PROPOSITION DE STAGE

Affectation : DRT/LETI/DACLE/SCSN/LIALP

Intitulé : Intégrité d'exécution en présence d'attaques par injection de fautes : conception d'un processeur sécurisé et compilation de code sécurisé pour RISC-V.

Responsable technique : Damien COUROUSSÉ
Téléphone : 04 38 78 04 66 Courriel : damien.courousse@cea.fr

Contexte :

Le Leti, institut de recherche technologique de Cea Tech, a pour mission de créer de la valeur et de l'innovation avec ses partenaires industriels. Il fait le lien entre la recherche fondamentale et la production de micro et nanotechnologies dans le but d'améliorer la qualité de vie de chacun. Fort d'un portefeuille de 2.800 brevets, le Leti façonne des solutions avancées pour améliorer la compétitivité de ses partenaires industriels: grands groupes, PME ou startups. Localisé à Grenoble (38), le Leti compte plus de 1 800 chercheurs et a des bureaux aux US et au Japon.

Au sein du Département d'Architecture, Conception et Logiciel Embarqué (DACLE), une des activités du laboratoire LIALP est de développer une chaîne d'outils pour l'application automatisée de contremesures contre les attaques physiques (attaques par canaux cachés et attaques par injection de fautes) sur des systèmes embarqués.

http://www.leti-cea.fr/cea-tech/leti

CEA Grenoble presqu'île

Sujet :

Les attaques physiques représentent un vecteur d'attaque très efficace pour extraire de l'information ou pour contourner des mesures de sécurité sur les systèmes embarqués. L'attaquant a sa cible entre les mains, littéralement, ce qui lui permet d'observer le comportement du circuit [1] (attaques par canaux cachés) ou de perturber le fonctionnement du circuit [2] (attaques par injection de fautes). Les attaques par injection de fautes visent à perturber le fonctionnement normal d'un circuit ou d'un programme, soit pour en extraire un secret comme une clé de chiffrement, soit pour contourner un mécanisme de sécurité comme une procédure d'authentification.

Jusqu'à présent, nous nous sommes intéressés aux mécanismes de protection par logiciel, applicables à tous types de programmes, et appliquées automatiquement lors de la compilation du programme cible [3, 4]. Cette solution repose sur l'adaptation du compilateur LLVM pour l'architecture ARM, notamment dans les passes de compilation du backend.

L'état de l'art des attaques par injection de fautes a connu de grandes avancées ces dernières années, et face à un attaquant plus puissant équipé par exemple d'un banc d'injection laser [5], il est difficile de mettre en œuvre des contre-mesures efficaces reposant uniquement sur du logiciel, à moins d'accepter un surcoût important en termes de temps d'exécution et d'empreinte mémoire. Nous cherchons donc à développer des contre-mesures mixtes, reposant à la fois sur des adaptations du matériel et du logiciel, afin de réduire le surcoût de la sécurisation, et

d'augmenter le niveau de sécurité du système. Dans un système de haute sécurité comme les cartes à puces, les contre-mesures développées peuvent venir compléter les mécanismes de protection déjà en place.

L'objectif du stage est d'implémenter une preuve de concept d'un schéma d'intégrité d'exécution pour l'architecture RISC-V [6]. La spécification du schéma d'intégrité d'exécution qui sera implémenté a déjà été réalisée dans le cadre de travaux précédents, mais l'étudiant aura l'opportunité de proposer des améliorations à ce schéma si le besoin se présente. RISC-V est une architecture ouverte et libre, en passe de devenir un standard d'architecture ouverte dans l'industrie. La plateforme d'expérimentation ciblera donc RISC-V ; elle sera basée sur le simulateur fonctionnel Spike, et sur la chaîne de compilation LLVM.

Les tâches à réaliser dans le stage sont les suivantes :

- Modifier le simulateur Spike pour simuler le support matériel d'intégrité d'exécution.
- Modifier le backend RISCV du compilateur clang (LLVM) pour apporter les aménagements de code nécessaires dans le code machine compilé
- Évaluer le niveau de sécurité apporté par la solution implantée, et l'impact sur les performances.

Ce stage entre dans le contexte du projet COFFI, financé par l'Agence Nationale pour la Recherche, qui démarrera en février 2019 pour une durée de 4 ans. Ce projet inclut des équipes de recherche d'industriels et d'académiques spécialisés dans la cyber-sécurité des systèmes embarqués. Le stagiaire participera aux réunions de projet et sera amené à interagir avec les autres équipes de recherche participant à ce projet.

La poursuite en thèse est possible à l'issue du stage. Le financement de thèse est assuré dans le cadre du projet COFFI.

[1] https://en.wikipedia.org/wiki/Side-channel_attack
[2] https://en.wikipedia.org/wiki/Fault_injection
[3] T. Barry, D. Couroussé, and B. Robisson "Compilation of a Countermeasure Against Instruction-Skip Fault Attacks," in *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems (CS2)*, 2016.
[4] http://llvm.org/devmtg/2017-03//2017/02/20/accepted-sessions.html
[5] https://www.youtube.com/watch?v=sNRYVCmlE80
[6] https://riscv.org

Profil :

Cette proposition est dédiée aux étudiants recherchant un stage au contenu technique ambitieux et désirant acquérir une expérience dans la recherche technologique en lien avec l'industrie. Cette proposition est par ailleurs particulièrement adaptée aux étudiants désirant poursuivre en doctorat, puisqu'elle est en lien avec un sujet de thèse à pourvoir dans le laboratoire à la rentrée 2019. La poursuite en doctorat n'est toutefois ni obligatoire ni systématique.
L'étudiant devra présenter un niveau équivalent de dernier année d'école d'ingénieur (ou master 2) avec de préférence une spécialité en informatique ou en conception de systèmes embarqués. Enfin, l'étudiant devra présenter une bonne capacité de travail personnel, une habilité à travailler en équipe dans un environnement pluridisciplinaire, et une motivation pour les challenges techniques.

Compétences techniques souhaitées :

- Développement C++, la connaissance de LLVM n'est pas nécessaire mais sera un plus,
- Logiciel embarqué,
- Git ,
- Connaissance de la micro-architecture des processeurs.

Formation requise	Durée du stage	Possibilité thèse
Ecole Ingénieur ou Master Recherche	6 mois	Oui

Unité d'accueil

Adresse postale	CEA GRENOBLE – campus Minatec 17 rue des Martyrs 38000 Grenoble