GPG: Présentation

Par jean-sébastien HUBERT,
pour l'association GRAL (GUL Réunionnais).
Révision 2 du 04/09/2004

Introduction

- Le site web: http://www.gnupg.org/
- Gpg est un logiciel libre appartenant à la FSF.
- Son but est d'être une alternative viable à PGP.
- Il respecte la norme RFC2440 (d'OpenPGP).
- Il permet de chiffrer / signer / créer et gérer des « réseaux de confiance »
- Il est utilisé dans de nombreuses applications: rpm, thunderbird, sylpheed.
- Il est autorisé en France (voir « #Aspect Légal»)
- Il existe sur toutes les plates-formes (merci gcc et les outils GNU ;)

GPG: chiffrement

- L'histoire de la cryptographique remonte à l'empire romain, voir même encore avant. Quelle personne n'a pas besoin, un jour ou l'autre, de savoir qu'un message ne pourra être lu QUE par le destinataire ayant la « clef » ou « méthode » de déchiffrement?
- La faiblesse du chiffrement était auparavant due aux algorithmes. En effet, point d'ordinateurs en 1900, il fallait qu'un Homme puisse retrouver le message original rapidement. Toute la protection du message reposait alors sur « la méthode » utilisée pour chiffrer, Par exemple, remplacer une lettre par celle d'après. Mais si un ennemi connaissait cette méthode (ou algorithme) il pouvait facilement retrouver le message.
- Aujourd'hui, on ne peut garder secret l'algorithme. La solution??? assurer la protection par la difficulté à trouver la « clef » qui permet de déchiffrer le message. Mais un problème subsiste: transmettre la clef au destinataire de façon sûre.
- GPG peut utiliser, en plus du traditionnel « chiffrement par clef secrète » (il faut transmettre la clef au destinataire, d'où des risques d'interception) un autre système, introduit par PGP: le chiffrement par clef publique.
- Cette méthode, dite « asymétrique » utilise au choix deux algorithmes: RSA ou ElGamal (par défaut dans Gpg). Tout repose sur la factorisation de grands nombres premiers, et donc la difficulté à trouver l'un des deux en ne connaissant que le produit.

GPG: clefs secrètes/publiques

- Quand vous utilisez gpg pour la première fois, vous devez générer un trousseau de clefs. Celui-ci contient une clef publique et une clef privée (=secrète).
- La clef publique: utilisée pour chiffrer un message ou authentifier une signature.
- La clef secrète: utilisée pour déchiffrer le message ou générer une signature.
- La clef publique doit être transmise sur un « serveur de clefs » (par exemple **pgp.mit.edu**). Ce serveur fait parti d'un réseau de machines qui se synchronisent entre elles (si vous envoyez votre clef publique sur pgp.mit.edu, elle sera copiée sur tous les autres serveurs auquel appartient pgp.mit.edu)
- La clef secrète (qui est d'ailleurs protégée par un mot de passe) doit rester en lieu sûr, car c'est **elle** qui est utilisée pour signer les messages ou décrypter tout document chiffré avec la clef publique correspondante.

Gpg: un petit schéma

Clef secrète de A

Signature

Déchiffrer un message crypté avec la clef publique de A

Résultat: Message déchiffré et/ou signé

Clef publique de A

Vérifier une signature faite par la clef secrète de A

Chiffrer un message

Résultat: message chiffré et/ou contrôlé

Gpg: utilisation courante

- **Voilà, vous avez votre paire de clefs! Et maintenant????**

  -> Procurez-vous les clefs publiques de vos contacts !!!!!!!!!!

- **Pourquoi?** Pour pouvoir chiffrer des messages!
- **Comment?** En chiffrant le message avec la clef publique du destinataire.
- **Exemple:**

  Admettons que Paul et Gilles ont leurs clefs privées/publiques

  Paul donne sa clef publique à Gilles. Et Gilles donne sa clef publique à Paul.

  Paul veut envoyer un document confidentiel à Gilles. Comment faire?

