Sécurité des transactions électroniques : le protocole SSL

Lors d'un achat en ligne ou plus généralement lors d'échange d'informations sensibles, il est indispensable de sécuriser la communication. En effet lorsqu'une information transite sur un réseau, comme le réseau Internet, elle passe de serveurs en serveurs jusqu'à joindre son destinataire. Entre temps un analyseur de réseaux a pu écouter le trafic : l'information ne peut donc être transmise en clair. De plus, il est possible de mystifier une adresse IP et donc de se faire pour quelqu'un que l'on n'est pas : l'identification des interlocuteurs est donc indispensable. Ces problèmes peuvent être résolus à l'aide de la cryptographie. Nous allons voir ici les principes de cryptographie à clés symétriques et asymétriques et présenter comment interviennent ceux-ci dans le protocole SSL qui est celui le plus utilisé pour la sécurisation des achats sur le Net.

Clés symétriques et asymétriques

La grille de Vigenère est un système de cryptographie que l'on dit être à clé symétrique car la même clé permet à la fois de chiffrer et de déchiffrer un message. De nos jours, le codage DES en est une complexification calculatoire mais le principe reste le même : qui sait chiffrer, sait aussi déchiffrer. Les cryptosystèmes asymétriques sont eux d'une autre nature : ce sont deux clés différentes qui chiffre et déchiffre. Seuls les concepteurs du code connaissent ces clés, et il est techniquement impossible de déduire l'une de l'autre. Le codage RSA ou l'algorithme Diffie-Hellmann sont les cryptosystèmes asymétriques les plus connus.

Atouts et faiblesses

Dans la pratique, les systèmes symétriques et asymétriques protègent aussi efficacement l'un que l'autre l'information qu'ils chiffrent. Néanmoins, les systèmes symétriques nécessitent l'existence d'un canal sécurisé pour permettre l'échange de la clé de chiffrement. A contrario, dans un système à clés asymétriques il est possible de communiquer la clé de chiffrement à quiconque sans pour autant affaiblir l'information chiffrée. Cette clé est dite publique, la clé de déchiffrement est dite privée et est sera gardée secrète par le concepteur du code. Malheureusement, les cryptosystèmes asymétriques sont gourmands en calculs alors que les cryptosystèmes symétriques sont beaucoup plus rapides. L'idée du protocole SSL est de créer par un système asymétrique un canal sécurisé permettant l'échange d'une clé symétrique et de poursuivre la communication en chiffrant par le biais de cette clé.

Le protocole SSL

Le protocole SSL (pour Secure Socket Layer) a été développé par Netscape Communications Corp. en collaboration avec RSA Data Sécurity Inc. afin de sécuriser les échanges d'information sur les réseaux.

Partons d'une situation concrète : Alice veut acheter un CD à la boutique en ligne de Bob. La communication va passer en mode sécurisé, l'adresse du serveur commencera par « https:// » au lieu du classique « http:// » et il apparaît généralement un cadenas fermé en bas du navigateur d'Alice. C'est toute la communication http qui sera sécurisée par le système qui va se mettre en place.

Mais avant de parler de cette transaction, revenons quelques temps en arrière : revenons au jour où Bob a décidé d'ouvrir un site de vente en ligne. Pour sécuriser ses futures transactions, Bob met au point un système de cryptographie à clés asymétriques. Il fait ensuite appel à une autorité de certification (voir l'article correspondant) qui va certifier sa clé publique. L'autorité de certification joue ici le rôle du tiers de confiance qui assure aux futurs consommateurs le sérieux du site de vente en ligne.

Revenons à la transaction d'Alice. Le navigateur d'Alice contacte le serveur de Bob en lui faisant part de son souhait de passer en mode sécurisé. Il transmet aussi la liste des systèmes de cryptographie symétriques qu'il supporte. En retour le serveur lui envoie la clé publique de Bob et précise le cryptosystème le plus performant avec lequel il est compatible. Le navigateur d'Alice vérifie que la clé publique de Bob est certifiée par au moins une autorité dont il reconnaît la compétence. Si tel est le cas, il génère aléatoirement une clé symétrique qu'il chiffre par le biais de la clé publique de Bob avant de la lui envoyer. Bob reçoit cette clé qu'il déchiffre à l'aide de sa clé privée.

