Ausschreibung: Studentische Hilfskraft

Development of a Fuzzing Framework for the Linux System Call API

Motivation
Fuzz testing is a technique for finding programming errors in software. Through fuzzing the correct functioning of software under the presence of malformed input is checked. For this, the software is stress-tested with a large number of malformed inputs in an attempt to cause an undefined behaviour of the software. The detection of undefined behaviour is an indicator for a programming error.

Task Description
As part of an ongoing research project, a virtualisation-based fuzz testing framework for the PikeOS system call API has been developed. The framework consists of two components, one for generating test cases (the fuzzing engine) and one for executing the test cases (the injection engine). The fuzzing engine is written in Python, whereas the injection engine is written in C.

As part of the research project, the task of this work is to adapt the framework to support fuzz testing of the Linux system call API. For this, the fuzzing engine and the injection engine have to be adapted. The fuzzing engine must be extended to generate Linux-specific test cases. The injection engine must be re-written from scratch in order to execute test cases on Linux.

Requirements
- Very good programming skills in Python & C
- Knowledge about the Linux system call API
- Experience in software development
- Interest in fuzz testing

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

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Product Protection and Industrial Security
Parkring 4, 85748 Garching (near Munich), Germany
http://www.aisec.fraunhofer.de

Date of publication: 14. Januar 2016