Fuzzing Embedded Devices using Feedback from Side-Channel Analysis (AISEC)

Fuzzing is a powerful and versatile technique to hunt security vulnerabilities. Embedded devices, however, usually lack suitable interfaces to apply established fuzzing-concepts known from software. Tapping side-channel information such as power consumption or electromagnetic radiation, can yield these interfaces and enable conventional grey-box fuzzing of an embedded device.

Task Description

Our current test set-up is capable of extracting code-coverage information during a fuzzing campaign from the power consumption of a STM32F417IGT microcontroller and feeding it back into our tool, which is based on the popular AFL++ fuzzer. Your task will be to measure the performance of this tool on additional microcontrollers and to increase its effectiveness where applicable. In detail, this entails hooking up a microcontroller to the test set-up, train a machine-learning model to the microcontroller-specific behavior, and measure the performance and effectiveness while fuzzing proof-of-concept and real-world software running on the microcontroller. As optional task, you can work towards tapping electromagnetic radiation as second side-channel next to power consumption.

Prerequisites

- High motivation and ability to work independently
- Good coding skills in python and general understanding of software architecture
- Interest in offensive security and bug-hunting

Contact

Please send your application with current CV and transcript of records to:
Ferdinand Jarisch
Fraunhofer Institute for Applied and Integrated Security (AISEC)
Product Protection and Industrial Security
Lichtenbergstr. 11, 85748 Garching near Munich
Mail: ferdinand.jarisch@aisec.fraunhofer.de
Phone: +49 89 322 9986-166
Publication Date: 21.11.2023

Advisors

Georg Sigl
Ferdinand Jarisch (Fraunhofer AISEC)