

# “Let the Glitch Strike Again!”

## Internship

Well known to hackers and cyber-criminals, the voltage glitch attack applies a short transient voltage with the intent of disrupting at a key instant the firmware execution, without doing permanent damage to the circuitry. For instance, the attacker can try to perturb the result of a non-legitimate user authentication. Even if documented for long (c.f.: *[Glitch Xbox360]*, *[Starlink Hacked]*), glitches remain a real threat for low-cost devices, especially because glitch can be tuned in many ways (amplitude, shape, direction) and may bypass hardware glitch detectors.

The objective of this internship is to extend eShard's portfolio of real use cases leveraging glitch attacks using eShard in house advanced tools, and investigate today's “garage” material capabilities.

### COMPANY

[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.

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, IC security 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.

As part of the development of our activity, we are recruiting an intern in our **Security Expert** team to work on this topic for a period of 6 months remunerated.

 **Desired start date:** February 2023.

 The position is based in **Pessac** (Bordeaux).



## Your day-to-day would be:

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

- Design and implement test codes on smartcards, microcontrollers or more complex devices;
- Perform experiments to showcase the glitch setup capabilities;
- Create notebooks to document the different steps of the glitch attack, from the setup including the embedded code to the exploitation of faults.

## You're perfect for us, if...

- You are preparing a master degree and are in your last year of study
- You have developed a particular interest in:
  - ◆ Conception of Electronic devices
  - ◆ Embedded code development
  - ◆ Python
- You have some knowledge of fault injection attacks
- You are hacker minded, 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

## 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?

Contact us by sending your resume to

[intern@eshard.com](mailto:intern@eshard.com)



## References 📜

[Glitch Xbox 360] *E. Debusschere, Mike McCambridge, Modern Game Console Exploitation, report.*

[Starlink Hacked] *Starlink Successfully Hacked Using \$25 Modchip article*