Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 01 mars 2005
N° CERTA-2005-REC-001

Affaire suivie par :
CERTA

RECOMMANDATION DU CERTA

Objet : La bonne utilisation des protocoles SSL/TLS

Gestion du document

Référence	CERTA-2005-REC-001
Titre	La bonne utilisation des protocoles SSL/TLS
Date de la première version	01 mars 2005
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Historique des protocoles SSL/TLS

Le protocole SSL (*Secure Socket Layer*) est un protocole développé par Netscape. La première version du protocole a été testée par l'éditeur en interne, et la deuxième version (SSL v2) a été publiquement diffusée en 1994.

Actuellement la version utilisée est SSL v3.

Le développement de ce protocole a été repris par l'IETF au sein du groupe TLS (*Transport Layer Security*).

Le protocole TLS v1.0 a été normalisé en 1999 par l'IETF dans la RFC 2246 (cf. section Documentation) et présente quelques évolutions mineures par rapport à la version SSL v3. Ces protocoles ne sont pas compatibles mais la plupart des serveurs et des navigateurs web peuvent mettre en œuvre les deux protocoles.

2 Principes de fonctionnement

Les protocoles SSL/TLS fonctionnent entre le protocole transport (TCP ou UDP) et le niveau applicatif pour sécuriser un protocole nativement peu sûr. Citons par exemple les protocoles HTTPS (port 443) ou POP3S (port 995).

L'utilisation de SSL/TLS permet l'authentification mutuelle du serveur et du client, le chiffrement et la vérification de l'intégrité des connexions.

Le protocole SSL/TLS est constitué des deux sous-protocoles : le protocole *TLS Record* et le protocole *TLS Handshake*.
Le protocole *TLS Record* a pour but de chiffrer les connexions avec un algorithme symétrique, et de vérifier leur intégrité à l'aide d'une fonction de type *HMAC*.

Le protocole *TLS Handshake* a pour rôle d'authentifier les deux parties, de leur permettre de négocier les algorithmes et les clés de session utilisées par le protocole *TLS Record* et de remonter des alertes. L'authentification peut avoir lieu à l'aide de certificats.

3 Attaques sur les protocoles SSL/TLS

3.1 Attaques sur les mise en œuvres des protocoles

Comme toutes les applications logicielles, les mises en œuvre des protocoles SSL et TLS peuvent présenter des vulnérabilités permettant à un utilisateur mal intentionné d'exécuter du code arbitraire à distance ou de provoquer un déni de service.

Il est dès lors indispensable d'appliquer les correctifs correspondants aux mises à jour de ces applications.

3.2 Attaque de type "*man in the middle*"

En dehors des attaques sur la mise en œuvre des protocoles, l'attaque la plus répandue sur les protocoles SSL/TLS est l'attaque de type "*man in the middle*" (MITM) encore appelée "attaque de l'intercepteur".
Cette attaque consiste à intercepter le trafic entre deux parties avant qu'elles ne débutent une session SSL. L'intercepteur négocie alors une session avec chaque partie et fait suivre le trafic en le déchiffrant et rechiffrant à la volée.

Par exemple, dans le cas de l'utilisation du protocole HTTPS par un client web pour authentifier un serveur, l'intercepteur crée un certificat ressemblant au certificat légitime du serveur et détourne le trafic.
Si, malgré l'avertissement du navigateur sur le certificat, le client poursuit sa session, l'intercepteur obtiendra toutes les informations que le client envoie au serveur (mots de passe, identifiants bancaires, ...) sans que ce dernier ne s'en rende compte.

De nombreux outils qui reproduisent cette attaque sont disponibles sur l'Internet.

4 Solution

Lors d'une connexion à un serveur avec le protocole SSL/TLS, il est primordial de vérifier correctement le certificat présenté par le serveur. C'est la seule manière de s'assurer que la connexion ne sera pas interceptée par un éventuel attaquant.

Un certificat valide le lien entre une clé publique et une identité. Il est signé par une autorité de certification.

Dans les navigateurs, les certificats racine de certaines autorités de certification sont pré-installés.

Lorsque le certificat présenté par un serveur n'a pas été signé par l'une de ces autorités, le navigateur demande confirmation avant d'accepter le certificat. Il faut alors s'assurer que le certificat présenté par le serveur est le bon certificat. Cette vérification peut se faire à l'aide de deux champs du certificat : le numéro de série et l'empreinte numérique (empreinte md5 ou sha1).

Pour vérifier la concordance des informations, il faut disposer d'un moyen de communication de confiance (téléphone, courrier, diffusion de la main à la main, ...) par lequel pourront être comparés les numéros de série et

les empreintes.

De même, il ne faut installer un certificat d'autorité qu'après s'être assuré que le certificat est correct.

5 Limites des protocoles SSL/TLS

Les protocoles SSL et TLS servent à sécuriser les *échanges* d'informations entre un client et un serveur et à obtenir un authentification mutuelle.

Une session SSL/TLS correctement établie va donc protéger les échanges entre les parties, mais ne sera en aucun une garantie de sécurité pour les systèmes client ou serveur.

Ainsi, si un pirate installe par exemple un enregistreur de frappe (ou *keylogger*) sur le poste client, il sera en mesure de récupérer les mots de passe ou toute information confidentielle, même si celle-ci a été émise lors d'une session SSL/TLS.

De même, un serveur qui utilise des sessions SSL/TLS pour récupérer des données sensibles peut être compromis et les données recueillies pourront être volées.

Il est donc primordial d'utiliser les protocoles SSL/TLS en prenant certaines précautions, et ne pas leur prêter une trop grande garantie de sécurité sur l'ensemble de la chaîne d'information.

6 Documentation

- RFC 2246 de l'IETF sur le protocole TLS 1.0 :
  http://www.ietf.org/rfc/rfc2246.txt
- Site Internet d'OpenSSL :
  http://www.openssl.org

Gestion détaillée du document

01 mars 2005 version initiale.