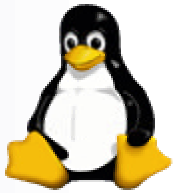
Philippe Perrin
François Lopitaux

OSSIR
Groupe de sécurité Windows

Interopérabilité de Systèmes Kerberos

MIT



Heimdal

Lundi 13 mai 2002

Plan

- Sujet de l’étude
- Le protocole Kerberos V5
- Tests d’interopérabilité
- Un exemple détaillé, démonstrations
- Single Sign On, mots de passe
- Conclusion

Sujet : une étude à l'ENSEIRB

- Etude du protocole Kerberos V5
- Etude des différentes implémentations du protocole (MIT, Windows 2000, Heimdal…)
- Tests d'interopérabilité
- Rédaction d'un document de référence

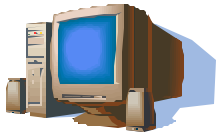
Introduction à Kerberos

Qu’est ce que Kerberos ?

- Protocole d’authentification réseau
  - Développé par le MIT
  - RFC 1510 (version 5)
- Authentification sécurisée
  - Pas de mot de passe envoyé
  - Ses messages sont cryptés (écoutes réseau)
- Connexion d’un client à un service
  - Authentification mutuelle
  - Clé de cryptage commune

Intervenants

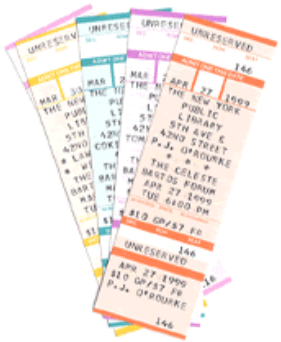
- 3 types
  - Utilisateurs
  - Services
    - FTP
    - telnet
    - ...
  - KDC (Key Distribution Center)



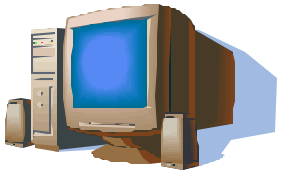
- Chacun a un *principal* et un mot de passe
  - Utilisateurs : « mémoire »
  - Services : fichier *keytab* local

Tickets

- Messages de base du protocole
- Délivrés par le KDC
- Garantissent l’authentification d’un utilisateur
- Cryptés avec des mots de passe
- Deux types
  - TGT (Ticket-Granting Ticket)
  - Ticket de service
- Périssables (besoin de synchronisation)
- Stockage par les utilisateurs

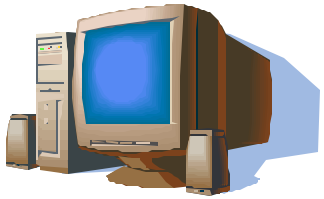


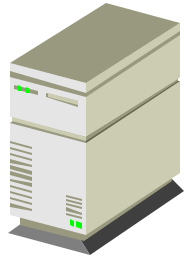
Key Distribution Center



- Rôle
  - Le seul à connaître tous les mots de passe
  - Le seul habilité à délivrer des tickets
  - Crée des clés de session
- Services
  - *Authentication Service* (AS) distribue des Ticket-Granting Ticket aux clients
  - *Ticket Granting Service* (TGS) distribue des tickets d'authentification pour les services

Protocole Kerberos





Utilisateur

KDC

Service

nom d’utilisateur

TGT

TGT, nom de service

ticket de service

ticket de service

acceptation, authentification mutuelle

échanges ultérieurs cryptés

nouveau service

réutilisation

Interopérabilité

Principe des tests

- Combinaisons KDC – Service – Client
- Implémentations testées
  - KDC : Windows 2000, MIT (Solaris)
  - Services : SEAM, MIT, Heimdal
  - Clients : SEAM, MIT, Heimdal, KTelnet (Windows)
- Marche à suivre par Microsoft (Windows / UNIX)

	Access to Windows 2000 Resources	Access to Non-Windows 2000 Resources
Windows 2000 Client Authentication to Windows KDC	**Native**	**One-way Trust or Service Account**
Windows 2000 Client Authentication to Non-Windows KDC	**Two-way Trust**	**Client Configuration**
Non-Windows Client Authentication to Non-Windows KDC	**Two-way Trust**	**Native**
Non-Windows Client Authentication to Windows KDC	**Client Configuration**	**One-way Trust or Service Account**

Microsoft

Les solutions (1)

- Utilisation native
  - Une seule implémentation
  - Sort du cadre de l’étude
- Configuration des clients
  - KDC et service dans une même implémentation
  - Client dans une autre
  - Exemple : MIT – MIT – Heimdal

Les solutions (2)

- Confiance de domaines
  - Un domaine de ressources, un domaine d’utilisateurs
  - Unilatérale ou bilatérale
  - Exemple : utilisateurs Windows, ressources UNIX
- Comptes de services
  - Un seul domaine, sous Windows
  - Exemple : Windows – MIT – Heimdal

Un exemple détaillé

Les conditions de l’exemple

- Windows – MIT – Heimdal
- Deux solutions
  - Comptes de services
  - Confiance unilatérale
- Services testés
  - FTP, telnet, rlogin…

Comptes de services (1)

- Principe
  - La solution la plus « naturelle »
  - Un seul domaine : utilisateurs et services
    - KDC : Windows 2000
    - Services : UNIX
    - Clients : quelconques
  - Les services ont des *principals* sur le KDC
  - Chaque serveur UNIX a son fichier keytab local créé par le KDC Windows

Comptes de services (2)

