Announcement: HiWi

Analysis of Fuzzing Crashes

Motivation and Task Description
Fuzzing is a method widely used for automated testing of software. Fuzzing frameworks, such as AFL and LLVM libfuzzer, are able to find various bugs by generating more or less random input for the program under test. Bugs are typically detected as crashes of the tested program. However, not all observed crashes are caused by bugs. For example, when fuzzing a library fuzz drivers might initialize functions incorrectly leading to misuses of the library. Moreover, the crash location is often different from the location of the underlying bug.

To tackle these problems and reduce the effort for large bodies of crashes tools for deduplication, reverse execution or automated root cause analysis as well as sanitizers are used.

In this work, an existing body of crashes from library fuzzing campaigns should be analyzed to identify possibly present bugs.

Requirements
- Ability to work independently and accurately
- Good C/C++ programming skills
- Ideally basic knowledge of fuzzing frameworks, e.g. AFL(++)
- Ideally basic knowledge of sanitizers, e.g. ASAN, UBSAN and/or MSAN

Contact

Vincent Ahlrichs
Telefon: +49 89 322-9986-114
E-Mail: vincent.ahlrichs@aisec.fraunhofer.de

Dr. Julian Horsch
Telefon: +49 89 322-9986-118
E-Mail: julian.horsch@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security (AISEC) Secure Operating Systems
Lichtenbergstraße 11, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de