Dossier documentaire

Document 1 : Recommandations de sécurité relatives à TLS de l'ANSSI

D'après ssi.gouv.fr.

Le protocole TLS est une des solutions les plus répandues pour la protection des flux réseau. Dans ce modèle client–serveur, les données applicatives sont encapsulées de manière à assurer la confidentialité, l'intégrité et empêcher leur rejeu. Le serveur est nécessairement authentifié, et des fonctions additionnelles permettent l'authentification du client si nécessaire.

Depuis l'apparition de son prédécesseur SSL en 1995, TLS a été adopté par de nombreux acteurs de l'Internet pour sécuriser le trafic lié aux sites web et à la messagerie électronique. Il s'agit par ailleurs d'une solution privilégiée pour la protection de flux d'infrastructure internes. Pour ces raisons, le protocole et ses implémentations font l'objet d'un travail de recherche conséquent. Au fil des années, plusieurs vulnérabilités ont été découvertes, motivant le développement de corrections et de contre-mesures pour prévenir la compromission des échanges.

Le déploiement TLS apportant le plus d'assurance en matière de sécurité repose donc sur l'utilisation de logiciels mis à jour, mais aussi sur l'ajustement des paramètres du protocole en fonction du contexte. Les explications apportées par le présent guide sont complétées par plusieurs recommandations visant à atteindre un niveau de sécurité conforme à l'état de l'art, notamment au sujet des suites cryptographiques à retenir.

Le document suivant détaille le problème posé par TLS v1.1 :

https://www.ssi.gouv.fr/uploads/2016/09/guide_tls_v1.1.pdf

Document 2 : Le protocole TLS-1.0 et les cartes de paiement

Le protocole TLS 1.0 est officiellement obsolète en raison de problèmes de sécurité. Il n'est pas considéré comme un système de cryptographie fort d'après la norme de sécurité de l'industrie des cartes de paiement PCI (Payment Card Industry[8]).

Document 3 : Chiffrement symétrique et asymétrique

Chiffrement symétrique : une clé unique est utilisée pour chiffrer et déchiffrer le message. Avec cette méthode, le chiffrement est simple. Sa faiblesse réside dans la transmission de la clé à un correspondant.

Chiffrement asymétrique : deux clés (clé publique, clé privée) sont nécessaires pour chiffrer et déchiffrer le message. La clé publique peut être transmise à des tiers et la clé privée est confidentielle. Cette technique permet de transmettre la clé de chiffrement symétrique à un tiers de manière confidentielle.

Document 4 : Fonctions de hachage d'après la CNIL

D'après cnil.fr.

L'utilisation d'une fonction de hachage permet de ne pas stocker les mots de passe en clair dans la base mais uniquement de stocker une empreinte de ces derniers. Il est important d'utiliser un algorithme

[8]PCI (Payment Card Industry) : La norme de sécurité de l'industrie des cartes de paiement est un standard de sécurité des données qui s'applique aux différents acteurs de la chaîne monétique. La norme PCI DSS est établie par les cinq principaux réseaux cartes et est gérée par le Conseil des normes de sécurité PCI.

public réputé fort afin de calculer les dites empreintes. A ce jour, MD5 ne fait plus partie des algorithmes réputés forts.

De même, les fonctions de hachage publiques réputées fortes étant par nature à la disposition de tous, il est techniquement possible pour tout un chacun de calculer des empreintes. Aujourd'hui, on trouve facilement sur internet des dictionnaires immenses d'empreintes MD5 précalculées et, grâce à ces données, il est aisé de retrouver instantanément le mot de passe ayant été utilisé afin de générer ces empreintes. Afin de limiter ce risque, il est conseillé d'utiliser des fonctions spécialisées appelées « fonction de dérivation de clé », telles que scrypt ou Argon2 par exemple, qui sont conçues spécifiquement pour stocker des mots de passe.