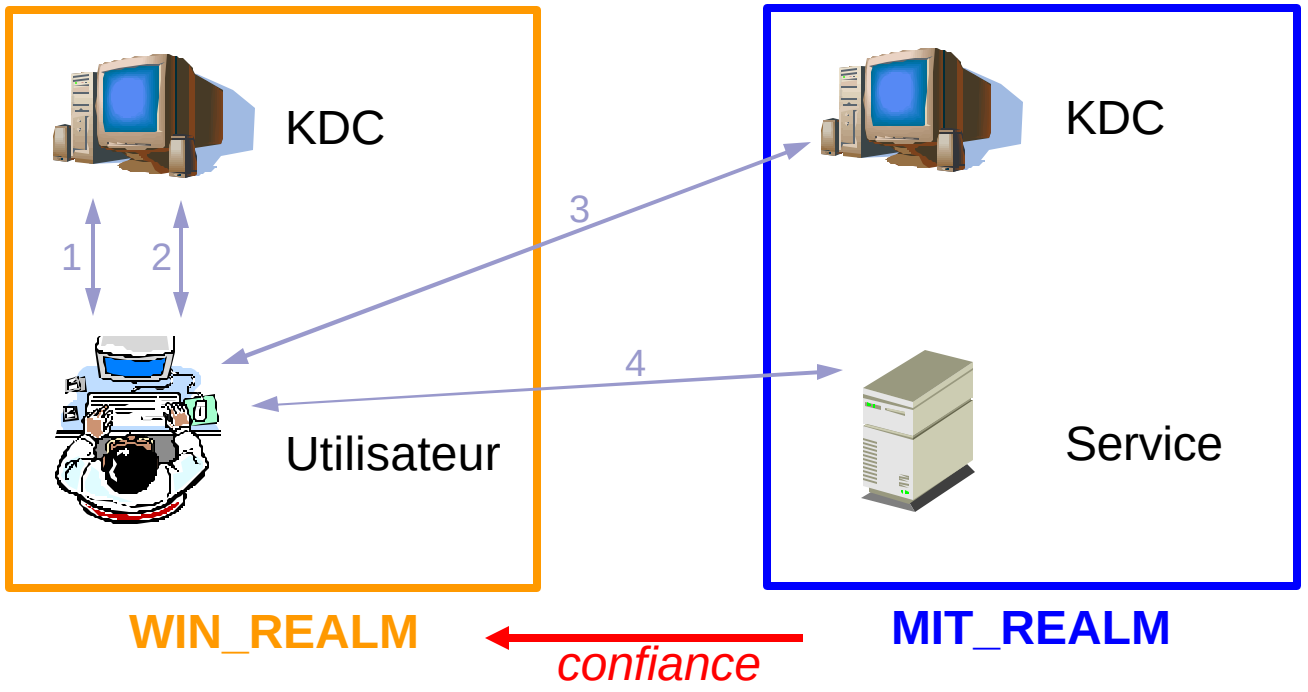
- Mise en place
  - Création de l'utilisateur Windows « sigmund » avec le mot de passe « freud »
  - Utilisation des Windows Support Tools
    - Mapping utilisateur / *principal*
    - Fichier keytab pour le service
    - **`C:\> ktpass –princ host/thot.mds@WIN_REALM –mapuser sigmund –pass freud –out thot.keytab`**
  - Copier le fichier thot.keytab sur thot.mds

Comptes de services (3)

```
root@verone:/# kinit kerby@WIN_REALM
Password for kerby@WIN_REALM: *****
```

TGT pour WIN_REALM

Confiance unilatérale (1)



Confiance unilatérale (2)

- Mise en commun d'un mot de passe
- Configuration du KDC de WIN_REALM
  - MMC Domaines et Approbations Active Directory
    ➔ domaine approuvant : MIT_REALM
    ➔ mot de passe commun
  - Déclaration du KDC de MIT_REALM
- Configuration du KDC de MIT_REALM
  - Nouveau *principal* : TGT émis par WIN_REALM
    ➔ krbtgt/MIT_REALM@WIN_REALM
    ➔ mot de passe commun
  - Déclaration du KDC de WIN_REALM

Confiance unilatérale (3)

```
root@verone:/# kinit kerby@WIN_REALM
Password for kerby@WIN_REALM: *****
```

TGT pour WIN_REALM

Confiance unilatérale (4)

```
root@verone:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
        Principal: kerby@WIN_REALM

  Issued           Expires          Principal
Mar  7 20:14:39  Mar  8 06:13:56  krbtgt/WIN_REALM@WIN_REALM
Mar  7 20:15:41  Mar  8 06:13:56  krbtgt/MIT_REALM@WIN_REALM
Mar  7 20:15:11  Mar  8 06:13:56  host/thot.mds@MIT_REALM
```

Single Sign On
Mots de passe

Single Sign On

- Une seule saisie de mot de passe pour tous les services du domaine
- Transmission des TGT d'une session à l'autre
  - Telnet, rlogin
- Concrètement :
  - Login graphique sur la console (PAM)
    - KDC Windows, client MIT
  - kinit –f en dehors du domaine

Changement de mot de passe

- Tests réalisés
  - KDC Windows : clients Heimdal et MIT
  - KDC MIT: clients Heimdal et KTelnet
- Résultat
  - Windows – MIT, seule réussite

Conclusion

Conclusion

- Rédaction d’un document énumérant tous les tests effectués avec tous les fichiers de configuration
- L’ensemble des tests est concluant
- Manque de services Windows avec des clients UNIX
- Abandon de SEAM pour le MIT

http://www.phperrin.fr.st/enseirb/annee3/kerberos/rapport.zip