Sujet de Master en Cybersécurité, mars 2018

EMSEC, IRISA

Université de Rennes 1

Cybersécurité logicielle : Mise en place d'outils automatiques pour la lutte contre les attaques physiques

Vincent Migliore (EMSEC, IRISA)
Benoit Gérard (DGA)
Adeline Roux-Langlois (EMSEC CNRS, IRISA)

26 février 2018

1 Sujet

Depuis une vingtaine d'années, notre société a subi une importante transformation vers le numérique qui fait aujourd'hui partie intégrante de notre quotidien. Mails, réseaux sociaux, partage de contenu en ligne, il existe une multitude de services où nous sommes amenés à partager des informations qui peuvent être privées et sensibles. Ces informations doivent donc être protégées. La cryptographie, discipline dont le rôle est de proposer différents mécanismes de protections, doit cependant faire face à de nouveaux défis.

Premièrement, l'ordinateur quantique, qui exploite des propriétés quantiques pour réaliser des calculs. Celui-ci a récemment mis à mal de nombreuses constructions réputées sécurisées comme les chiffrements asymétriques basés sur RSA [RSA78], omniprésents sur le web, via notamment l'utilisation de l'algorithme de Shor [Sho95].

Deuxièmement, le problème des attaques dites physiques. Alors que la sécurité usuelle est basée sur la complexité de résolution de problèmes réputés difficiles, les attaques physiques utilisent certaines failles des composants pour modifier ou récupérer de l'information qui devrait rester secrète. Elles se retrouvent à différents niveaux, allant des attaques sur les caches de processeurs de type *FLUSH and RELOAD* [YF14], aux composants matériels par injection de faute [CP95] en passant par analyse des canaux auxiliaires [AARR03] [ZF05] [KJJR11]. Le chiffrement symétrique AES, également omniprésent sur le web, a fait par exemple l'objet de nombreuses attaques par timing sur les caches [Ber05] [BM06] [OS10].

En particulier, les attaques physiques par canaux auxiliaires [AARR03] [ZF05] [KJJR11] prennent une place de plus en plus importante. Le principe de ces attaques est basé sur le fait que l'exécution sur un composant matériel d'algorithmes crée des fuites (champ electromagnétique, consommation, ...) dont la lecture peut révéler des informations qui devraient rester secrètes.

Pour éviter de telles fuites, une solution standard consiste à utiliser des techniques dites de masquage. Au lieu de manipuler l'information secrète directement, ces techniques manipulent des variables dites partagées, possédant une partie de l'information secrète mélangée à du bruit. Cependant, l'évaluation de l'efficacité de telles mesures reste complexe, et les solutions couramment utilisées restent empiriques.

L'objectif du sujet du stage est la mise en place d'outils pour la protection de logiciels contre les attaques physiques, et plus particulièrement les attaques par canaux auxiliaires. L'équipe a développé en interne une implémentation protégée d'algorithmes de cryptographie post-quantique. L'objectif du stage est de prendre en main l'outil EasyCrypt afin de tester et de valider l'implémentation. L'étudiant pourra tirer profit des compétences de l'équipe sur les attaques par canaux auxiliaires, et des compétences des membres de l'INRIA ayant participé à l'élaboration de l'outil EasyCrypt.

2 Profil

L'étudiant recruté devra posseder des compétences solides en algorithmique et en programmation. ces compétences sont des prérequis indispensable afin de pouvoir prendre en main la syntaxe propre au langage EasyCrypt et de pouvoir convertir les implémentations actuelles dans la syntaxe EasyCrypt.

3 Contact

Les étudiants intéressés sont invités à envoyer CV et lettre de motivation à :
Vincent MIGLIORE, vincent.migliore [at] irisa.fr, EMSEC, IRISA, Université de Rennes 1.