Code automodifiant pour la sécurité des systèmes embarqués
Stage de Master 2

CEA/LIST/LIALP

Sujet

Notre laboratoire développe un outil appelé `deGoal` utilisé dans plusieurs contextes applicatifs et actuellement supporté sur une grande variété d'architectures. Il s'agit de faire en sorte qu'une application puisse modifier au vol tout une partie de son code, afin de tenir compte du contexte d'exécution et en particulier les données à traiter. La technologie `deGoal` permet d'obtenir des générateurs de code rapides et à très faible empreinte mémoire, ce qui permet d'ouvrir des domaines applicatifs jusque là inaccessibles à la génération de code, dont la cryptographie, et de cibler des plateformes très contraintes en ressources.

Ce stage se déroule dans le cadre du projet COGITO [1], dont l'objectif est d'étudier l'intérêt de la génération dynamique de code pour la sécurité logicielle. Dans ce cadre, nous envisageons la capacité de modifier le code à la volée comme un moyen d'apporter de la sécurité à des composants logiciels sécurisés, notamment contre les attaques physiques [2].

Une preuve de concept a déjà été réalisée sur AES et l'approche a été validée expérimentalement. Dans le cadre du stage, il s'agira :

1. d'améliorer la performance de l'implémentation existante
2. de mettre en œuvre un nouveau démonstrateur
3. de faire la validation expérimentale de l'efficacité apportée en termes de sécurité

Profil recherché

— expérience du développement C : si possible une bonne expérience de la programmation proche du matériel, et des techniques d'optimisation logicielles dépendantes du matériel cible

— connaissance des techniques de compilation classiques

— une connaissance de la cryptographie ou de la sécurité logicielle n'est pas requise, mais est un plus

Contexte

Le stage se déroulera dans le cadre du projet COGITO (ANR).

Le stage s'effectuera sur le site de Grenoble du CEA, au sein du laboratoire LIALP du CEA-LIST (Laboratoire Infrastructures et Ateliers pour le Logiciel sur Puces).

Le stage est indemnisé.

Contact

Damien Couroussé
CEA/LIST/LIALP
`damien.courousse@cea.fr`
+33 456 520 451

1. `http://www.cogito-anr.fr/`
2. `https://en.wikipedia.org/wiki/Side_channel_attack`, `https://en.wikipedia.org/wiki/Power_analysis`