Offer #2024-07655

Formal Verification and Embedded Rust for Low-Power Open Source Distributed System Software

Contract type : Fixed-term contract

Level of qualifications required : PhD or equivalent

Other valued qualifications : MSc

Fonction : Post-Doctoral Research Visit

About the research centre or Inria department

The Inria Saclay-Île-de-France Research Centre was established in 2008. It has developed as part of the Saclay site in partnership with **Paris-Saclay University** and with the **Institut Polytechnique de Paris** .

The centre has **39 project teams**, 27 of which operate jointly with Paris-Saclay University and the Institut Polytechnique de Paris; Its activities occupy over 600 people, scientists and research and innovation support staff, including 44 different nationalities.

Context

Scientific context: this position will focus on designing and leading the development of formally verified open source buidling blocks for a cybersercure embedded software platform : a Rust-based, general-purpose OS running on the main low-power 32-bit microcontrollers (Arm Cortex-M, RISC-V, ESP32...) in the context of the RIOT-rs project.

The approach aimed for in this project includes the use of formal verification tools uising functional Rust as speficiation language (such as hax, in partnership with Cryspen) and fostering integration of formal verification workflows in the operating system's continuous integration processes to automate proofs on the OS as it evolves, such as in this blueprint.

For further reading, see the output of RIOT-fp, a cybersecurity research project w.r.t. which the work envisionned here will be a follow-up. The targeted low-power devices are typically connected to the network via various low-power wireless techniques (BLE, 802.15.4, LoRa...) and low-power IPv6 secure protocol stacks. Recently, new standards have been specified in this domain, including the protocols necessary for SUIT-compliance, the new state-of-the-art regarding IoT software update security. In parallel, the development and integration of various relevant or upcoming cryptographic libraries (in particular NIST contenders) has become necessary to prepare for next-generation, post-quantum attacks.

Complementary information: Every year Inria International Relations Department proposes a few postdoctoral positions in order to support Inria international collaborations. The postdoctoral fellow will be recruited by one of the Inria Centres in France (Saclay in our case) but time will shared between France and the partner's country (Berlin, Germany in our case). Please note that the postdoctoral fellow has to start his/her contract located in France and that the visits abroad have to respect Inria rules for missions.

Candidates for postdoctoral positions are recruited after the end of their Ph.D. or after a first post-doctoral period: for the candidates who obtained their PhD in the Northern hemisphere, the date of the Ph.D. defense must be later than September 1, 2022; in the Southern hemisphere, later than April 1, 2022. The postdoctoral position must take place in a scientific environment that is different from the one of the Ph.D. (and, if applicable, from the position held since the Ph.D.). A particular emphasis is thus put on French or international candidates who obtained their doctorate abroad.

Deadline to apply: June 2nd 2024

Assignment

Collaboration :
The recruited person will be in connection with RIOT-rs developers, the community developing hax, the Rust Embedded and the RIOT open source communities, as well as Inria researchers in the domain of secure low-power IoT, cryptography and formal verification.

Responsibilities :
The recruited person will be in particular in charge of steering interactions between RIOT-rs developers and the community developing hax. The main goal will be to "hax" up an increasing perimeter of central

RIOT-rs software modules, on which a number of proofs (t.b.d.) will have to be performed, and maintained, as the OS if being developed and fleshed out further down the line.

Steering/Management :
The person recruited will be in charge of steering the developer community snowballing around the open source code base.

Main activities

Main activities:

- propose and steer hax-based formal verification for existing and upcoming RIOT-rs building blocks
- propose formally verified Rust rewrites for RIOT building blocks
- implementation, documentation and CI of formally verified embedded Rust modules
- interact with cryptography experts and formal verification experts
- interact with secure low-power IoT network protocols experts
- upstreaming and steering of open source communities

Skills

Technical Skills
- embedded C/Rust
- formal verification
- git
- open source software workflows
- RTOS or bare-metal experience on 32-bit microcontrollers such as ARM Cortex-M, RISC-V, ESP32
- cybersecurity basics (communication protocols, cryptography)

Non-Technical / Soft skills
- distributed team work
- good english skills (written, spoken, read)
- consensus building

Benefits package

- Subsidized meals
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training

Remuneration

According to experience

General Information

- **Theme/Domain :** Distributed Systems and middleware
  System & Networks (BAP E)
- **Town/city :** Paris
- **Inria Center :** Centre Inria de Saclay
- **Starting date :** 2024-08-01
- **Duration of contract :** 2 years
- **Deadline to apply :** 2024-09-30

Contacts

- **Inria Team :** TRIBE
- **Recruiter :**
  Baccelli Emmanuel / Emmanuel.Baccelli@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.

The keys to success

This job is for people who are passionate about formal verification, embedded Rust, serious cybersecurity and who are open source enthusiasts.

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

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.