Smart Social Network
Rapport de projet SSI

26 février 2013

Table des matières

1 Introduction

De nos jours, les réseaux sociaux ont pris une grande ampleur sur internet et accueillent chaque jour de plus en plus d'adhérents. Le principe consiste à y créer un profil, y insérer des données que l'utilisateur désire partagées, telles que des photos, des vidéos, des messages, etc. Sur ce réseau, des « amis » seront ajoutés : ils pourront alors accéder à ces informations.

La problématique soulevée était de limiter la diffusion des informations à certaines personnes dans nos « amis », mais surtout limiter la diffusion d'informations vis à vis du réseau social lui-même. En effet, lorsque nous partageons une donnée, celui-ci détient cette information qu'elle soit définie comme privée ou non.

L'idée de ce projet était alors de limiter cette fuite d'information, afin de garantir la confidentialité des données des utilisateurs et ce, renforcé par une authentification forte. Nous nous concentrerons sur le réseau social Facebook puisqu'il est le plus utilisé.

La concrétisation du projet s'est traduite par le développement d'une extension pour le logiciel Mozilla Firefox permettant à l'utilisateur de gérer le chiffrement et le déchiffrement de ses données sur le réseau social Facebook, les traitements lourds étant confiés à une application Java.

Concernant l'authentification forte, nous avons utilisé des cartes à puce de type Java Card J3A (marque NXP) avec 40 Kilo-octets (Ko) d'EEPROM, via des lecteurs Omnikey 3121.

L'intérêt du projet était également d'analyser la sécurité de ces cartes à puce, à savoir la génération de nombres aléatoires, de clefs (sysmétriques et asymétriques), chiffrement, déchiffrement et signature. C'est cette même carte à puce qui contiendra à posteriori les données sensibles de l'utilisateur comme son identifiant, son mot de passe, sa clef privée... Le dialogue avec la carte se fait par l'intermédiaire d'un client Java : « SoftCard ».

Initialement prévu comme deux projets différents, un par groupe, il s'est avéré que nous travaillerions conjointement pour se concentrer sur un unique projet regroupant :

- l'étude et la mise en œuvre de solutions d'authentifications et de signatures par cartes à puce, proposé par Magali Bardet ;
- les solutions cryptographiques pour les réseaux sociaux, proposé par Ayoub Otmani ;