Multi-Objective Optimised Synthesis to Improve Cybersecurity (MOOSIC)

Porteur :	Roselyne Chotin, Sorbonne Université/Laboratoire d'Informatique de Paris 6
Consortium :	CEA Tech, LIP6, LIRMM, Secure-IC
Financement :	AAPG ANR 2018 - PRCE - CES Sécurité Globale et Cybersécurité
Durée :	4 ans du 01/10/2018 au 30/09/2022

Un Cheval de Troie Matériel (CTM) est un matériel malveillant introduit durant la conception ou la fabrication d'un circuit intégré (CI) par des entreprises tiers. Il représente une réelle menace, notamment pour la sécurité automobile et militaire. Les CTMs ont pour but de désactiver, de perturber ou de détruire le circuit concerné, ou bien de permettre la fuite d'informations confidentielles. De telles attaques représentent une perte de plusieurs milliards de dollars pour l'industrie des semi-conducteurs.

Il existe des contre-mesures pour lutter contre les CTMs que l'on peut diviser en deux catégories : la détection et la prévention. Depuis 10 ans, les recherches menées ont montré que la détection des CTMs était un défi majeur étant donné la nature furtive de la menace et les multiples formes que peut prendre un CTM. A contrario, la prévention consiste à modifier le flot de conception en tenant compte des problèmes de sécurité. Malgré son coût important, cela reste le meilleur moyen de contrer l'insertion de CTMs. Ainsi des méthodes de conception pour la confiance matérielle (Design for Hardware Trust ou DfHT) ont vu le jour récemment avec différents objectifs et impacts sur les performances.

Le projet MOOSIC propose une méthodologie dédiée à la sécurité, complètement intégrée dans le flot de conception habituel des CIs. Le but est de prendre en compte le plus en amont possible, non seulement les contre-mesures contre les CTMs, mais aussi les performances. Cela permet ainsi d'assurer que le comportement du CI soit garanti malgré la présence d'entreprises non dignes de confiance dans la chaîne de production du CI. Pour cela, le projet vise à établir et évaluer des propriétés de sécurité et les intégrer dans le flot de conception à l'aide de techniques d'optimisation multi-objectifs qui seront construites sur une modélisation mathématique du problème tenant compte à la fois des performances et des effets des CTMs. Cela permettra ainsi trouver un bon compromis entre le niveau de sécurité et les performances.

La méthodologie sera validée sur des cas d'usage provenant du milieu industriel. Le CI ainsi conçu permettra de lutter contre la cybercriminalité tout en maîtrisant les coûts additionnels.

Le consortium du projet est consistué de 2 laboratoires de recherche reconnus dans la conception des CIs (LIRMM et LIP6), d'un institut public (CEA Tech) dédié à la recherche technologique et de Secure-IC la "security science company".

Le projet est divisé en 4 lots scientifiques :

1. L'évaluation des architectures en terme de sécurité et les solutions matérielles permettant de l'augmenter (LIRMM)
2. La modélisation mathématique du problème (basée sur la théorie des graphes ou la programmaation mathématique) qui tient compte à la fois des contraintes et des objectifs (sécurité, surface, fréquence, consommation) et proposition de stratégies de résolution optimales pour l'insertion automatique de contre-mesures (CEA Tech)
3. L'intégration de la méthodologie tenant compte du modèle établi et des solutions matérielles trouvées (LIP6)
4. La validation sur des cas d'usage povenant du milieu industriel (Secure-IC)