République Algérienne Démocratique et Populaire
الجمهورية الجزائرية الديمقراطية الشعبية
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
وزارة التعليم العالي و البحث العلمي

ESI ECOLE NATIONALE SUPÉRIEURE D'INFORMATIQUE

المدرسة الوطنية العليا للإعلام الآلي
(المعهد الوطني للتكوين في الإعلام الآلي سابقا)
Ecole nationale Supérieure d' Informatique
ex. INI (Institut National de formation en Informatique)

SSL

REALISER Par:

HAISSAM Ichrak

CHABANE Salsabil

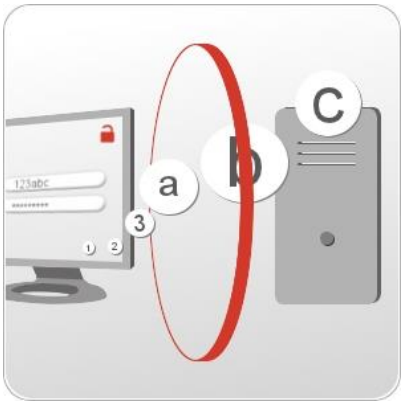
2015/2016

Table des matières

Introduction 2
Définition 3
Fonctionnement 4
Les certificats 4
Etapes du fonctionnement du protocole SSL 5
Les protocoles de SSL : 6
1. SSL Handshake Protocol 6
2. La communication SSL 6
Les avantages et les inconvénients : 7
Les avantages 7
Les inconvénients 7
Les utilisations de SSL 8
SSL en Algérie 9
Conclusion 9
BIBLIOGRAPHIE 10

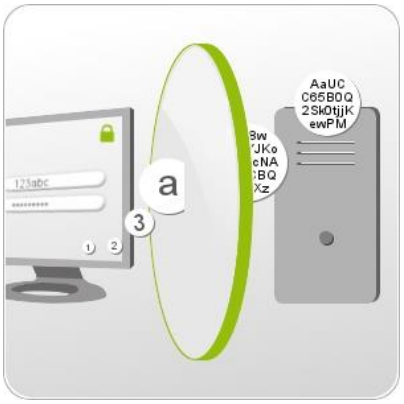
Introduction

On fait, à cette époque, beaucoup de transactions via internet. Qu'il s'agisse d'acheter des billets d'avion, de réserver un spectacle, de télécharger de la musique payante, de commander un livre …



Et on a besoin de protéger toutes ces informations échangées. Pour éviter d'être espionner ou de délivrer et/ou recevoir de l'information faussée.

D'où la nécessité d'un canal de communication entre le client et le serveur indépendamment du protocole utilisé et qui sécurise ainsi les transactions sur le web.



C'est ce que SSL fait. Il est derrière l'immense majorité de ces opérations. Presque tous les sites qui opèrent le paiement par la transmission du numéro facial de carte de crédit, utilisent SSL.

Définition

SSL = Secure Sockets Layers, couche de sockets sécurisée.

C'est un protocole de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet. Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.

Le SSL garantit aux visiteurs du site web que leurs données ne seront pas interceptées de manière frauduleuse.
Il permet d'échanger les informations entre 2 ordinateurs de façon sûre.
SSL assure 3 choses :

