Chair of IT Security
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Student Assistant (m/f/)*

Fuzzing of an embedded device actively used in industry

Motivation and Task Description

Nowadays, many security vulnerabilities in software are found either via static application security testing (SAST) or via dynamic methods such as fuzzing. Depending on the target, however, both methods have limitations and require different amount of effort to be set up.

Your task will be to set up the dynamic part: the fuzzer kAFL should be used to test the kernel module of an embedded device actively used in industry that handles network traffic.

This device is running a common Linux kernel with custom extensions written in C/C++. A first setup is already in place and should be extended to improve the fuzzing campaign. The results of the fuzzing campaign have to be analyzed and reported.

Requirements

- Basic programming experience (C/C++)
- Ability to work self-directed and systematically
- Experience and knowledge in fuzzing is an asset
- Experience with Linux is an asset

If you are interested and would like to know more, please refer to the persons mentioned below. Please send your application with current CV and transcript of records to:

Contact

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

Ferdinand Jarisch
Tel.: +49 89 322-9986-166
E-mail: ferdinand.jarisch@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

Publication Date: 17.12.2024