



Offre n°2025-08797

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

Type de contrat : Fixed-term contract

Niveau de diplôme exigé : Graduate degree or equivalent

Fonction : Temporary scientific engineer

Niveau d'expérience souhaité : Recently graduated

Mission confiée

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.

Principales activités

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

Compétences

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

Avantages

- 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

Informations générales

- **Thème/Domaine** : Architecture, Languages and Compilation
Software engineering (BAP E)
- **Ville** : Rennes ou Grenoble
- **Centre Inria** : [Centre Inria de l'Université de Rennes](#)
- **Date de prise de fonction souhaitée** : 2025-06-01
- **Durée de contrat** : 1 year, 6 months
- **Date limite pour postuler** : 2025-06-11

Contacts

- **Équipe Inria** : [PACAP](#)
- **Recruteur** :
Rohou Erven / erven.rohou@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

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

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.