Étude et implantation d'un outil graphique de gestion de clefs PGP

proposé par Magali Bardet

14 octobre 2014

1 L'outil OpenPGP

Le standard OpenPGP, défini dans la RFC 4880, utilise une combinaison de cryptographie symétrique et asymétrique dans le but de fournir des services sécurisés pour de la messagerie électronique ou du stockage de messages (chiffrement, authentification, intégrité, signature électronique, fonctionnalités de gestion de clefs). Le standard définit un format de messages adapté à ces outils cryptographiques.

Le logiciel GnuPG (GNU Privacy Guard) est une implantation Open Source de OpenPGP. Le standard se base sur le logiciel PGP (Pretty Good Privacy) développé par Philip Zimmermann depuis 1991. C'est un logiciel libre de cryptographie qui permet de signer ou de chiffrer un document.

Pour pouvoir communiquer de manière confidentielle et authentifiée à l'aide de `GnuPG`, les utilisateurs doivent s'échanger de manière authentifiée leurs clefs publiques. Pour cela, `GnuPG` propose un modèle de *Toile de confiance]*, qui permet de gérer :

1. la validité d'une clef publique (i.e. la clef publique appartient bien à l'utilisateur identifié),
2. la confiance que l'utilisateur a en chaque personne dont il possède la clef publique.

Grâce à ce modèle, les utilisateurs peuvent s'échanger de nouvelles clefs, sans risque d'attaque du type « Man in the Middle », sur le principe « les amis de mes amis sont mes amis ».

2 Objectifs du projet

Il existe de nombreux éditeurs graphiques (comme `KGpg, GPA, Seahorse`). Cependant, ces éditeurs ne permettent pas une gestion fine des clefs (par exemple, choix des algorithmes de chiffrement symétriques utilisés), et la partie Toile de confiance n'est pas très intuitive.

L'objectif du projet est de réaliser une étude complète de `GnuPG` et du logiciel `OpenPGP` (en ligne de commande), d'en comprendre le fonctionnement détaillé et de rédiger un rapport illustrant toutes les fonctionnalités.

Il est ensuite demandé de proposer une interface graphique permettant à un utilisateur novice en PGP, mais averti en sécurité, de faire facilement des réglages techniques sur ses clefs et de pouvoir mettre en place sa toile de confiance. Le logiciel devra donc être à la fois pédagogique et précis (vous devrez en particulier livrer un document d'explications et de recommandations pour l'utilisation de votre logiciel). Il devra fonctionner sous kde et gnome. Il est demandé un effort particulier sur la partie « Toile de confiance » : un bel exemple de visualisation graphique d'une toile de confiance est donné sur le site archlinux.

Il est enfin demander d'effectuer des recherches sur les limites cryptographiques de PGP et de produire un document d'analyse de ces limites. On pourra en particulier implanter l'attaque sur les KeyId décrite dans le n° 75 de MISC, « Surveillance généralisée : aux limites de PGP ».

Enfin on étudiera les différentes possibilités suivantes :

— mise en place d'un serveur de clefs PGP « sécurisé »,
— utilisation des clefs PGP sur carte à puce,
— utilisation de clefs PGP pour de la connexion SSH ou SSL,
— étude de la législation (française ou d'autres pays) en terme d'utilisation, import ou export de matériel cryptographique (en particulier les restrictions),
— utilisation de GPG dans le logiciel Tor, ou dans les distributions linux comme ubuntu, Fedora, Archlinux.