Soutenance de thèse de Julien Proy

« Sécurisation systématique d'applications embarquées contre les attaques physiques »

La soutenance aura lieu en amphithéâtre HS002,
Lundi 17 Juin 2019 à 14h30, Campus G. Charpak Provence.

Composition du jury :

Mr Alexandre Berzati, INVIA, Encadrant
Mr Albert Cohen, Google et ENS, Directeur de thèse
Mr Damien Couroussé, CEA–LIST, Examinateur
Mr Jean–Max Dutertre, EMSE, Examinateur
Mr Louis Goubin, Université de Versailles, Rapporteur
Mme Karine Heydemann, Sorbonne Université, Directrice de thèse
Mr Erven Rohou, INRIA, Rapporteur

Résumé :

La sécurité des systèmes embarqués contenant des données sensibles est un enjeu crucial.
La disponibilité de ces objets en fait une cible privilégiée pour les attaques physiques, nécessitant l'ajout de protections matérielles et logicielles.
La recherche de réduction des coûts de développement pousse les industriels à opter pour du déploiement automatique de protections.
L'objet de la thèse consiste à étudier l'intégration de contre–mesures logicielles contre les attaques par faute dans les outils de développement, en particulier dans le compilateur, afin d'automatiser l'application de contre–mesures variées.
Pour cela, nous proposons deux schémas de protection génériques et automatiquement déployables contre ces attaques : un dédié à la sécurisation des boucles et le deuxième à la sécurisation du graphe d'appel.
Ces schémas spécifiques, intégrés dans un même compilateur (LLVM) permettent la sécurisation de parties sensibles et choisies du code limitant ainsi leur surcoût en performances.
Les fautes exploitables variant d'un composant à l'autre, nous proposons également une caractérisation des effets des fautes au niveau du jeu d'instructions sur une plateforme intégrant un processeur superscalaire typique des téléphones mobiles.
Ces travaux montrent la nécessité d'étudier les injections de faute sur des plateformes complexes, de concevoir de nouveaux schémas de protection adaptés, et de continuer à intégrer dans un même compilateur plus de schémas de sécurisation.