DÉPARTEMENT
Sciences Informatiques

Licence Pro R&S
2012–2013
Chiffrement et authentification
T.T. Dang Ngoc
dntt@u-cergy.fr

TD3- Applications

1 Hachage : MD5/SHA

- Créez un fichier texte dans lequel vous y écrirez un petit texte
- À l'aide de la commande `md5sum` calculez son empreinte
- Recalculez son empreinte toujours à l'aide de la commande `md5sum`
- Modifiez très peu ce fichier (remplacez un caractère par exemple)
- Recalculez son empreinte toujours à l'aide de la commande `md5sum`

Même exercice avec `sha1sum`, `sha256sum`, `sha384sum` et `sha512sum` Comparez la taille des empreintes.

2 GPG

GPG est la version Open-Source de PGP.

1. Créez votre paire de clef (utilisez l'algorithme DSA-ElGamal) avec une clef de 2048 bits
2. Listez votre trousseau de clefs publiques et votre trousseau de clefs privés
3. Exportez votre clef publique et envoyez la par mail à votre camarade (qui fera de même de son côté)
4. Importez la clef publique de votre camarade
5. Listez votre trousseau de clefs publiques et votre trousseau de clefs privés
6. Créez un fichier texte.
7. Chiffrez le à l'aide de la clef publique de votre camarade et envoyez lui par mail le texte ainsi chiffré.
8. Recevez de même le texte chiffré avec votre clef publique du texte que vous a aussi envoyé votre camarade.
9. Déchiffrez le à l'aide de votre clef privée.
10. envoyez un texte en clair signé avec votre clef privée.
11. vérifiez qu'un texte signé par votre camarade est bien de lui.

Utilisation de GPG

1. Créer une paire de clé avec gpg
   - création d'une paire de clé : `gpg --gen-key`
   - connaître la liste des clefs publiques : `gpg --list-key`
   - connaître la liste des clefs privées : `gpg --list-secret-keys`

Toutes les clés existantes sur le système apparaîtrons et auront chacune une ligne avec : `pub 1024D/num_key 2008-01-14`

- supprimer une clé privée : `gpg --delete-secret-keys id_key`
- supprimer une clé publique : `gpg --delete-key id_key`
- exporter une clé publique : `gpg --armor --export id_key > publicKey.asc`
- exporter une clé privée : `gpg --armor --export-secret-key id_key > privateKey.asc`

– importer une clé publique sur le système : `gpg --import publicKey.asc`
– importer une clé privée : `gpg --import --allow-secret-key-import privateKey.asc`
2. Cryptage de fichier avec une clé
– crypter un fichier : `gpg --recipient id_key --encrypt --armor monfichier`
– décrypter un fichier : `gpg --decrypt monfichier > nouveaufichier`
3. Signature d'un fichier
– signer un fichier en chiffrant : `gpg --armor --sign monfichier`
– signer un fichier sans chiffrer : `gpg --armor --clear-sign monfichier`
– vérifier la signature d'un fichier : `gpg --verify monfichier`

3 SSH

Vous travaillerez par binôme. Soit *login1* sur la *machine1* d'adresse IP *ip1* et *login2* sur la *machine2* d'adresse IP *ip2*.

3.1 Utilisation simple de ssh

Depuis la machine1, connectez-vous sur la machine2 à l'aide de la commande `ssh login2@ip2`. Constatez que vous êtes logiquement connecté à l'autre machine.
Regardez le fichier `.ssh/known_hosts` de `login1@ip1`, que signifie son contenu ?

Déconnectez-vous et reconnectez-vous à `login2@ip2` en utilisant l'option `-v` de ssh.

Création d'une paire de clés

Sur `login1@ip1`, créez une paire de clefs (publique, privée) à l'aide de la commande :

```
ssh-keygen -t dsa
```

Régardez les fichiers `id_dsa` et `id_dsa.pub` Que signifient-ils ?

Déposez la clef publique générée sur la machine2 dans le fichier `.ssh/authorized_keys`. Connectez-vous depuis `login1@ip1` sur `login2@ip2`. Que se passe-t-il ?

Forward X11

Connectez-vous à `login2@ip2` avec l'option `-Y` de `ssh`. Lancez des applications graphiques (xterm, firefox). Que constatez-vous ? Où tournent ces applications ?

4 telnet

Pour faciliter les interceptions, vous brancherez toutes vos machines sur les hub.
Vous êtes ici dans un environnement non-sécurisé (risque d'écoute sur le réseau) et vous n'avez pas la possibilité d'utiliser un protocole chiffré comme SSH (par exemple, vous utiliser un ordinateur en libre service ne possédant que telnet).

