M1 2015 - 2016

Introduction à la Sécurité **TP 5**

Exercice 1 - GnuPG

GnuPG (ou GPG, pour GNU Privacy Guard) est une implémentation du standard OpenPGP défini dans la RFC 4880. Il permet à ses utilisateurs de transmettre des messages signés ou chiffrés. Cela permet ainsi de garantir l'authenticité et l'intégrité dans le premier cas ou, dans le second cas, la confidentialité du message.

But du TP : Prendre en main l'interface en ligne de commandes de gpg et tenter de comprendre la différence entre la chaîne de certification X.509 d'openssl qui régit la confiance et la notion de confiance proposée par gpg. Des plugins comme enigmail pour thunderbird en simplifient l'utilisation mais il est utile de comprendre le fonctionnement "à la main" de cet outil.

Questions : Pour toutes les questions suivantes, reportez-vous à la documentation de gnupg. Voir, par exemple, `http://www.gnupg.org/howtos/fr/index.html`. Pensez à utiliser l'option *-armor* de gpg pour éviter les problèmes de codage de caractères. Ce TP est noté, vous devez rendre un fichier (par binôme) contenant pour chaque question les commandes utilisées ainsi qu'une description des différents paramètres.

1. Créez une paire de clés ainsi qu'un certificat de révocation pour Alice puis pour Bob en prenant soin de les rendre transmissibles.
2. Alice exporte sa clé publique sous forme d'un fichier ASCII et le transmet à Bob par mail.
3. Bob importe la clé reçue d'Alice.
4. Bob vérifie son trousseau.
5. Bob, qui connaît la clé d'Alice, rédige un message, le chiffre puis lui transmet.
6. Alice déchiffre le message qu'elle a reçu.
7. Alice lui répond par un message signé mais non chiffré (pour plus de lisibilité, utilisez l'option *-clearsign* pour éviter la compression du message).
8. Bob vérifie l'intégrité de ce message et l'authenticité de la signature. Cependant, comme la signature d'Alice n'est pas certifiée, il obtient un avertissement.
9. Pour mieux valider la signature d'Alice, Bob décide de la signer pour la certifier (option *-edit-key*).
10. Il vérifie à nouveau l'intégrité et l'authenticité de ce message et il ne devrait plus avoir d'erreurs.
11. Il renvoie à Alice sa clé publique certifiée pour qu'elle puisse la transmettre à d'autres utilisateurs.

12. Alice envoie ensuite à Bob un message chiffré et signé.
13. Bob le lit et le vérifie.
14. Comment Charles, un autre utilisateur, peut entrer en lice et communiquer avec Alice et Bob ? Quelle confiance accorde-t-il à la clé d'Alice ? de Bob ?
15. Les clés des personnes suivantes ont été exportées sur le serveur `http://pgp.mit.edu` : `Alice@ie2000.fr`, `Hakim@ie2000.fr`, `Bernard@ie2000.fr`, `Stephane@ie2000.fr`, `Francois@ie2000.fr`, `Chloe@ie2000.fr` et `Elodie@ie2000.fr`.
    a) Allez sur le site du serveur vérifier les propriétés de chacune des clés exportées (date de création, date d'expiration, les personnes qui les ont signées...).
    b) François reçoit un email d'Elodie qu'il ne connaît pas. Peut-il être assuré que ce mail provient vraiment d'elle ? Pourra t-il donc lui faire confiance ?
    c) Tracez le graphe de reconnaissance de signatures : une arête d'Alice à Bernard indique qu'Alice a signé la clé publique de Bernard (Alice fait confiance à Bernard avec un certain niveau).
    d) Tracer le graphe de signature des clés publique : la relation Alice $\rightarrow$ Bernard indique que si Bernard reçoit un message signé avec la clé d'Alice, il est en mesure de s'assurer que le message vient bel et bien d'Alice. Quel est le rapport entre ce graphe et le graphe de reconnaissance de signatures ?
16. L'élaboration d'un réseau de confiance nécessite des algorithmes spécifiques pour valider les clés (relations de confiance). Une clé est considérée comme valide si vous l'aviez signée personnellement. L'algorithme le plus flexible retenu est le suivant : Une clé K est considérée comme valide si elle remplit deux conditions :
    — elle est signée par suffisamment de clés valides, c'est-à-dire si :
        • vous l'avez signée personnellement
        • elle a été signée par une clé à laquelle vous accordez toute votre confiance
        • elle a été signée par trois clés auxquelles vous accordez une confiance marginale.
    — le chemin des clés signées conduisant de K jusqu'à votre propre clé mesure moins de cinq étapes.

    Reprenez le graphe de reconnaissance de la question précédente, puis étudiez la validité des clés, du point de vue d'Alice, dans les cas suivants :
    a) Confiance complète en Stéphane.
    b) Confiance complète en Bernard, Chloé et Elodie.
    c) Confiance marginale en Bernard et Stéphane.
    d) Confiance marginale en Chloé et Stéphane.
    e) Confiance marginale en Bernard, Chloé et Stéphane.