

# 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, dhcpkliens
- ▶ 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)

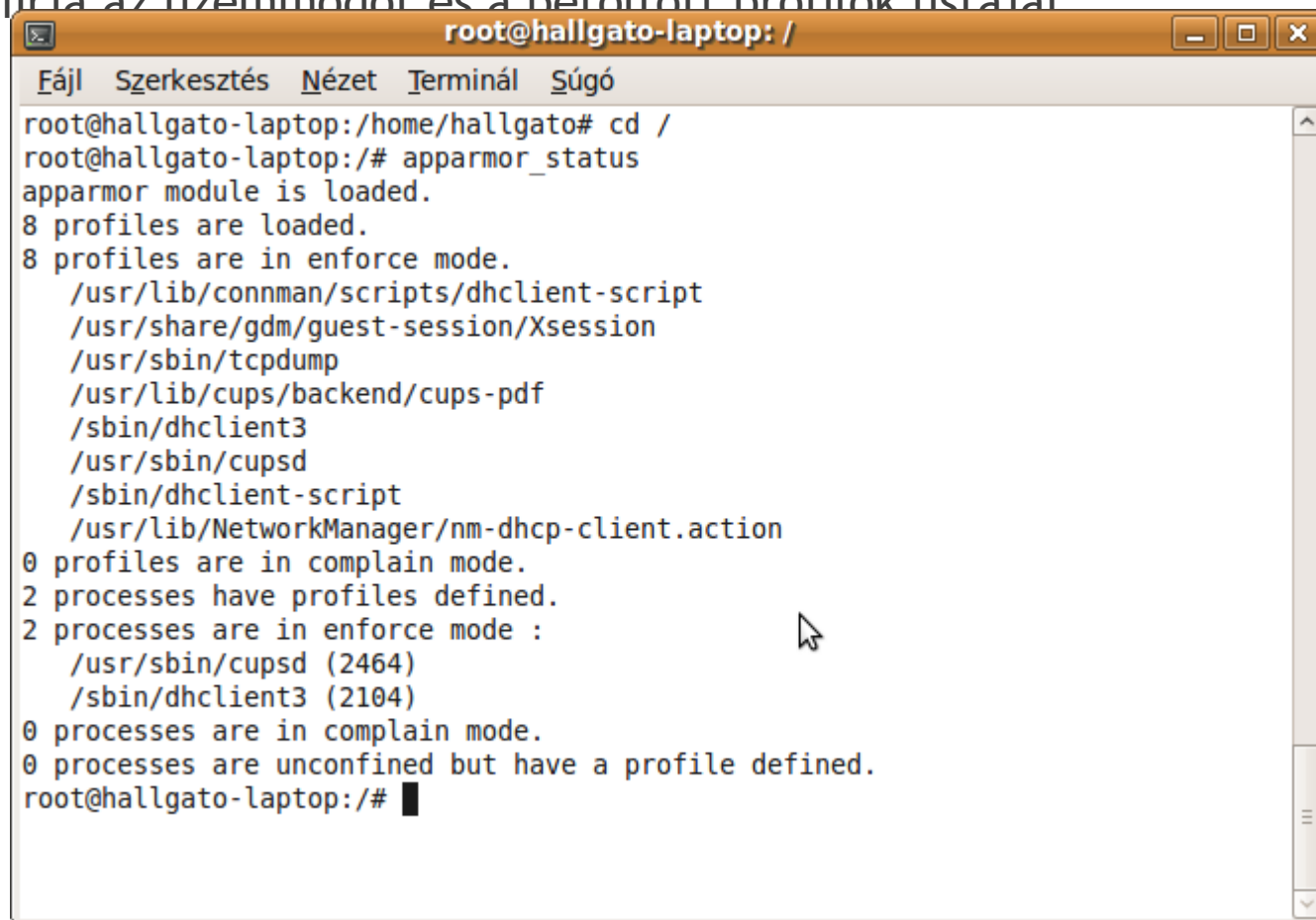


# AppArmor

- ▶ 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.nscd
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.tcpcdump
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**

