TD SSL/TLS

Table of Contents

A partir des explications des annexes 1 et 2, répondre aux questions suivantes :

Question 1 : Définir l'avantage et l'inconvénient du cryptage symétrique

Réponse 1 :

Avantage : Rapide, peu de surcharge du processeur pour les calculs

Inconvénient : Attention à la transmission de la clé de cryptage, c'est la même clé qui sert pour le cryptage et le décryptage.

Question 2 : Définir l'avantage et l'inconvénient du cryptage asymétrique

Réponse 2 :

Avantage : plus de sécurité, impossible de décrypter avec la clé de cryptage (publique).

Inconvénient : algorithme plus complexe et plus long, utilise beaucoup de ressources processeur

Question 3 : Quelle est la différence d'utilisation entre la clé privée et la clé publique ?

Réponse 3 :

Clé publique : ne sert que pour le cryptage, on peut la donner à tout le monde pour recevoir des documents cryptés.

Clé privée : sert à décrypter, ne pas la transmettre

Question 4 : Que garantit l'algorithme de hachage ?

Réponse 4 :

L'intégrité des informations transmises, on est sûr que le message n'a pas été modifié

Question 5 : Quel est l'intérêt pour une entreprise de commerce en ligne d'obtenir un certificat auprès d'une autorité de certification ?

Réponse 5 :

- Donner une image de fiabilité, de sécurité, sérieux auprès des clients
- Pouvoir crypter les transmissions avec les clés privées et publiques.

Question 6 : SSL peut-il être utilisé pour protéger tous les échanges IP ?

Réponse 6 :

Non, il agit au niveau application, notamment pour les protocoles HTTP, FTP, POP,

1. Annexe 1 : Introduction aux certificats et au protocole SSL

1.1. Les certificats

Les certificats sont des documents signés qui font correspondre des clés publiques à d'autres informations telles qu'un nom ou une adresse de messagerie électronique. Ils sont signés par les Autorités de certification qui les délivrent. La signature d'une Autorité de certification garantit que la clé publique appartient bien à la partie qui la présente.

Une Autorité de certification (C*A, Certification Authority*) est chargée de fournir et d'affecter des clés de cryptage, de décryptage et d'authentification. Elle distribue les clés en délivrant des *certificats*, qui contiennent la clé publique et un ensemble d'attributs. Une Autorité de certification peut délivrer des certificats pour un ordinateur, un compte d'utilisateur ou un service.

Le processus de délivrance d'un certificat suit les quatre étapes ci-dessous.

- L'Autorité de certification accepte une demande de certificat.
- L'Autorité de certification vérifie les informations du demandeur,
- L'Autorité de certification utilise sa clé privée pour appliquer sa signature numérique au

certificat.

- L'Autorité de certification délivre le certificat qui servira d'information d'identification dans une infrastructure de clé publique.

En outre, chaque Autorité de certification possède un certificat pour confirmer sa propre identité.

Dans le cas d'un site de commerce électronique, l'entreprise qui met en ligne le site fait appel à une société dont l'activité est la gestion de certificats (Autorité de certification commerciale) qui lui fournit (c'est pas gratuit !) un certificat dans lequel les clients **pourront avoir confiance**. Les autorités commerciales les plus connues sont Verisig, Thawte, Securenet, GlobalSign.

Une autorité de certification peut-être aussi privée, dans ce cas, l'entreprise gère elle même la délivrance de certificats pour ses différents services ou pour traiter avec des partenaires.

1.2. Le protocole SSL (Secure Sockets Layer)*

Ce protocole effectue un cryptage des données au niveau de la couche application, SSL utilise des ports applications particuliers :

- 443 pour https (http sécurisé) au lieu de 80 pour http,
- 995 pour pop3 au lieu de 110,
- 993 pour imap4 au lieu de 143,

Exemple de Fonctionnement de SSL avec un client se connectant sur un site sécurisé https :

- Le client se connecte au serveur SSL et demande au serveur de s'authentifier. Le serveur envoie au client son propre certificat. Le client vérifie le certificat (date de validité, signature digitale digne de confiance), si la vérification est négative, un message prévient l'utilisateur que le certificat n'est pas digne de confiance et demande confirmation pour poursuivre le dialogue.
- Le client envoie alors au serveur une requête de négociation de l'algorithme de chiffrement et de la fonction de hachage, le serveur sélectionne le plus puissant qu'ils ont en commun.
- Les clés de cryptages sont générées par un dialogue entre le client et le serveur.
- Les données peuvent alors être envoyées de façon cryptée par les clés que seuls le client et le serveur connaissent.

