Cybersecurity Research at Fraunhofer AISEC

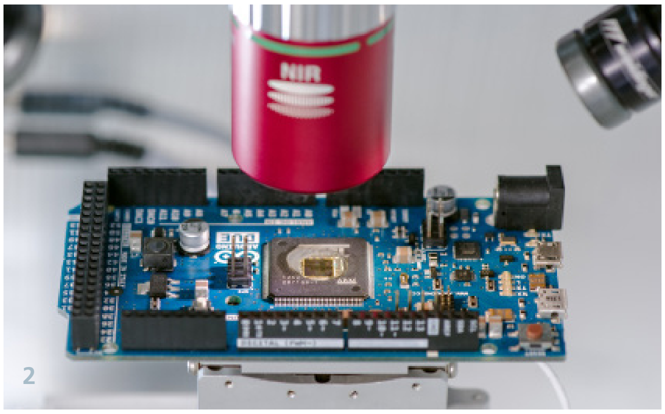
Hardware Security Lab

Information security is crucial for dedicated security devices (e.g. smartcards) as well as all IoT devices in a wide range of applications including the automotive industry, aviation, digital medicine as well as industrial and home automation. However, most of those devices are physically accessible for adversaries, meaning powerful hardware-based attacks such as side-channel attacks pose a significant security threat to all these devices.

Side-Channel Attacks

Side-channel attacks against cryptographic implementations exploit measurements of the power consumption or the electromagnetic emanation of devices to extract secret keys using statistical processing of measurements. Software and hardware implementations are both vulnerable to side-channel attacks if no countermeasures are implemented. On unprotected microcontrollers or FPGA devices, secret keys can be extracted with low effort. In security assessments, Fraunhofer AISEC researchers successfully attack even highly protected implementations.

High-resolution electromagnetic attacks utilize measurement probes with coil diameters as small as 100 µm to isolate the signal of small relevant parts of a chip. For a successful evaluation and attack, the measurement setup automation, signal processing and statistical processing is key. Evaluation of protected devices requires extensive measurement post-processing for synchronization and feature selection. Fraunhofer AISEC's hardware security lab provides all required equipment for chip preparation and high-end measurements as well as extensive tooling developed in-house to support the evaluation of powerful side-channel attacks.

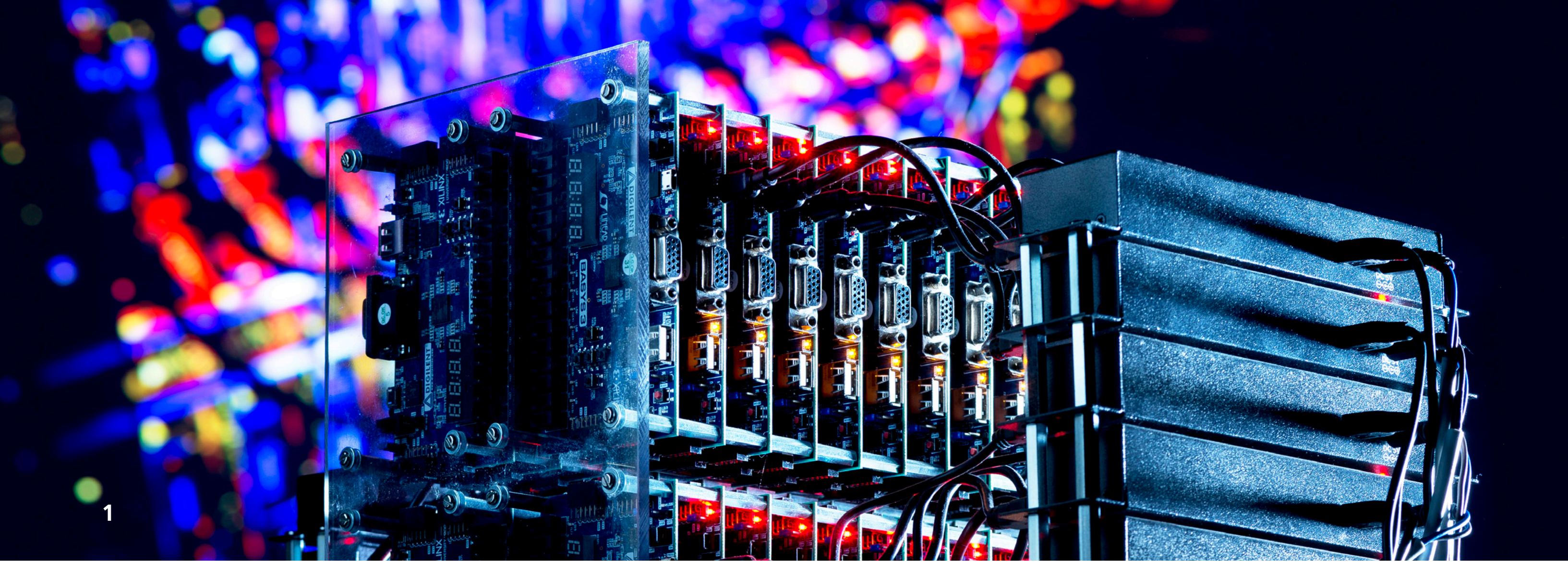


1 *Electromagnetic side-channel analysis*
2 *High-precision laser fault injection*

