Chapitre 4 : Outil d'authentification en réseau Kerberos

SÉcurité et Cryptographie
2013-2014

Sup Galilée INFO3

Kerberos

Kerberos est un protocole d'authentification à tierce personne de confiance (*i.e.*, une entité ayant la connaissance de toutes les clefs). Il offre l'authentification sûre en réseau en permettant à une personne d'accéder à différents services du réseau. Kerberos est basé sur le système DES de cryptographie à clef secrète. Kerberos connaît la clef secrète de chaque entité du réseau.

Le service d'authentification Kerberos a initialement été développé au MIT dans le cadre d'un projet appelé Athena. La version pour UNIX fait partie du domaine public.

Modèle de Kerberos

Les entités de Kerberos sont les clients et les serveurs du réseau. Pour un utilisateur humain, la clef secrète est un mot de passe haché (c'est le haché que connaît Kerberos). Les services réseau qui nécessitent une authentification, ainsi que les clients qui désirent utiliser ces services, enregistrent leur clef secrète auprès de Kerberos.

Puisque Kerberos connaît la clef secrète de tout le monde, il peut créer des messages pour convaincre une entité de l'identité d'une autre (comme nous le verrons). Kerberos crée également des clefs secrètes temporaires, appelées clefs de session, qui sont données au client et au serveur. Une clef de session servira pour le chiffrement de messages entre ces deux entités puis sera détruite.

Modèle de Kerberos

Kerberos offre trois niveaux de protection :

- Il offre l'authentification au début d'une connexion au réseau, après quoi toutes les autres communications sont supposées venir de l'entité authentifiée.

- Il offre l'authentification de tout message envoyé entre deux entités,

- Il offre l'authentification et le chiffrement de tout message envoyé entre deux entités.

Fonctionnement général

Comment un client peut-il utiliser un service via Kerberos ?

Un client demande au service Kerberos un ticket pour le service de délivrance des tickets (abrégé en SDT). Ce ticket, appelé ticket d'obtention de ticket (abrégé en TOT) est envoyé au client, chiffré avec la clef secrète du client.

Pour utiliser un service particulier, le client demande un ticket pour ce service au SDT. Pour ce faire, il lui envoie le TOT déchiffré.

Si tout est correct, alors le SDT lui transmet un ticket de service (lequel est un message chiffré avec la clef secrète du serveur demandé qui contient notamment une clef de session).

Le client présente ensuite le ticket au service demandé avec un authetifiant (un message chiffré avec la clef de session qui contient notamment cette clef de session).

Structure des tickets

- Le TOT est un message qui contient notamment un chiffré (avec la clef secrète K_c du client) $E_{DES}(K_{SDT,c}, K_c)$ où $K_{SDT,c}$ est une clef secrète de session entre le SDT et le client c.

- Un ticket est utilisé pour passer au serveur de façon sûre, l'identité d'un client. Il contient également des informations que le serveur peut utiliser pour s'assurer que le client qui utilise le ticket est bien celui à qui le ticket a été délivré. Un ticket n'est valable pour un seul client et un seul serveur. Le client ne peut pas déchiffrer les informations contenues dans un ticket. En effet un ticket est constitué comme suit :
$T_{s,c} = s, E_{DES}((c, addr, times), K_s)$ où s est l'identifiant du serveur, c celui du client, *addr* l'adresse réseau du client, *times* les heures de début et de fin de validité du ticket. On notera $K_{s,c}$ une clef de session pour s et c.

Authentifiant

C'est une accréditation supplémentaire qui est présentée avec le ticket. Contrairement au ticket, l'authentifiant n'est utilisable qu'une seule fois. L'authentifiant contient des informations chiffrées avec la clef de session. Ceci a pour but de prouver que l'expéditeur de l'authentifiant connaît cette clef. Parmi les informations se trouve une date : afin qu'il ne soit valable qu'une fois.

La structure d'un authentifiant est : $A_{s,c} = E_{DES}((c, date, K_{s,c}), K_{s,c})$.

Obtention d'un ticket

Le client prouve son identité par mot de passe. Mais on ne veut pas que ce mot de passe soit compromis en étant transmis sur le réseau. Cela fonctionne donc comme suit.

1. Le client envoie au serveur Kerberos son identité et le nom du service SDT (c, SDT) (il peut y avoir plusieurs SDT actifs.)

2. Kerberos recherche l'identification reçue dans sa base de données. S'il la trouve, alors il engendre une clef de session $K_{SDT,c}$.Puis crée un TOT $TOT_c = E_{DES}(K_{SDT,c}, K_c), E_{DES}(T_{SDT,c}, K_{SDT})$ qu'il transmet au client. Rappelons que $T_{SDT,c} = SDT, E_{DES}((c, addr, times), K_{SDT})$.

Obtention d'un ticket

3. Le client envoie au SDT :
$s, E_{DES}(T_{SDT,c}, K_{SDT}), E_{DES}(A_{SDT,c}, K_{SDT,c})$ afin de prouver qu'il connaît la clef de session, où $A_{SDT,c} = E_{DES}((c, date, K_{SDT,c}), K_{SDT,c})$.

4. Si tout est correct, alors le SDT engendre une clef de session $K_{s,c}$ pour le client et le serveur s demandé, qu'il chiffre avec sa propre clef de session partagée $K_{SDT,c}$, crée un ticket de service $T_{s,c}$ chiffré avec la clef secrète K_s du service, et envoie le tout au client.

Autrement dit le client reçoit du SDT le message suivant
$E_{DES}(K_{s,c}, K_{SDT,c}), E_{DES}(T_{s,c}, K_s)$ où
$T_{s,c} = s, E_{DES}((c, addr, times), K_s)$.

Obtention d'un ticket

5. Le client transmet au serveur s le message suivant $E_{DES}(T_{s,c}, K_s), E_{DES}(A_{s,c}, K_{s,c})$ où $A_{s,c} = E_{DES}((c, date, K_{s,c}), K_{s,c})$.

6. Si tout est correct, alors le service réalise l'opération demandée par le client désormais authentifié.

Sécurité de Kerberos

Kerberos n'est bien sûr pas parfait. Parmi les reproches qui lui sont faits :

- Possibilité de rejouer des tickets pendant leur période de validité (c'est une vulnérabilité).

- Besoin de synchronisation horaire du réseau. Or la plupart des protocoles de synchronisation horaire ne sont pas eux-même sécurisé (ou horodaté).