Gilles.Roussel©univ-mlv.fr

SSL et TLS

SSL et TLS

- SSL v1.0 v2.0 v3.0 Netscape
- TLS v1.0 (RFC2246)
  http://www.ietf.org/rfc/rfc2246.txt
- TLS v1.0 et SSL v3.0 équivalents
- Nombreux protocoles au dessus de SSL
  - HTTPS
  - IMAPS
  - SSMTP
  - SLDAP

SSL et TLS

- Protocole entre Transport (TCP) et Application

- Assure :
  - Authentification possible du serveur et de client
  - Confidentialité et intégrité des données
- Largement utilisé dans WWW

SSL et TLS

- Authentification du client ou du serveur après l'échange de certificats
  - Utilisation de CA pour vérifier le certificat
- Confidentialité et intégrité des sessions *via* génération de clef secrète de session
- Compression optionnelle
- Deux sous-protocoles :
  - SSL Record Protocol (encapsule/fragmente les données)
  - SSL handshake protocol (configuration)

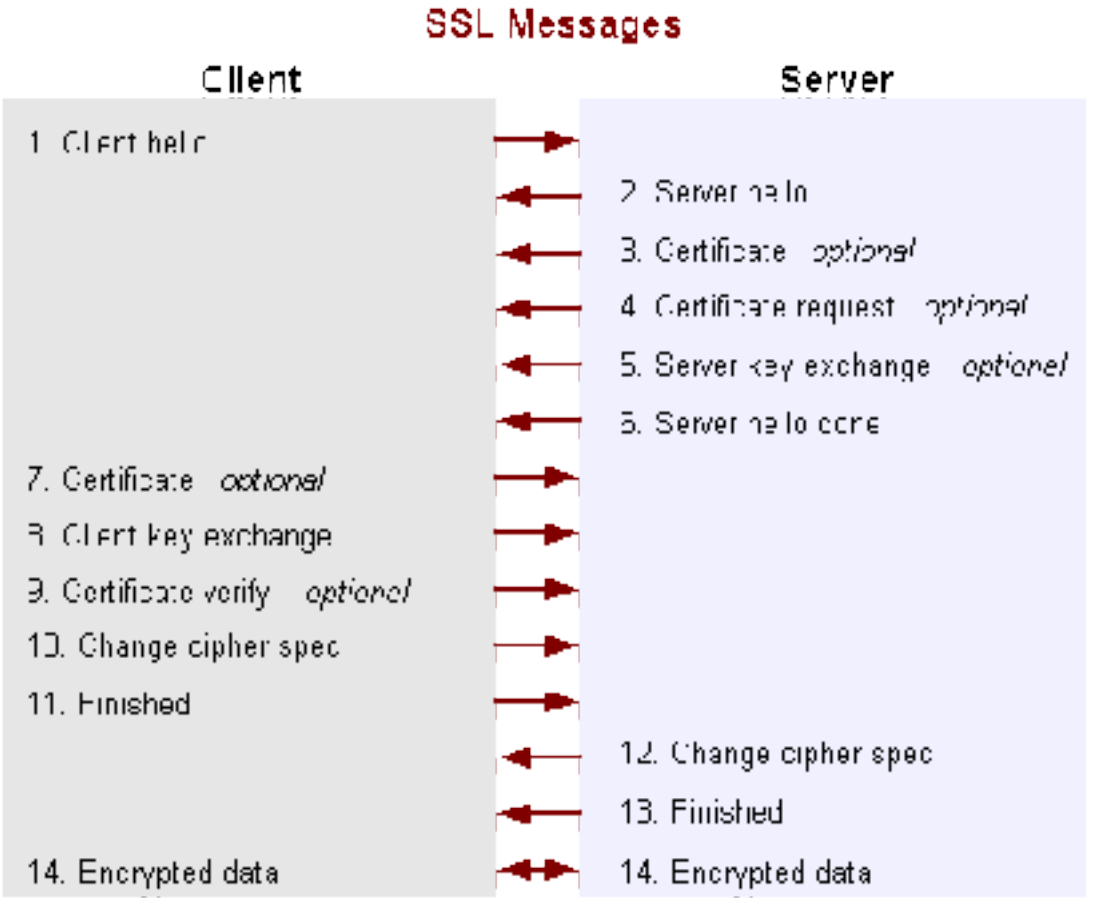
SSL et TLS

- Utilisation transparente pour les protocoles de la couche supérieure. Mode tunnel.
- Initialisation et utilisation de l'authentification SSL par le protocole de la couche supérieur nécessite redéfinition. Mode natif ?

SSL Handshake

- Authentification optionnelle du client et du serveur
- Choix des algorithmes cryptographiques
- Génération de clef privée *via* des méthodes à clefs publiques
- Établissement de la connexion chiffré
  - confidentialité + intégrité
- Possibilité de restreindre les choix d'algorithmes
- Cache de session possible

SSL Handshake



SSL Handshake

1. Client Hello
   émission en particulier de :