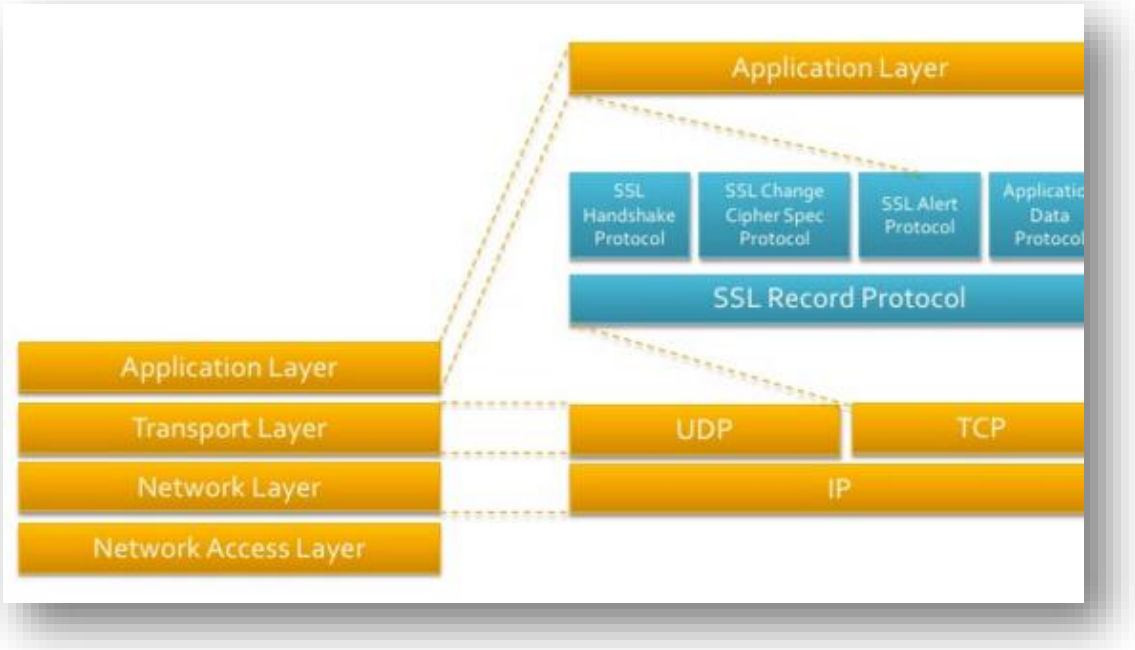
- Confidentialité
- Intégrité
- Authentification

Il a été créé et développé par la société *Netscape* et *RSA Security en 1994*. On trouve désormais des versions open source ainsi qu'un protocole libre similaire : TLS.

Ses versions :

- SSL Version 1.0
- SSL Version 2.0
- SSL Version 3.0
- TLS Version 1.0 (Transport Layer Security). Ce changement de nom marque le rachat du brevet SSL par l'IETF.

Fonctionnement



En effet, SSL agit telle une couche supplémentaire imaginée, permettant d'assurer la sécurité des données, située entre la couche application et la couche transport. Il est un complément à TCP/IP et permet (potentiellement) de sécuriser n'importe quel protocole ou programme utilisant ce dernier.
Il transforme le protocole « http » en « https » en assurant un niveau de sécurité dont l'efficacité dépend des certificats. Par ailleurs, force est de constater que de nombreux sites optent pour un cryptage de 128 bits, un niveau largement efficace en termes de sécurité. Comme les opérations financières sont les plus susceptibles de faire l'objet d'un piratage informatique, ce n'est donc pas étonnant si la plupart des banques en ligne choisissent un cryptage de 256 bits.

Les certificats

Ils permettent de savoir à qui appartient une clé, qui l'a vérifié et qui l'utilise. Un certificat numérique est une sorte de "carte d'identité" d'une entité informatique. Le certificat numérique d'un serveur va évidemment contenir la clé publique de celui-ci mais également un certain nombre de champs, d'attributs, reliés à son identité.

Etapes du fonctionnement du protocole SSL

1. Les blocs de données applicatives sont découpés en fragments de 16Ko (2^14 octets) maximum
2. Le fragment subit une compression (facultative). Si les blocs sont très courts, cette compression peut augmenter la taille du bloc initial. Toutefois, la longueur du contenu ne peut être augmentée de plus de 1024 octets.
3. Une empreinte est prise de C.1 (le fragment compressé).
4. L'empreinte est ajoutée à la suite de C.1 et donne le message M.1
5. Le message M.1 est chiffré par l'algorithme symétrique en utilisant la clé symétrique échangée. La résultante est le message Mc.1, crypté !
6. Un en-tête de 5 octets est ajouté. Le champ “Type” de cet en-tête définit le type du protocole de niveau supérieur au Record Protocol.
7. Le message est transmis à la couche Transport de l'émetteur, la plupart du temps il s'agit du protocole TCP.

