TP Arichitectures de Sécurité
GPG
Aurélien Monnet-Paquet - Francesco Furfaro

1 Prise en main de PGP

1a)

1. gpg --gen-key
2. gpg --gen-revoke francesco.furfaro.ujf@gmail.com La création d'un certificat de révocation permet de révoquer une clé si celle ci devient compromise. Le fait de le générer maintenant permet d'anticiper sa révocation et etre sur de pouvoir la révoquée en temps voulu.
3. gpg --list-key : 2048D/266835E0
4.
    a. Empreinte : E7DD 1115 098F 099F 10CD FCB8 54E2 DDC0 2668 35E0
    b. addkey RSA 4096 4
    c. setpref SHA512 SHA384 SHA256 SHA224 AES256 AES192 AES CAST5 ZLIB BZIP2 ZIP Uncompressed
    d. addphoto (photo de taille 240*288)
    e. primary (boris -> boris@jenexistepas.com)
    f. uid 3 -> placeboris comme utilisateur principal

5. On enchaine des deluid 1 sur l'image et le fake user.
   expire (avec 1y) pour la clé principale et la sous clé
   Nous avons choisi un an car cela nous semble raisonnable comme delai.

6. gpg --export francesco.furfaro.ujf@gmail.com > mykey.asc

1b)
Nous avons importer la clé d'un autre groupe avec la commande : gpg --import key.txt
Puis nous avons assigné une confiance : trust 4 (confiance complète)
Nous avons signé une clé d'un autre groupe grace a la commande : gpg --default-key FD… --edit-key puteau...
Ensuite nous avons signé un message (gpg --clearsign message.txt) avec notre clé privée puis envoyé ce message à un autre groupe. Ce groupe à pu vérifier ce message avec notre clé publique.
Un autre groupe nous a envoyé un message signé et on pu verifié la signature grace a la commande : gpg --verify message.txt

1c)
Pour chiffrer un message on utilise la commande : gpg -e message
Pour déchiffrer un message on utilise la commande : gpg -d message > message_en_clair.txt

2 Analyse des fichiers OpenPGP

2a) Dissection d'un paquet OpenPGP

1. Il s'agit d'un paquet au format ancien (le bit 6 est à 0). Son type est "Public key packet" car le packet tag est "0110" (du deuxième au cinquième bit du premier octet). La taille du paquet est de 814 octets. Le fichier contient plusieurs paquets (Public key Packet, User ID Packet, Signature Packet, Signature Packet, Public subkey Packet).
2. Le corp du paquet contient la date de création de la clé publique. L'algorithme utilisé pour la signature (pub 17).

2b) Dissection d'un fichier OpenPGP
Nous avons utilisé pgpdump pour dissequé les paquets.
Disponible à cette adresse : http://www.mew.org/~kazu/proj/pgpdump/en/