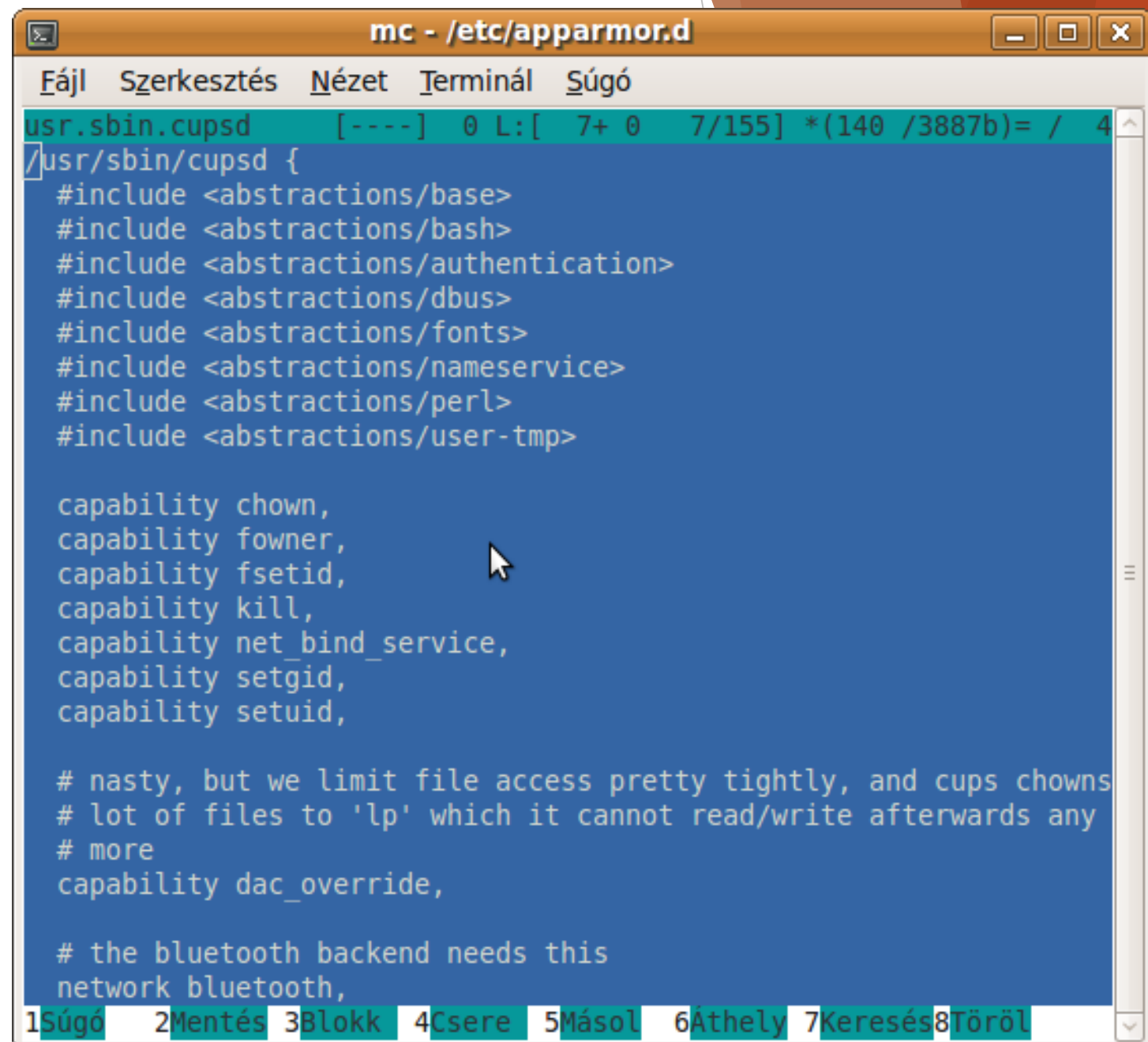
# Profil tartalma

- ▶ **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>