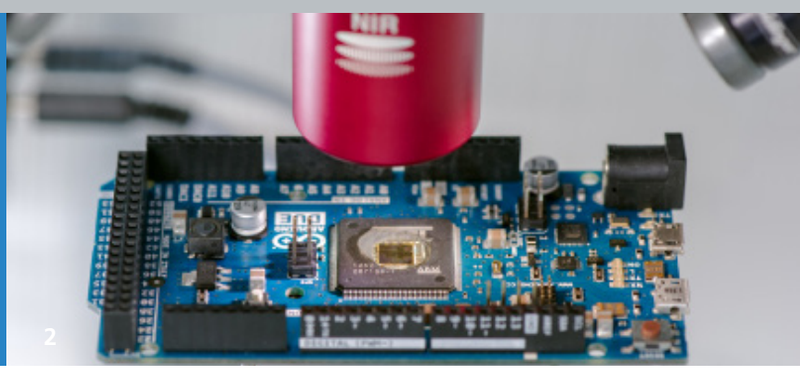
Fraunhofer
AISEC

FRAUNHOFER INSTITUTE FOR APPLIED AND INTEGRATED SECURITY AISEC


1


2

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

HARDWARE SECURITY LAB

Information security is crucial for dedicated security devices (i.e. smartcards) as well as all IoT devices in a wide range of applications including the automotive domain, aviation, digital medicine, defense, home automation and more. Interestingly, most of those devices are physically accessible for adversaries. This means that powerful hardware-based attacks such as side channel attacks pose a significant threat to all those devices.

Fraunhofer AISEC has more than 10 years of experience in analyzing the hardware security of embedded systems and smartcards and runs an extensive hardware security lab on 120 square meters with top-level equipment. Fraunhofer AISEC routinely evaluates and investigates known and new attacks and respective countermeasures. Moreover, as part of the Cybersecurity Training Lab, training courses and further education on the subject of hardware security are offered.

SIDE CHANNEL ATTACKS

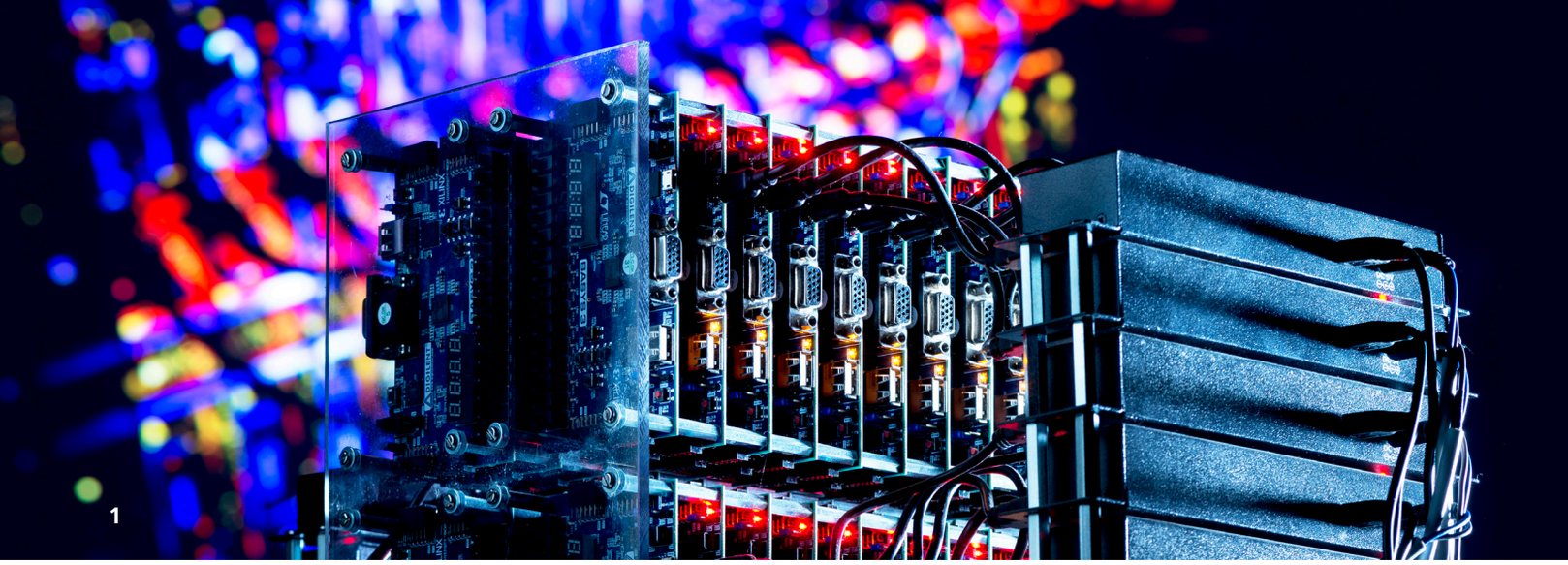
Side channel attacks against cryptographic implementations exploit measurements of the power consumption or the electromagnetic emanation of devices to extract secret keys using statistical processing of measurements. Software and hardware implementations are both vulnerable to side channel attacks if no countermeasures are taken. On unprotected microcontrollers or FPGA devices, secret keys can be extracted with low effort. Using high-end equipment available in the AISEC lab, even highly protected implementations can be attacked successfully, which needs to be evaluated for security assessments.
High-resolution EM attacks utilize measure-ment 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 respectively, 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 includes all required equipment for chip preparation and high-end measurements as well as extensive tooling developed at AISEC to support the evaluation of powerful side channel attacks.

