

# Védelem

Alkalmazások - AppArmor

# Tipikus hozzáférés szabályozási megoldások

- ▶ DAC - Discretionary Access Control (tetszés szerinti)
  - ▶ Minden objektumnak tulajdonosa van, aki szabályozhatja a hozzáférést
  - ▶ Pl. állományok
- ▶ MAC - Mandatory Access Control (kötelező)
  - ▶ Hozzáférés-jogosultság kiosztása előre meghatározott módon

# MAC implementáció Ubuntuban

- ▶ AppArmor (Application Armor) - alapértelmezett
- ▶ SELinux (Security Enhanced Linux)

# AppArmor

- ▶ Név alapú MAC-et megvalósító biztonsági modul
- ▶ Elsősorban hálózati alkalmazások védelmére: www, ftp, Samba, CUPS, dhcpcd
- ▶ Szabályozás **biztonsági házirendekkel**
- ▶ Csomagok: apparmor, apparmor-utils, apparmor-profiles
- ▶ `sudo apt-get install apparmor apparmor-utils apparmor-profiles`
- ▶ Minden szabályozás alá tartozó alkalmazáshoz egy profil állomány (biztonsági házirend)

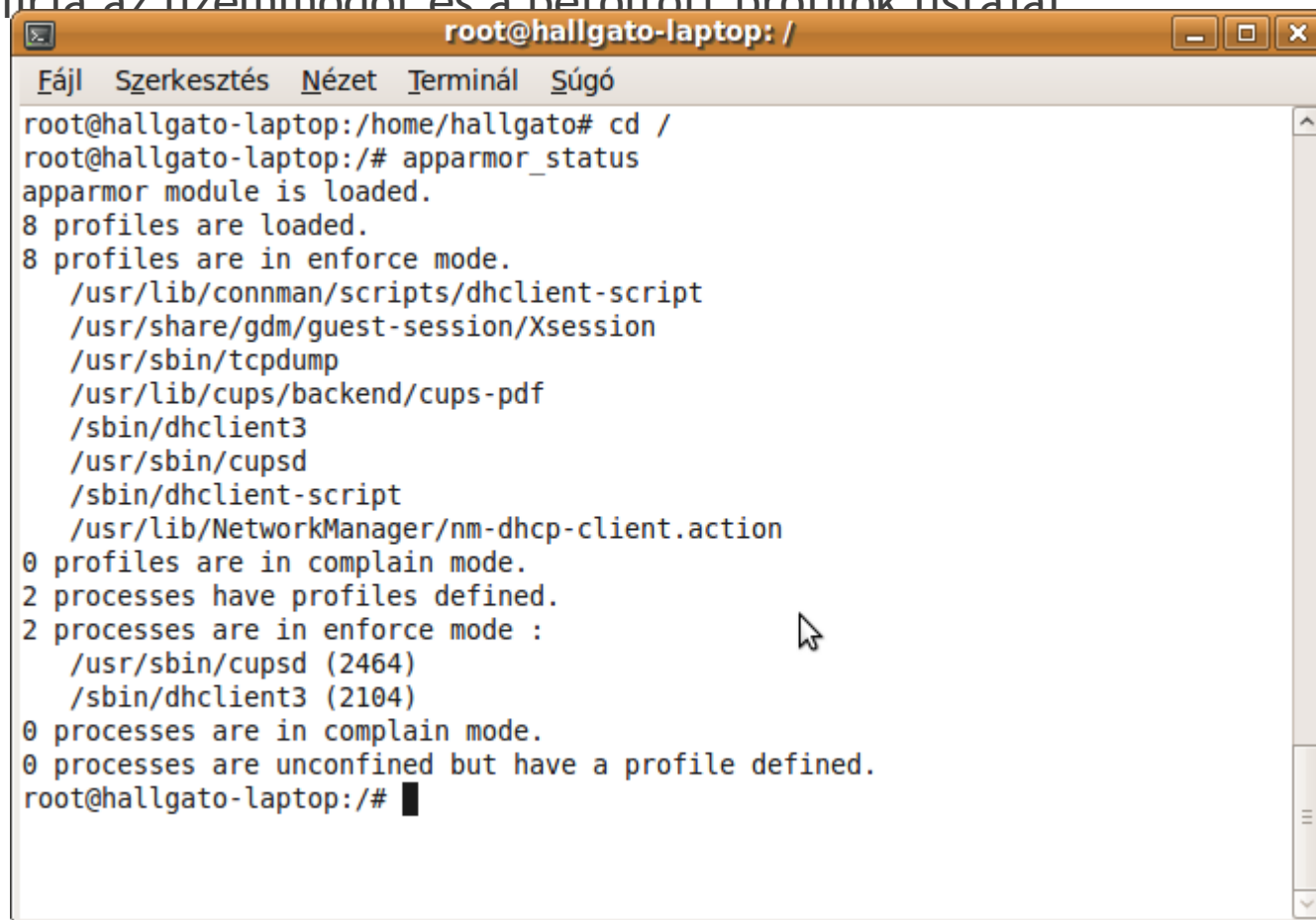


# AppArmor

- ▶ Indítás: `/etc/init.d/apparmor start|stop|restart`
- ▶ Kiszolgáló (pl. Apache, Samba, SQUID, Postfix) telepítéskor települ a hozzá tartozó profil
- ▶ További profilok az `apparmor-profiles` csomagban
- ▶ Üzem módok
  - ▶ Enforce - kikényszerítő
  - ▶ Complain - figyelmeztető

# apparmor-utils

- `apparmor_status` - kiírja az üzemmódot és a betöltött profilok listáját



```
root@hallgato-laptop: /
Fájl Szerkesztés Nézet Terminál Súgó
