Ausschreibung: HiWi, Forchungspraxis, IDP, Master thesis

Fuzzing Framework for Configuration Interfaces

Motivation and Task Description

Embedded systems typically include different interfaces for debug and configuration of a device. One such widely deployed configuration and debug port is the JTAG interface. In spite of being a standardised interface, JTAG can be extended to include hidden vendor-specific functionality. These extensions are typically included to provide manufacturers better debugging capabilities but they could also be exploited and pose a threat to the overall system security.

Your task would be to integrate common software fuzzing frameworks like American Fuzzing Lop [1] or BooFuzz [2] for the JTAG interface to find and analyse the scope of such functionalities on the overall system security.

1. American Fuzzing Lop
   http://lcamtuf.coredump.cx/afl/

2. BooFuzz
   https://boofuzz.readthedocs.io/

Requirements

- Good programming skills
- Basic knowledge in security concepts
- Basic knowledge on using lab equipment
- Creativity and independent working style

Contact

Nisha Jacob
Telefon: +49 89 322-9986-116
E-Mail: nisha.jacob@aisec.fraunhofer.de

Dieter Schuster
Telefon: +49 89 322-9986-134
E-Mail: dieter.schuster@aisec.fraunhofer.de

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

Date of publication: 9. Juli 2018