Les protocoles de SSL :

SSL consiste en 2 protocoles :

- **SSL Handshake protocol** : avant de communiquer, les 2 programmes SSL négocient des clés et des protocoles de chiffrement communs.
- **SSL Record Protocol** : Une fois négociés, ils chiffrent toutes les informations échangées et effectuent divers contrôles.

1. SSL Handshake Protocol **: La** négociation SSL

Au début de la communication le client et le serveur s'échangent :

- la version SSL avec laquelle ils veulent travailler,
- la liste des méthodes de chiffrement (symétrique et asymétrique) et de signature que chacun connaît (avec longueurs de clés),
- les méthodes de compression que chacun connaît,
- des nombres aléatoires,
- les certificats.

2. La communication SSL ("*record*")

L'expéditeur des données :

- découpe les données en paquets.
- compresse les données.
- signe cryptographiquement les données.
- chiffre les données.
- les envoie.

Celui qui réceptionne les données :

- déchiffre les données.
- vérifie la signature des données.
- décompresse les données.
- réassemble les paquets de données.

Les avantages et les inconvénients :

Les avantages :

- Aucun logiciel supplémentaire ne doit être installé sur les postes des utilisateurs.
- On peut accéder à des applications en toute sécurité depuis n'importe quel endroit, on n'a besoin que d'une machine munie un navigateur web.
- Une très grande variété de navigateurs Web est prise en charge.
- Peu de formations sont nécessaires pour les utilisateurs (user friendly).
- Les utilisateurs peuvent généralement être authentifiés grâce à plusieurs méthodes, y compris les mots de passe statiques, les certificats, ou les services d'annuaire. Avec les services d'annuaire, un unique processus de connexion est utilisé pour l'authentification de l'utilisateur auprès de passerelle SSL, en plus de l'authentification auprès du service d'annuaire.

Les inconvénients :

Les inconvénients se posent spécialement dans la partie de serveur et pas dans la partie de l'utilisateur.

- renouvellement régulier : le certificat SSL expire après une courte période de temps, généralement un à cinq ans. Vous devez renouveler la protection SSL régulièrement et payer le prix de souscription à nouveau pour toujours afin de maintenir la protection. Si vous oubliez de renouveler la protection SSL, votre site affichera une erreur sur l'ordinateur de l'utilisateur indiquant que le certificat n'est pas valide.
- Installation complexe : la technologie SSL peut être difficile à installer sur un site, Le fournisseur vous enverra un ensemble de fichiers à installer dans un dossier de votre serveur Web. Vous devez également activer le certificat à l'aide des instructions spécifiques du fournisseur.

Les utilisations de SSL : HTTPS, SSH, FTPS, POPS…

SSL peut être utilisé pour sécuriser pratiquement n'importe quel protocole utilisant TCP/IP.

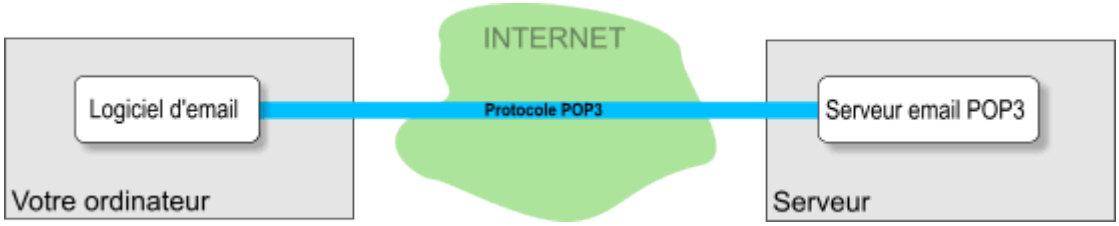
Certains protocoles ont été spécialement modifiés pour supporter SSL :

- **HTTPS** : c'est HTTP+SSL. Ce protocole est inclus dans pratiquement tous les navigateurs, et vous permet (par exemple) de consulter vos comptes bancaires par le web de façon sécurisée.
- **FTPS** est une extension de FTP (File Transfer Protocol) utilisant SSL.
- **SSH** (Secure Shell) : c'est une sorte de Telnet (ou login) sécurisé. Cela permet de se connecter à un ordinateur distant de façon sûre et d'avoir une ligne de commande. SSH possède des extensions pour sécuriser d'autres protocoles (FTP, POP3 ou même X Windows).