root@hallgato-laptop:/home/hallgato# cd /
root@hallgato-laptop:/# apparmor_status
apparmor module is loaded.
8 profiles are loaded.
8 profiles are in enforce mode.
  /usr/lib/connman/scripts/dhclient-script
  /usr/share/gdm/guest-session/Xsession
  /usr/sbin/tcpdump
  /usr/lib/cups/backend/cups-pdf
  /sbin/dhclient3
  /usr/sbin/cupsd
  /sbin/dhclient-script
  /usr/lib/NetworkManager/nm-dhcp-client.action
0 profiles are in complain mode.
2 processes have profiles defined.
2 processes are in enforce mode :
  /usr/sbin/cupsd (2464)
  /sbin/dhclient3 (2104)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
root@hallgato-laptop:/#
```

# Profil

- ▶ Profil módosítása után újratöltés
- ▶ `cat profil | sudo apparmor_parser -r`
- ▶ Az összes profil újratöltése
- ▶ `sudo /etc/init.d/apparmor reload`
- ▶ Alkalmazási módok
  - ▶ `enforce` - kikényszerített
  - ▶ `complain` - figyelmeztető

# Kapcsolók

- ▶ **enforce** - kikényszerített módba helyezi az apparmor
- ▶ **aa\_enforce** alkalmazás - csak egy profilt (alkalmazást)
- ▶ **complain** - figyelmeztető módba helyezi az apparmor
- ▶ **aa\_complain** alkalmazás - csak egy profilt (alkalmazást)
- ▶ **unconfined** - kilistázza azokat az alkalmazásokat, amelyeket nem szabályoz az apparmor
- ▶ **autodep** alkalmazás - egy alap profilt készít egy alkalmazáshoz
- ▶ **audit** alkalmazás - naplózza az alkalmazás tevékenységét



