2018-00374 - Secure micro-architectures
PhD thesis

Level of qualifications required: Graduate degree or equivalent
Function: PhD Position

About the research centre or Inria department
Inria, the French National Institute for computer science and applied mathematics, promotes “scientific excellence for technology transfer and society”. Graduates from the world’s top universities, Inria’s 2,700 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

Context
This thesis will take place under the supervision of Jean-Louis Lanet, head of the High Security Laboratory (LHS) at INRIA Rennes, co-supervised by Jacques Fournier from CEA-Leti and advised by Ronan Lashermes (INRIA Rennes). The student will have access to LHS platforms (for physical attacks in particular) for her research work.

Assignment
The architecture of modern processors has gotten more and more complex in order to optimize performance and energy consumption. Meanwhile, the security of such systems has not been taken enough into account, as has been shown by recent Spectre and Meltdown attacks.

The PhD student will have to review the state-of-the-art on how to improve System-on-Chip (SoC) security and she will have to propose new solutions. In particular, we are interested in control-flow integrity, memory isolation and linear execution guarantees. The student will have to ensure that proposed solutions can be integrated into the application development process. The targeted SoC is lowRISC, an open RISC-V based SoC.

Main activities
- Assess the state-of-the-art
- Propose new solutions
- Implement these solutions
- Evaluate them
- Publish

Skills
Technical skills and level required:
- microelectronics and digital electronics (VHDL, verilog, Chisel, ...)
- processor architecture and system programming (C, assembly, ...)
- cryptography
- knowledge on the inner working of a compiler and in theoretical computer science is a plus

Languages:
- only english is required

Relational skills:

Other valued appreciated:

Benefits package
- Subsidised catering service
- Partially-reimbursed public transport

General Information

- Theme/Domain: Security and Confidentiality
  Information system (BAP E)
- Town/city: Rennes
- Inria Center: CRI Rennes - Bretagne Atlantique
- Starting date: 2018-10-01
- Duration of contract: 3 years
- Deadline to apply: 2018-05-31

Contacts
- Inria Team: CIDRE
- Recruiter: Lashermes Ronan / ronan.lashermes@inria.fr

The keys to success
Because the student will have to master numerous disciplines (microelectronics, computer science, cryptography, ...), we expect from the candidate that she is proactive in her education to fill the gaps. We suggest that the candidate enjoy computer programming and physics experimentation (for physical attacks).

Conditions for application
Please submit online: your resume, cover letter and letters of recommendation.

For further information, please contact Ronan Lashermes (ronan.lashermes@inria.fr)

Defence Security:
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy:
As part of its diversity policy, all Inria positions are accessible to people with disabilities.
• Sports facilities

Remuneration

Monthly gross salary amounting to 1982 euros for the first and second years and 2085 euros for the third year online on the Inria website. Processing of applications sent from other channels is not guaranteed.