Généralités sur SSH

Mathieu DURAND

Introduction

Afin de protéger les données transitant sur les réseaux informatiques, de nombreux programmes aux fonctions diverses ont été développés, intégrant les recherches récentes en cryptographie. Parmis eux, SSH permet la prise de contrôle à distance (type Telnet) d'une machine, tout en protégeant les informations circulant sur le réseau, comme les mots de passe.
L'utilisation de SSH permet également de protéger d'autres types de connexions : ftp, e-mail, html...
Vous trouverez ici des explications sur SSH, son utilisation et son fonctionnement.

Qu'est ce que SSH ?

SSH (***S**ecure **SH**ell*) est un protocole de connexion à distance à une machine par une interface texte (appelée *shell*).
Ses fonctions sont très similaires à celles de Telnet. Cependant, contrairement à Telnet, toutes les données circulant entre le client et le serveur sont cryptées.

Pourquoi utiliser SSH ?

A l'origine, les réseaux étaient privés et les données y circulant n'avaient pas besoin d'être cryptées. Avec le développement d'Internet, les réseaux ont été interconnectés et les informations transitent par plusieurs machines.
Telnet, ftp et même les *e-mails* envoient tous vos *logins* et mots de passe à travers le réseau, sous forme de texte clair et non encodé. Quand vous passez la commande "telnet" vers une machine distante, l'information n'est pas envoyée directement : elle est acheminée à travers plusieurs machines (routeurs) pour y arriver. De cette facon, Internet ressemble un peu à un réseau routier : vous ne prenez pas une route privée directe vers votre destination mais vous utilisez plusieurs routes qui se croisent à des carrefours..

Cela pose quelques problèmes car n'importe qui sur le chemin peut voir ce que vous envoyez, comme toute personne attendant à un carrefour peut regarder votre voiture passer sur la route et en tirer des

informations. Cela veut dire qu'on peut facilement intercepter vos *login* et mot de passe. Muni de ceux-ci, on est libre d'accéder à votre système grâce à votre compte. Une fois que c'est arrivé, votre système n'est plus sûr. Vos fichiers peuvent avoir été modifiés ou effacés ou on peut essayer d'obtenir les droits de super-utilisateur (*root*) et causer des dégats plus importants.

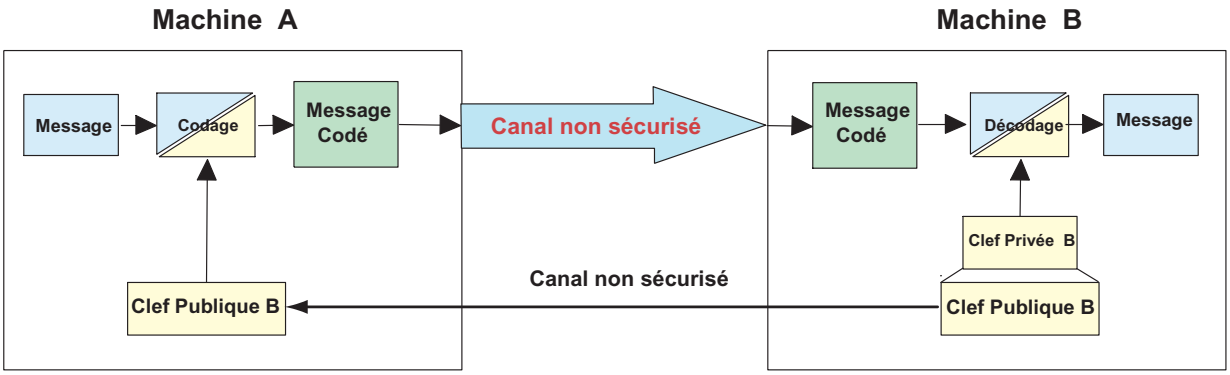
Pour protéger votre compte et votre système contre cette menace, il est recommandé d'utiliser SSH au lieu de Telnet. C'est la première étape pour éviter de transmettre les mots de passe en clair sur le réseau. Comme SSH crypte toutes les informations avec un schéma de "**clef publique/privée**", seul votre serveur peut les décrypter et tout personne interceptant les données en cours de transit n'obtiendra que des informations inutilisables.

Clef publique/privée

Les clefs publique et privée forment un ensemble de deux clefs utilisées pour la "cryptographie à clef publique". Un fournisseur de service de cryptographie (CSP) fournit à chaque utilisateur ces deux clefs publique et privée ; elle seront utilisées pour réaliser le cryptage des données échangées et pour réaliser une signature digitale des messages envoyés par cet utilisateur. Les clefs sont attribuées à la machine et conservées dans des répertoires ; elles sont valables pour toutes les sessions.

