TD8 – Sécurité et protocoles cryptographiques (2ème partie)

{Emmanuel.Godard, Yann.Esposito}@lif.univ-mrs.fr

1 décembre 2005

☞ Le but de ce TD va être de se familiarisé avec les crypto-systèmes et en particulier les cryptosystèmes à clef publique comme PGP et son équivalent Gnu, GPG.
Ce TD s'inspire grandement du How To de GPG.

1 Cryptosystèmes à clef publique 1

1.1. Sans systèmes à clef publique, quels sont les deux préalable nécessaire à l'établissement d'une connexion sécurisée utilisant des clef symétriques ?

1. L'expéditeur et le destinataire doivent s'échanger la clef de chiffrement **avant** de pouvoir s'échanger des messsages chiffrés ;
2. L'échange de la clef nécessite l'existance d'un canal de transmission **protégé** de toute écoute extérieure pour éviter qu'un intrus puisse prendre connaissance de la clef de chiffrement ;

1.2. Quels sont les trois missions d'un cryptosystème ?

– intégrité : le message reçu est distinguable du message envoyé ;
– confidentialité : le message est incompréhensible à toute personne non autorisée ;
– authentification : l'authenticité du message est vérifiable ;
Un cryptosystème est donc un système assurant la confidentialité, l'intégrité et l'authentification de massages transitant sur des canaux de communications.

(a) Quelles sont les utilisations pour lesquelles un tel cryptosystème est particulièrement adapté (donnez au moins trois exemples) ?

– établissement de contrats ou de preuves ;
– non répudiation de messages ;
– communication privée sensible (négotiation salariale) ;

1.3. Donnez le schéma d'encryption d'un cryptosystème à clef publique.

Dans les systèmes récent, le message chiffré de façon asymétrique est en fait une clé symétrique. Le reste du message se fait déchiffrer avec cette clé symétrique.

1.4. Quel est le rôle d'une signature numérique ?

Le rôle d'une signature numérique est d'authentifier l'émeteur d'un message.

(a) Comment signer numériquement un document ? Donnez un exemple schématique.

Émeteur : M – hash -> M' – crypté avec la clef privée de l'émeteur -> M'' Réception :

1. M – hash -> M'
2. M'' – decrypte avec la clef publique -> M'

Si les deux étapes ne renvoient pas M' alors le message n'est pas signé par la bonne personne.

1.5. Dans le cryptosystème décrit jusqu'ici ; quel est le maillon de la chaîne qui semble le plus faible.

(a) Expliquez comment un intrus peu lire les messages d'une personne utilisant un cryptosystème en ayant très peu de chance d'être détecté.

Il suffit qu'un intru fasse accepter sa clef publique comme la clef publique d'une autre personne pour se faire passer pour le second individu. Pour être aussi discret que possible, il suffit de faire suivre tous les messages en utilisant la vrai clef publique du destinataire.

(b) Comment éviter ce problème ?

Il suffit de signer les clefs publiques. L'idée étant que si vous avez confiance en une clef publique, vous pouvez étendre cette confiance à toutes les clefs signées par cette clef après en avoir vérifier la signature. Le problème se réduit alors à faire confiance à la première clef. La solution consiste à disposer d'un canal de communication assurant *l'intégrité et l'authentification* des messages pour comparer l'empreinte d'une clef publique que vous avez reçue à l'empreinte calculée par le propriétaire de la clef publique. Ce canal peut, par exemple, être le téléphone ou une rencontre directe.

1.6. Expliquez à quoi peut servir certificat de révocation.

La révocation sert à publier que vous n'utilisez plus une clef parce qu'elle n'est plus assez sécurisée ou pour d'autres raisons. Le certificat de révocation permet à tous de vérifier que ce n'est pas une autre personne qui révoque votre clef.

1.7. Est-il possible de lire mes messages chiffrés sans mon accord lorsque j'utilise un cryptosystème ?

La sécurité d'une chaine est égal au maillons le plus faible. Chiffrer un message que vous écrivez sur une machine compromise (Virus, keylogger, rootkit...) permettra tout de même de lire ce message.
C'est pour celà qu'il faut veiller à l'intégriter de son système.

1.8. Les client de mail récent intègrent des cryptosystèmes. Vous remarquerez que beaucoup de certificats sont déjà intégrés à l'intérieur de ceux-ci. Pourquoi ? Peut-on leur faire une confiance absolue ?

cela permet si on fait confiance comme la plupart des gens à des entreprises comme Verisign de pouvoir être certain que l'on parle au bon interlocuteur. En particulier pour vérifier l'identité de certaines grosses entreprises comme Microsoft, Apple, AOL ou encore Visa eCommerce.
La question de la confiance dépend de chaque personne. Mais les entreprises comme Verisign n'auraient aucun intérêt à modifier et à tricher sur leur diffusion de certificat à moins que l'ordre ne vienne d'un gouvernement suffisament puissant ce qui reste très improbable.

1.9. Lorsque vous surfez sur internet, il vous est parfois dit que le certificat est introuvable. Le site que vous allez visiter est-il celui d'une personne malhonnête ?

Certainement pas. Si ce message apparaît alors que vous allez sur un site comme Microsoft, alors, il y a certainement un problème car ils ont publié leur certificat chez Verisign.
Si par contre il s'agit d'un site qui n'appartient pas à une entreprise suffisamment riche, l'administrateur veut simplement que vous ayez ce certificat pour que vous puissiez détecter tout changement à l'avenir.

❦