A ce stade, le navigateur d'Alice et le serveur de Bob ont convenu d'un cryptosystème symétrique et se sont échangé une clé par le biais d'un canal sécurisé. Cette clé ne servira qu'à cette transaction, on dit que c'est une clé de session. Les messages échangés seront ensuite décomposés par blocs, chaque bloc sera signé numériquement afin d'en assurer l'intégrité et le tout sera chiffré par la clé de session.

Les atouts de SSL

Ce protocole est rapide. L'intégralité de la transaction est chiffrée par une clé de session qui est échangée via un canal sécurisé. Le client est assuré de l'identité du

Quelles sont les autorités de certification dont votre navigateur reconnaît la compétence ?

Avec Internet Explorer : Menu Outils|Options Internet, onglet Contenu puis bouton « Certificats. »

Avec Firefox : Menu Outils|Options, onglet Avancé puis bouton « Gérer les certificats »

Comment désactiver tous les certificats ? Il suffit de changer la date de l'ordinateur et de passer en l'an 2029 car bon nombre de certificats auront expiré en 2028…

serveur, car la clé publique est certifiée par un tiers de confiance. Si quelqu'un usurpe l'identité du serveur il ne pourra déchiffrer la clé de session formée car il n'est pas en possession de la clé privée du serveur. De son côté, le serveur est certain de communiquer avec le créateur de la clé de session car il peut vérifier l'intégrité des messages déchiffrés par leur signature.

Les faiblesses de SSL

La principale faiblesse du protocole SSL se situe au niveau de la liste des autorités de certification, il suffit qu'une seule d'entre elles valide la clé publique de Bob pour que celui-ci soit jugé digne de confiance. De plus, le protocole SSL ne prévoit pas de vérification systématique de la non révocation des certificats. Cela reste donc essentiellement au client de vérifier l'intégrité du site sur lequel il transmet des informations sensibles.

Les faiblesses en dehors du protocole

Le principal souci d'Alice est que son numéro de carte bancaire ne soit pas dévoilé durant la transaction. Le protocole SSL protège la transmission de ce numéro mais ne protège pas celui-ci no au départ ni à l'arrivée. Si l'ordinateur d'Alice est espionné par un keylogger (programme qui enregistre les saisis du clavier) alors le numéro de carte bancaire d'Alice peut être piraté. D'autre part, une fois le numéro de carte bancaire parvenu sur le site de Bob, celui-ci doit le transmettre à sa banque et Alice n'a aucun contrôle sur la fiabilité de cette transmission. De plus Bob sera peut être amené à stocker le numéro de carte bancaire dans ses archives afin de garder une preuve de la transaction.

De son côté, le principal souci de Bob est qu'Alice soit la véritable détentrice de la carte bancaire dont elle transmet le numéro. Le protocole SSL ne fournit aucune garantie à Bob de cela. Si le porteur de la carte bancaire conteste le paiement, Bob devra rechercher l'identité du destinataire de la marchandise afin d'en exiger le règlement.

Le protocole SET (pour Secure Electronic Transaction) pallie à ces faiblesses en faisant intervenir l'autorité bancaire. Le numéro de carte est directement transmis à la banque accompagné d'une signature électronique du client empêchant toutes contestations ultérieures. L'autorité bancaire transmet alors au site marchand l'autorisation de transaction et Bob est ainsi assuré du paiement de sa marchandise. Pour des raisons économiques et de lobbying le protocole SET ne parvient pas encore à s'imposer.

Le phishing

Vous recevez un jour un courriel de la « SouthTrust Bank » qui, suite à un incident technique, vous demande de bien vouloir lui communiquer à nouveau vos identifiants bancaires…Vous êtes surpris car vous n'êtes pas client de cette banque ! Vous êtes en fait victimes de phishing, phénomène responsable de nombreux spam. Le mail que vous venez de recevoir contient un lien menant sur un site pirate très semblable à celui de la « SouthTrust Bank ». L'objectif du pirate est de récolter les identifiants bancaires de quelques clients de cette banque. En général la connexion vers ces sites n'est pas sécurisée contrairement à ce qu'ils peuvent prétendent, en effet, ici, cela ne servirait pas à grand-chose ! Pour en savoir plus : www.antiphishing.org.