# Real versus Simulated Fault Injection

*Internship - Pessac*

## Introduction

eShard is a technology company specializing in the security of mobile or connected objects:electronic chips, mobile applications or any other communicating object for which there is both the storage of personal data and the exchange of information. This applies to all parts of objects: from chips in semiconductors to mobile applications.
Our role is to provide our customers, designers or users of connected objects with the means to control cyber risk and to ensure that the objects integrate the right level of protection: understand the threat, carry out automatic checks, obtain the knowledge of attacks.

To do this, we have assembled a team of specialists, researchers who are experts in cryptography and security of mobile applications, and we offer our customers a range of tools and services: SaaS platform, software, technical training and security testing service.

Recent IC Security firmware embed counter measures against physical attacks such as fault injection. esFirmware (**[JAIF-2021]**) was developed to help the end user to bridge the gap between the faulty outcome of the simulation and the real product detected flaw. It also allows intensive validation without physical device and expensive material.

As part of the development of our activity, we are recruiting an intern to attack a new "system on a chip" (SoC) with Electro-Magnetic Fault Injection and leverage esFirmware to qualify the product security level. This internship is for a period of 6 months remunerated. Desired start date: February 2022.

The position is based in Pessac (Bordeaux).

# Job description

## Responsibilities

Directly attached to the Chief Scientist, you will be in charge of the following missions:

- Attack a SoC based on ARM or RISC-V architecture with Electro-Magnetic Fault Injection attacks:
    - Develop test codes to characterize the SoC sensitivity to fault injection,
    - Attack the secure bootloader.
- Leverage esFirmware to generate simulated fault campaigns with the objective to reproduce and understand the previous results.
- A step further would be to implement and validate counter-measures with the simulation tools, and then check their efficiency with real fault campaigns.

## You are

- You are preparing a master degree and are in your last year of study
- You have developed a particular interest in:
    - Python, C and assembly  programming
    - Hardware architecture
    - fault injection attacks, acquisition systems and instrumentation
- You are curious by nature, responsive and have the spirit of initiative
- You demonstrate autonomy in your assignments
- You demonstrate good interpersonal skills that will allow you to work as a team effectively
- You have a good writing level in English

## Your benefits

- Support from professionals in a cutting-edge and booming business sector
- Dynamic work environment within a young and friendly team
- High performance work equipment
- Flexible working hours
- Space dedicated to talent development
- Mutual health insurance with good medical and dental coverage
- “Tickets restaurant” covered up to 50%
- Annual events, snacks and drinks

**Interested?**

Send your resume and motivation letter to:

**career@eshard.com**

eShard

# Get in touch

✉ contact@eshard.com

🔗 www.eshard.com

## France

Bâtiment GIENAH
11 avenue de Canteranne
33600 PESSAC

7 rue Gaston de Flotte
13012 Marseille

## Singapore

#04-01 Paya Lebar Quarter
1 Paya Lebrar Link
Singapore 408533

## Germany

Lebacher Str. 4
66113 Saarbrücken
Germany