Chair for IT Security
Prof. Dr. Claudia Eckert

Announcement: Student Assistant (m/f/) at Fraunhofer AISEC*

Extension of Code Property Graph to find vulnerabilities and critical code regions

Motivation and Task Description

The Code Property Graph (CPG)[1] is an open source tooling, developed at AISEC, that facilitates data flow analysis on a language independent graph representation of source code. We want to extend the CPG to help finding vulnerabilities in C++ code. For this, preparational work was already done, to use a domain specific language to query the CPG interactively. First queries exist, which have to be extended. It is possible, but not necessary to touch the underlaying data flow analysis algorithms.

Requirements

- Programming skills, preferably in Kotlin
- Ability to work self-directed and systematically
- Knowledge of (C++) vulnerabilities
- Background knowledge of code representations and static code analysis

Contact

Hannah Schmid
Tel.: +49 89 322-9986-130
E-mail: hannah.schmid@aisec.fraunhofer.de

Tobias Specht
Tel.: +49 89 322-9986-187
E-mail: tobias.specht@aisec.fraunhofer.de

Fraunhofer Research Institute for Applied and Integrated Security AISEC
Department Product Protection and Industrial Security
Lichtenbergstraße 11, 85748 Garching near Munich, Germany
https://www.aisec.fraunhofer.de

[1] https://github.com/Fraunhofer-AISEC/cpg