Module PGP
(Pretty Good Privacy)

IUT Béziers, dépt. R&T © 2012-2023
http://www.borelly.net/
Christophe.BORELLY@umontpellier.fr

Généralités

- PGP (Pretty Good Privacy) a été créé par Phil Zimmerman en 1991.
- RFC 1991 (1996), RFC 2440 (1998) puis RFC 4880 (2007).
- Il permet de crypter/décrypter des fichiers, des messages email et aussi d'authentifier des utilisateurs.
- PGP fourni aussi les fonctions de génération de certificat et de signature électroniques.
- PGP utilise de la cryptographie symétrique (rapidité du chiffrement) et de la cryptographie asymétrique (sécurité de l'échange de clés).

Logiciels

- **GnuPG** (Gnu Privacy Guard) est la version Libre de PGP (RFC 2440).
  - http://www.gnupg.org/
- **GPA** : GNU Privacy Assistant
- **Kleopatra** (KDE) : Certificate Manager and Unified Crypto GUI
- **GPG4Win** (GnuPG, Kleopatra et GPA)
  - http://www.gpg4win.org/

Trousseaux de clés

- Les clés sont stockées dans des fichiers pubring.pgp et secring.pgp (e.g. dans ~/.gnupg).
- Une clé privée ne peut pas être restaurée à partir d'un fichier secring.pgp.
- Si un utilisateur perd sa pass-phrase, sa clé est perdue !!!

Fonctionnement du cryptage

- Le cryptage fonctionne suivant le principe suivant :
  - Compression des données.
  - Création d’une clé secrète de session.
  - Cryptage des données compressées.
  - Cryptage de la clé de session avec la clé publique du destinataire.

Compression

- Cette étape permet de réduire le temps de transmission des données, et améliore également la sécurité.
- En effet, la compression détruit les modèles du texte (fréquences des lettres, mots répétés). Ces modèles sont souvent utilisés dans les analyses cryptographiques.

Chiffrement du message

- Une clé de session aléatoire est générée, et le message est chiffré par un algorithme symétrique (**AES**, CAST5, BLOWFISH, Camelia, 3DES, ...).
- La clé de session est chiffrée en utilisant la clé publique du destinataire (RSA, ELG, DSA, ECDH, ECDSA, EDDSA).

Décryptage

- Seul le destinataire d'un message crypté avec PGP peut décrypter la clé de session (car lui seul possède la clé privée associée à la clé publique qui a été utilisée pour crypter la clé de session) et donc par la suite le message.

Signature électronique

- Quand des données sont cryptées avec la clé privée d'un utilisateur, on peut vérifier l'identité de l'émetteur du message :
  - Si la signature peut être décryptée avec la clé publique de l'émetteur.
- En général, c'est un hash du message (message digest) qui est signé (taille fixe).

Certificat PGP

- Un certificat PGP contient au moins :
  - Un numéro de version
  - Une clé publique (RSA, DSA, ElGamal...)
  - L’identité du propriétaire
  - L’auto-signature des données
  - La période de validité
  - L’algorithme de chiffrement préféré (AES, CAST5, 3DES, ...).

Serveurs de clés PGP

- Ces serveurs permettent de publier et/ou récupérer une clé publique sous la forme d'un certificat PGP.
  - https://keyserver.ubuntu.com/, https://www.rediris.es/keyserver/, http://the.earth.li/pgp_lookup.html, ...
- Contrairement à une PKI X.509 (relation de confiance de type arborescente), il n'y a pas d'autorité centrale de certification, mais un grand rôle est donné à la proximité sociale (i.e. les amis de mes amis sont mes amis).

Niveaux de confiance

- Il y a 5 niveaux de confiance dans PGP :
  - Confiance ultime
  - Confiance complète
  - Confiance marginale
  - Aucune confiance
  - Inconnue

Validité d'une clé

- Confiance ultime
- Signée par 1 clé de confiance complete
- Signée par 3 clés de confiance marginale
- Le chemin des signatures de cette clé jusqu'à une clé de confiance ultime est inférieur à 5

Révocation de clé

- Une clé (certificat) PGP/GPG possède une période de validité.
- Cependant, on peut révoquer une signature sur une clé (ou la clé entière) pour diverses raisons (perte de confiance, compromission de la clé privée, perte de la pass-phrase, etc...).

S/MIME

- S/MIME (Secure/Multipurpose Internet Mail Extensions) est une norme de cryptographie et de signature numérique de courriels encapsulés au format MIME.
- S/MIME est un standard qui s'appuie sur les certificats numériques X.509.
- Outil : `gpgsm`
- Trousseau de clés : `~/.gnupg/pubring.kbx` et `~/.gnupg/private-keys-v1.d/`

Références

- http://www.gnupg.org
- http://www.gpg4win.org/
- http://www.gnupg.org/gph/en/manual.html
- http://en.wikipedia.org/wiki/PGP
- http://en.wikipedia.org/wiki/GNU_Privacy_Guard