Offer #2021-03556

PhD Position F/M Security-enhancing compiler against side-channel attacks

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Level of experience : Recently graduated

About the research centre or Inria department

The Inria Rennes - Bretagne Atlantique Centre is one of Inria's eight centres and has more than thirty research teams. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institute, etc.

Context

In 2018, the Spectre and Meltdown attacks have shown that most systems are vulnerable to side-channel attacks. In those attacks, an attacker running processes on the same device as a victim process is able to discover information that should be private to the victim process. This is possible not because of flaws in the operating systems, but rather because of microarchitectural elements (e.g. cache) that are observable by the attacker.

Classical countermeasures can be implemented in software (constant-time programming [3]) or hardware (complex cache architectures). These approaches incur a significant overhead.

In the SCRATCHS project, we aim at co-designing (1) a secure processor architecture based on RISC-V, and (2) a compiler for that new architecture. The hardware will provide security features (cache eviction policy, cache partitioning...) that can be control by the software.

Partners of the SCRATCHS project are LabSticc (UBS-ENSTAB), the Celtique team (Inria) and the CIDRE team (Inria/CentraleSupélec). This Ph.D. thesis will be supervised by members of the Celtique and CIDRE teams.

Assignment

This thesis focuses on building a security-enforcing compiler, and will collaborate with another Ph.D. student working on designing and implementing the secure processor. A possible roadmap for that thesis is as follows:
- study the state-of-the-art related to secure compilation and side-channel attacks
- design the input language: an extension of the C language with annotations describing which variables or memory zones should be considered confidential.
- specify, in collaboration with our partners, the security mechanisms that should be provided by the hardware.
- extend an existing compiler (Jasmin [1] or CompCert [2]) to enforce the security policy described by the annotations, leveraging the security mechanisms exposed by the hardware.
- securely optimise the programs: by performing a static timing analysis of the input program, the compiler may realise that some protections are superfluous, and can be skipped while still meeting the security requirements.

[1] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Arthur Blot, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Hugo Pacheco, Benedikt Schmidt, Pierre-Yves Strub: Jasmin: High-Assurance and High-Speed Cryptography. CCS 2017: 1807-1823
[2] Xavier Leroy: Formal verification of a realistic compiler. Commun. ACM 52(7): 107-115 (2009)
[3] S. Cauligi, G. Soeller, B. Johannesmeyer, F. Brown, R. S. Wahby, J. Renner, B. Grégoire, G. Barthe, R. Jhala, and D. Stefan. Fact: a DSL for timing-sensitive computation. InK. S. McKinley and K. Fisher, editors,Proceedings of the 40th ACM SIGPLAN Conferenceon Programming Language Design and Implementation, PLDI 2019, Phoenix, AZ, USA,June 22-26, 2019, pages 174–189. ACM, 2019

Main activities

The candidate will participate in the SCRATCHS CominLabs project, specifically in the task related to building a compiler that secures programs against side-channel attacks.

The candidate will publish his/her work in international conferences and journals.

Skills

The candidate should have experience in the following domains:
- compilation
- functional programming
and interest in:
- security
- CPU architecture
- formal methods

Languages : English read/written/spoken

Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours)
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Remuneration

Monthly gross salary amounting to 1982 euros for the first and second years and 2085 euros for the third year.

General Information

- **Theme/Domain :** Architecture, Languages and Compilation
  System & Networks (BAP E)
- **Town/city :** Rennes
- **Inria Center :** Centre Inria de l'Université de Rennes
- **Starting date :** 2021-09-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2021-06-30

Contacts

- **Inria Team :** CELTIQUE
- **PhD Supervisor :**
  Besson Frederic / frederic.besson@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Please submit online : your resume, cover letter and letters of recommendation eventually

For more information, please contact pierre.wilke@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.