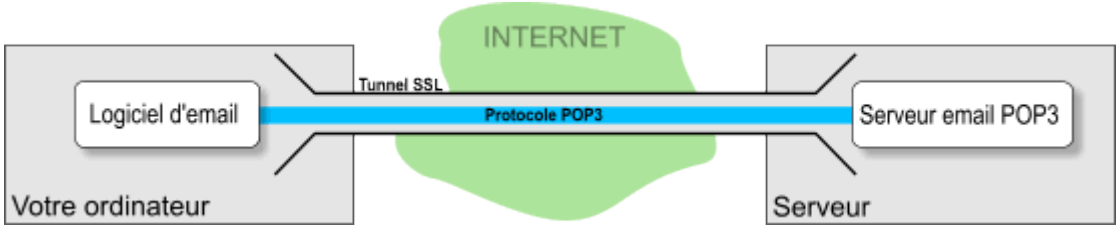
Il est possible de sécuriser des protocoles en créant des tunnels SSL. Une fois le tunnel créé, vous pouvez faire passer n'importe quel protocole dedans (SMTP, POP3, HTTP, NNTP…). Toutes les données échangées sont automatiquement chiffrées.

On peut faire cela avec des outils comme **STunnel** ou **SSH**.

Voici un exemple avec le protocole POP3:



Avec le protocole POP3 que vous utilisez habituellement pour aller lire votre courrier, les mots de passe et les messages transitent **en clair** sur Internet. Il est possible de voler vos mots de passe et vos messages.



Avec le tunnel SSL, et **sans rien changer aux logiciels client et serveur**, vous pouvez sécuriser la récupération de vos mails : personne ne peut vous volez vos mots de passe ou emails puisque tout ce qui passe à travers le tunnel SSL est chiffré.
Mais cela nécessite d'installer STunnel sur le client **et** sur le serveur.

Certains fournisseurs d'accès proposent ce service, mais ça reste trop rare. Demandez à votre fournisseur d'accès s'il a ce genre de service en place.

STunnel permet ainsi de sécuriser la majorité des protocoles basé sur TCP/IP sans modifier les logiciels. Il est très facile à installer.

SSL en Algérie : Dans le tableau suivant vous trouvez les prix de quelques certificats SSL en Algérie.

Certificats	Prix DZ/an
THATE SSL	3989
COMODO SSL	2000
GeoTrust SSL	9999
SYMANTEC SSL	34000
RAPIDSSL SSL	1999

Conclusion

Le SSL maintenant est essentiale pour sécuriser tout échange sur le réseau. Il peut être utilisé avec n'importe quel protocole TCP/IP. Ce protocole utilise plusieurs méthodes de chiffrement symétriques est asymétriques.

Malgré la grande sécurité que ce protocole nous donne, il était casse par des chercheurs suisses. Qui confirme que la sécurité totale n'existe pas.

BIBLIOGRAPHIE

- Mieux comprendre les certificats SSL, Certificat Thawate
- NOUVELLES TECHNOLOGIES RESEAUX SSH – SSL– TLS, auteurs :STEPHANE BRINSTER ,GUILLAUME LECOMTE ,AYMERIC BERNARD , UNIVERSITE DE MARNE LA VALLEE 2002,2003
- Introduction to Secure Sockets Layer , cisco system
- Technology Primer: Secure Sockets Layer (SSL) : bluecoat
-

Des sites web

- Tbs internet : https://comodo.tbs-certificats.com/ssl_explication.html.fr
- Wikipidia : https://fr.wikipedia.org/wiki/Netscape_Communications
- Droit et technologies : http://www.droit-technologie.org/actuality-624/le-protocole-ssl-a-ete-casse-par-des-chercheurs-suisses.html

Des vidéos :

- SSL Certificate Explained : https://www.youtube.com/watch?v=SJJmoDZ3il8
- How SSL works tutorial - with HTTP example https://www.youtube.com/watch?v=iQsKdtjwtYI