

Domæne kontrol med Linux

sw6 8/4 - 05

Centraliseret Windows autentificering mod Linux Server

- Via Samba som DC
 - NT4 style samba domæne
 - Samba kan *ikke* være AD – DC (endnu ;-))
- Direkte til LDAP server på Linux
 - pGINA plugin til Windows
 - + pGINA ldap plugin
 - pgina.xpasystems.com
 - LDAP database på Linux
 - Linux Klienter kan også autentificere mod denne vha pam modul !

Samba som DC essentielle parametre

- netbios name = MYDC1
 - Serverens NetBIOS navn
- workgroup = MYDOMAIN
 - domæne navn
- domain logons = Yes
- domain master = Yes
 - vi er DC !
- security = User

Mere komplet eksempel (Samba HowTO 4.3.1)

[global]	[netlogon]
netbios name	path = /var/lib/samba/netlogon
workgroup	read only = yes
passdb backend = tdbsam	write list =
os level = 33	
preferred master = yes	[profiles]
domain master = yes	path = /var/lib/samba/profiles
local master = yes	read only = no
security = user	create mask = 0600
domain logons = yes	directory mask = 0700
logon path = \\%N\profiles\%U	
logon drive = H:	
logon home = \\homeserver\%U\winprofile	
logon script = logon.cmd	

Samba passwd database

- Normalt smbpasswd fil
- Kan være en data base
 - MySQL, PostgreSQL , LDAP
 - Se Samba Howto kap 10

LDAP

- En protokol for at tilgå en database
- Flere Implementationer
 - MS AD, OpenLDAP , SunOne, eDirectory ...
 - database backend kan variere !
- Træ struktur fig 8-1 (LIAWW)
- Gemmer objekter af forskellig type
 - f. eks. posixAccount

LDAP servere

- Optimeret for læsning
- Kan tilgås krypteret via TLS
 - ldaps
- Kan replikeres til (slave?) LDAP servere

LDAP til 'UNIX' accounts

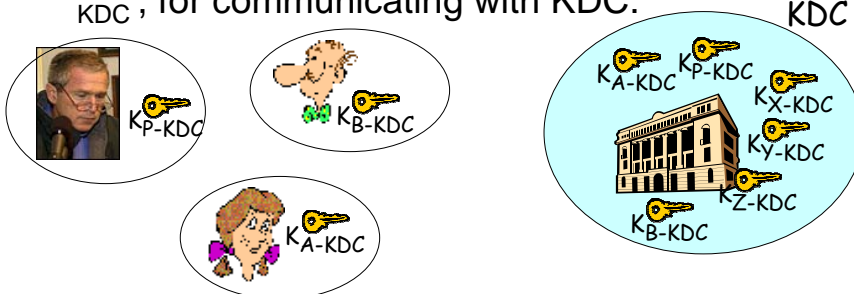
- Standardiserede database schemas findes til
 - posixAccount
 - data som i /etc/passwd
 - shadowAccount
 - data som i /etc/shadow
 - for password aging information !
 - fig 8.1 og 8.2 i "Linux In A Windows World"
- Værktøjer til import af eksisterende passwd filer findes !

Kerberos Autentificering

- Gensidig autentifikation vha en delt krypteringsnøgle
- Servere i "Kerberos net" kan selv validere klient uden at kontakte central pwd server
 - reduceret netværkstrafik / server belastning
- Forsimplet udgave på følgende slides
 - Se f. eks. "Windows 2000 Kerberos Authentication Whitepaper"
 - Eller referencer fra sidst ...

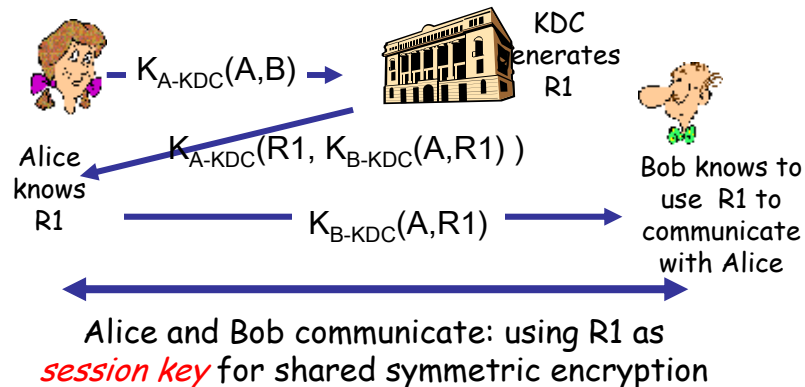
Key Distribution Center (KDC)

- Alice, Bob need shared symmetric key.
- **KDC:** server shares different secret key with *each* registered user (many users)
- Alice, Bob know own symmetric keys, K_{A-KDC} K_{B-KDC} , for communicating with KDC.



Key Distribution Center (KDC)

Q: How does KDC allow Bob, Alice to determine shared symmetric secret key to communicate with each other?



NT 4 Domæner

- Fælles bruger database på Domæne Controllere
 - En autoritativ primær server + backup servere
 - PDC/BDC
- Mulighed for at sætte forskellige værdier i registreringsdatabasen på arbejdsstationerne vha "System policies"
 - For (grupper af) maskiner eller bruger(e)

Domæner fortsat

- Arbejdsstationer der er medlem af domænet har en maskinkonto i brugerdatabasen
 - Password genereres når maskinen adderes til domænet
 - Det skiftes automatisk med mellemrum
 - Kan komme ud af sync ved restore af backup
 - Arbejdsstationen må adderes til domæne på ny
- Der etableres en krypteret kanal til DC for logon
- Der er stadig adgang for brugere på maskiner der ikke er medlem af domænet – blot brugernavn – adgangskode kendes !!

NT4 - rester

- WINS
- NetBIOS
- Browsing