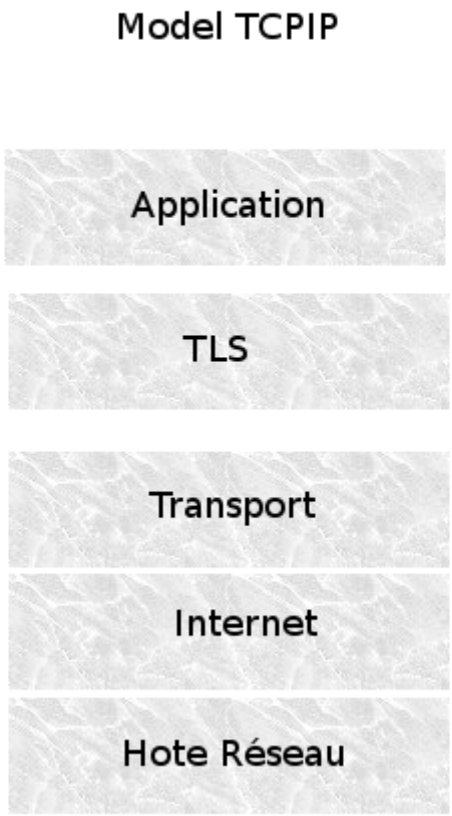
Transport Layer Security protocol Version 1.0

Présentation et étude du protocole.

Transport Layer Security (couche de transport sécurisé).

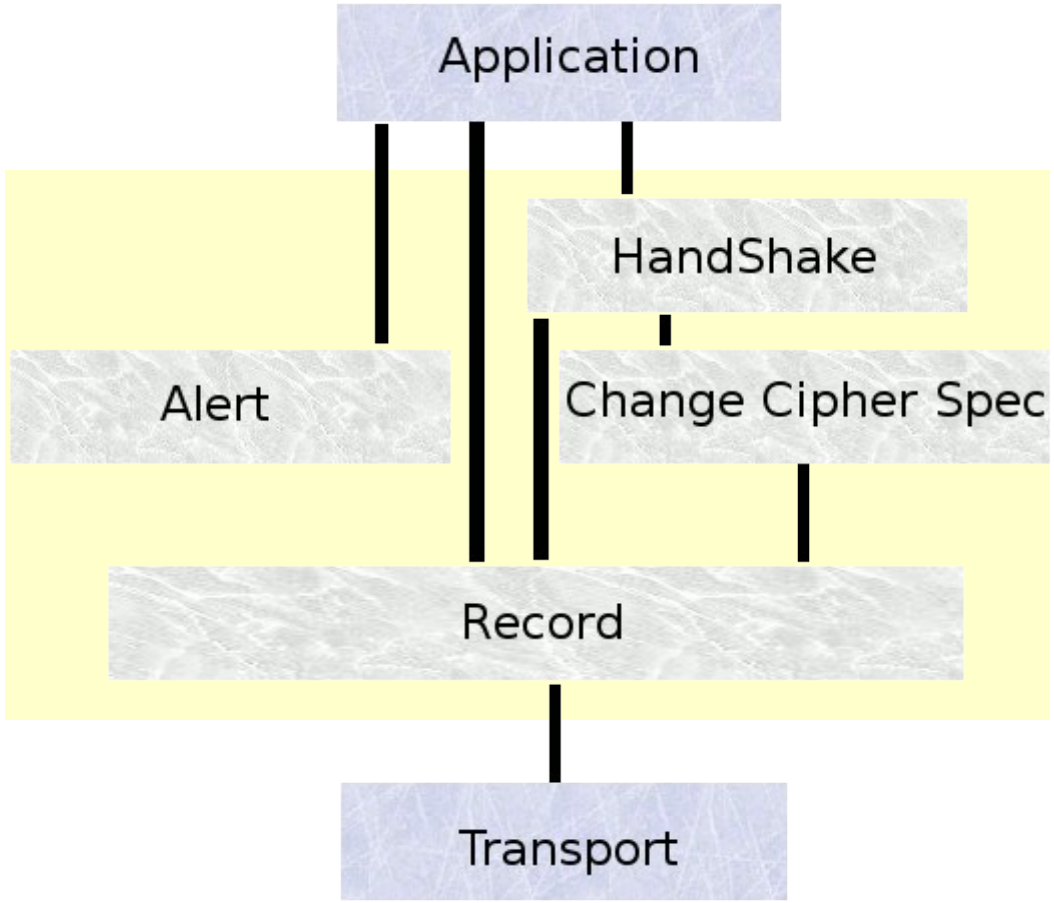
Détenu actuellement par IETF,c'est un protocole de sécurisation des échanges sur Internet, développé à l'origine par Netscape (SSL version 2 et SSL version 3).



Localisation dans la pile de protocoles.

Un protocole Composé de quatre parties distinctes.

Handshake Protocol.	: Négociation.
Change Cipher Spec Protocol.	: Annonce.
Alarm Protocol.	: Gestion des erreurs et alertes.
Record Protocol.	: Communication.



