BILAN SSL

Généralités

SSL (Secure Socket Layer) ,TLS (Transport Layer Security)

Utilisé pour les communications réseaux sécurisées

Assure l’authentification et le chiffrement

Fonctionne au dessus de la couche transport

TLS

évolution de SSL

SSL utilise du MD5, TLS utilise SHA

repose sur un procédé de chiffrement à clé publique

indépendant du protocole utilisé

On peut mettre en œuvre TLS pour des transactions HTTP, du mail du FTP etc.

Pour http les urls sont de la forme: https://

Les algorithmes supportés

Confidentialité: Algosymétrique (3DES, AES, IDEA, ...)

Intégrité: HMAC: Hash Message AuthenticationCode

Authentification: X.509 et MAC

TLS est composé de deux parties

-Le protocole TLS Record

Sécurise la connexion en utilisant les méthodes de chiffrement

symétriques supportées

Vérifie l’intégrité des données à l’aide de HMAC

-Le protocole TLS Handshake

Authentifie le client et le server lors de l’initiation de la connexion

Négocie entre le client et le serveur l’algorithme de chiffrement et les clés de session à

utiliser

Remonter des alertes

La connexion SSL

niveau transport proposant un service

Fonctionne en point à point de manière transitoire

Associée à une session

La session SSL

une association crée entre un serveur et un client par le Handshake

Définit les paramètres de sécurité à utiliser et pouvant être partagés par plusieurs connexions

La session évite de renégocier les paramètres à chaque connexion (ex HTTP)

peut avoir plusieurs session en parallèle mais pas implémenté en pratique

Le protocole TLS Record

Assure la confidentialité et l’intégrité 29

Manipule des fragments d’au plus 214 octets

Une compression peut également être appliquée si nécessaire

Le protocole TLS Handshake

-le plus complexe de TLS et permet aux deux parties de s’authentifier

-Le protocole se découpe en fait en 4 phases

L’Initiation de connexion

L’échange de certificat et de clés

La vérification du certificat par le client et le paramétrage de la connexion

La mise en place finale de la connexion sécurisée

-Ce protocole a été pensé pour résister

Aux attaques par abaissement de version (rollback)

Aux attaques par rejeu

Quelques applications sur SSL/TLS

très largement utilisé à l’heure actuelle, quasiment tous les principaux protocoles ont leur équivalent sécurisé

ex : HTTPS (port 443 au lieu de 80),SSMTP (port 465), SPOP3 (port 995), IMAPS, Telnets même si on lui préfèrer a SS

Avantages

Protocole assez bien pensé et complet pour les échanges réseaux sécurisés

Supporté par quasiment tous les navigateurs modernes

Transparent par rapport au protocole de transport

Largement utilisé

On le retrouve dans d’autres architectures comme WAP (WTLS)

Inconvénients

Les mêmes que pour les solutions basées sur des PKIs à grande échelle

On n’est pas averti si le certificat est répudié par exemple

La renégociassions de session n’est pas prévue (pratique pour HTTP mais pénalisant

pour FTP ou telnet par exemple)

La négociation sur les algorithmes de chiffrement et de signature utilisés peuvent

amener à utiliser des solutions faibles

BILAN Crypto

BILAN Firewall