



Offre n°2024-07655

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

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Thèse ou équivalent

Autre diplôme apprécié : MSc

Fonction : Post-Doctorant

A propos du centre ou de la direction fonctionnelle

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.

Contexte et atouts du poste

Scientific context: this position will focus on designing and leading the development of formally verified open source building blocks for a cybersecurity 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 using functional Rust as specification 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 envisioned 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 be 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

Mission confiée

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.

Principales activités

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

Compétences

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

Avantages

- 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

Rémunération

According to experience

Informations générales

- **Thème/Domaine** : Systèmes distribués et intergiciels
Système & réseaux (BAP E)
- **Ville** : Paris
- **Centre Inria** : [Centre Inria de Saclay](#)
- **Date de prise de fonction souhaitée** : 2024-08-01
- **Durée de contrat** : 2 ans
- **Date limite pour postuler** : 2024-09-30

Contacts

- **Équipe Inria** : [TRIBE](#)
- **Recruteur** :
Baccelli Emmanuel / Emmanuel.Baccelli@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de

nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

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

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :

Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.