technicolor

Technicolor R&D France Snc
975 av des Champs Blancs – CS 17616
35576 Cesson-Sévigné Cedex - France

tél. + 33 (0)2 99 27 30 00
fax + 33 (0)2 99 27 30 01

Proposition de stage de fin d'études – Année 2014
Ref: PSL_SCP_004

PSL_SCP_004 : « Techniques d'obfuscation pour les algorithmes de chiffrement à clé publique »

Summary of the subject

The goal of the internship is to study obfuscation techniques and propose new ones to protect against extraction of cryptographic keys from data memory. On an open platform like a PC, any software that performs cryptographic operations must, at some point, have the instructions and the key material loaded into the memory. A user can easily access that memory and then the key material. Obfuscation consists in hiding sensitive data, storing it in a modified representation in the code. Sensitive data are then recomputed during execution using a layer of complex code. Obfuscation forces an attacker to use reverse-engineering to locate and extract the keys from a memory dump.

Sujet détaillé

Contexte

Dans de nombreux cas d'utilisation, les systèmes de protection sont sujets à des attaques sur les machines hôtes sur lesquels les services de protection sont assurés. C'est le cas sur un PC par exemple, où les clés secrètes peuvent être facilement accessibles lorsque celles-ci transitent dans la mémoire vive. La protection des clés est un aspect essentiel de la sécurité de ces systèmes. Différentes techniques d'obfuscation ont été développées dans la littérature. Elles apportent une solution pratique et permettent d'atteindre, dans certains cas, un niveau de sécurité acceptable.

But

Le but du stage est l'implémentation obfusquée d'un algorithme à clé publique ainsi qu'une analyse de la robustesse de ces implémentations. Concernant les algorithmes de chiffrement, l'étudiant étudiera les crypto-systèmes tels que RSA ou ElGamal. Pour la signature numérique, il s'intéressera aux systèmes DSA et ECDSA.

Description des travaux

Le stage consiste à identifier un ou plusieurs algorithmes et d'étudier différentes techniques d'obfuscation ainsi que leurs performances. Cela impliquera notamment le choix de l'algorithme de chiffrement, du corps sous-jacent et de sa représentation, de l'arithmétique, ainsi que des techniques de masquage choisies.

Mots clés

Cryptographie, obfuscation, DPA, side-channel attacks.

Environnement de travail

Le stagiaire sera intégré à la cellule « Secure Design » du Laboratoire « Content Platforms & Security / Security & Content Protection » de Technicolor composé de 12 ingénieurs et chercheurs.
Le stage est basé à Cesson-Sévigné.

Profil du stagiaire / Compétences requises

Cryptographie, programmation en C, anglais technique

Durée et période du stage

6 mois, début du stage entre février er avril 2014.