**Crosoft (suite 18/01/16)**

LDAP

Annuaire

1. Arbre

* Sio.local

Utilisateurs

Machines

Nnaudier

Eleves

SI3-3805-PRF

SI3-3807-PRF

DC

OU

CN

SIO1

SIO2

SLAM

SISR

SLAM

SISR

Profs

1. Représentation

DC -> Domain Component

OU -> organizational unit

CN -> Common Name

DC = sio

OU = Utilisateurs

CN = nnaudier

Préfixe = information

CN : nnaudier, OU Utilisateurs, DC : Sio, DC : local

CN = eleves, OU : Utilisateurs, DC : Sio. Local ;

CN : SIO-3807-PRF, OU : Machines, DC : sio, DC : local

CN : ssoualy, OU : SISR, OU : Eleves, OU : utilistateurs, DC : local ;

CN : sio-3806-prf, Ou : Prof, OU : 3806, OU : Machines, DC : Sio, DC : local ;

Kerberos

1. Introduction

Chiffrement asymétrique -> 2 clés

Clé publique (source) -> chiffrer

Clé privée (destinataire) -> déchiffrer

Ksrc(Données)

1. Fonctionnement

1

2

3

4

5

6

**1**: le client demande une clé en kdc

**2**: le kdc renvoi une clé (ttgs)

Ttgs est chiffré avec ktgs

Clé Kc, TGS

Le client reçoit KC, TGS chiffré avec Kc



|  |  |
| --- | --- |
| |  | | --- | | Demande |   Kc, TGS |

Client

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | TTGS | KC,TGS |   KTGS |

TGS :

|  |  |
| --- | --- |
| TTGS | KC,TGS |
|  |  |

**4.**

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | Ts | Kc,S |   Ks |

|  |  |
| --- | --- |
| |  | | --- | | Kc,S |   Kc,TGS |

**5.**

|  |  |
| --- | --- |
| |  | | --- | | Demande |   KC,S |

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | Ts | Kc,S |   Ks |

III – Sécurité

Si les clé sont compromises, tout est compromis.

Si on intercepte les tickets on peut usurper l’identité du client.

IV – Utilisation

Authentification, windows, unix, apache (serveur web), filezilla (ftp),

Mac os x 10.2

Win2000

Samba (smb)