Vous utiliserez l'option `-d` à chaque fois que vous lancerez un client `telnet` afin d'avoir un maximum d'information sur le déroulement de la session.

4.1 telnet classique

Utilisez avec `wireshark` pour capturer les paquets transitant entre deux machines utilisant le protocole telnet de base. Comme la version de telnet installée sur votre système utilise quand même du chiffrement (nouvelle version de telnet), vous allez pour le besoin du TP forcer la commande à adopter son comportement original (sans aucun chiffrement) en tapant :

```
telnet -d -Xsra -y -N machinedistante
```

- -Xsra : forcer telnet à ne pas utiliser de chiffrement pour l'authentification
- -y : forcer telnet à ne pas utiliser de chiffrement pour les données
- -N : pas de résolution DNS

Si le serveur telnet n'est pas lancé sur vos machines, il faudra le lancer une fois pour toute en décommentant la ligne adéquate dans le fichier `/etc/inetd.conf` et en forçant inetd à relire sa configuration par la commande

```
killall -HUP inetd
```

Vérifiez que vous pouvez ainsi intercepter :

1. le login et mot de passe d'une session
2. tous les messages échangés lors de la session.

4.2 telnet avec OPIE

One Time Passwords in Everything (OPIE) est un kit d'authentication permettant d'utiliser les mot de passe jetables S/KEY avec différents services Unix nécessitant un mot de passe.

Vous voulez accéder à votre compte `tp` sur votre machine `PCa` sécurisée depuis un `PCb` non sécurisé (coordonnez-vous avec un camarade) par telnet avec l'hypothèse que le réseau est non-sécurisé (et donc que la communication entre les deux peut être écoutée).

On considère ici trois types de mots de passe :

1. le mot de passe demandé par l'application (ici le mot de passe UNIX du compte que vous voulez utiliser). Pour des raisons de sécurité évidente, vous ne voulez pas qu'il transite en clair sur le réseau.
2. le mot de passe permettant de générer les clefs jetables
3. les mots de passe jetables générés avec OPIE à partir du mot de passe de génération précédent.

Initialisation de la connexion sécurisée

Sur votre machine `PCa` sécurisée comportant votre compte, vous devez initialiser OPIE :

```
opiepasswd -c -f -s graine
```

Votre mot de passe (secret pass phrase) sera alors initialisée sur votre machine `PCa`. Une fois ceci rentré, deux lignes vous seront affichées :

- la première ligne (commençant par ID) affiche votre login, un compteur d'itération (on en est au nième mot de passe jetable, par défaut 499) et une graine.
- la deuxième ligne vous donne votre premier mot de passe jetable.

L'association utilisateur graine, mot de passe haché est enregistré dans le fichier `/etc/opiekeys` (effacer l'entrée en cas d'erreur de manip).

Génération de mots de passe jetables

Sur une machine sécurisée, vous pouvez générer les n mots de passe jetables suivants à l'aide de la commande

```
opiekey -f -n nb_mdp_a_generer num_dernier_mdp graine
```

ou directement

```
opiekey -f num_mdp graine
```

Ces mots de passes recopiés (à la main sur un papier) pourront ensuite être utilisé depuis une machine non sécurisée.
Générez 3 mots de passe jetables.

Utilisation de mots de passe jetables

Sur la machine `PCb` non sécurisée, vous lancerez telnet non sécurisé (avec `telnet -d -Xsra -N -y` *`adresse_machine`* vers la machine `PCa`. Vous constaterez qu'après que vous ayez tapé votre login, telnet vous affichera une séquence de type

```
otp-md5 num_mdp graine ext
```

Il vous suffira de recopier le mot de passe correspondant au numéro demandé pour accéder à votre compte. (pour ne pas vous tromper dans la frappe, en tapant la touche "Entrée" après la première demande de mot de passe, vous arrivez dans le mode "Echo On" où ce que vous tapez au clavier vous est affiché à l'écran)

Vérifiez que si vous relancez un autre `telnet` que le mot de passe précédent ne marche plus et que le numéro de séquence du mot de passe demandé a changé.

(Notez que le mot de passe jetable vous garantie juste qu'un pirate interceptant votre connexion et donc ce mot de passe, ne pourra rien en faire. Par contre, toute la session reste toujours en clair...)

Regardez le fichier `/etc/opiekeys` pour voir ce que le serveur conserve comme information au fur et à mesure de l'utilisation des mots de passe jetables.