2. Annexe 2 : la cryptographie (Adapté de documents de Microsoft)

Trois mécanismes importants pour la sécurité des réseaux sont mis en œuvre par la cryptographie :

- la confidentialité des données,
- l'intégrité des données,
- l'authentification de l'émetteur et/ou du destinataire.

2.1. Cryptage symétrique

Une *clé* est une chaîne aléatoire (un nombre, une valeur ASCII, un mot ou une expression) qui est utilisée conjointement avec un algorithme pour chiffrer (crypter) des données.

Le cryptage symétrique, encore appelé cryptage à clé secrète, utilise une même clé et algorithme de cryptage afin de crypter et décrypter un document. L'utilisation d'une telle méthode de cryptage favorise la rapidité de chiffrement. Les algorithmes utilisés se nomment : DES, 3DES

2.2. Cryptage asymétrique : le cryptage par clé publique

Le cryptage par clé publique garantit la confidentialité grâce au cryptage des données, que celles-ci soient sous la forme de messages électroniques, de numéros de cartes de crédit envoyés sur Internet ou de trafic réseau. Comme les clés publiques peuvent être publiées librement, des personnes totalement étrangères les unes aux autres peuvent établir des communications privées sur des réseaux publics en récupérant simplement les clés publiques correspondantes et en cryptant les données.

Le cryptage par clé publique utilise deux clés liées mathématiquement. Dans le cas du cryptage par clé publique, chaque utilisateur dispose d'une paire de clés liées mathématiquement :

- une **clé privée**, qui est confidentielle ;
- une **clé publique**, qui est diffusée librement à tous les correspondants potentiels.

Le cryptage a pour objectif de cacher des données pour que seul le destinataire prévu puisse les lire. Dans un scénario standard, un expéditeur utilise la **clé publique** du destinataire pour crypter un message. Seul, le destinataire dispose de la **clé privée** qui permet de décrypter le message. Si vous mettez votre clé publique à disposition, d'autres personnes peuvent vous envoyer des données cryptées, qui ne peuvent à leur tour être décryptées qu'en utilisant votre clé privée. L'utilisation de clés par les programmes PKI de cryptage de données est en général transparente pour l'utilisateur. L'algorithme utilisé se nomme RSA.

2.3. Algorithme de hachage

Le principe de cette technique est de soumettre un message à une fonction (fonction de hachage) pour obtenir un résultat sous forme d'empreinte numérique (appelé condensé). Le message et son condensé sont transmis au destinataire, qui applique le même algorithme de hachage au message et doit obtenir le même condensé si le message n'a pas été modifié pendant la transmission. Les algorithmes utilisés se nomment : SHA, MD5.

2.4. Signatures numériques

La signature numérique permet à l'auteur d'un message, d'un fichier ou de toute autre information codée numériquement, de lier son identité aux informations.

La signature proprement dite est une séquence de bits ajoutée au document numérique. Une

signature numérique garantit les éléments ci-dessous.

- Seul le détenteur de la clé privée peut avoir créé la signature numérique.
- Quiconque possède la clé publique correspondante peut vérifier la signature numérique.

Par exemple, lorsque vous consultez un site Web et êtes invité à télécharger un fichier, une boîte de dialogue vous informe que ce dernier a été signé numériquement par une entité approuvée. Une signature numérique vous assure que le fichier ou le programme que vous allez télécharger provient d'une source digne de confiance.

La signature numérique s'appuie sur l'algorithme de hachage et l'utilisation d'une clé privée pour crypter le condensé qui devient la signature digitale.

2.5. Conclusion

Le cryptage garantit la sécurité et la confidentialité, les signatures numériques permettent de fournir une preuve d'authenticité et d'origine.