   - la version maximale de SSL supportée (TLS = 3.1)
   - la liste des suites d'algorithmes supportées
   - une valeur aléatoire
2. Server Hello
   choix de la meilleure :
   - version SSL
   - suite d'algorithme supportée
   - valeur aléatoire

SSL Handshake

3. *Certificate (serveur)
   envoie d'un certificat ou d'une chaîne de certificats par le serveur
4. *Certificate request (serveur)
   demande un certificat du client (rare)
5. * Server key exchange (serveur)
   message complémentaire pour l'échange des clefs
6. Server hello done (serveur)
   Fin des émissions du serveur

SSL Handshake

7. * Certificate (client)
   certificat éventuel du client
8. Client key exchange (client)
   envoi d'une clef pre-master chiffrée avec la clef publique du serveur
9. * Certificate verify (client)
   signature par le client de tous les messages précédents

SSL Handshake

10. Change cipher spec (client)
    passe en mode chiffré avec clef master générée
11. Finished(client)
    permet de vérifier le changement de chiffrement
12. Change cipher spec (serveur)
    passe en mode chiffré avec clef master générée
13. Finished (serveur)
    permet de vérifier le changement de chiffrement

Authentification du serveur

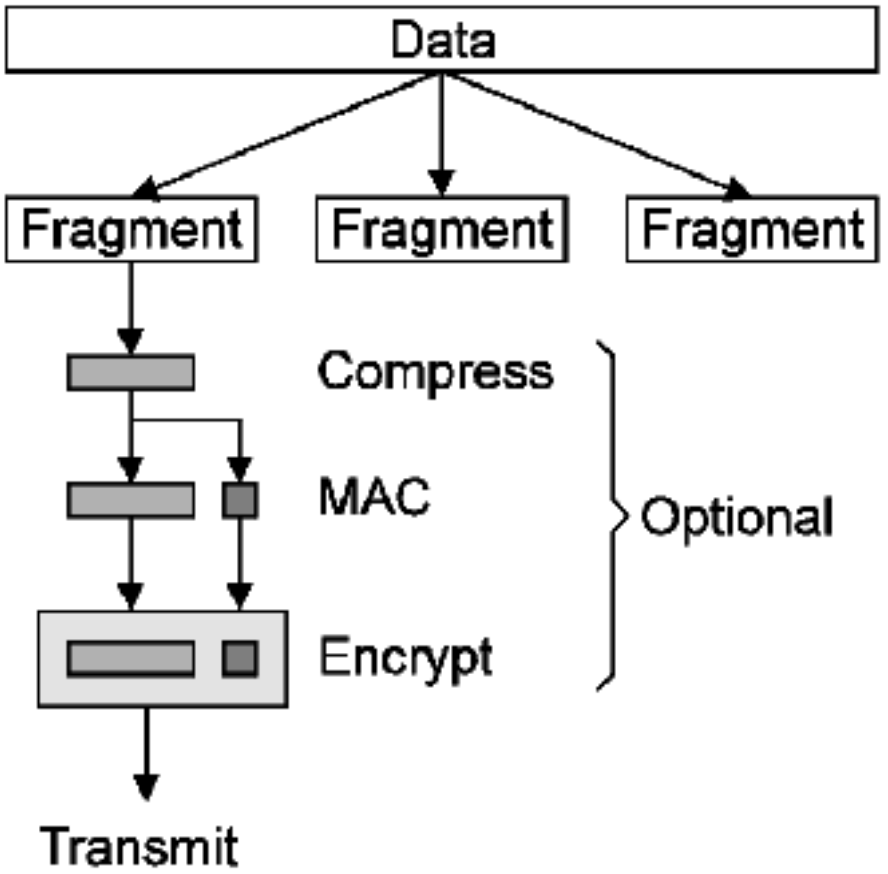
- Vérification du certificat
  - Date valide
  - Issuer CA de confiance
  - Vérification de la signature du certificat par le CA
  - DN correspond au serveur
- Le serveur doit ensuite récupérer avec sa clef privée la clef *pre-master*

