Assistant (Student)

Development of Fault-Attack Research Tooling
AISEC

The Hardware Security Group (HWS) at Fraunhofer AISEC does active research on Fault-Attack techniques, including Voltage and Clock Glitching or EM and Laser Fault Injections. With these techniques adversaries disturb systems through a physical channel to trigger specific faults in their operation. The faults can be used to actively compromise a system’s security: E.g., one possible exploit is forcing a system to skip firmware integrity checks during a secure boot. But also, actively introducing faults into cryptographic computations can be exploited to obtain information about a used cryptographic secret key.

At HWS we conduct Fault-Injections on real targets of various architectures, like ARM Cortex microcontrollers, FPGAs and SoCs as part of our research. We are looking for a motivated student research assistant (HIWI) to help us improve and extend existing research tooling. The position offers the opportunity to get first experience with Fault-Attacks and embedded security. Possible topics are:

* SoC and microcontroller firmware development (e.g., operating cryptographic hardware accelerators)
* FPGA hardware development in VHDL (e.g., Clock-Glitch-Generator)
* Fault-Attack framework development in Python 3 (e.g., orchestrating setup instrumentation)

Prerequisites

Prerequisites
* Interest in learning about Fault-Attacks
* Interest in hands-on development of attack tooling
* Advanced skill in either:
  o Microcontroller Programming in C
  o Python 3
  o VHDL
* Experience in using Git
* Structured way of working
* Fluency in German or English

The position requires working on site. It is limited to 3 months, with the possibility of extension.

Contact

Kilian Zinnecker
Telephone: +49 89 3229986 1031
E-Mail: kilian.zinnecker@aisec.fraunhofer.de
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Hardware Security Department
Lichtenbergstraße 11, 85748 Garching bei München, Germany https://www.aisec.fraunhofer.de

Advisors

Georg Sigl
Kilian Zinnecker (Fraunhofer AISEC)