

Alkalmazott számítástechnika

dr. Beinschróth József

Security - file security

Jogosultságok (permissions):

Relációk a felhasználók és erőforrások között

r-read

- Olvasási jog, birtokában a fájl
 - Olvasásra megnyitható
 - Másolható
 - Menthethető
 - Nyomtatható

w-write

- Írási jog, birtokában a fájl
 - Tartalma módosítható (megváltoztatható, kiegészíthető...)
 - Tartalma törölhető
- **DE! Ezen jog birtokában a fájl nem törölhető!**

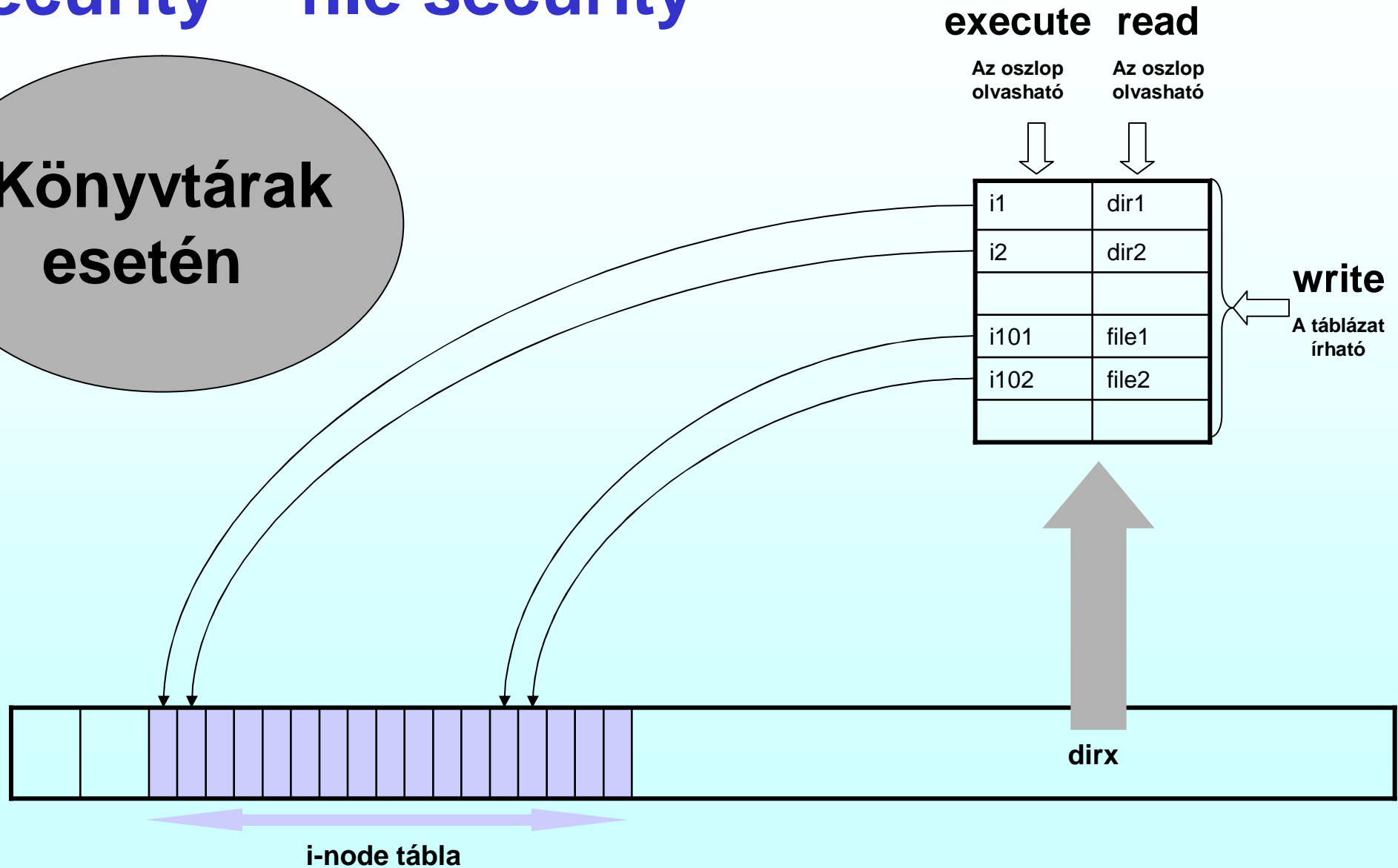
x-execute