Contact

Dr. Matthias Hiller
Head of Hardware Security
Phone +49 89 3229986-162
matthias.hiller@aisec.fraunhofer.de

Fraunhofer AISEC
Lichtenbergstr. 11
85748 Garching near Munich
www.aisec.fraunhofer.de



Fault Injection Attacks

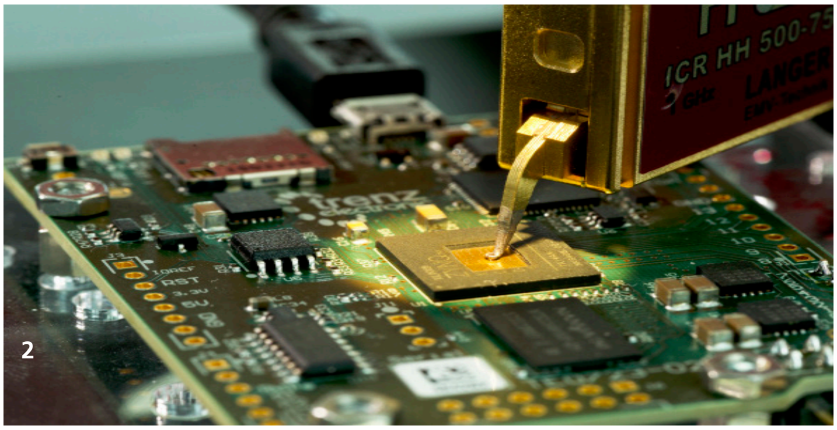
Fault injection attacks lead to computation errors within devices which are exploited to extract secret information and keys or to influence the execution flow for adversarial purposes. The most sophisticated and precise fault attacks are carried out by injecting current in electronic circuits using highly focused laser beams. These temporally and spatially precise lasers inject faulty values into one or more internal signals. At the Fraunhofer AISEC lab, we use high-end dual laser stations with two independent laser beams to induce faults even with dedicated countermeasures in place. Precise single bit manipulations have been demonstrated on integrated circuits manufactured in 45 nm technology nodes.

Less invasive attacks are so called glitching attacks. The supply voltage or clock frequency is changed for fractions of a clock cycle or electromagnetic pulses are introduced to achieve faulty computations. This may change the execution flow of the device to e.g. skip security queries. The full range of glitching attacks from clock to electromagnetic fault injection is readily available at Fraunhofer AISEC's hardware security lab.

Hardware Pentesting

Hardware attacks not only target cryptographic implementations, but there are many more attack paths to consider which need to be evaluated and eventually prevented. Exploitable design flaws may be found in different parts of a system and may even occur due to the composition of building blocks. Simple examples for hardware attack vectors are sniffing of bus communications, exploiting insecure debug interfaces and reading out memories. Many IoT devices rely on security features such as read-out protections within their chips, e.g. microcontrollers. Research at Fraunhofer AISEC has shown critical vulnerabilities. Hence, we emphasize the need for thorough hardware security evaluations.

1 *FPGA analysis cluster* 2 *Near-field electromagnetic probe*



Services

Side-channel evaluation

- Power analysis of IoT devices
- High-precision and standard EM measurements for side-channel analysis
- Multi-probe EM measurement setups
- Dedicated setups for the evaluation of smartcards, including contactless interface card measurements using EM
- Capable backend for trace storage
- Large library of trace alignment filters
- Sophisticated trace pre-processing, e.g. PCA, LDA
- SPA, DPA, correlation enhanced collision attacks, MIA, template attacks and linear regression based attacks
- Development and improvement of countermeasures

Hardware pentesting

- Security evaluation of embedded systems against a broad range of hardware-based attack vectors
- Evaluation of firmware and IP protection features in microcontrollers
- Source code audit

Fault injection attacks

- Multiple laser stations for front- and backside fault injection
- High-precision dual laser system for independent injection of two faults
- Regular and fuzzy clock glitching
- PLL clock glitching
- Voltage glitching setup for over-/undervoltage glitches
- Arbitrary waveform glitches
- Tooling for fault attack evaluation, e.g. DFA, SIFA
- Electromagnetic fault injection