Simulating and Modelling the Effects of Thermal Laser Stimulation on Integrated Circuits

Context and Goal of the Project

Secure systems and circuits and connected objects used in the industrial IoT are prone to attacks that aim at taking advantage of hardware vulnerabilities. Particularly menacing are active hardware attacks, which consist in injecting faults at run time for the purpose of recovering secret information or gaining unauthorized access. In the early 2000s, S. Skorobogatov [1] reported the use of laser illumination in the near-infrared range to induce faults into integrated circuits. Since then, Laser Fault Injection (LFI) has been intensively studied [2, 3]. Simulation and modelling of LFI induced photocurrent has also been proposed in the literature [4, 5].

Thermal Laser Stimulation (TLS) is a failure analysis technique, which can also be deployed by an adversary to localize and extract sensitive information of a secure device. To this date, a few proof-of-concept experiments based on TLS or similar approaches have been reported in the literature [6, 7]. And to the best of our knowledge, no TLS simulator has been developed and published yet. Similarly, the corresponding countermeasures able to detect and react to a TLS attack are not well studied.

Within this context, the goal of this work is to propose an electrical and gate level simulation methodology based on standard CAD tools to forecast the effects of TLS in large scale circuits. This will allow designers to investigate and assess the capability of attacks carried out against security primitives before the circuit's fabrication. This work primarily aims at developing electrical models and countermeasures against TLS attacks as they start to emerge.

The main goal of this project is to guarantee the integrity of hardware security primitives against TLS attacks. It will be achieved in two main steps:
1. assessing and modelling TLS attacks on an experimental basis;
2. developing a methodology to simulate the effects of TLS on ICs based on CAD tools;
3. developing and validating countermeasures against this type of attacks.

State-of-the-art

TLS attacks started to emerge in recent years as a new class of *active* attacks. Optical attack using TLS was introduced and later studied by [7, 8, 9]. These attacks demonstrated the potential of TLS to localize the key storage of chips (eg. SRAM and Flash memory) and extract its contents. Pioneer work by Skorobogatov [10] demonstrated that UV light can modify the content of EPROM. Emerging non-volatile memories are also susceptible to this type of attack and can be altered by a magnetic field [11]. TLS setups are gaining popularity in recent years. They are more accessible (in terms of complexity and equipment cost) than techniques such as Focused Ion Beam that allow to modify the wires and connections of a circuit. The capability of TLS to address the security issues of a circuit remain interesting. Even for advanced technology nodes, the ability to target single logic elements, allowing for example, the content of memory to be altered, as shown in [8] where the look-up tables of an FPGA are tampered with.

Methodology

The methodology described hereafter aims at observing and modelling the effects of TLS attacks against the building blocks of circuits also used to design hardware security blocks. This work will mainly target three kinds of primitives: standard cells (used to design complex digital circuits), Flash memory of microcontrollers (used to store data) and security monitoring systems (eg. current, voltage and frequency sensors). Experimental TLS attacks will be carried out on existing and already available circuits.

The main steps of the methodology are:

1.*Laser campaign and measurements, to model the effect of TLS on CMOS devices*: TLS-based experiments on devices will be performed with the TLS sources available at Mines Saint-Etienne (MSE). First, the characterization of TLS effects on CMOS devices will be assessed on circuits already available: a MSE designed CMOS 65nm circuit (RadHard) and commercial microcontrollers are available with a large range of structures. For the circuit designed at MSE, SRAM cells, laser sensors, delay elements and digital logic are available. RadHard will be used to fine-tune the model of TLS effect on CMOS devices. For the microcontrollers, it is available four different references from three different manufacturers, the goal here is to investigate the effects of TLS-based attack on commercial SRAMs and Flash memories. These experiments will be conducted from the beginning of the project.

2. Simulation methodology: experimental results obtained from the previous step will be used to propose a methodology to simulate the effects of TLS on complex ICs using standard CAD tools. To validate the electrical model, we will correlate experimental and simulation results. These results will also be useful to later propose effective countermeasures and detectors of LTS-based attacks.

3. TLS-based a*ttacks*: Security exploits will be developed to demonstrate the potential of LTS-based attacks against hardware primitives. Flash memories will be the first target. Previous works demonstrate attacks on a Flash memory by means of Laser Fault Injection (LFI). A recent study [12] demonstrated on 32-bit MCUs embedding a NOR Flash that LFI induces non-permanent faults when instructions and data are read from the Flash. Similarly, [13, 14] report faults during Flash programming operations. This model induces permanent faults directly on the data stored in the Flash, providing new attack scenarios. A research hypothesis of this project is to demonstrate that we can induce faults in the flash memory by means of TLS during the reading and programming operations. Security monitoring sensors [15] will be the second target of attack exploitation. These sensors monitor, at runtime, parameters of the circuits in order to detect abnormal effects due to fault injection attacks. TLS-based attacks may succeed in evading detection by biasing these sensors to shift the threshold of detection and even disable them.

