Objet :
Sujet de thèse

Dossier suivi par :
Nom : Potin
Prénom : Olivier

Tél : 0442616737

N / Ref :

PJ : 0
Copie : 0

Durcissement matériel/logiciel d'un processeur pour le contrôle de l'intégrité du flot d'exécution

L'objectif de la thèse concerne la conception de contre-mesures contre les attaques en fautes sur des processeurs par une approche de co-conception logicielle et matérielle en tenant compte des interactions possibles entre la micro-architecture ouverte du processeur RISC-V et la versatilité du développement logiciel (code dédié, stratégie de compilation, ...). En conséquence, de nouveaux scenarii de protections contre les attaques en fautes pourront être envisagés.

Sujet :

La complexité de plus en plus importante des systèmes embarqués s'accompagne d'un fort corollaire sécuritaire : le niveau de sécurité des systèmes doit aussi croître puisque de nouvelles attaques tirent profit de failles matérielles et/ou logicielle. Parmi ces menaces, les attaques dites "physiques" sont considérées comme particulièrement sérieuses et puissantes pour attaquer la confidentialité, l'intégrité et l'authenticité des systèmes. Traditionnellement, la recherche sur les analyses par canaux cachés (« side-channel ») ou par perturbation (« fault injection ») ont porté sur des primitives cryptographiques. Mais récemment, les attaques par perturbation ont permis de s'attaquer à l'intégrité de l'exécution d'un programme [Schaumont2016] élargissant le spectre des applications sujettes à ces attaques (bootloader, mise à jour de firmware, ...). Pour contrecarrer ces menaces, la communauté de sécurité a proposé plusieurs contre-mesures par des approches logicielles pour l'intégrité du flot de contrôle (CFI) et/ou des approches matérielles de contrôle ou d'intégrité du code (au prix de forts "overheads") [Clercq2016][Werner2018] [Lashermes2018].

Néanmoins, les schémas de protections développés se basent encore trop sur l'amoncellement de couches matérielles supportées par les couches logicielles.
Le projet de thèse doit permettre l'exploitation des interactions matérielles et logicielles pour atteindre les meilleurs compromis entre performances et propriétés de sécurité face aux attaques par perturbations et ainsi, permettre de protéger l'ensemble des niveaux structurels d'un système : micro-architecture du processeur, ISA, logiciel.

Synthèse des objectifs :
Le travail de recherche s'articulera autour des points listés ci-après :

- Modélisation des attaques en fautes sur la micro-architecture du processeur RISC-V
- Instrumentation du processeur permettant la détection de l'injection de fautes sur le jeu d'instructions ou des données.
- Développement de nouveaux schémas de protections par une approche de co-conception logicielle/matérielle (i.e modification légère du cœur de processeur conjointement avec l'exécution de jeu d'instructions dédié à la sécurité).
- Évaluation des protections vis-à-vis des algorithmes de sécurité standard (calcul cryptographique ou processus d'authentification)

Compétences recherchées :

- Environnement de développement des systèmes embarqués (C++, Assembleur, compilateur…)
- Micro-architecture de processeur (ISA, RISC, …)
- Langage de description matérielle (HDL, Verilog, Chisel, …)
- Flot de conception FPGA (Xilinx Vivado)
- Attaques matérielles par LASER ou EM
- Cryptographie

Direction de thèse, encadrements :
Jean-Max Dutertre (Directeur de thèse),
Jean-Baptiste Rigaud et Olivier Potin (co-encadrants)

Bibliographies :
[Yuce2016] : Yuce, Bilgiday & Farhady Ghalaty, Nahid & Santapuri, Harika & Deshpande, Chinmay & Patrick, Conor & Schaumont, Patrick. (2016). « Software Fault Resistance is Futile: Effective Single-Glitch Attacks ». 47-58. 10.1109/FDTC.2016.21.
[deClercq2016] : de Clercq, Ruan, Ronald De Keulenaer, Bart Coppens, et al. « SOFIA : Software and Control Flow Integrity Architecture » Proceedings of the 2016 Design, Automation & Test in Europe Conference (DATE). New york: IEEE, 2016. 1172–1177.
[Werner2018] : Werner, M., Unterluggauer, T., Schaffenrath, D., & Mangard, S. Sponge-Based Control-Flow Protection for IoT Devices. in 2018 IEEE European Symposium on Security
[Lashermes2018] : Lashermes R., Le Bouder H., Thomas G. (2018) Hardware-Assisted Program Execution Integrity: HAPEI. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. Lecture Notes in Computer Science, vol 11252. Springer

Durée :

3 ans

Environnement :

Le candidat à la thèse intégrera le laboratoire Systèmes et Architectures Sécurisés (SAS) regroupant les équipes de recherches de Mines Saint-Etienne et du CEA sur le site du Centre de Microélectronique de Provence (CMP) de Gardanne - 5ème centre de recherche et formation de Mines de Saint Etienne. Le département de recherche SAS adresse les problématiques d'attaques par canaux auxiliaires, par injection de fautes via leurs plateformes d'illumination laser et d'injection électromagnétique (EM) et la conception de contre-mesures (capteurs de détection et architecture sécuritaire). Cette thèse se déroulera dans le cadre du projet COFFI (cf. https://anr.fr/Projet-ANR-18-CE39-0003) financé par l'ANR et la SGSDR. Ce projet a commencé en 2019 et son consortium est composé de : Mines Saint-Etienne, CEA (CEA-LSAS et CEA-Dacle à Grenoble), Sorbonne Université (LIP6) et un partenaire industriel INVIA.

Candidature :

La candidature sera envoyée à Jean-Max Dutertre, Olivier Potin et Jean-Baptiste Rigaud aux adresses dutertre@emse.fr, olivier.potin@emse.fr et rigaud@emse.fr. Elle comportera un CV détaillé, une lettre de motivation et des lettres de recommandation éventuelles.