Side-channel Attack on Neural Networks

Internship

Artificial intelligence has become increasingly important in all aspects of digital services. OEM or service providers can invest a lot of money into the training of their Neural Networks (NN) which are then loaded into connected devices for inference purpose. They can be executed on a CPU, GPU or dedicated neural network processor depending on the type of chip. As the neural network has a lot of value, it is thus an asset that deserves protections against various types of attacks aiming at its extraction.

Side-channel analyses usually target cryptographic secret keys. But they can be used to extract a fixed code structure or data in the device. Side-channel is therefore a threat that could disclose valuable data such as: a neural network structure, its weights and biases, or its inputs and outputs. Recent research has shown that the technique is efficient: a survey can be found here.

The purpose of this internship is, inspired by existing reports from the side-channel community, to showcase a practical example. Guided by eShard experts, the intern will start with hands-on implementation of a Neural Network application using an IoT accelerator. Then, mount side-channel analysis to qualify the implication on neural network applications. Finally, mitigation directions and their effectiveness will be studied.

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).

eShard

Your day-to-day would be:

You will be in charge of the following missions:

- Create a knowledge notebook giving an overview of state-of-the-art attacks published in the literature.
- Understand and summarize the operation of the NN accelerator, and how it is used in a typical application.
- Identify attack scenarios and mount proof of concept side-channel extractions
- Study the mitigation aspect and identify directions to solve the issues.

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:
  - Python
  - Deep-Learning based on Neural Networks
- 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

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