- Végrehajtási jog, birtokában a fájl
 - Futtatható, ha a fájl egyébként futtatható típusú (pl. bin. végrehajtható fájl vagy shell script)

Fájlok esetén

Security - file security

Könyvtárak
esetén



Security - file security

Tulajdonos

- Az a user, aki létrehozta a fájlt ill. akinek a fájlt a rendszeradminisztrátor a tulajdonába adta
- Pontosan egy tulajdonos van
- A tulajdonosnak külön jogok adhatók

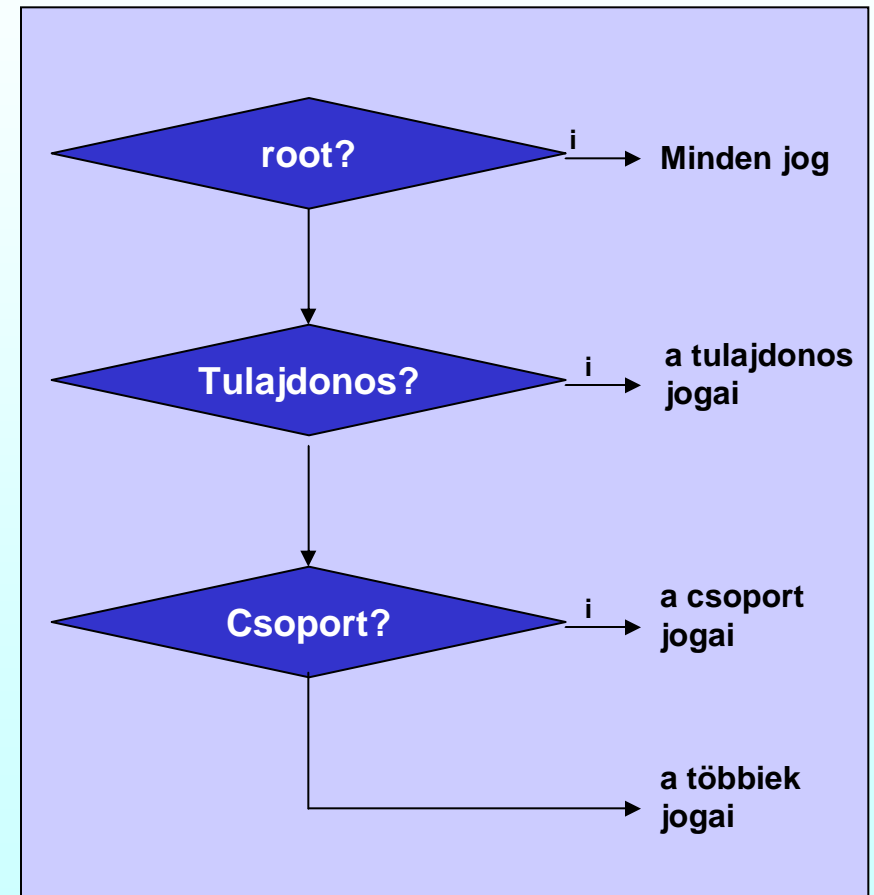
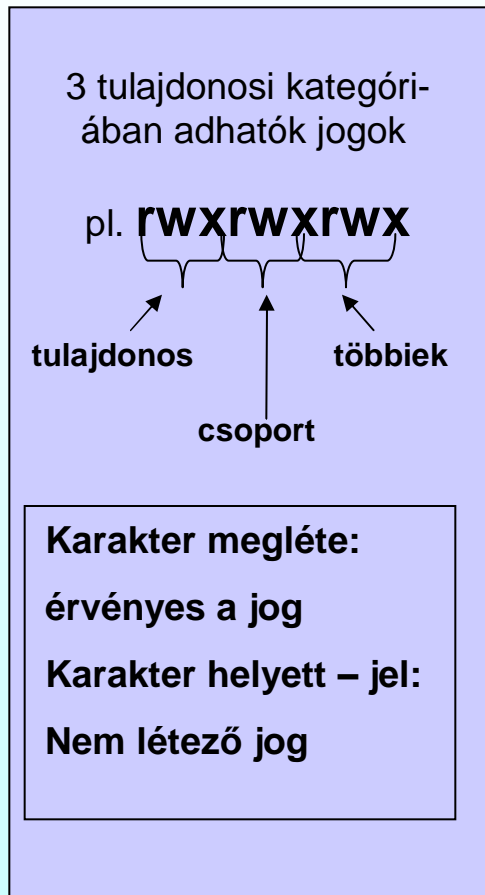
Csoport

