TD SSL/TLS

On utilise souvent le protocole HTTPS (HTTP sur SSL/TLS) pour sécuriser les communications entre un serveur Web et un navigateur. Lors de l'établissement de connexion, le serveur envoi au navigateur sa clé publique certifié (stockée dans un certificat). Le navigateur calcule une clé secrète K (master key) et l'envoi au serveur dans un canal sécurisé. Six clés seront dérivée de K et seront utilisées pour sécuriser les communications.

1. L'utilisation de SSL/TLS permet-elle de chiffrer les entêtes des protocoles niveau transport (TCP, UDP)? Expliquer.
2. Expliquer pourquoi le client présente au serveur plusieurs suites de chiffrement alors que ce dernier ne lui présente qu'une seule suite?
3. Comment l'utilisateur du navigateur s'assure bien que la clé publique envoyée par le serveur correspond bien à l'organisme dont il souhaite accéder?
4. Quelle attaque peut-on avoir si la clé publique est envoyée directement (non certifiée) au navigateur?
5. Préciser comment le canal sécurisé est établit pour envoyer la clé K?
6. Pourquoi certains services Web, utilisant pourtant HTTPS, demandent-ils en plus à l'utilisateur de fournir un nom de compte et un mot de passe pour compléter l'ouverture de session?
7. À votre avis, la clé privée du serveur web est stockée en clair ou protégé par mot de passe? Expliquer.
8. Il est possible d'utiliser un certificat client stocké sur le navigateur pour l'échange HTTPS. Donnez un avantage et un inconvenient de procéder ainsi.
9. Avec un certificat client, l'utilisateur doit parfois fournir un mot de passe(une «passphrase»): de quoi s'agit-il? Quel est son utilité? Ce mot de passe est-il envoyé au serveur web?

TD SSL/TLS (correction)

On utilise souvent le protocole HTTPS (HTTP sur SSL/TLS) pour sécuriser les communications entre un serveur Web et un navigateur. Lors de l'établissement de connexion, le serveur envoi au navigateur sa clé publique certifié (stockée dans un certificat). Le navigateur calcule une clé secrète K (master key) et l'envoi au serveur dans un canal sécurisé. Six clés seront dérivée de K et seront utilisées pour sécuriser les communications.

1. L'utilisation de SSL/TLS permet-elle de chiffrer les entêtes des protocoles niveau transport (TCP, UDP)? Expliquer.

==> **Non, SSL/TLS est au dessus de la couche transport**

2. Expliquer pourquoi le client présente au serveur plusieurs suites de chiffrement alors que ce dernier ne lui présente qu'une seule suite?

==> **Le client présente les suites de chiffrement qu'il supporte. Le serveur choisit l'une de ces suites.**

3. Comment l'utilisateur du navigateur s'assure bien que la clé publique envoyée par le serveur correspond bien à l'organisme dont il souhaite accéder?

==> **La clé est récupérée à partir du certificat du serveur envoyé par ce dernier au client.**

4. Quelle attaque peut-on avoir si la clé publique est envoyée directement (non certifiée) au navigateur?

==> **Attaque MITM (Man In The Middle).**

5. Préciser comment le canal sécurisé est établit pour envoyer la clé K?

==> **Généralement, la clé K est généré par le client puis chiffré par la clé publique du serveur qui la déchiffre avec sa clé privée (sinon, le protocole de DH est utilisé pour construire K)**

6. Pourquoi certains services Web, utilisant pourtant HTTPS, demandent-ils en plus à l'utilisateur de fournir un nom de compte et un mot de passe pour compléter l'ouverture de session?

==> **Il s'agit d'authentifier l'utilisateur par le service web pour l'accès à base de rôle.**

7. À votre avis, la clé privée du serveur web est stockée en clair ou protégé par mot de passe? Expliquer.

==> **La clé privée du serveur est stockée en clair car le serveur doit répondre automatiquement aux requêtes des clients sans attendre la saisie d'un mot de passe par l'administrateur du serveur web.**

8. Il est possible d'utiliser un certificat client stocké sur le navigateur pour l'échange HTTPS. Donnez un avantage et un inconvenient de procéder ainsi.

==> **Avantage: le serveur authentifie le client, ce qui permet d'éviter certaines attaques**

==> **Inconvenient: les certificats sont le plus souvent payant**

9. Avec un certificat client, l'utilisateur doit parfois fournir un mot de passe(une «passphrase»): de quoi s'agit-il? Quel est son utilité? Ce mot de passe est-il envoyé au serveur web?

==> **C'est le mot de passe (clé) de chiffrement de la clé privée. Il permet la confidentialité de la clé privée. Ce mot de passe n'est pas envoyé au serveur: il sert à déchiffrer la clé privée chez le client.**