Chiffrement et authentification

AES :

Advanced Encryption Standard (standard de chiffrement avancé) est un algorithme de chiffrement symétrique datant de 2000.

L'algorithme prend les16 er octets de la clé, les permutent puis les placent dans une matrice qui va subir une rotation vers la droite puis une transformation linéaire.

La clé peut faire 128, 192 ou 256 bits.

Il remplace le DES devenu obsolète (clefs de 56 bits uniquement).

Il est utilisé par les organisations gouvernementales américaines.

L'AES est peu sensible aux attaques basées sur la cryptanalyse linéaire et différentielle. Par contre la force brute pourrait un jour le casser.

DES :

Data Encryption Standard (standard de chiffrement de données) est un algorithme de chiffrement par bloc utilisant des clés de 56 bits datant des années 1970.

DES a été utilisé pour chiffrer les mots de passe dans les systèmes UNIX.

Il est abandonné et remplacé par l'AES qui résiste mieux aux attaques.

EAP :

Extensible Authentication Protocol est un mécanisme d'identification utilisé dans les réseaux sans fil (wifi) et les liaisons point à point.

L'EAP permet de négocier une clé entre le client et le point d'accès.

Les protocoles WPA et WPA2 utilise l'EAP comme mécanisme d'identification.

LEAP :

Lightweight Extensible Authentication Protocol est une implémentation propriétaire de EAP conçu par Cisco.

Sensible aux attaques par dictionnaire.

EAP-TLS :

EAP-TLS est un Standard ouvert IETF. Il est implanté chez de nombreux fabricants de matériel sans fil.

C’est le seul protocole EAP qui doit obligatoirement être implanté sur un matériel pour pouvoir porter le logo WPA ou WPA2.

EAP-TLS utilise deux certificats (un coté serveur, un coté client) afin de créer un tunnel sécurisé qui permettra l’identification.

La sécurité est bonne car même si le mot de passe est découvert, l’identification sera impossible car il faut le certificat client.

EAP-TTLS :

EAP-Tunneled Transport Layer Security est un standard ouvert IETF.

L’EAP-TTLS offre un très bon niveau de sécurité. Il utilise des certificats X-509 uniquement sur le serveur d'identification. Le certificat est optionnel du côté client.

Il est plus sécurisé que PEAP car il ne diffuse pas le nom de l'utilisateur en clair.

PEAP :

Protected Extensible Authentication Protocol est une méthode de transfert sécurisée d'informations d'identification, pour les réseaux sans fil.

C’est un standard ouvert de l'IETF.

PEAP n'est pas une méthode de chiffrement, c'est une procédure pour identifier un client sur un réseau.

PEAP est le concurrent d’EAP-TTLS, il utilise tous les deux une Infrastructure à clés publiques (PKI) du côté serveur uniquement, pour la création d'un tunnel TLS protégeant l'identification.

TLS :

Transport Layer Security, anciennement nommé SSL, est un protocole de sécurisation des échanges sur Internet,

TLS est compatible avec SSL.

TLS diffère de SSL pour la génération des clés symétriques. Cette génération est plus sécurisée car l'algorithme ne repose pas uniquement sur MD5 pour lequel sont apparues quelques faiblesses en cryptanalyse.

SSL fonctionne en client-serveur. Il assure :

- l'authentification du serveur ;
- la confidentialité des données échangées ;
- l'intégrité des données échangées ;
- l'authentification ou l'authentification forte du client avec l'utilisation d'un certificat numérique.

SSL :

La nouvelle version de SSL s’appelle maintenant TLS.

RSA :

Rivest Shamir Adleman est un algorithme asymétrique de cryptographie à clé publique écrit en 1977.

Le RSA est très utilisé dans le commerce électronique sur internet pour échanger des données confidentielles.

En 2008, c'est le système à clef publique le plus utilisé (carte bancaire française, de nombreux sites web commerciaux…).