4. *Countermeasures against TLS-based attacks*: The final goal will be to propose countermeasures against TLS-based attacks. The results obtained in the modelling and attacks phase will help to set-up such countermeasures. A possible approach will consist in developing on-line test dedicated to security primitives in order to detect any out of specification effects, ie. abnormal current, voltage and frequency, which may be caused by a TLS attack.

Attack target #1:

ANR LIESSE BBICS sensor [15]: the sensor developed during this project (including TIMA, LCIS and MSE) was to detect laser attacks. A BBICS monitors CMOS bulk currents in order to detect any anomalous transient current due to the effect of laser attacks. This protection targets a particular model threat which considers the device is being attacked on-line. Within this demonstrator we will show that is possible to attack BBICS in order to either bias or disable its detection capability during a combined attack by using LFI and TLS attack. Another conjecture is that if the protected circuit is attacked with TLS, BBICS will not be able to detect the attack as TLS does not induce current in the circuit. Elementary structures like MOS gates present in this target will be used to improve the simulation of electrical and gate models, and to validate simulation results by means of comparison with experimental ones.

Attack target #2:

Commercial secure and non-secure microcontrollers: MCUs are ubiquitous in fields such as Internet of Things (IoT) and the automotive industry. A malicious attacker may try to discover vulnerabilities in the target embedded by an application or device dealing with sensitive data. Security analysts and researchers try to find weaknesses in devices with the goal of patching them. With a specific MCU in mind, the attacker sets out to acquire clones of it. Having copies of the MCU target is desirable for reverse-engineering it to find vulnerabilities without damaging the device to be attacked. Some of the preparation steps (e.g depackaging an IC of unknown layout) can damage and even destroy the circuit. Replacing a test MCU is cheaper and easier than replacing the whole product embedding it, which may be expensive or difficult to find. This demonstrator will show some of the vulnerabilities a commercial MCU may expose in face of TLS-based attacks.

Candidate Profile

Master's degree on Microelectronics / Computer Engineering
Object Oriented Programming (Python or similar)
Lab. instrumentation skills (oscilloscope, voltage sources etc.)
Notion of hardware security is a plus (fault-injection, side-channel)
English or French (written and spoken)

Start Date

The desired start date for the thesis is September 2024.
Selection of candidates scheduled for May 2024.

Salary

The monthly net salary is fixed at approximately 2000 euros.

Contacts

Thesis director: Jean-Baptiste Rigaud (rigaud@emse.fr)
Thesis advisor: Raphael Viera (raphael.viera@emse.fr)

References related to the project

[1] Optical Fault Induction Attacks. Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), 2002.
[2] J.-M. Dutertre, D. Hély, G. Di Natale, et al., Laser fault injection at the CMOS 28 nm technology node: an analysis of the fault model, FDTC 2018.
[3] S. Tajik, et al., Laser Fault Attack on Physically Unclonable Functions, FDTC 2015.
[4] R. Viera, J.-M Dutertre, et. al., Simulation and Experimental Demonstration of the Importance of IR-Drops During Laser Fault Injection, IEEE TCAD 2020.
[5] William Souza Da Cruz, Raphael Viera et. al., Experimentally Tuned Compact Electrical Model for Laser Fault Injection Simulation, IOLTS 2022.
[6] David Samyde, Sergei Skorobogatov, et. al. On a new way to read data from memory. In Security in Storage Workshop, 2002. Proceedings. First International IEEE, 2002.
[7] S. Skorobogatov, Local heating attacks on flash memory devices, HOST 2009.
[8] Lohrke, H., Tajik, S., et. al. (2018). Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs. CHESS 2018.
[9] Thilo Krachenfels and Heiko Lohrke et. al. Evaluation of Low-Cost Thermal Laser Stimulation for Data Extraction and Key Readout, Journal of Hardware and Systems Security, 2019.
[10] S. Skorobogatov, Data Remanence in Flash Memory Devices, CHES 2005.

[11] A. Krakovinsky, et al., Thermal laser attack and high temperature heating on hfo2-based oxram cells, IOLTS 2017.
[12] Colombier B., et. al. Laser-induced Single-bitFaults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller. HOST 2019.
[13] Viera R., et. al. Injecting Permanent Faults into the Flash Memory of a Microcontroller with Laser Illumination During Read Operations. ASHES 2022.
[14] Viera, Raphael et. al., Tampering with the flash memory of microcontrollers: permanent fault injection via laser illumination during read operations, Journal of Cryptographic Engineering
[15] J.-M. Dutertre, et. al., Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS, Microelectronics Reliability (Elsevier), 2014.