Ausschreibung: HiWi, Forchungspraxis, IDP, Master thesis

Development of a Fuzzing Framework

Motivation and Task Description
Embedded systems typically include different interfaces for debug and configuration of a device. One such widely deployed configuration and debug interface is the JTAG. In-spite of being a standardised interface, JTAG can be extended to provide vendor-specific functionality. These extensions may also include functionalities to give manufacturers better debugging capabilities which could be exploited and pose threats to the overall system security.

Your task would be to develop a python-based fuzzing framework for the JTAG interface to find and analyse the scope of such functionalities on the system security.

Requirements
- Python, C programming
- Basic knowledge on using lab equipment
- Basic knowledge in security concepts
- VHDL programming is advantageous
- Create and independent working style

Contact
Nisha Jacob
Telefon: +49 89 322-9986-116
E-Mail: nisha.jacob@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: 19. Januar 2018