Public key Side Channel attacks

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.

In the context of IC Security, the Public Key Cryptography (PKC) algorithms have taken an important role in many applications, and the **[side-channel]** community put the focus on the resistance of PKC implementations against side-channel attacks. Counter-measures such as randomization are deployed but are still challenged by specific attack techniques. In this context, most publications are based on simulation and there is a lack of practical experiments showing the real impact of these attacks on commercial products. We want to bridge this gap and demonstrate the real benefit of advanced attack techniques.

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 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:

- Collect and summarize principal publications regarding horizontal attacks on public key cryptography
- Apply selected attacks on products and compare them
- Collaborate with eShard security experts to deploy the different attacks, supervised or not, which potentially overcome deployed counter-measures on real devices
- Work on different techniques, including the one introduced recently by eShard experts, named **[SCATTER]**

You are

- You are preparing a master degree and are in your last year of study
- You have developed a particular interest in:
    - Python
    - Public Key Cryptography
- You have some knowledge of side-channel, signal processing and statistics
- 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.

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

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