Offer #2021-03774

Post-Doctoral Research Visit F/M Deploying Proof-Oriented Programming at Scale

Contract type : Fixed-term contract

Level of qualifications required : PhD or equivalent

Fonction : Post-Doctoral Research Visit

Assignment

Structuring programs with proofs in mind is a promising way to reduce the effort of building trustworthy software. Such an approach results in a myriad of benefits. On one side, the program can be structured to simplify proofs, reducing the burden on the developer while enabling strong, formal guarantees about its correctness and security. On the other hand, proofs can simplify and optimize the program, for instance by eliminating checks and cases that can be statically ruled out

Main activities

The research aims at applying a proof-oriented methodology to improve the reliability of real-world software. To this end, the candidate will investigate fundamental improvements to the expressiveness and programmability of proof-oriented languages, while demonstrating their usefulness on security-critical real-world systems. Secure communication protocols, for instance TLS, QUIC, or Wireguard, foundation of Internet security, are a prime target for verification. They build on secure cryptographic implementations such as EverCrypt, but use them to implement a protocol, commonly described as a state machine, while enabling communication with several parties at the same time; their implementations thus must be concurrent.

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
  Information system (BAP E)
- **Town/city :** Paris
- **Inria Center :** Centre Inria de Paris
- **Starting date :** 2021-09-01
- **Duration of contract :** 2 years
- **Deadline to apply :** 2021-07-31

Contacts

- **Inria Team :** PROSECCO
- **Recruiter :**
  Mourey Mathieu / mathieu.mourey@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.