# Konfigurálás

- ▶ Konfigurációs állományok /etc/apparmor
- ▶ Profilok /etc/apparmor.d
- ▶ A profilnév az alkalmazás teljes elérési útvonalát tartalmazza, /-k helyett pontokkal

```
root@ubuntu-server:/etc/apparmor.d# ls
abstractions      sbin.syslog-ng      usr.sbin.dnsmasq
apache2.d         tunables             usr.sbin.dovecot
bin.ping          usr.bin.chromium-browser  usr.sbin.identd
cache             usr.lib.dovecot.deliver   usr.sbin.mdnssd
disable           usr.lib.dovecot.dovecot-auth  usr.sbin.nmbd
force-complain    usr.lib.dovecot.imap        usr.sbin.ncsd
local             usr.lib.dovecot.imap-login   usr.sbin.rsyslogd
program-chunks    usr.lib.dovecot.managesieve-login  usr.sbin.smbd
sbin.dhclient     usr.lib.dovecot.pop3        usr.sbin.tcpdump
sbin.klogd         usr.lib.dovecot.pop3-login    usr.sbin.traceroute
sbin.syslogd       usr.sbin.avahi-daemon
root@ubuntu-server:/etc/apparmor.d# _
```

# Könyvtárak

- ▶ **abstractions, tunables** - olyan profil szabályokat tartalmaz, amelyeket több profil közösen használ
- ▶ **disable** - az ide belinkelt profilok le vannak tiltva
- ▶ **force-complain**

