Summary of ANR[1] POP Project

Introduction

The POP[2] project studies power-off laser attacks on unpowered security hardware like PUFs[3]. It aims to :

1. Test attack feasibility
2. Model the effects
3. Design countermeasures.

The focus of the project relies on PUF cloning and sensor deactivation. Steps include chip design, laser experiments, threat analysis, and developing defenses. The end goal of the project is to secure hardware against power-off attacks.

Objectives

The most threatening attacks are active hardware attacks. Among the countermeasures developed against them, stand hardware security primitives[4]. Since the state of the art is based almost solely on power-on attacks, be it attacks or countermeasures, the goal of this project is to examine the feasibility of attacks against security primitives using laser illumination carried out when a circuit is powered off, hence its name: Power-Off laser attacks on security Primitives (POP). In this project, we focus specifically on two security primitives :

1. Core parts of PUFs, as power-off laser attacks could induce a bias in responses, that could lead to clone-forging of the attacked PUFs
2. Embedded sensors used to detect laser fault injection, as power-off laser attacks could be used to deactivate or permanently inject bias in them in an undetectable way.

Other security primitives (such as TRNGs[5], non-volatile memories storing configuration settings, or cryptographic coprocessors) will be considered should specific vulnerabilities undetectable with common embedded tests emerge during the project.

The use of the laser will be tuned from local annealing, modifying the electrical parameters of transistors, to targeted destructives effects (melting metal interconnects, destroying some transistors). These attacks won't be detected by usual active power-on countermeasures.

Position of the project in the state of the art

The project positions itself at the forefront of power-off laser attacks, a novel class of active attacks targeting hardware security primitives like PUFs and sensors. While prior work explored UV light, heating, magnetic fields, X-rays, and FIBs[6] for tampering, these methods are either limited or require heavy equipment. Laser fault injection, however, is more accessible and precise, capable of altering memory and logic elements even in advanced nodes. Recent studies show lasers can induce thermal effects to permanently degrade or modify circuits while powered off, making them ideal for power-off attacks.

The project innovates by:

1. Exploring power-off laser attacks on PUFs, potentially breaking their unclonability by biasing outputs or reverse-engineering them.
2. Investigating attacks on online attack sensors, enabling their offline deactivation.
3. Developing countermeasures to mitigate these threats.

This work is novel as it addresses underexplored vulnerabilities, particularly in PUFs, and proposes scalable, hard-to-detect attacks that could be exploited by rogue manufacturers. The project aims to significantly advance the state of the art in hardware security by identifying new threats and designing robust defenses.

Methodology and risk management

The POP project aims to study power-off laser attacks on hardware security primitives like PUFs and sensors, and develop countermeasures. The methodology involves:

1. Designing a test chip with common security primitive blocks for laser experiments.
2. Conducting laser tests on existing and custom chips to model the effects of power-off laser attacks.
3. Developing attacks to demonstrate threats, such as biasing PUFs to clone them or disabling attack sensors.
4. Designing countermeasures, including online monitoring for PUFs and sensors, and offline sensors to detect power-off laser attacks.
5. Creating demonstrators using two use cases: a PUF-based licensing scheme and a laser attack sensor.

The project is organized into five work packages:

1. WP1: ASIC design and manufacturing.
2. WP2: Laser experiments and modelling.
3. WP3: Countermeasures design.
4. WP4: High-level attacks and demonstrators.
5. WP5: Project management and dissemination.

LCIS plays a key role in WP3, leading the design of online and offline countermeasures against power-off laser attacks. They also contribute to WP2 (experiments and modelling) and WP4 (attacks and demonstrators), while supporting overall project management and dissemination in WP5.

Risks include potential ASIC malfunctions or limited laser effects, mitigated by using existing hardware and FPGA targets. The project aims to advance hardware security by addressing underexplored power-off laser threats.

Organisation and implementation of the project

The POP project will be conducted by 4 research laboratories :

1. TIMA (PUF primitives design and evaluation)
2. LCIS (countermeasures design, and providing of test vehicles for attack experiments)
3. Lab. H. Curien (PUF and TRNG characterisation, modelling and security analysis)
4. MSE (laser security characterization, assessing new threats against security primitives, and devising original countermeasures)

All laboratories will also design ASIC.

Since the project is highly exploratory, no industrial partner's are included in the project. Indeed,the perspective of power-off attacks means a huge change in perspective, but the potential of those attacks could be devastating if applied.

Impact and benefits of the project

Short, medium or long term impacts

Here are the impacts expected of the POP project :

1. Short-term: Contribute to academic hardware security by publishing results from WP2 (laser experiments and modelling), impacting the scientific community.
2. Medium-term: Influence the industrial community, particularly security evaluation labs (e.g., SERMA, CEA LETI, THALES) and certification entities like ANSSI, through an advisory board.
3. Long-term: Establish power-off laser attacks as a significant threat to mobile devices, driving the need for countermeasures (WP3) to protect future electronics. WP4 demonstrators will showcase the attack's effectiveness, convincing designers of its dangers.

Dissemination of the project results

The project aims at producing high-quality scientific articles in the best peer-reviewed conferences or journals of the field.

MSE and the Lab. H. Curien also organize every year two workshops dedicated to hardware security which will be an opportunity to make "work in progress" presentations.

At the end of the project, the results will also be demonstrated during scientific events where the scientific articles are presented, or via the website of the project and dedicated YouTube channel of the laboratories involved.

All of the project participants are involved in the "hardware security group", a joint working group of the two CNRS GDR "Sécurité informatique" and "SoC²". The project results could be disseminated during workshops organized by these two GDR.

Other dissemination actions at the national level are possible to also target a more industrial audience by using for example the regional SCS and the MINALOGIC clusters of excellence which include all the POP project partners. The project outcomes will also be disseminated within the IRT Nanolec and the Grenoble Alpes Cybersecurity institute, projects in which the many project members are involved.

The project partners will do their best to present the project objectives and results in dedicated events in which they have already been involved in previous years like: La nuit européenne des chercheurs, Fête de la Science, Pint of Science Festival, Science & You, etc. But also by promoting their works in mainstream newspapers like Le Monde.

Benefits to education

At Grenoble INP Esisar & Phelma, at Telecom Saint-Etienne engineer school of University Jean Monnet, and at the Ecole des Mines de Saint-Etienne, the hardware security courses will incorporate the work of POP.

Also, POP will be promoted with student-oriented security conferences and international challenges such as CSAW which is organized by Grenoble INP for Europe (website).

Pentesting challenges can be organised to ask students to participate to the definition and evaluation of original countermeasures against power-off threats.

Glossary

1. ANR = National Agency of Research (Agence Nationale de Recherche)
2. POP = Power-Off laser attacks on security Primitives
3. PUF = Physically Unclonable Functions, type of embedded hardware security primitives
4. Security primitives = basis of construction for cryptography algorithms and protocols. These primitives include encryption, decryption, digital signature, and key exchange.
5. TRNG = True Random Number Generators, are devices that generates random numbers from a physical process capable of producing entropy
6. FIB = Focused Ion Beams