Offer #2022-04915

PhD Position F/M Compositional verification of system program modules in Rust

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

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

Project RIOT-fp [b] is an Inria Challenge with the objective of developing future-proof operating system libraries [1,2,4] for application to IoT: RIOT [a]. Our PhD project is interested in one of the futures of RIOT: RIOT-rs, implemented in Rust [c]. This computing base provides access to a vast ecosystem of analysis, code generation, verification and proof tools [d,e,f]. It offers us to rethink a system software validation process that would suit both system programming and verification requirements (as one may expect from using, e.g., a theorem prover).

Assignment

The notion of contract [3] is one ideal such interface between the development and verification of system programs in Rust. A contract allows, on one hand, to formally document the hypothesis and guarantees of system modules, functions, artifacts, with respect to global safety ad security requirements. Contracts can be sufficiently abstract and comprehensible for system programmers, and adequately refined to meet the strongest requirements of mechanized verification.

Main activities

Our project will focus on the development of such a modular validation flow by case-studying the core of RIOT's implementation in Rust [riot-rs-core]. We define and exercise this workflow to characterize and validate global requirements ranging from race-condition, deadlock avoidance, priority management and schedulability, and/or memory isolation, faul isolation, information flow control.

BIBLIOGRAPHY
[a] RIOT: http://www.riot-os.org
[b] RIOT-fp: https://future-proof-iot.github.io/RIOT-fp
[c] riot-rs-core: https://github.com/future-proof-iot/RIOT-rs/tree/main/src/riot-rs-core/src
[d] F*: https://www.fstar-lang.org
[e] Lean: https://leanprover.github.io
[f] Electrolysis: https://kha.github.io/electrolysis

REFERENCES
[1] "Verified Functional Programming of an Abstract Interpreter". Static Analysis Symposium. ACM, 2021.
[2] "Verified Functional Programming of an IoT operating system's boot-loader". International Conference on Formal Methods and Models for System Design. ACM, 2021.
[3] "A Mechanically Verified Theory of Contracts". International Colloquium on Theoretical Aspects of Computing. Springer, 2021.
[4] "End-to-end Mechanized Proof of an eBPF Virtual Machine for Microcontrollers". International Conference on Computer Aided Verification, 2022.

Skills

It requires a Master degree with solid background in proof theory and mathematical logic, programming languages and type theory, as well as motivation and interest in both the implementation and verification of operating systems. Prior knowledge and experiences with both Rust, F*, Coq, Lean will stand out.

Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Possibility of teleworking (90 days per year) and flexible organization of working hours
- partial payment of insurance costs

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 :** Proofs and Verification
- **Town/city :** Rennes
- **Inria Center :** Centre Inria de l'Université de Rennes
- **Starting date :** 2022-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2022-09-30

Contacts

- **Inria Team :** TEA
- **PhD Supervisor :**
  Talpin Jean-pierre / jean-pierre.talpin@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

The project will be implemented with teams Tea and Celtique at Inria, Rennes, in close collaboration with teams Tribe and Prosecco at Inria, Paris. The project will require weekly multi-center meetings and hence excellent communication and team-working skills in both french and english.

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

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.