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

Fraunhofer AISEC

Announcement: Student job

Memory Safety Sanitizer for Linux

Motivation

Memory errors, such as buffer overflows or use-after-free errors, are vulnerabilities in unsafe programming languages (e.g. C or C++) which are commonly used as starting point for different kinds of low-level exploits.

To secure systems and programs against those attacks, many different defensive strategies have been proposed. Some of those techniques, such as Data Execution Prevention (DEP), Stack Canaries and Address Space Layout Randomization (ASLR), are widely used in state-of-the-art systems. Compiler-based memory safety mechanisms, often called *sanitizers*, are typically only used in testing scenarios, mainly because of their high performance overhead. LLVM's Address Sanitizer (ASan) is a prominent example.

Task Description

We at Fraunhofer AISEC are currently developing such a memory safety sanitizer for the Linux platform. The sanitizer is built on top of the LLVM compiler framework as a LLVM optimization pass. As such, it operates on the LLVM Intermediate Representation (IR) of a compilation module to carry out its analysis and instrumentation tasks.

For this student job, you will be fully included into the development process. There, you will get in touch with setting up compilation toolchains, implementing IR passes in LLVM (for analysis and instrumentation), setting up sanitizer runtime environments (for the execution of the sanitizer), and running CPU benchmarks (for evaluating the sanitizer).

Requirements

- Familiar with Linux and compiler toolchains.
- High interest in compilers and memory safety.
- Having fun solving compiler/linker errors and 'getting things to run'!

Contact

Philipp Zieris
Telefon: +49 89 322-9986-183
E-Mail: philipp.zieris@aisec.fraunhofer.de

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

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Lichtenbergstr. 11, 85748 Garching (near Munich), Germany
http://www.aisec.fraunhofer.de