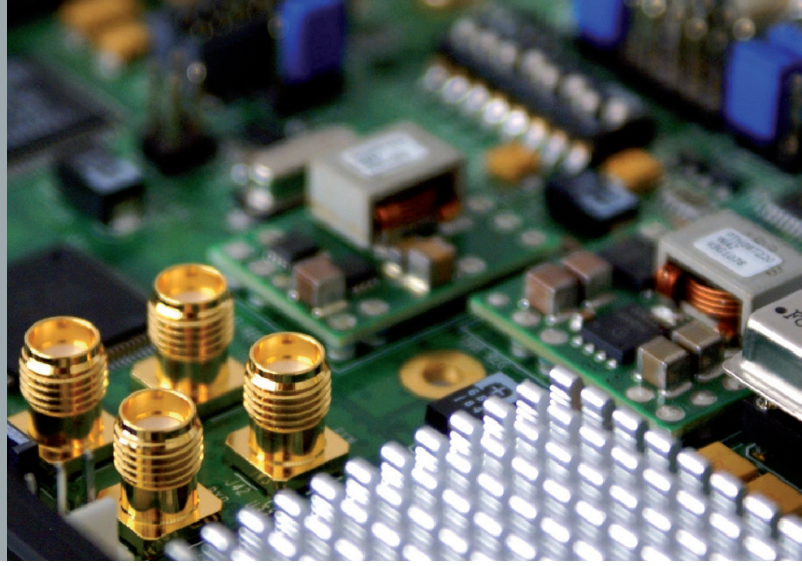
Fraunhofer
AISEC

FRAUNHOFER RESEARCH INSTITUTION FOR
APPLIED AND INTEGRATED SECURITY AISEC



Fraunhofer Research Institution for
Applied and Integrated Security AISEC

Contact:
Dr. Johann Heyszl
Parkring 4
85748 Garching (near Munich)
Germany

Phone: +49 89 322-9986-172
Fax: +49 89 322-9986-299
johann.heyszl@aisec.fraunhofer.de
www.aisec.fraunhofer.de

HARDWARE TEST LAB

ATTACK IS THE BEST DEFENSE

In today's information era, smartcards and hardware-security modules are used in a variety of applications, e.g., RFID systems, industrial embedded systems or even in off-the-shelf PCs. New methods to attack these modules, namely, side channel attacks or fault attacks, pose a threat to modern security devices. Fraunhofer AISEC applies and enhances these attacks in order to develop highly sophisticated countermeasures.

RFID Systems

Due to its ease of use and its batteryless energy supply, wireless radio frequency identification (RFID) technology is spreading quickly into new application fields, e. g., access control systems. For example: searching for access cards gets unnecessary because RFID-based access systems read ID cards through bags and clothes. RFID tags also have economic advantages because of low-cost production. Furthermore, a system operator can remove lost cards from the system and change access rights whenever needed.

However, RFID technology introduces formerly unknown threats like eavesdropping from a distance of up to a few meters. This can be exploited, e.g., to track a person by his/her unique identification number. In the last years, several cryptographic algorithms used in RFID systems have been proven insecure or implemented insecurely. This lack of security enables to clone RFID tags and to impersonate somebody else. To protect RFID systems and applications, Fraunhofer AISEC analyzes protocols as well as RFID implementations and develops new protocols and security concepts.

Side Channel Attacks

Side channel attacks differ fundamentally from conventional attack methods. In the latter case, attackers try to solve a complex mathematical problem or try to search the entire key space to break cryptographic systems. By contrast, side channel attacks operate on information like the runtime, the power consumption or the electro-magentic emission. An attacker can use this information to gain knowledge about the secret key stored inside the device.

Passive Attacks

Passive attacks allow drawing conclusions about sensitive data within security modules by analyzing the information leaked by the execution of an algorithm implemented inside the security module. The most basic attack is called simple power analysis (SPA). The attacker monitors the chip's power consumption and maps each peak oft the power trace to a specific step in the algorithm. Other attacks are possible by looking at the runtime of a chip operation (timing attacks). In some cases, for example, the computation of a correct PIN code digit takes longer than the computation of a wrong one. An experienced attacker could therefore look at the runtime and could retrieve the correct PIN digit by digit.

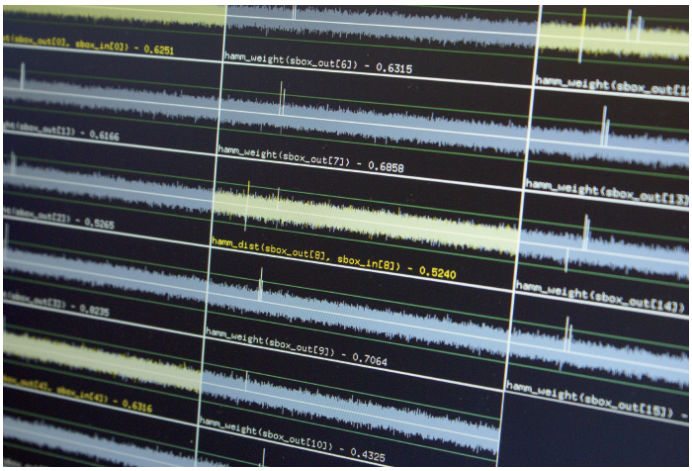
Electro-magnetic emission analysis setup

Microcontroller under test in laser station

In a differential power analysis (DPA), the attacker uses statistics to analyze a system. For example, one can determine the secret key of a system by looking at a few hundred power traces. If the attacker collects several reference traces, he can compare these references with a recent power trace and thereby break the system under test within a few minutes. All the above mentioned methods are not restricted to power consumption traces, but can also be performed by analyzing electro-magnetic emission.

Active Attacks

While passive attacks do not influence a system, active attacks are based on precise fault injections in program flows or integrated circuits. The way a system reacts on injected faults, e.g., delivering wrong results or issuing error signals, provides information about the implemented secrets, e.g., the secret key of a device. Fault attacks are carried out by injecting laser beams on electronic circuits. These temporal and spacial precise laser beams change the electrical potential and can influence the current value of one or more signals. If an attacker varies the supply voltage and clock frequency for fractions of a clock cycle, he can change the program flow significantly in order to skip security queries (glitching attack). For example, it is possible to circumvent the password control by jumping over a verify-password-operation and continuing with the password-correct-path in the program flow.



Differential power analysis correlation results

Safety and Reliability Tests

Weaknesses in security can have a severe impact on safety and vice versa. With its laser equipment, Fraunhofer AISEC can penetrate application-specific integrated circuits (ASICs) and field prgrammable gate arrays (FPGAs) in a defined way to observe the systems reactions on occurring faults. Based on a defined error model, safety critical devices can be evaluated regarding their behaviour in artificially created rough environments. Additionally, methods like micro probing/forcing allow to monitor and alter signals within integrated circuits in order to analyze and judge devices' reliability characteristics.

Evaluation Services

With a modern laboratory and a broad basis of know-how, Fraunhofer AISEC offers a variety of evaluation services for security/safety critical applications and devices. With the following services the Institute supports hardware manufacturers and embedded system developers of several platforms, e.g., microcontrollers, smartcards and many more:

- Embedded system tests (black/grey/white box) with focus on specific protocols, algorithms or interfaces
- Passive side channel attacks (SPA, DPA, template attacks, etc.)
- Active side channel attacks (fault attacks, glitching attacks, etc.)
- Development/improvement of countermeasures
- Tamper resistant design strategies
- Evaluation of safety and reliability properties (micro probing/forcing, etc.)