Solutions cryptographiques pour les réseaux sociaux

(Client: M. Otmani)

Le succès à travers le monde entier des réseaux sociaux et de partage d'information comme Facebook, LinkedIn, Google+, Twitter *etc.* soulève plusieurs questions concernant la protection de leurs utilisateurs. Pourtant tous ces réseaux se positionnent comme des plate-forme où des données sensibles et personnelles peuvent être stockées et échangées avec un risque potentiel de fuite d'information non contrôlée. La seule garantie qu'a un utilisateur réside dans sa confiance envers le prestataire de service, en l'occurrence ici, des entreprises comme Facebook ou Google qui collectent des informations sur des millions d'utilisateurs. Pire, les clauses d'utilisation que doivent valider tout utilisateur de ces plates-formes d'échange stipulent explicitement que les données stockées sur leur site sont leur propriété exclusive.

But du projet Le but de ce projet est d'étudier/proposer des solutions cryptographiques qui garantissent la protection de la vie privée des utilisateurs vis-à-vis de la plate-forme de stockage Facebook. L'idée est de donner le pouvoir à l'utilisateur pour qu'il contrôle lui-même quelle information doit être diffusée et à qui. On peut ainsi imaginer que toutes les données sensibles (comme les photos personnelles) soient systématiquement chiffrées qui ne peuvent être déchiffrées que par des utilisateurs appartenant à un certain cercle de confiance. Ainsi seules les personnes appartenant à ce cercle peuvent voir en clair les données. L'utilisateur doit aussi pouvoir contrôler la visibilité de ses relations : les personnes appartenant à un même cercle peuvent se voir et à l'inverse celles n'y appartenant pas ne voient aucune de ces relations (ou ne voient que des pseudonymes). De même certains commentaires du mur peuvent n'être visibles que pour certains certains cercles de confiance, *etc.*

Travail exigé

1. Analyser les exigences sécuritaires.
2. Étudier les différentes solutions existantes.
3. Production d'un rapport technique complet.
4. Implantation de la solution adaptée.
5. Intégration sur la plate-forme Facebook.

Le point de départ sera par exemple d'analyser le mécanisme proposé par dans l'article *A Security API for Distributed Social Networks*[1]. Il est important de se rappeler que le projet doit aboutir sur une application informatique opérationnelle démontrant la validité de l'approche adoptée sur le réseau social Facebook (ou autre suivant la difficulté rencontrée).

1. Les auteurs proposent aussi une API à l'adresse `www.lbs.cs.uni-saarland.de/sapi`