AVIS DE SOUTENANCE DE THESE
DE DOCTORAT

Le **24-11-2017**
A **14h** Amphi Palladium2

CEA Grenoble
17 rue des martyrs
38000 Grenoble

Soutiendra en vue de l'obtention du titre de Docteur de l'Ecole Nationale Supérieure des Mines de Saint-Etienne dans la spécialité : MICROELECTRONIQUE

Thierno Ousmane BARRY

Une thèse ayant pour sujet :

Sécurisation à la compilation de logiciels contre les attaques en fautes

MEMBRES DU JURY :

Président
(Le président est désigné le jour de la soutenance)

Rapporteurs :

Guilley	Sylvain	Professeur	TELECOM-Paris Tech
Rohou	Erven	Directeur de recherche	INRIA

Examinateurs :

POTET	Marie-Laure	Professeur	ENSIMAG, GRENOBLE INP
Cohen	Albert	Professeur	INRIA d'Informatique
de Grandmaison	Arnaud	Ingénieur	ARM
Heydemann	Karine	Maître de conférences	Université Pierre et Marie Curie
Robisson	Bruno	Ingénieur de recherche	CEA Cadarache
Couroussé	Damien	Ingénieur de recherche	CEA Grenoble

Thèse préparée dans le centre CMP-GC à l'Ecole Nationale Supérieure des Mines de Saint-Etienne.
Travail co-encadré par : ROBISSON Bruno

Destinataires : DRI, Accueil, SCIDEM, Centre,
D.CORTIAL « Le Progrès », 24 rue de la robotique – 42000 Saint-Etienne

Résumé :

L'objet cette thèse est la génération automatisée de protections logicielles contre les attaques par injection de fautes sur les systèmes embarqués.

Les approches "source" et "binaire" consistent à insérer les protections respectivement dans le code source et binaire de l'application.

Cette thèse explore l'utilisation d'une approche compilation consistant à intégrer les protections dans le "compilateur".

Nous avons proposé un compilateur basé sur LLVM permettant l'application automatisée, lors de la compilation, de plusieurs schémas de protection : (1) un schéma de tolérance aux sauts d'instructions, (2) un schéma d'intégrité de flot de contrôle (CFI) permettant de garantir la validité du chemin d'exécution suivi et (3) un schéma combinant CFI et intégrité des instructions, garantissant à la fois la validité du chemin d'exécution suivi mais aussi qu'aucune instruction le long de ce chemin n'a été sautée ou altérée.

Notre approche, basée sur un compilateur modifié, permet de faire coexister "protection de code" et "optimisation de code", permettant ainsi de générer un code binaire sécurisé et optimisé en termes d'empreinte mémoire et de temps d'exécution.

Nous avons développé un simulateur de faute afin de valider la robustesse de nos implémentations vis-à-vis des modèles de fautes considérés.

Cette thèse montre que l'approche compilation est un bon compromis entre l'approche source qui ne garantit pas la conservation des propriétés de sécurité dans le code binaire et l'approche binaire qui impacte considérablement les performances de l'application sécurisés.

Thierno BARRY, CMP