Détail d'une connexion SSL

Rolland Balzon Philippe
Department of Computer Science
SEPRO Robotique
ZI les ajoncs, 85000 La roche sur Yon, France
prolland@free.fr

16 juillet 2002

Supposons qu'un client, pourvu d'un couple clé publique - clé privée (A,a), se connecte à un serveur muni du couple de clé (B,b) pour une connexion sécurisée par le protocole SSL ; étudions alors le principe de cette connexion :

Choix des algorithmes et spécifications à utiliser :

Le client envoie la liste des algorithmes de chiffrement qu'il accèpte, et un nombre aléatoire.

Le serveur confirme avoir reçu le nombre aléatoire et indique les spécifications de chiffrement choisies. Celles-ci sont choisies parmis celles proposées par le client en fonction des préférences du serveur.

Le serveur envoie alors son certificat (clé publique B) et la liste des certificats acceptables, ainsi que la liste des Authorités de Certification (CA) autorisées.

Le client indique alors son propre certificat (parmis la liste proposée), et envoie également la chaîne de CA acceptées.

Authentification :

Le client chiffre alors le nombre aléatoire avec sa clé privée a et l'envoie au serveur.

Celui-ci déchiffre avec la clé publique du client A et vérifie que ce nombre est bien le bon.

Choix de la clé de session :

Le client envoie alors une pré-clé au serveur, chiffrée avec la clé publique de celui-ci B.

Le client et le serveur peuvent alors calculer la clé de session. Elle est calculée à partir de la pré-clé précédente et des nombres aléatoires de départ. Une fonction de hachage est alors appliquée au résultat, afin d'obtenir la clé définitive de longueur voulue (40 bits ou 128 bits par exemple).

Transfert de données :

Maitenant que la clé de session a été choisie, le transfert de données peut s'effectuer de manière sécurisée à l'aide de cette clé de session.