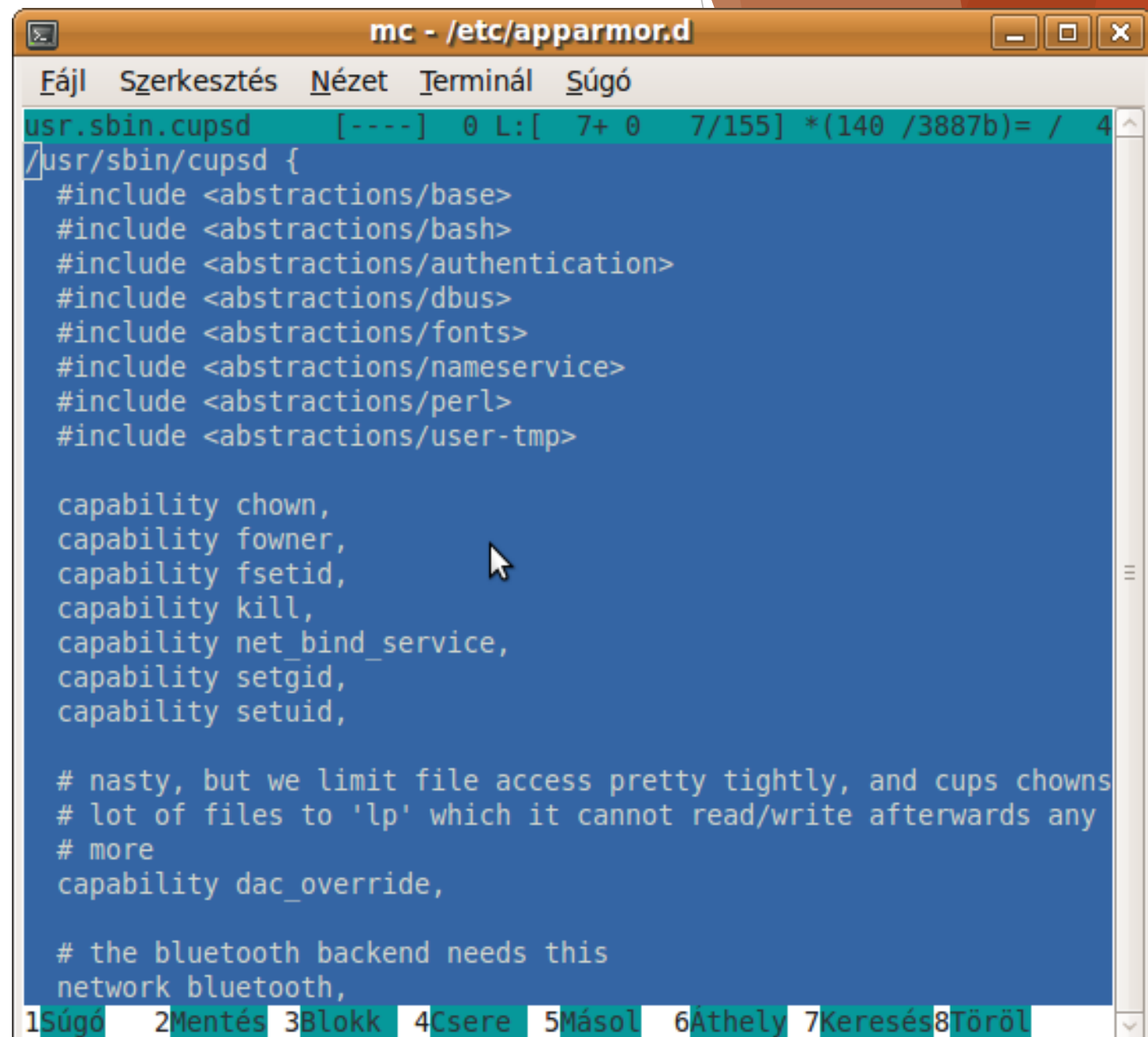
# Profil tartalma

- ▶ **Útvonal** - milyen állományokhoz férhet hozzá az alkalmazás
- ▶ Ha az útvonal \*-ban végződik, akkor az adott könyvtár összes állományára vonatkozik
- ▶ Jogosultságok r,w,x,l (link), stb.
- ▶ Pl. /var/log/samba/log.\* w, - az alkalmazás írhatja a samba könyvtár összes log. kezdetű állományát
- ▶ **Képesség** (Capability) - milyen privilégiumokat használhat a folyamat
- ▶ Pl. capability chown - lecserélheti egy fájl felhasználói- és csoport tulajdonosát



```
mc - /etc/apparmor.d/a
Fájl Szerkesztés Nézet Terminál Súgó
Fájl: samba 100%
/etc/samba/smb.conf r,
/usr/share/samba/*.dat r,
/var/lib/samba/**/*.tdb rw,
/var/log/samba/cores/* w,
/var/log/samba/log.* w,
/var/run/samba/*.tdb rw,
1Súgó 2NemTör 3Kilép 4Hex
```

- ▶ include - direktívával illesztik be a hivatkozásokat



```
mc - /etc/apparmor.d
Fájl Szerkesztés Nézet Terminál Súgó
usr.sbin.cupsd [----] 0 L:[ 7+ 0 7/155] *(140 /3887b)= / 4
/usr/sbin/cupsd {
#include <abstractions/base>
#include <abstractions/bash>
#include <abstractions/authentication>
#include <abstractions/dbus>
#include <abstractions/fonts>
#include <abstractions/namespace>
#include <abstractions/perl>
#include <abstractions/user-tmp>

capability chown,
capability fowner,
capability fsetid,
capability kill,
capability net_bind_service,
capability setgid,
capability setuid,

# nasty, but we limit file access pretty tightly, and cups chowns
# lot of files to 'lp' which it cannot read/write afterwards any
# more
capability dac_override,

# the bluetooth backend needs this
network bluetooth,
1Súgó 2Mentés 3Blokkl 4Csere 5Másol 6Athely 7Keresés8Töröl
```

# Források

- ▶ **A quick guide to AppArmor profile Language**  
<http://wiki.apparmor.net/index.php/QuickProfileLanguage>
- ▶ **AppArmor**  
<https://wiki.ubuntu.com/AppArmor>
- ▶ **Ubuntu Manual - AppArmor**  
<http://manpages.ubuntu.com/manpages/utopic/man5/apparmor.d.5.html>



