Étude des options de compilation influençant l'analyse statique du binaire en vue de la vérification de l'intégrité du flot de contrôle.

L'objectif du projet d'étude (PE) concerne la compréhension des options de compilation et son impact sur la génération des schémas de protection du CFI sur un cœur RISCV.

Sujet :

La conception de schémas de protection pour l'intégrité du flot d'exécution se déduit de l'analyse des discontinuités dans le lot de contrôle d'un programme. Cette analyse peut s'effectuer lors du processus de compilation en instrumentant le compilateur ou par l'analyse statique du code binaire produit. Dans le cadre du projet ARSENE, l'équipe SAS travaille sur la conception d'un schéma de protection pour l'intégrité du flot de contrôle (CFI) tirant partie de l'analyse du binaire pour extraire les appels/retours de fonctions ainsi que les instructions de rupture du flot (i.e. instruction de branchement).
Néanmoins les options du compilateur influencent grandement le code produit (-Os, -O3, …) et par conséquent la manière dont sont appelées les fonctions comme la taille des « Basic blocks » entre deux instructions de discontinuité. Cette production de code a aussi une influence sur la complexité des solutions CFI.

Le travail du PE consiste à évaluer l'influence des options du processus de compilation par l'analyse du code assembleur RISC-V sur des programmes de la suite de test IoT-EMBench [2] et ainsi proposer des stratégies de compilation pour lever des verrous dans la conception du schéma de protection développé dans le département SAS.

Compétences recherchées :

GCC ou LLVM
Assembleur RISC-V
C/C++ ou Python

Encadrements :
Olivier Potin / Jean-Max Dutertre / Jean-Baptiste Rigaud / Théophile Gousselot

Bibliographies :

[1] T. Chamelot, D. Couroussé, and K. Heydemann, "Mafia : Protecting the microarchitecture of embedded systems against fault injection attacks." Cryptology ePrint Archive, https://eprint.iacr.org/2023/1323 , 2023

[2] Embench.org, "Embench-iot github repository," 2019, https://github.com/embench/embench-iot

Durée : 1 mois

Environnement :
Ce stage de PE se déroule au sein du laboratoire Systèmes et Architectures Sécurisés (SAS).