COFFI

Intégrité du flot d'exécution
du logiciel à la microarchitecture

anr agence nationale de la recherche

Appel : AAPG

Année : 2018

Instrument : PRCE

Contact : olivier.potin@emse.fr

COORDINATEUR : Olivier POTIN

PARTENAIRES :
CMP-ARMINES / CEA tech / INVIA / Sorbonne Université

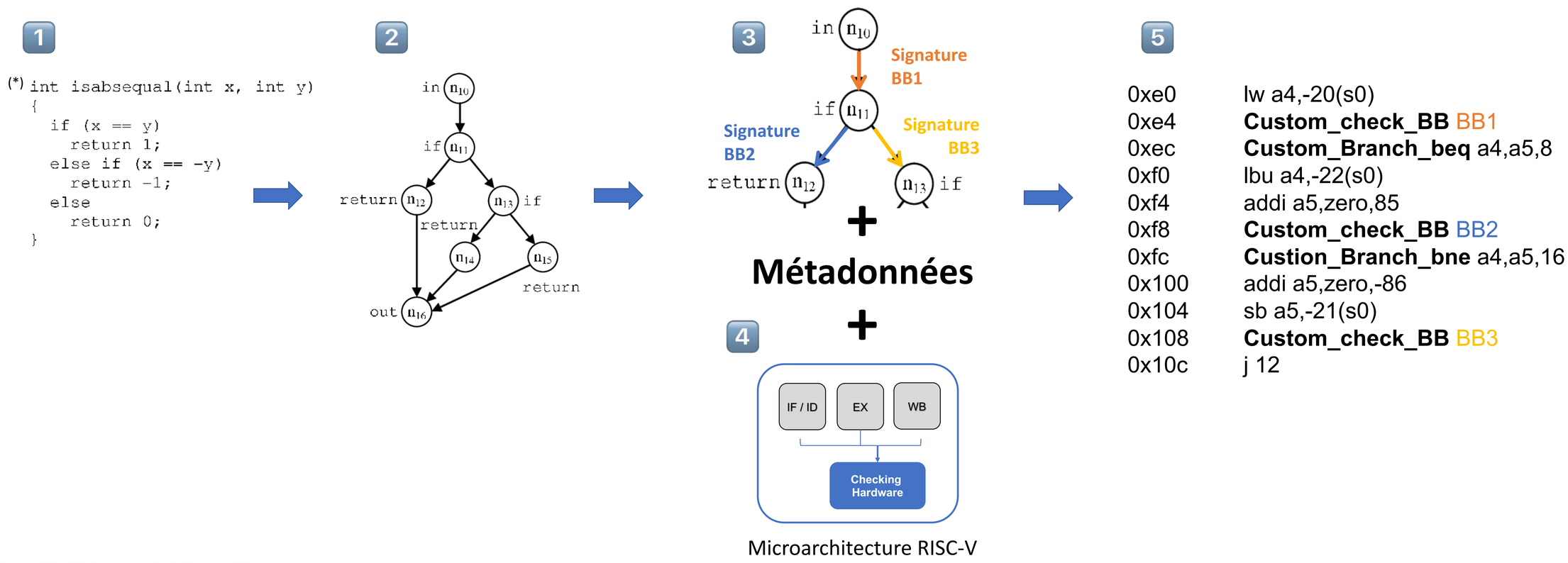
Résumé :
Les attaques en fautes, dans les systèmes embarqués, compromettent l'intégrité d'exécution d'un code par l'introduction de perturbations induisant une faute intentionnelle sur le programme ou ses données. Le projet COFFI propose différents schémas de protection garantissant cette intégrité en couvrant tous les niveaux structurels d'un système: matériel, ISA et logiciel.

CONTEXTE ET OBJECTIFS

Se protéger contre les attaques physiques et garantir l'intégrité d'exécution d'une application nécessite de concevoir des protections qui couvrent la frontière entre le logiciel et le matériel. Le projet **COFFI** vise le développement de schémas de protection exploitant les interactions entre le matériel et le logiciel pour offrir un plus haut niveau de sécurité tout en offrant de meilleurs compromis entre sécurité et performance.

MÉTHODOLOGIE

L'analyse statique du code de l'application (1) permet l'extraction d'informations sur les suites d'instructions et chemins d'exécution autorisés par le programme (Control Flow Graph - 2). Ces informations sont exploitées pour générer des métadonnées de sécurité comme des signatures dépendantes des instructions et/ou des chemins d'exécution (3). Ces signatures exploitent des connaissances de la microarchitecture du processeur open-source RISC-V. Les schémas de protection matériels et logiciels proposés permettent d'assurer les propriétés de sécurité : intégrité, authenticité et confidentialité. Ils reposent sur l'introduction de blocs matériels (4), d'instructions dédiées à la sécurité dans le code et de métadonnées (5).



RÉSULTATS et IMPACTS

Architectures RISC-V cibles	CV32E20 / CV32E40P / CVA6 - OpenHW Group
Propriétés de sécurité	Intégrité du flot de contrôle, intégrité de l'exécution, authenticité du code, intégrité et confidentialité du code
Publication & Communication	DATE 2022 / JAIF 2021
Impact industriel	1 dépôt de brevet

(*) Gold, Robert. "Control flow graphs and code coverage." *Int. J. Appl. Math. Comput. Sci.* (2010).

ARMINES · FROM RESEARCH TO INDUSTRY cea tech · INVIA Invia Secure Semiconductor Meyreuil · SORBONNE UNIVERSITÉ