2022-05232 - Starting Research Position F/M Restricting ISA semantics for increased security

Type de contrat : CDD
Niveau de diplôme exigé : Thèse ou équivalent
Fonction : Chercheur contractuel
Niveau d'expérience souhaité : Do 3 à 5 ans

A propos du centre ou de la direction fonctionnelle

The Inria Rennes - Bretagne Atlantique Centre is one of Inria's eight centres and has more than thirty research teams. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institute, etc.

Contexte et atouts du poste

The security of embedded systems and the components they integrate is of growing importance in the cybersecurity arena. To address these challenges, the already-rich French research community in embedded systems security is joining forces within the PEPR Cysterecurity project ARSENE in order to accelerate research & development in this field. The main objectives of the project are to allow the French community to make significant advances in the field, to strengthen the community's expertise and visibility on the international stage. The first part of the ARSENE project is on the study and implementation of two families of RISC-V processors: 32-bit RISC-V for low power secure circuits against physical attacks for IoT applications and 64-bit RISC-V secure circuits against micro-architectural attacks for rich applications. The second aspect of the project pertains to the secure integration of such new generations of secure processors into System of Chips, to the research and development of secure building blocks for such SoCs like secure and robust Random Number Generators, memory blocks secured against physical attacks, memories instrumented for security and agile hardware accelerators for next generation of cryptography. This work on hardware security is completed by studies on software tools for dynamic annotation of code for next generation of secure embedded software, by the implementation of a secure kernel for an embedded OS and by research work on the dynamic embedded supervision of the system. A last, but very significant, aspect of this project is the implementation of FPGA and ASIC demonstrators integrating the components developed in this project. Those demonstrators shall offer a unique opportunity to showcase the results of the project.

Mission confiée

The candidate will integrate a team of researchers dedicated to inventing new security solutions at the level of microarchitecture, architecture and compilation. They will be assigned the design and development of code generation tasks, either within the compiler, or as a dynamic binary rewriting component. Currently envisioned solutions include the following.

- Restricting the usage of indirect jump instructions. We have experience in dynamic binary rewriting of indirect jumps, and we are interested in exploring this direction in more depth.
- Constant-time execution. We assume that constant-time execution can only be achieved through a hardware/software contract of the timing behaviour of the chip during execution. The RISC-V Zkt extension explores this direction by considering constant-time execution of instructions taken independently. We would like to guarantee the constant-time execution of instruction sequences. The idea consists in tagging registers that contain sensitive information. These registers shall therefore not be used by any non constant-time instruction, depending on the microarchitecture. The role of the compiler will be to make sure this does not happen, and the hardware will control if this condition holds.
- Handling explicit security domains. The microarchitecture introduces semantics to isolate security domains with various side effects. In particular, the hardware must guarantee that there is no possible architectural covert channel between two different security domains.
- Robustness against speculation attacks. The concept of speculation barrier has many flaws that prevent it from being widely applicable on any microarchitecture. We want to explore alternatives. Either control-flow instructions exist in two flavours: with possible speculation and without. The compiler shall decide when to emit each flavour, based on an analysis of the risk of an attack at a given point in the code. Or we may tag a register as security critical and any instruction handling this register must prevent speculation attacks. These solutions must be evaluated, compared, and integrated in the compiler workflow.

The candidate will also be encouraged to propose new schemes, to be discussed with the team.

As this research is of interest to the RISC-V Foundation, there is a possibility that developments are merged into RISC-V official repositories.

Principales activités

- Conduct bibliographic study
- Elaborate and discuss of new ideas
- Implement ideas in an experimental compiler framework
- Conduct performance evaluation and experimentation
- Give feedback to architects
- Write scientific papers
- Give research talks

Compétences

Required technical skills:

- Thème/Domaine : Architecture, langages et compilation
- Ingénierie logicielle (BAP E)
- Ville : Rennes
- Centre Inria : Centre Inria de l'Université de Rennes
- Date de prise de fonction souhaitée : 2022-10-01
- Date limite pour postuler : 2022-12-31

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences du numérique et au numérique. Il emploie 2600 personnes. Ses 200 équipes-projets agiles, en général communées avec des partenaires académiques, impliquent plus de 3500 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines technologiques. Inria fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. Il accueille de nombreux 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.

Consignes pour postuler

Please submit online : your resume, cover letter and letters of recommendation eventually
For more information, please contact damien.hardy@inria.fr or erven.rohou@inria.fr

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.
- proficiency in C, C++
- understanding of assembly language, in particular RISC-V
- knowledge of compiler internals, in particular LLVM
- knowledge of processor microarchitecture

Languages: English (read, written, spoken)

Relational skills:
- ability to work in a team
- autonomy

Avantages
- Subsidized meals
- Partial reimbursement of public transport costs
- Possibility of teleworking (90 days per year) and flexible organization of working hours
- Partial payment of insurance costs

Rémunération

gross monthly salary from 3039 euros to 4296 euros depending on profile and experience