La **clef publique** est utilisée :

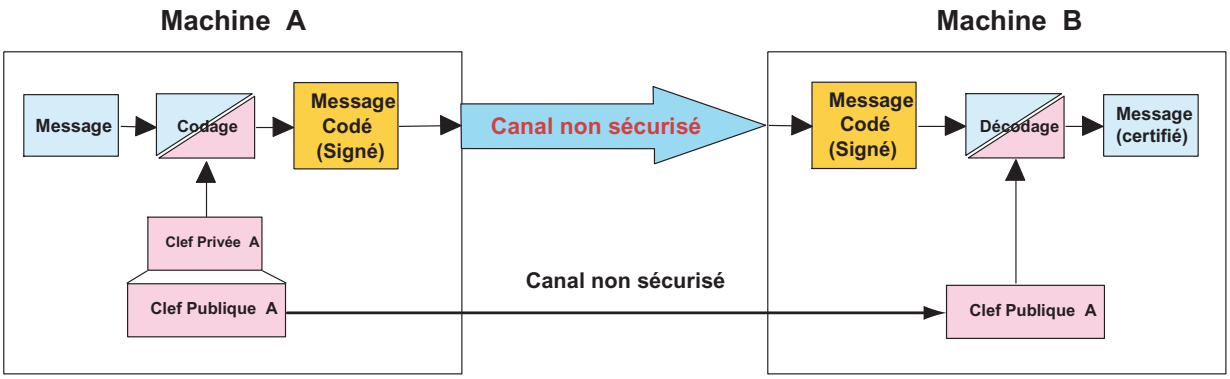
- pour **décrypter une signature digitale**, afin d'être certain de l'auteur du message et de garantir la validité des données,
- pour **crypter un message**, garantissant ainsi que seule la personne possédant la **clef privée** correspondante pourra **décrypter le message**.



La figure ci-dessus illustre le : **Cryptage** d'un message par clef publique/privée.

- La machine "**B**" donne sa **clef publique** à la machine "**A**" (à l'aide d'une connexion non sécurisée ou par un support quelconque).
- "**A**" crypte le message grâce à la clef publique de "B".
- "**B**" décrypte le message grâce à sa **clef privée**.

Si quelqu'un récupère le message crypté, il doit posséder la clef privée de "B" pour pouvoir le lire. Tout le monde peut donc envoyer un message crypté à "B", mais seul "B" lui-même peut les **décrypter**.



La figure ci-dessus illustre la : **Signature** d'un message par clef publique/privée.

- La machine "**A**" donne sa **clef publique** à la machine "**B**" (à l'aide d'une connexion non sécurisée ou par un support quelconque).
- "**A**" crypte son message avec sa **clef privée**.
- "**B**" décrypte le message grâce à la **clef publique** de "A". S'il reçoit une erreur c'est que le message a été modifié.

Tout le monde peut lire les messages de "A", mais seul "A" lui-même peut les **signer**.

Les deux cryptages sont, bien sûr, tout à fait compatibles.
Il est donc possible de garantir l'origine des données ainsi que leur protection. On commence alors par crypter le message pour assurer une protection contre la lecture des données, puis on signe le message afin de garantir que ce message provient bien de la bonne personne et qu'il n'a pas été modifié.

Dans le cas du SSH, on utilise le cryptage des messages afin de garantir la protection des données envoyées : seul le destinataire peut lire les messages. Les clefs publiques sont échangées au début de la communication entre les deux machines, avant même l'envoi des informations de connexion (*login* et mot de passe).

Le *tunneling* SSH

Le "***tunneling***" est une méthode d'utilisation des services conventionnels, comme Telnet ou ftp, à travers un canal SSH crypté.

Quand on met en place un tunnel SSH, on crée un canal sécurisé, entre une machine locale et une machine distante, à travers lequel n'importe quelles données peuvent être envoyées. Pour reprendre l'analogie avec le réseau routier, cela revient à fabriquer un tunnel direct entre son point de départ et sa destination, puis de conduire dans ce tunnel, empêchant ainsi d'être vu par quiconque, soi ou sa façon de conduire. Cependant, il s'agit d'un processus simple avec SSH.

Une fois que le client SSH est configuré pour créer un tunnel, il est alors nécessaire de configurer le programme Telnet/ftp/email pour qu'il se connecte sur la machine locale plutôt que sur la machine distante.
Le programme SSH de la machine locale acceptera cette connexion et renverra les données au serveur distant à travers un canal SSH.

Une fois les données arrivées sur le serveur distant, elles seront décryptées et renvoyées vers le service local de la machine. Le client et le serveur Telnet/ftp/mail distant fonctionnent normalement mais le trafic entre les deux machines est entièrement crypté et protège donc les mots de passe et les données.