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

Fraunhofer AISEC

Announcement: Student job in cooperation with Fraunhofer AISEC, Garching

Making incomplete code compilable

Motivation and Task Description

In source code audits, often (to the hassle of the auditor) the auditor gets only access to parts of the source code for an application. This is a challenge for static code analysis, as many tools and techniques require a compilable code. In this project you will research different possibilities to transform incomplete C/C++ source code (missing declarations, missing definitions / headers) into compilable code and implement the most promising approach. At the end, the goal is to be able to use clang on the transformed code to generate LLVM IR. The IR can then be used with existing tools to find possible bugs and vulnerabilities in the code.

Requirements

- Basic knowledge about compiler construction
- Programming skills: C/C++ and optional Java/Kotlin
- Knowledge about AST and control flow graph
- Practical experience with software testing, mock/stub generation (optional)
- Practical experience with LLVM/clang (optional)
- Knowledge about Language Server and LSP (optional)

Contact

Hannah Wester
Telefon: +49 89 322-9986-130
E-Mail: hannah.wester@aisec.fraunhofer.de

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

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