Fraunhofer Institute for Applied and Integrated Security AISEC

Lichtenbergstraße 11
85748 Garching near Munich
Germany

Contact
Dr.-Ing. Johann Heyszl
Telefon +49 89 322 99 86-172
johann.heyszl@aisec.fraunhofer.de

www.aisec.fraunhofer.de



FAULT INJECTION ATTACKS

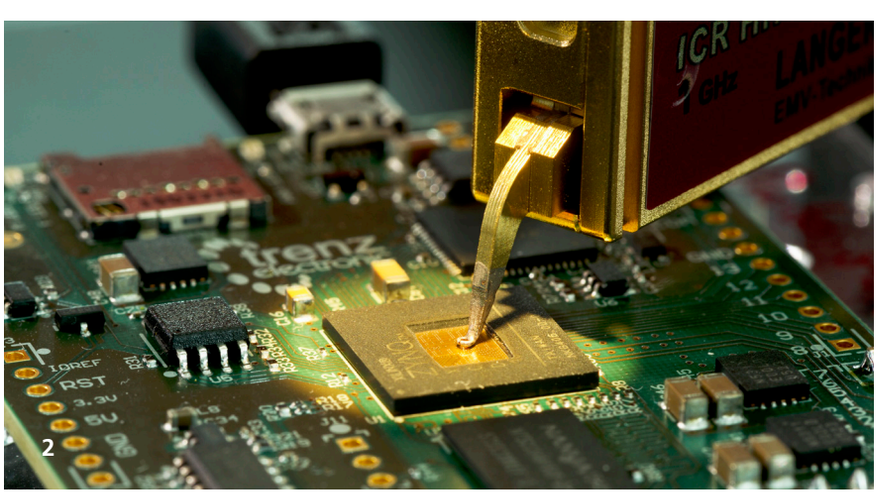
Fault injection attacks lead to computation errors within devices which are exploited to extract secret information, keys or to influence the execution flow for adversarial purposes. The most sophisticated and precise fault attacks are carried out by injecting current in electronic circuits using highly focused laser beams. These temporally and spatially precise lasers inject faulty values into one or more internal signals. At the AISEC lab, we use a high-end dual laser station with two independent laser beams to induce faults even in the presence of dedicated countermeasures. Precise single bit manipulations have been shown down to 45 nm chips. Less invasive attacks are so called glitching attacks. The supply voltage or clock frequency is changed for fractions of a clock cycle to achieve faulty computations. This may change values or the execution flow of the device to e.g. skip security queries. The full range of glitching attacks is readily available in AISEC's hardware security lab.

HARDWARE PENTESTING

Hardware attacks do not only target cryptographic implementations. 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 even be 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 in many products from different manufacturers in this regard. 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 preprocessing, e.g. PCA, LDA
- High standard attacks, including 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 broad range of hardware-based attack vectors
- Evaluation of firmware and IP protection features in microcontrollers

Fault injection attacks

- Multiple laser stations for front- and backside fault injection
- High-precision dual laser system with separate scanners 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