Authentification du client

- Vérification de la signature des messages précédents par clef publique
- Vérification du certificat comme pour le serveur

SSL Record Protocol

- Assure le transfert des données
  - compression + MAC + chiffrement



Algorithmes cryptographiques

- Protocole extensible
- Algorithmes à clefs publics utilisés pour l'authentification et le partage d'une clef secrète de session
- Algorithmes à clef secrète utilisés pour le chiffrement des données car plus rapides

Algorithmes cryptographiques

- DES. Data Encryption Standard
- DSA. Digital Signature Algorithm
- KEA. Key Exchange Algorithm
- MD5. Message Digest algorithm
- RC2 and RC4. Rivest ciphers
- RSA. Public-key algorithm
- RSA key exchange.
- SHA-1. Secure Hash Algorithm
- Triple-DES. DES applied three times.

Algorithmes cryptographiques

- Choix des mécanismes de sécurité dépend de :
  - la politique de sécurité de « l'entreprise »
  - la version du protocole SSL
  - les lois gouvernementales

Algorithmes cryptographiques

- MEILLEURES GARANTIES :
  - 3DES avec un chiffrement à 168 bits couplé avec SHA-1 pour l'intégrité. Mécanisme uniquement autorisé aux USA. 3DES est nettement moins rapide que RC4. Supporté par SSL 2.0 et 3.0

Algorithmes cryptographiques

- BONNES GARANTIES :
  - RC4 avec un chiffrement 128 bits couplé à MD5. RC4 est le plus rapide des modes de chiffrement offert. Supporté par SSL 2.0 et 3.0.
  - RC2 avec un chiffrement 128 bits couplé à MD5. RC2 est plus lent que RC4. Supporté uniquement par SSL 2.0.
  - DES avec un chiffrement 56 bits couplé avec SHA-1. Moins performant que RC4 ou RC2. Supporté par SSL 2.0 et 3.0 à la différence que SSL 2.0 utilise MD5 pour authentifier les messages.

Algorithmes cryptographiques

- CHIFFREMENT DEDIE A L'EXPORTATION : Chiffrement procurant la plus haute sécurité pour une exportation internationale
  - RC4 avec un chiffrement 40 bits couplé avec MD5. Supporté par SSL 2.0 et 3.0
  - RC2 avec un chiffrement 40 bits couplé avec MD5. Supporté par SSL 2.0 et 3.0

Algorithmes cryptographiques

- FAIBLES GARANTIES :
  Intégrité des données sans le chiffrement.
  - Authentification des messages avec MD5 sans chiffrement. Utilisée si le serveur et le client n'ont aucun chiffrement en commun.