



## 5th Workshop on the Security of Software/Hardware Interfaces

Guillaume Hiet<sup>1</sup> Jan Tobias Mühlberg<sup>2</sup>

<sup>1</sup>IRISA, CentraleSupélec/Inria

<sup>2</sup>Université Libre Bruxelles





CentraleSupélec



## Organization of different events:

- ▶ a summer school: <https://silm-school.inria.fr/>
- ▶ **SILM workshop:** <https://silm-workshop.github.io/>
- ▶ SILM seminar: <https://silm-seminar.gitlabpages.inria.fr/>

<https://silm.inria.fr/>

## 1. Analysing the behavior and state of hardware components

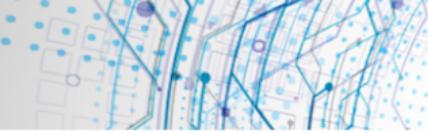
- Fuzzing
- Reverse-engineering
- Trace mechanisms
- Automated specification analysis

## 2. Assessing the security of these hardware components

- Side-channel attacks
- Fault injection
- Exploiting unspecified behaviors

## 3. Detecting or preventing software attacks

- Using dedicated hardware components
- Software countermeasures against hardware vulnerabilities



Full Programme: <https://silm-workshop.github.io/2023-program/>

**Opening** – 09:00-09:30 – Guillaume Hiet & Jan Tobias Mühlberg

**Session 1** – 09:30-10:30 – Session 1: "**Microarchitectural Attacks and Defences in Microcontrollers**" (Chair: Jan Tobias Mühlberg)

**Coffee** – 10:30-11:00

**Session 1** – 11:00-11:30 – Session 1.1 (Chair: Frédéric Tronel)

**Invited Talk** – 11:30-12:30 – **Sergej Proskurin** (Chair: Jan Tobias Mühlberg)

**Lunch** – 12:30-14:00

**Session 2** – 14:00-15:00 – Session 2: "**Attacks and Defences for Crypto Implementations**"

(Chair: Guillaume Hiet)

**Coffee** – 15:00-15:30

**The Future of SILM** – 15:30-16:00 – Guillaume Hiet & Jan Tobias Mühlberg

**Session 3** – 16:00-17:30 – Session 3: "**Side Channels, Static & Dynamic Analysis**"

(Chair: Jo Van Bulck)

**Dinner ???** – 19:30-???:???

- ▶ **IEEE Euro S&P** organisation and workshop committee
- ▶ **Funding and supporting institutions** : DGA, Inria, Centrale-Supélec, Université Libre Bruxelles
- ▶ **Program and organization co-chairs** : Guillaume Hiet and Jan Tobias Mühlberg
- ▶ **Program committee** : Pascal Cotret (ENSTA Bretagne), Chris Dalton (HP Labs), Lesly-Ann Daniel (KU Leuven), Merve Gülmез (Eriscon/KU Leuven), Karine Heydemann (LIP6), Vianney Lapôtre (Univ. South Brittany), Clémentine Maurice (CNRS), Cristofaro Mune (Raelize B.V.), Kaveh Razavi (ETH Zurich), Simon Rokicki (ENS Rennes), Shweta Shinde (ETH Zurich), Volker Stolz (HVL), Marcus Voelp (Uni Luxembourg), Pierre Wilke (CentraleSupélec/Inria), Yuval Yarom (University of Adelaide and Data61)
- ▶ **Inria Staff** : Lydie Mabil

- ▶ Workshop website : <https://silm-workshop.github.io/>
- ▶ Do not hesitate to ask questions
- ▶ Speakers :
  - join 10 min before your session for testing
  - send us your slides
- ▶ Wifi code: → registration info



- ▶ **Moeke Delft**, Beestenmarkt 16, 2611 GB Delft
- ▶ 19:00
- ▶ Guillaume pays! :-)



## Express your feelings!

- ▶ What's good about SILM this year? What is less ideal?

## Express your feelings!

- ▶ What's good about SILM this year? What is less ideal?

## What do we do next year?

- ▶ Organisation of SILM?
- ▶ Scoping? New topics?
- ▶ Reviewing process?
- ▶ Publication?
- ▶ Longer talks? Shorter talks? Time for interaction?
- ▶ More or fewer invited talks?
- ▶ Panels?