# Kerberos

# Szolgáltatások védelme Kerberos segítségével

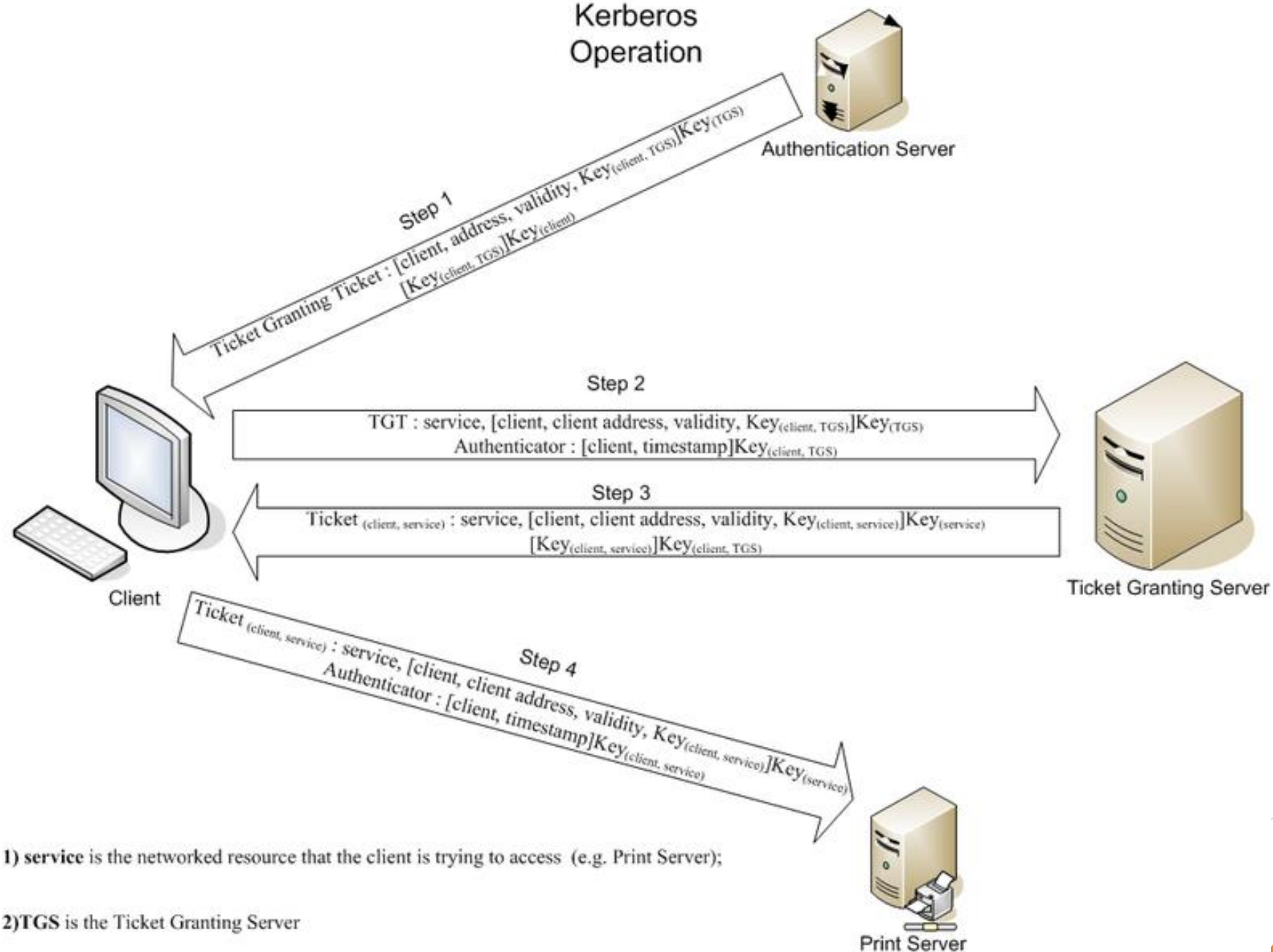
- ▶ Kerberos - Hádész háromfejű kutyája
- ▶ Hálózati autentikációs protokoll
- ▶ Ügyfél és kiszolgáló közötti kapcsolatok titkosított autentikációja
- ▶ Cél: Single Sign On rendszer megvalósításának támogatása
- ▶ Az ügyfél titkosított jelszóval igazolja magát, majd a további kommunikáció is titkosítva történik
- ▶ Védelem belső és külső támadások ellen
- ▶ Biztonságos változatok az rsh, rcp, telnet, ftp kliensek helyett

