Nicolas Grenèche

Centre de Ressources Informatique - Université d'Orléans

JRES 2011

Sommaire

Plan

Pourquoi Kerberos ?

- SSO système
- Environnement hétérogène
- Tolérance aux pannes
- Supporté par beaucoup d'applications

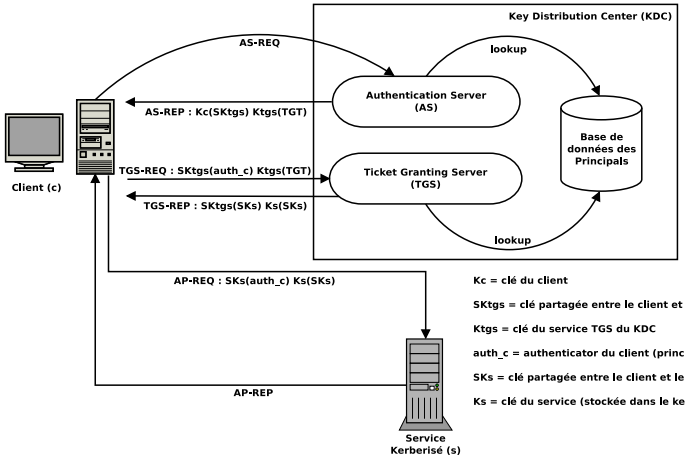
Plan

Les acteurs

- KDC (Key Distribution Center)
  - AS (Autentication Server) → TGT (Ticket Granting Ticket)
  - TGS (Ticket Granting Server) → Ticket de services
- Principals (Utilisateurs, machines et services) : nom associé à un jeu de clés (la même passphrase dérivée selon plusieurs algorithmes ou enctypes)
- Realm

Plan

Le protocole



A retenir

- Cryptographie symétrique
- AS_REQ :
  - Pré authentification
- AS_REP :
  - Le client déchiffre la clé de session TGS avec sa clé privée
- TGS_REP :
  - Le ticket de service est chiffré avec la clé privée associée au service (clé stockée dans le keytab)
  - La clé de session avec le service est chiffrée avec la clé de session TGS

Plan

Objectif

Principes à suivre :

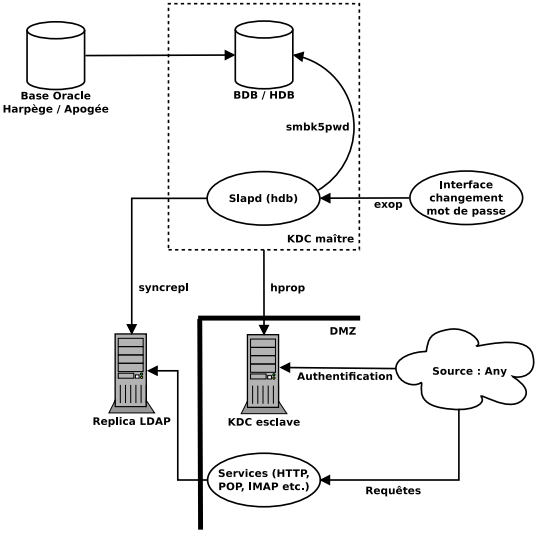
- Séparation de privilèges
- Moindre privilège

Services

Le service Kerberos est divisé en plusieurs sous programmes (indépendants) :

- Kpasswd : changement de mot de passe
- Kadmind : administration distante de la base de donnée du KDC
- Kdc : service AS et TGS

Schéma


Base Oracle
Harpège / Apogée
BDB / HDB
smbk5pwd
Slapd (hdb)
exop
Interface
changement
mot de passe
KDC maître
syncrepl
hprop
DMZ
Authentification
Source : Any
Replica LDAP
KDC esclave
Services (HTTP,
POP, IMAP etc.)
Requêtes

Réplication

Plusieurs méthodes de réplication :

- syncrepl
- iprop
- hprop (retenu)

Plan

Politique de filtrage

- Kerberos : protocole d'authentification sur réseaux non surs
- Service LDAP utilisé en backend d'application frontales
- La politique de filtrage diffère :
  - KDC esclaves "from any"
  - Replica LDAP "from applications"

Surface

KDC maître :

- Slapd
- Pas de service Kpasswd (smbk5pwd)
- Pas de service Kadmind (ssh + kadmin -l)
- Pas de service Kdc
- hprop type push

KDC esclave :

