Compilation prouvée sécurisée vers processeur RISC-V

2023-2024

Laboratoire VERIMAG (Grenoble)
Thèmes PACS (Preuve et Analyse de Code pour la Sécurité) et Preuves Formelles
Encadrants: David Monniaux & Bruno Ferres
david.monniaux@univ-grenoble-alpes.fr
bruno.ferres@univ-grenoble-alpes.fr

Mots-clef: compilation sécurisée; `CompCert`; sécurité matérielle; micro-architecture

Contexte

Les attaques en fautes (par faisceau laser, injection électromagnétique, ou même purement logicielle) constituent une menace sévère contre tous les systèmes embarqués [1, 2]. Bien qu'il existe des contre-mesures (matérielles, logicielles, ou hybrides) pour chaque modèle de faute, il est souvent complexe d'ajouter ces contre-mesures dans le flot de compilation des programmes. En outre, la question de l'efficacité de ces contre-mesures dans le code généré se pose, notamment dans des contextes ou plusieurs contre-mesures peuvent être composées pour durcir le code contre plusieurs modèles de fautes.

Dans le contexte de sa participation au PEPR Arsene, un projet national visant à développer des solutions logicielles et matérielles robustes et validées, le laboratoire VERIMAG s'intéresse aux flots de compilation sécurisés. Dans de tels flots, les contre-mesures peuvent être ajoutées automatiquement dans le code généré par le compilateur, sans intervention du programmeur. En particulier, VERIMAG s'intéresse à l'intégration de fonctionnalités de compilation sécurisée dans le compilateur CompCert. CompCert[1] [3] est un compilateur depuis le langage C vers les langages d'assemblage de plusieurs architectures qui a la particularité unique d'avoir une preuve mathématique et vérifiée dans un assistant de preuve (Coq[2]) que le code objet correspond au code source.

L'implémentation de contre-mesures de sécurité dans CompCert permettrait donc, à long terme, de fournir des garanties fortes sur la sécurité du code compilé. En particulier, cela permettrait de prouver la résistance du code développé par rapport à diverses attaques à l'état de l'art.

Objectifs du stage

Dans ce contexte, nous nous intéressons à l'implémentation dans le compilateur CompCert de contre-mesures de bas-niveau pour la sécurité. Ces contre-mesures devront prendre en compte les détails de la micro-architecture du processeur, et pourront, au besoin, s'appuyer sur des primitives matérielles dédiées. En particulier, lors de ce stage, il sera attendu que le ou la candidat(e):

- identifie une ou plusieurs contre-mesure(s) de bas-niveau pour le durcissement du code. Parmi les contre-mesures envisagées, notons les mesures de protection de l'intégrité du flot de contrôle (ou CFI pour *Control Flow Integrity* [4]), ou encore le durcissement des pointeurs [5].

[1] https://compcert.org/
[2] https://coq.inria.fr/

- implémente l'ajout de cette contre-mesure à la compilation dans CompCert
- étudie les différents impacts de cet ajout :
  - traçabilité : comment prouver que la contre-mesure est présente dans le code machine généré ?
  - correction : l'ajout de la contre-mesure modifie-t-elle la sémantique du programme compilé ?
  - efficacité : la contre-mesure est elle efficace contre le modèle de faute cible ?
  - performance : quel est l'impact de l'ajout de la contre-mesure sur les performances du programme ?

Ce sujet s'appuiera sur l'expertise de VERIMAG dans le domaine de la compilation vérifiée, en particulier avec CompCert[3], ainsi que sur les travaux préliminaires menés au sein du laboratoire sur les aspects de sécurisation des systèmes embarqués. Le sujet pourra en outre être décliné de différentes façons, suivant les intérêts du candidat/de la candidate.
De plus, selon le déroulement du stage, une continuation en thèse dans le cadre du PEPR Arsene[4] pourra être considérée.

Profil recherché

Ce stage s'adresse à des candidat(e)s inscrit(e)s dans des formations en informatique, idéalement au niveau M2[5] (ou dernière année d'école d'ingénieur).
Le ou la candidat(e) devra justifier des compétences et connaissances suivantes :

- solides connaissances en compilation et en méthodes formelles
- appétence pour les aspects bas-niveaux de l'informatique, en particulier l'architecture des micro-processeurs

En outre, une appétence pour les questions liées à la sécurité informatique (sécurité matérielle, protection du code, ...) est vivement souhaitée. Cependant, le ou la candidat(e) pourra acquérir les compétences liées au cours du stage.

Candidatures

Pour candidater, envoyez un e-mail à david.monniaux@univ-grenoble-alpes.fr et bruno.ferres@univ-grenoble-alpes.fr avec votre CV, une courte lettre de motivation, et tout document pouvant étayer votre candidature.

[3] https://gricad-gitlab.univ-grenoble-alpes.fr/certicompil/Chamois-CompCert
[4] https://www.pepr-cyber-arsene.fr/
[5] Les candidatures motivées au niveau M1 seront également étudiées

Localisation

Le stage se déroulera au sein du laboratoire VERIMAG, sur le campus de Grenoble :

Laboratoire VERIMAG, Bâtiment IMAG,
150 place du Torrent,
38401 Saint-Martin-d'Hères

Bibliographie

[1] B. Colombier, A. Menu, J.-M. Dutertre, P.-A. Moëllic, J.-B. Rigaud, and J.-L. Danger, "Laser-induced single-bit faults in flash memory: Instructions corruption on a 32-bit microcontroller," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 1–10, IEEE, 2019.

[2] I. Alshaer, B. Colombier, C. Deleuze, V. Beroulle, and P. Maistri, "Variable-length instruction set: Feature or bug?," in *2022 25th Euromicro Conference on Digital System Design (DSD)*, pp. 464–471, IEEE, 2022.

[3] S. Blazy and X. Leroy, "Formal verification of a memory model for C-like imperative languages," in *International Conference on Formal Engineering Methods (ICFEM 2005)*, vol. 3785 of *Lecture Notes in Computer Science*, pp. 280–299, Springer, 2005.

[4] M. Abadi, M. Budiu, U. Erlingsson, and J. Ligatti, "Control-flow integrity principles, implementations, and applications," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 1, pp. 1–40, 2009.

[5] Inc. Qualcomm Technologies, "Pointer Authentication on ARMv8.3 - Design and Analysis of the New Software Security Instructions." https://www.qualcomm.com/media/documents/files/whitepaper-pointer-authentication-on-armv8-3.pdf.