COLLEGE ED MATHEMATIQUES
DOCTORAL STIC
PAYS DE LA LOIRE

Nantes Université

THÈSE DE DOCTORAT DE

NANTES UNIVERSITÉ

ÉCOLE DOCTORALE N° 641
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Électronique*

Par
Téo BITON

Execution control and anomaly detection in real-time embedded systems

Thèse présentée et soutenue à Nantes Université, le 3 novembre 2026.
Unité de recherche : IETR UMR 6164

Rapporteurs avant soutenance :

Mme. Karine HEYDEMANN	Experte Sécurité/HDR, Thales CDI
M. Guillaume HIET	Professeur des Universités, CentraleSupélec, IRISA

Composition du Jury :

Président :	-	
Examinateurs :	Mme. Karine HEYDEMANN	Experte Sécurité/HDR, Thales CDI
	M. Guillaume HIET	Professeur des Universités, CentraleSupélec, IRISA
	M. Loïc LAGADEC	Professeur des Universités, ENSTA Bretagne, Lab-STICC
	Mme. Clémentine MAURICE	Chargée de recherche HDR, CNRS
Dir. de thèse :	Sébastien PILLEMENT	Professeur des Universités, Nantes Université
Enc. de thèse :	Olivier GILLES	Ingénieur de recherche, Thales Research & Technology

COLLEGE ED MATHEMATIQUES
DOCTORAL STIC
PAYS DE LA LOIRE

Nantes Université

Titre : Détection d'anomalies du flot d'exécution au sein des systèmes embarqués temps-réels

Mot clés : Intégrité du flot de contrôle, attaques par réutilisation de code, sécurité matérielle, RISC-V

Résumé : Les vulnérabilités logicielles, qu'elles soient causées par des bugs ou l'utilisation de langages non sécurisés, représentent une source courante de menaces pour la sécurité des systèmes, permettant aux attaquants de détourner l'exécution des programmes et de compromettre l'intégrité du système à l'exécution. Les attaques par réutilisation de code (CRAs) exploitent spécifiquement les transferts indirects du flot de contrôle et redirigent l'exécution vers du code existant, rendant inefficaces les protections de mémoire non-exécutables. Le sujet principal de cette thèse est la détection dynamique des anomalies du flot de contrôle, à l'aide de mécanismes matériels. La thèse se concentre sur des solutions ayant un impact minimal sur le système, en termes de performances, d'utilisation des ressources matérielles, d'empreinte mémoire et de taille du code. Elle présente plusieurs mécanismes de sécurité matériels innovants visant à protéger les systèmes embarqués contre les CRAs. Tous les mécanismes proposés sont implémentés sur le CVA6, un cœur RISC-V open source, et évalués sur cible FPGA. Cela permet d'obtenir des informations concrètes sur leur efficacité, leur coût et leur applicabilité dans le monde réel pour sécuriser les systèmes embarqués modernes. La deuxième partie de la thèse se concentre sur l'analyse binaire, en mettant l'accent à la fois sur la compréhension des mécanismes des CRAs et sur l'évaluation de la vulnérabilité aux CRAs.

Title: Execution control and anomaly detection in real-time embedded systems

Keywords: Control-flow integrity, code-reuse attacks, hardware-based security, RISC-V

Abstract: Software vulnerabilities, whether caused by bugs or unsafe languages, represent a common source of security threats, enabling attackers to subvert program execution and compromise system integrity. Code-reuse attacks (CRAs) specifically abuse indirect control-flow transfers and redirect execution toward existing code, making non-executable memory protections inefficient. The primary topic of this thesis is the development of hardware-based mechanisms that detect control-flow anomalies. The thesis focuses on solutions with minimum impact on the system, with regard to performance, utilization of hardware resources, memory footprint and code size. It introduces several novel hardware security mechanisms aimed at protecting embedded systems from CRAs. All proposed mechanisms are implemented on the CVA6, an open source RISC-V core, the CVA6, and evaluated on FPGA prototypes. This offers concrete insights into their efficiency, cost, and real-world applicability for securing modern embedded and general-purpose systems. A second part of the thesis focuses on binary analysis, with a focus both on understanding the mechanisms of CRAs, and on vulnerability assessment to CRAs.