Attacking Software-based Countermeasures (AISEC)

Fault attacks pose a serious threat to embedded systems and their applications. Due to the powerful nature of fault attacks, it may allow to fully compromise a target device. Most Common-Off-The-Shelf Hardware do not contain any viable hardware features against fault attacks. Thus, a viable approach, for such hardware, is to apply Software-based Countermeasures. In the simplest approach this could be duplication of calculation and checks. Thus, requiring the attacker to inject multiple faults to compromise the device. More complex Software-based countermeasures split the existing registers into primary and shadow registers to effectively detect more possible faults. Despite, the countermeasures being more complex, they all assume certain capabilities of an attacker.

In this thesis, the goal is to stress these arbitrary limits by working in our hardware lab with the existing setup for Electro-Magnetic Fault Injection (EMFI). Thus, this work consists of working hands-on in the laboratory, writing test firmware and test routines, analyzing observed faults and deriving fault models.

The work is designed for a master thesis, but can also be carried out in a limited form within an research or engineering internship.

Prerequisites

- Experience with Python
- Experience with C and Assembly
- Experience working with embedded devices, oscilloscopes or debuggers is beneficial
- Experience in Fault Injection is beneficial, but optional

Contact

Please send an email with a short CV, your last grading sheet and provide 3-5 dates, which fit to your schedule, for a meeting.

Alexander Wagner, alexander.wagner@aisec.fraunhofer.de
Michael Gruber, m.gruber@tum.de

Advisors

Georg Sigl
Alexander Wagner (Fraunhofer AISEC)