# Fogalmak

- ▶ **Résztevő (Principal):** minden felhasználó, számítógép és kiszolgálók által biztosított szolgáltatást
- ▶ **Példány (Instance):** szolgáltatás-résztevők és speciális adminisztratív résztvevők megnevezése
- ▶ **Tartomány (Realm):** a Kerberos rendszer által biztosított egyedi felügyeleti tartomány - a DNS-tartomány nagybetűssé alakítva (KEFO.HU).
- ▶ **Kulcsszolgáltató (KDC):** a résztvevők adatbázisa + a hitelesítési kiszolgáló (AS) + jegymegadási kiszolgáló
- ▶ **Jegybiztosító jegy (TGT):** a hitelesítési kiszolgáló (AS) adja ki, evvel kérhet a felhasználó hozzáférést egy szolgáltatáshoz
- ▶ **Jegykiadó szolgáltatás (TGS)** szolgáltatásjegyeket ad ki a klienseknek
- ▶ **Szolgáltatásjegy:** segítségével férhet hozzá az ügyfél a szolgáltatáshoz. Igazolja a két résztvevő (ügyfél és szolgáltatás) identitását
- ▶ **Kulcstáblafájlok:** egy szolgáltatás vagy gép titkosítási kulcsát tartalmazzák



## Kerberos Operation



# Autentikáció

1. Bejelentkezéskor automatikusan
2. A felhasználó kezdeményezi kinit-tel

Ez utóbbi menete

- ▶ A Kerberos felhasználónevet elküldi az Authentication Server (AS)-hez
- ▶ Az AS visszaküld egy tikett kiutaló tikettet (Ticket Granting Ticket - TGT), amit a felhasználó nyilvános kulcsával titkosít
- ▶ A kinit bekéri a jelszót, dekódolja a TGT-t

# Autentikáció menete

- ▶ A kliens program (pl. levelező ügyfél) elküldi a TGT-t a tikett kiadó szerverhez (Ticket Granting Server - TGS)
- ▶ A TGS generál egy tikettet a levelező szerver szolgáltatás eléréséhez, és titkosítva elküldi az ügyfélhez
- ▶ Az ügyfél ezzel a tikettel igénybe veszi a szolgáltatást
- ▶ Ha a felhasználó egy másik szolgáltatást akar igénybe venni, akkor ugrás a dia első pontjához

# Források

- ▶ <https://help.ubuntu.com/lts/serverguide/kerberos.html>
- ▶ <http://sugo.ubuntu.hu/10.10/html/serverguide/hu/kerberos.html>

SSH

# Távoli elérés biztonságosan

- ▶ A telnet, rcp, rsh, rlogin titkosítás nélkül továbbítja az információt
- ▶ SSH - Secure Shell
- ▶ Kereskedelmi vált.: SSH Tectia
- ▶ Szabad vált.: **OpenSSH** (main Ubuntu tároló)
- ▶ Hitelesítés nyilvános/titkos kulcspáros alapú megoldással vagy egyes szolgáltatások esetén Kerberos kiszolgáló segítségével (Kerberos tikett)

# Hitelesítés

- ▶ A kulcshozzáférést külön jelszóval is korlátozhatja
- ▶ Először a hoszt hitelesítése, majd a felhasználó hitelesítése
- ▶ A további információáramlás már a kiszolgáló és az ügyfél által közösen választott (vagy előre meghatározott) algoritmussal
- ▶ Nyilvános kulccsal titkosít a kiszolgáló

# Kiszolgáló

- ▶ Kiszolgáló telepítése
  - ▶ `sudo apt-get install openssh-server -y`
- ▶ Kiszolgáló indítása, leállítása, újraindítása, állapota
  - ▶ `sudo service ssh start|stop|restart|status`
- ▶ A 22-es porton várja a kéréseket
- ▶ Nyilvános kulcsot a `~/.ssh/authorized_keys` állományhoz kell hozzáadni



# Kiszolgáló konfigurálás

## /etc/ssh/sshd\_config

- ▶ Port 22 (ez az alapért., de célszerű mást beállítani 1024... 49152, pl. 2222)
- ▶ Üdvözlőszöveg, figyelmeztetés, stb.
  - ▶ Banner /etc/issue.net
- ▶ Az autentikáció történhet jelszó vagy SSH kulcs alapon\*
- ▶ Jelszó alapú letiltása:
  - ▶ PasswordAuthentication no
- ▶ Nyilvános kulcs alapú:
  - ▶ PubkeyAuthentication yes
  - ▶ RSAAuthentication yes

