Offer #2025-08797

Dynamic binary rewriting for long-term support of RISC-V processors

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : Temporary scientific engineer

Level of experience : Recently graduated

Assignment

Within the context of an Inria Challenge, the project-teams PACAP and MADMax join forces to develop a demonstrator of dynamic binary rewriter to explore long-term support of RISC-V processors.

RISC-V provides an opportunity to update the ISA and the executable format to mandate that any instruction being fetched by the processor that is not supported by it trigger a fault. This includes unimplemented encodings but also encodings implemented as part of a different extension (e.g., processor supports extension A with encoding E, and the binary has an instruction from extension B with encoding E). This facility would allow to provide compatibility layers as part of an operating system service, whereby any binary compiled targeting – almost – any extension could be run on hardware that does not feature these extensions, with the missing extensions being emulated in software. This would decrease the burden placed on software to either target a common set of extensions, thereby limiting performance if the hardware has extensions that could accelerate the code, or target specific extensions, thereby making binaries even less portable.

The objective consists in developing such facility as a demonstrator based on dynamic binary rewriting. The mechanism could be implemented either in the OS kernel or in userland. The kernel offers the advantage of sharing the portability across all processes. Userland, on the other hand, does not require any privilege and lets different users handle different instructions. As a first step, we will emulate the instruction semantics when the unsupported instruction raises an exception. We will then give back control to the user program. However, this mechanism will incur significant overhead as the cost of trapping into the kernel is in the hundreds of cycles, without even considering the cost of the emulation itself. As a result, a second, more optimized mechanism will attempt to dynamically patch the user binary with regular jumps to library functions emulating the unsupported instructions. Further optimizations such as chaining such calls if the user code features several contiguous unsupported instructions and even optimizing such chained calls on the fly could be envisioned as future work. Nevertheless, this can be seen as an efficient but also transparent dynamic binary translation mechanism, with RISC-V as both the host and target.

Travels between Rennes and Grenoble are expected, typically three or four days every six months. Travel expenses will be reimbursed within the limits of current regulations.

Main activities

The candidate will be expected to

- setup a RISC-V platform based on qemu
- specify an emulation mechanism based on the SIGILL signal
- specify which RISC-V extensions can be emulated, and which ones cannot
- implement a first demonstrator the dynamic binary rewriter
- analyze the SAIL language to automatically generate the emulation code

In addition, the candidate is expected to

- write the documentation
- follow development good practices such as use version control, continuous integration
- assess the performance of the tool
- contribute to the open-source strategy for the software

Skills

Technical skills and level required :

- Good knowledge of C/C++
- Good knowledge of Linux programming
- Basics of RISC-V assembler (possibly x86)
- Good knowledge of software engineering : source code organization, testing, version management, continuous integration

Languages: French and English read and written, spoken a bonus

Interpersonal skills: teamwork required, and in particular team project management

Benefits package

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail (après 6 mois d'ancienneté) et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle
- Sécurité sociale

General Information

- **Theme/Domain :** Architecture, Languages and Compilation
  Software engineering (BAP E)
- **Town/city :** Rennes ou Grenoble
- **Inria Center :** Centre Inria de l'Université de Rennes
- **Starting date :** 2025-06-01
- **Duration of contract :** 1 year, 6 months
- **Deadline to apply :** 2025-06-11

Contacts

- **Inria Team :** PACAP
- **Recruiter :**
  Rohou Erven / erven.rohou@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

Expected soft skills:

- Technical autonomy: ability to compare technical alternatives, list the pros and cons to reach an informed decision and to defend it
- Ability to convey information orally and in writing
- Ability to listen to constructive criticism and take it into account
- Ability to present work orally at annual project meetings

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.