



Offre n°2023-06891

Proof and Verification Software Engineer

Level of qualifications required : Graduate degree or equivalent

Other valued qualifications : PhD

Fonction : Temporary scientific engineer

Context

Over the past decade, formal verification encountered several high-profile successes which were integrated in industrial products, including verified compilers, operating systems, and cryptographic libraries. Building upon these advances, the CIRCUS project aims to make verification techniques more accessible to mainstream software development, by building a new integrated development and verification environment (IDVE) fostering collaboration between software engineers, proof engineers, and domain-specific experts such as cryptographers.

CIRCUS is a collaboration between Cryspen (cryspen.com) and the Prosecco team at Inria Paris (<https://team.inria.fr/prosecco/>), which especially targets the Rust ecosystem, and builds on several state-of-the-art specification and verification technologies, namely, the hax framework (<https://github.com/hacspec/hacspec-v2>) and the Aeneas toolchain (<https://github.com/AeneasVerif/aeneas>), which enable the use of several proof assistants, including Coq, F*, HOL4, and Lean to state and verify properties about safety- and security-critical software.

Assignment

We are currently looking for a research engineer to develop and improve the integration of proof assistants into the CIRCUS IDVE. The work will be done in collaboration with a small team of engineers and researchers currently developing and working with the CIRCUS IDVE.

Main activities

- Design and implement extraction procedures to proof assistants
- Develop efficient proof methodologies for reasoning about the extracted programs
- Interact with researchers to extend the subset of the Rust language currently supported by the toolchain
- Write documentation and tutorials to verify Rust programs using the CIRCUS IDVE
- Give presentations about the CIRCUS IDVE, including to non-technical audiences.

Skills

- Expertise in formal verification and compilation
- Proficiency with OCaml
- Familiarity with Rust
- Experience with one or more proof assistant (Coq, F*, HOL4, Lean, ...)
- Ability to work in a team, and in an international setting
- Ability to give presentations, including to non-expert audiences

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) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) 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
- Social security coverage

General Information

- **Theme/Domain :** Security and Confidentiality
Software engineering (BAP E)

- **Town/city** : Paris
- **Inria Center** : [Centre Inria de Paris](#)
- **Starting date** : 2024-01-01
- **Duration of contract** : 2 years

Contacts

- **Inria Team** : [PROSECCO](#)
- **Recruiter** :
Fromherz Aymeric / aymeric.fromherz@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

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.