  Chiffrer le document confidentiel avec la Clef publique de Gilles! Car seule la clef secrète de Gilles peut « déchiffrer » tout document crypté avec la clef publique correspondante (soit celle de Gilles)

- **Où?** Soit en utilisant un serveur de clefs, soit en demandant à la personne ;)

Gpg: utilisation courante (suite)

- **Mais? Comment faire pour retrouver une clef publique sur un serveur de clefs? Et si quelqu'un a le même nom? Ou la même adresse email?**

  C'est simple: en fait, une clef publique dispose de ce que l'on appelle une « **empreinte** » (ou **fingerprint**), c'est une suite de nombres hexadécimaux qui identifie une clef publique. Donc, si vous devez télécharger une clef publique de quelqu'un, demandez-lui son empreinte !

  Normalement, pour plus de facilité, on ne donne que les **8 derniers chiffres** de l'empreinte. Cela permet, par exemple, de les mettre sur une carte de visite ;-)

Gpg: signons nos clefs!

- Et oui, c'est bien beau de s'échanger les clefs publiques, mais encore faut il être certain de l'identité de la personne qui vous donne sa clef (publique)!
- La **Key-signing party** est là pour ça!

  Le concept: tout le monde vient avec son empreinte (de sa clef publique) et une pièce d'identité. Généralement, l'empreinte est sur une carte de visite (ou un bout de papier ... au pire).

  Ensuite, il faut « **donner** » ses empreintes aux autres participants (en justifiant que vous être bien la bonne personne. Par exemple si vous vous appelez « pif le chien » et que votre clef publique indique « hercules le chat » ça ne pourra pas aller ;-)

  Une fois de retour chez vous, téléchargez les clefs publiques des personnes qui vous ont donné leurs empreintes (et qui ont justifié leurs identités) et signez leur clef publique AVEC votre clef secrète.

  Enfin, renvoyez leur clef publique sur un serveur de clef. Vous verrez apparaître sur le serveur leur clef « signée » par vous-même. Voilà, vous venez de créer un petit réseau de confiance :)

GPG: le réseau de confiance

- Quel est l'intérêt d'un réseau de confiance? Comme cela a été dit juste avant, il permet de s'assurer que les personnes se connaissent entre elles, qu'il n'y a pas usurpation d'identité.
- Un exemple de réseau de confiance?

  Le projet Debian! Et oui, pour devenir développeur Debian, il faut, en outre, qu'un Développeur Debian signe votre clef (et donc qu'il vérifie votre identité) sans cela, vous ne pourrez faire parti du projet Debian. Une carte géographique est disponible ici -> http://www.debian.org/devel/developers.loc.fr.html regardez bien en bas .. rien à la Réunion mais quelqu'un en Antarctique !

GPG: les outils graphiques

- Il existe de nombreux outils « graphiques » pour gérer vos clefs et votre trousseau (qui contient les clefs publiques de vos contacts) voici une liste:
- Sous Windows:

  WinPT (http://winpt.sourceforge.net/fr/)
- Sous Linux:

  Kgpg (inclus dans la suite KDE3.2 et supérieur)

  Gpa

  SeaHorse

  N'oubliez pas que les MUA (Clients de courrier électronique) supportent la signature et le chiffrement de messages!:

  Thunderbird (avec le module enigmail/enigmime)

  Kmail

  Sylpheed/Sylpheed-claws etc..

Aspect légal

- Nul n'est censé ignorer la loi (c'est discutable et facile à dire mais bon)
- L'utilisation de la cryptographie est libre, selon l'article 30(I) du numéro 2004-575 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (Loi pour la confiance dans l'économie numérique).
- Extrait (article 31 de la loi no 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (1) parue au J.O n° 266 du 16 novembre 2001 page 18215
- Après l'article 11 de la loi no 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, il est inséré un article 11-1 ainsi rédigé :
- « Art. 11-1. - Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en oeuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.
- « Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30 000 Euro d'amende.

Pour finir

- Cette présentation est libre de droit tant que vous ne « vendez » pas le contenu(vous pouvez faire payer les frais d'impression mais le contenu de ce document doit rester gratuit).
- Si vous voulez distribuer cette présentation, ajoutez le fichier original (au format OpenOffice Impress) pour que n'importe qui puisse modifier/corriger le document.
- Des remarques? Écrivez-moi sur jshubert@free.fr