

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 envoie au navigateur sa clé publique certifiée (stockée dans un certificat). Le navigateur calcule une clé secrète K (master key) et l'envoie au serveur dans un canal sécurisé. Six clés seront dérivées 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 établi 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 protégée 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 inconvénient 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?