Cryptographie basée sur l'identité

Encadrant :

Olivier Blazy : olivier.blazy@unilim.fr, (05 87 50 68 20)

Etablissement :

Université de Limoges, Laboratoire Xlim, équipe PICC / Cryptis.

Introduction :

La cryptographie a connu plusieurs évolutions au cours de sa longue existence. Auguste Kerckhoffs en 1883 a proposé les bases de la cryptographie moderne, en avançant dans son traité sur la cryptographie militaire que la sécurité par l'obscurité était une mauvaise idée ("Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi", "La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants").

Plus récemment, en 1976, Whitfield Diffie et à Martin Hellman ont proposé le principe de cryptographie asymétrique / à clé publique. Dans un tel système, au lieu d'avoir un secret commun partagé par les 2 participants, un interlocuteur possède un secret / une clé privée et publie une clé publique qui sera connue de tous. Un tel procédé permet de d'éviter de posséder un canal sécurisé préalable.

Cependant, notre monde moderne demande de plus en plus d'interactions avec des interlocuteurs divers et variés, et bien que les coûts de stockage soit en baisse, la multiplication des clés publiques à connaitre posent de nouveaux problèmes, comment les stocker efficacement, les mettre à jour, s'assurer que la base n'a pas été compromise, que la personne publiant la clé publique est bien qui il dit être…

Pour cela en 1984, Adi Shamir a proposé le principe de cryptographie basée sur l'identité. Dans celle-ci les utilisateurs sont enregistrés dans un système (une entreprise, une organisation …) avec une identité (humainement compréhensible, donc un email, un numéro de téléphone, …), et cette identité (avec une faible entropie) est l'unique information publique les concernant.

Le stage en lui-même :

Ce stage serait modulable autour de deux points :

- Implémenter divers schémas de chiffrements basés sur l'identité pour pouvoir comparer leur efficacité réelle.
- Comprendre, et améliorer les schémas de signatures basés sur l'identité.

Pour les étudiants hésitant entre un profil compilation / cryptographie, des résultats récents ont montré comment faire une recherche exhaustive pour construire certaines signatures (optimales sous un certain aspect) prouvable dans le modèle générique (c'est à dire où il n'existe pas de système linéaire pouvant mettre en défaut la sécurité du schéma). Il pourrait être très intéressant de comprendre cette méthodologie, et de l'appliquer à la construction de signature basée sur l'identité.

Profil Recherché :

Le candidat devra avoir un goût marqué pour la cryptographie et les questions de sécurité ; une certaine capacité d'abstraction est un vrai atout, et idéalement une maîtrise d'un langage de programmation comme C ou Java serait un net plus.

Dans le cadre de l'approche par recherche exhaustive, un langage comme Ocaml ou Prolog serait utile, ainsi qu'une certaine maîtrise de la notion de grammaire / langage.

Pour toute question n'hésitez pas à me contacter par mail