- Pas de Slapd
- Kdc

Ouverture de session

- Unix : PAM et SSSD
- Windows
  - Domaine (relation d'approbation, realm par défaut = celui du CRI)
  - Standalone
  - Mapping Principal / SID

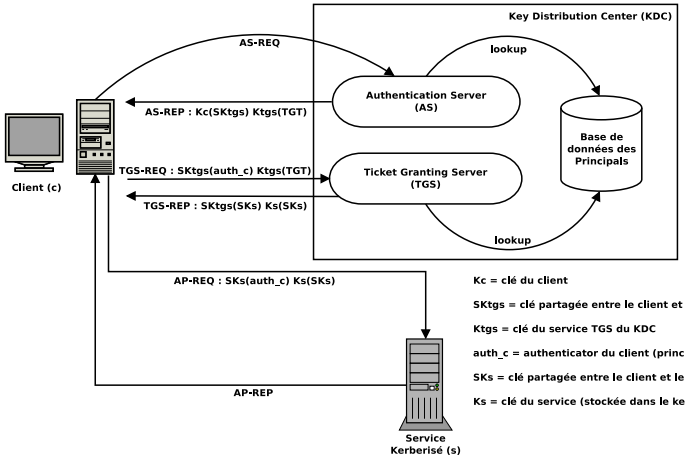
Sécurité

- KDC spoofing
- Pass the ticket

KDC Spoofing

- Man in the Middle (MiM) KDC et client
- Obtention d'un TGT inutilisable (pas chiffré avec la clé privé du vrai KDC) ...
- ... Mais valide au sens cryptographique (la clé de session avec le TGS est déchiffrable)

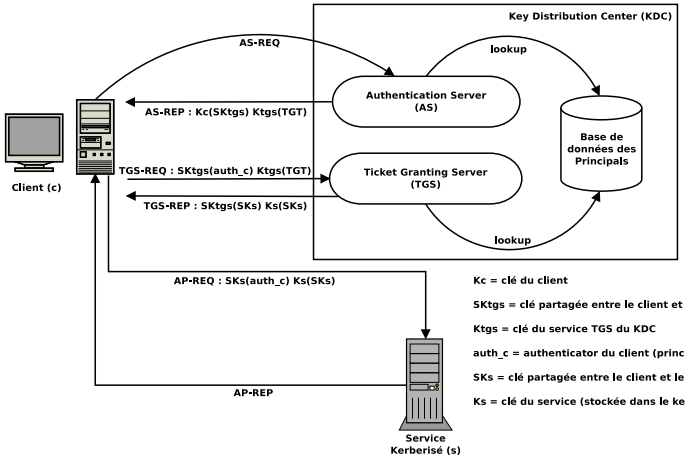
KDC Spoofing



Pass the ticket

- Interception d'une réponse TGS_REP valide
- KDC Spoofing
- Rejeu
- Obtention d'un ticket de service déchiffrable avec la clé privée du service demandé ...
- ... Mais la clé de session avec le service contenue dans le ticket est différente de celle utilisée pour l'authenticator $\rightarrow$ AP_REQ invalide

Pass the ticket



Plan

Bilan

- Problème Horde
  - Authentification côté Horde
  - Instance séparée de dovecot dédiée à Horde avec juste PLAIN
- Chroot (localisation du keytab)
- Les postes standalone Windows

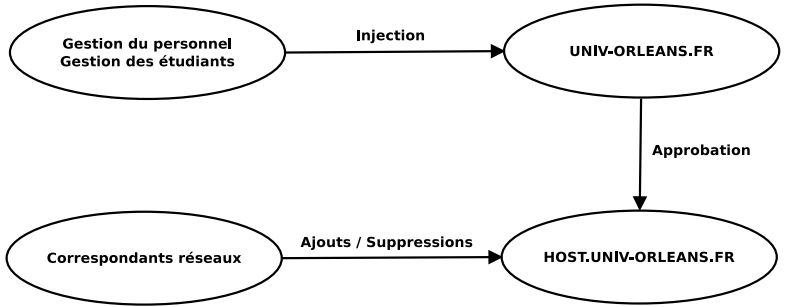
Plan

Problème ouvert

Windows en standalone :

- Gestion du ticket host
- Accès (écriture) à ce KDC
- Spécification du principal utilisé pour la validation ?

Piste


Gestion du personnel
Gestion des étudiants
Injection
UNIV-ORLEANS.FR
Approbation
Correspondants réseaux
Ajouts / Suppressions
HOST.UNIV-ORLEANS.FR

Questions ?