eShard

In Real Life Attacks

Internship

Nowadays, the market is paved with electronic devices claiming security against side-channel attacks, or fault injection attacks, but only few of them have in house IC security experts, or paid the expensive price of a third party security evaluation like proposed in the Common Criteria Evaluation scheme. Most of the time, the developer is not really aware of the efficiency offered by side-channel attack software suites, and neglect the skill of attackers [Hacking of Tesla Model X].

The purpose of the internship is to investigate the side-channel leakage of chosen commercial devices using the capabilities of esDynamic, the IC Security evaluation platform developed by eShard. The purpose is to contribute to the security awareness of players involved in the electronic market.

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:

- Analyse device specification and command set, eventually develop embedded code to trigger cryptographic operations.
- Define attack paths according to device specification and command set analysis.
- Acquire side-channel traces using eShard facilities.
- Pre-process traces (filtering, synchronization) and identify areas of interest.
- Perform side-channel analysis using esDynamic.

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:
    - Side-channel, signal processing and statistics
    - Embedded code development
    - Python
- 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

References 📜

Hacking of Tesla Model X L. Wouters, B. Gierlichs, B. Preneel, My other car is your car: compromising the Tesla Model X keyless entry system [article]