# Konfigurálás

- ▶ Távoli asztal, grafikus alkalmazások, stb. engedélyezése a kapcsolaton
  - ▶ AllowTcpForwarding yes
  - ▶ X11Forwarding yes
- ▶ Mely felhasználói fiókok/csoportok használhatják
  - ▶ AllowUsers hallgato geza
- ▶ Mely felhasználói fiókok/csoportok nem használhatják
  - ▶ DenyUsers jeno istvan

# Tűzfal

- ▶ Tűzfal profil települ:  
/etc/ufw/applications.d/openssh-server

```
[OpenSSH]
title=Secure shell server, an rshd replacement
description=OpenSSH is a free implementation of the Secure Shell protocol
.
ports=22/tcp
```

- ▶ sudo ufw allow OpenSSH

# OpenSSH átngedése a tűzfalon

```
root@ubuntu-server:/# ufw allow OpenSSH
Rule added
Rule added (v6)
root@ubuntu-server:/# ufw status
Status: active
```

To	Action	From
Anywhere	ALLOW	192.168.1.0/24 2049
Anywhere	ALLOW	192.168.1.0/24 8975
Anywhere	ALLOW	192.168.1.0/24 111
Anywhere	ALLOW	192.168.1.0/24 8976
Anywhere	ALLOW	192.168.1.0/24 Samba
137	ALLOW	192.168.1.0/24
138	ALLOW	192.168.1.0/24
139	ALLOW	192.168.1.0/24
445	ALLOW	192.168.1.0/24
OpenSSH	ALLOW	Anywhere
OpenSSH (v6)	ALLOW	Anywhere (v6)

# Ellenőrzés

- ▶ Fut-e? `ps -A | grep sshd`
- ▶ Milyen porton várja a kéréseket? `ss -lnp | grep sshd`

```
root@ubuntu-server:/etc/ssh# ss -lnp | grep sshd
LISTEN      0      128          :::22          :::
*      users:((("sshd",11409,4))
LISTEN      0      128          *:22          *:
*      users:((("sshd",11409,3))
root@ubuntu-server:/etc/ssh# _
```

- ▶ Helyi bejelentkezés: `ssh -v localhost`

```
d6:06
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is d4:49:70:d8:54:2d:23:31:65:7e:9d:c0:5d:44:d6:06.
Are you sure you want to continue connecting (yes/no)? yes_
```

# Ellenőrzés

- ▶ Fogad-e kapcsolatot?
  - ▶ `sudo netstat --inet -ltn | grep sshd`
  - ▶ `tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN <PID>/sshd`

# Ügyfél gép

- ▶ Ügyfélszoftver telepítése
  - ▶ `sudo apt-get install openssh-client`
- ▶ Kulcsok létrehozása RSA vagy DSA titkosítással
- ▶ `ssh-keygen -t rsa|dsa`
- ▶ Kulcsok: `~/.ssh/id_rsa.pub` és `~/.ssh/id_rsa`
- ▶ Titkos kulcsok betöltése a memóriába
  - ▶ `ssh-add -l`





# Ügyfélprogramok

- ▶ **ssh** - parancssori és grafikus (-X kapcsoló) távoli kapcsolatoknál
  - ▶ `ssh felhasználónév@gépnév`
- ▶ **scp** - fájlok másolása gépek között. Pl. helyi gépről távoli gépre
  - ▶ `scp forráfájl felh@gépnév:/könyvtár/célfájl`
  - ▶ `-r` egész könyvtár másolható
- ▶ **sftp** - a kiszolgálón sftp-server kell fusson (SSH File Transfer Protocol)
  - ▶ `sftp gépnév`
- ▶ **ssh-copy-id** - nyilvános kulcs átmásolása a kiszolgálóra
  - ▶ `ssh-copy-id felhasználó@gépnév`