Kerberos

I)Généralité

Un serveur Kerberos permet d'identifier des utilisateurs distants afin de les autoriser à accéder à des services réseaux.

Kerberos repose sur un système de cryptographie (algorithme DES) à base de clé secrètes (clé symétriques ou clé privées). La clé secrète est partagée avec chaque client.

Kerberos s'appuie sur deux services pour fonctionner, le serveur d'authentification (AS) et le service de délivrement de tickets de service (TGS).

Le serveur d'authentification (AS) prend en charge l'authentification pure des clients en délivrant une clé de session qui permettra ensuite à l'utilisateur de communiquer avec les autres services Kerberos.

Quand les utilisateurs sont authentifiés et disposent d'une clé de session, le TGS prend en charge les demandes d'accès aux services.

II) Fonctionnement :

Le client envoie une demande en clair (trame contient heure, IP, identifiant) au serveur d'authentification (AS).

Le serveur d'authentification envoie au client un ticket TGT (chiffré avec la clé du service de délivrement et la clé utilisateur).

Le client déchiffre le ticket TGT avec le mot de passe utilisateur.

Le client envoie au serveur d'authentification le ticket TGT (trame contient nom service voulu, heure, IP).

Le serveur d'authentification vérifie le ticket TGT afin d'envoyer le ticket service.

Le client présente le ticket service au service distant qui déchiffre le ticket pour obtenir la clé de session du client

Le service distant est désormais accessible.

III) Avantages :

Le mot de passe ne circule jamais sur le réseau.

L'authentification est unique (c'est le principe du SSO Single Sign On).

Kerberos garantit l'intégrité des données, leur confidentialité, la non répudiation et l'authentification mutuelle des clients services.

IV) Inconvénients :

Chaque service doit être adapté à Kerberos.

Les machines doivent être synchronisées au niveau horaire. En effet la validité des tickets Kerberos est en partie basée sur un horodatage (validité de 5 min).

Tous les mots de passe sont sauvegardés et chiffrés (symétrique avec la clé du serveur) sur le serveur d'authentification. S'il est compromis, tous les mots de passes sont utilisables.

Si un mot de passe utilisateur est compromis, un attaquant peut l'utiliser pour déchiffrer d'autres tickets et accéder à différents services.