



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



Announcement: Student job in cooperation with Fraunhofer AISEC, Garching

Detecting Vulnerabilities in Source Code

Motivation and Topic

Static analysis is a well-developed research field that has yielded various techniques to find security vulnerabilities and anti-patterns in source code. However, existing analysis tools either focus on fast and superficial pattern matching, 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 work is to develop a plugin for the Eclipse IDE that helps developers identify and fix even complex programming errors and to support the research staff in further developing the existing analysis framework for Java, C, and C++. You will develop an initial prototype 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 look forward to your application for this research assistant position.

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

Requirements

- Programming experience, preferably in Java
- Experience with Eclipse or even Eclipse plugin development is a plus, but not required
- 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