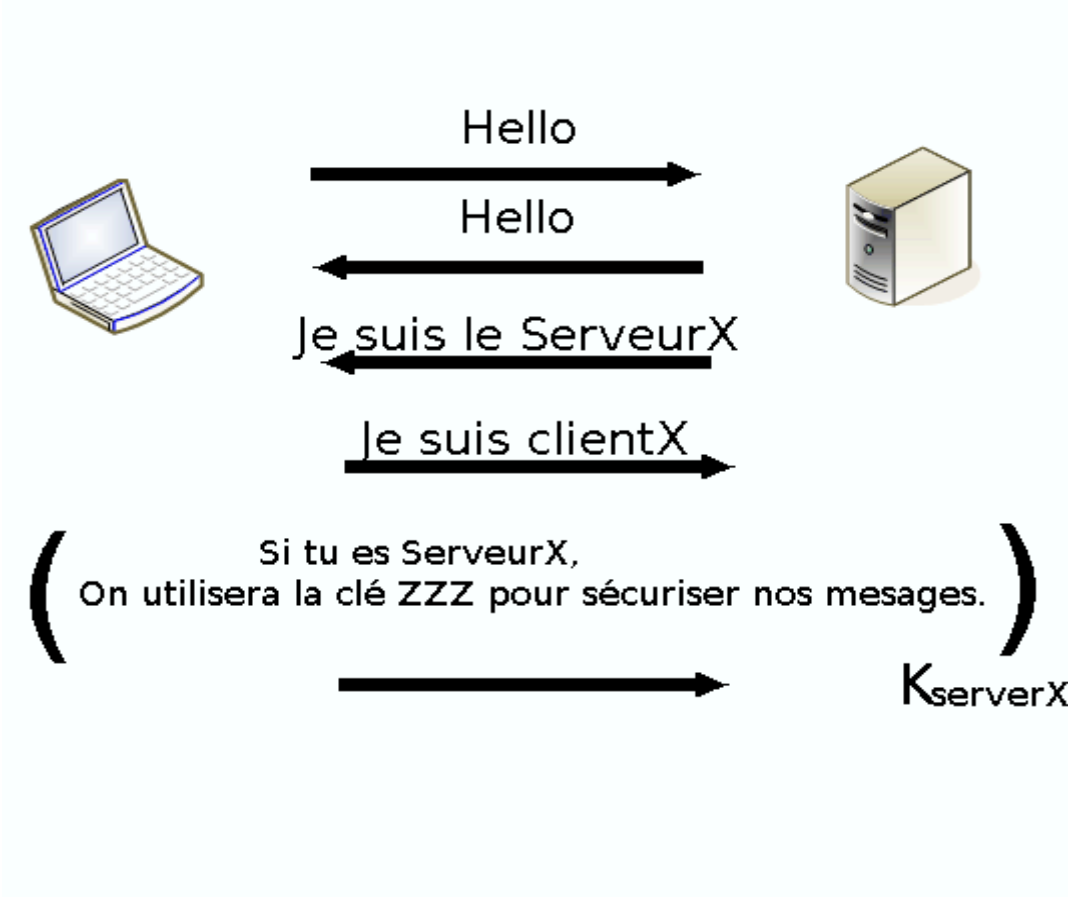
Quatre sous protocoles présent dans TLS.

Le protocole Handshake. - Négociation.

Négociation des paramètres de cryptage qui seront mis en œuvre lors de la connexion.

Type	Longueur	Contenu
1 Octet	3 Octets	+ de 1 Octet

Format d'une trame.



Échange client serveur.

Le protocole Change Cipher Spec. - Annonce.

Un protocole contenant un unique message.

```
Struct {
          enum { change_cipher_spec(1), (255) }
type;
       } ChangeCipherSpec;
```

Spécification donné par le standard

Le protocole Alarm. - Gestion des erreurs et alertes sur deux octets.

Gestion des erreurs.

Des erreurs fatales :

Unexpected_message , Bad_record_mac, Decompression_failure , Handshake_failure , Illegal_parameter .

Les warnings sont :

Close_notify , No_certificate , Bad_certificate , Unsupported_certificate , Certificate_revoked , Certificate_expired , Certificate_unknown .

Le protocole Record. - Communication.

Une interface unifiée.

Encapsulation.

- Permet aux données SSL et TLS d'être transmises et reconnues sous une forme homogène.

Confidentialité.

- Assure que le contenu du message ne peut pas être lu par un tiers : les données sont chiffrées en utilisant les clés produites lors de la négociation.

Intégrité et Identité.

- Permet de vérifier la validité des données transmises, grâce aux signatures MAC : cette signature est elle aussi générée l'aide des clés produites lors de la négociation.

Un protocole développé pour sécuriser les communications.

TLS fonctionne suivant un mode client-serveur, puisque développé en tant que tel.
Il fournit les objectifs de sécurité suivants, **et pas que pour les serveur Http** :

- l'authentification du serveur.
- la confidentialité des données échangées (ou session chiffrée).
- l'intégrité des données échangées.
- l'authentification ou l'authentification forte du client avec l'utilisation d'un certificat numérique (en option).

- la spontanéité.
- la transparence.

Aspects cryptographiques.

Les différents points d'un protocoles plein de ressources.

Chiffrement symétrique ou à clé secrète.

Chiffrement asymétrique ou clé publique.

Signature et hachage.

Apparition de la notion de Certification (X.509).

Man in the middle.

Note.

IETF : Internet Engineering Task Force

L’Internet Engineering Task Force, abrégée IETF, littéralement traduit de l'anglais en « Détachement d'ingénierie d'Internet » est un groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards pour Internet. L'IETF produit la plupart des nouveaux standards d'Internet.

Biblio.

`The TLS Protocol Version 1.0`
http://tools.ietf.org/html/rfc2246

SSL et TLS par Vincent LIMORTE, François VERRY et Sébastien FONTAINE (_SebF)

http://www.authsecu.com/ssl-tls/ssl-tls.php

SSL Man-in-the-Middle Attacks

http://www.sans.org/reading_room/whitepapers/threats/ssl_maninthemiddle_attacks_480?show=480.php&cat=threats