerabilities in Large Code Bases

Motivation and Topic

Static analysis is a set of well-researched techniques to find security vulnerabilities and anti-patterns in source code. However, existing analysis tools either focus on fast and superficial syntax checks, annoying developers with a large amount of false positives and missing more complex vulnerabilities. Other tools focus on a highly precise context-sensitive analysis, but are memory- and computation-intensive and must be specifically tailored to a programming language and oftentimes also the application framework to be analyzed.

A promising trade-off are graph-based approaches which represent a program in form of a property graph and perform static code analysis by querying a graph database.

The subject of this research is to work on the combination of existing parsers for languages like Java, C, C++ or others, extend existing graph representations and support the research staff with the design of new analysis techniques. You will develop a tool from initial prototyping to a near-productive maturity level, conduct experiments, and work with the research team to design novel code analysis approaches.

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

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

Requirements

- Programming experience, preferable in Java and/or C/C++. Python might be a plus.
- Interest in learning about graph databases
- Experience or at least interest in learning about static code analysis
- 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