- (A csoport felhasználókból áll, a csoportokat ill. tagjaikat a rendszeradminisztrátor határozza meg)
- (Minden felhasználó legalább egy csoporthoz tartozik)
- (A felhasználó csoportjai között van egy a felhasználó szempontjából kitüntetett csoport: a felhasználó elsődleges csoportja)
- A fájl az őt létrehozó felhasználó elsődleges csoportjához tartozik (ezen a rendszeradminisztrátor és bizonyos korlátokkal a tulajdonos tud változtatni).
- A csoportnak (tagjainak) külön jogok adhatók

Többiek

- Azok a felhasználók, akik sem nem tulajdonosok, sem nem tartoznak a fájl csoportjához
- A többieknek külön jogok adhatók

Security - file security



Security - file security

Jogosultságok megadása oktálisan

- Az rwx jogosultság megadásban a karakterek sorrendje kötött
- Emiatt az egyes karakterekhez súlytényezők rendelhetők
 - r: 2^2
 - w: 2^1
 - x: 2^0
- Példák
 - rwx: 7
 - r-x: 5
 - --x: 1

Pl.:777: mindenkinek minden joga megvan

Tipikus jogosultság kombinációk

- Adat (szöveg) fájl
 - rw-
 - r—
 - ---
- Végrehajtható fájl
 - rwx
 - r-x
 - --x
 - ---
- Könyvtár
 - rwx
 - r-x
 - ---

Security - file security

Default jogosultságok

- Milyen jogosultságok állítódnak be egy újonnan létrehozott fájlra? (Default jogosultságok)
 - A fájlt létrehozó user (tulajdonos) határozza meg
 - Umask (user mask) - a felhasználói környezet része
 - A létrejövő jogok az umaskból számíthatók
 - Szempontok
 - Fájlra ne legyen x jog!
 - Könyvtárra legyen x jog!

- Könyvtár esetén
 - Mindhárom tulajdonosi kategóriában elvégezzük a számítást (oktális számok)
 - Jogosultság:
 - Az umask értéket 7-ből kivonjuk

- Fájl esetén
 - Mindhárom tulajdonosi kategóriában elvégezzük a számítást (oktális számok)
 - Jogosultság:
 - Az umask értéket 7-ből kivonjuk
 - Ha eredményül x jogot kapunk, az x-et levesszük (1-et levonunk), ha nem kaptunk x jogot, akkor nem változtatunk

Security - file security

Az umask – jogosultság összefüggés táblázatos formában

Umask (oktális)	7-umask (oktális)	Könyvtár	Fájl	Értelme
0	7	rwX	rw-	Írható/olvasható objektumok
1	6	rw-	rw-	Nincs értelme
2	5	r-X	r--	Csak olvasható objektumok
3	4	r--	r--	Nincs értelme
4	3	-wX	-w-	Nincs értelme
5	2	-w-	-w-	Nincs értelme
6	1	--X	---	Nincs értelme
7	0	---	---	Nincs hozzáférés

Security – file security

Speciális jogosultságok: setuid, setgid (s)



– Példa:

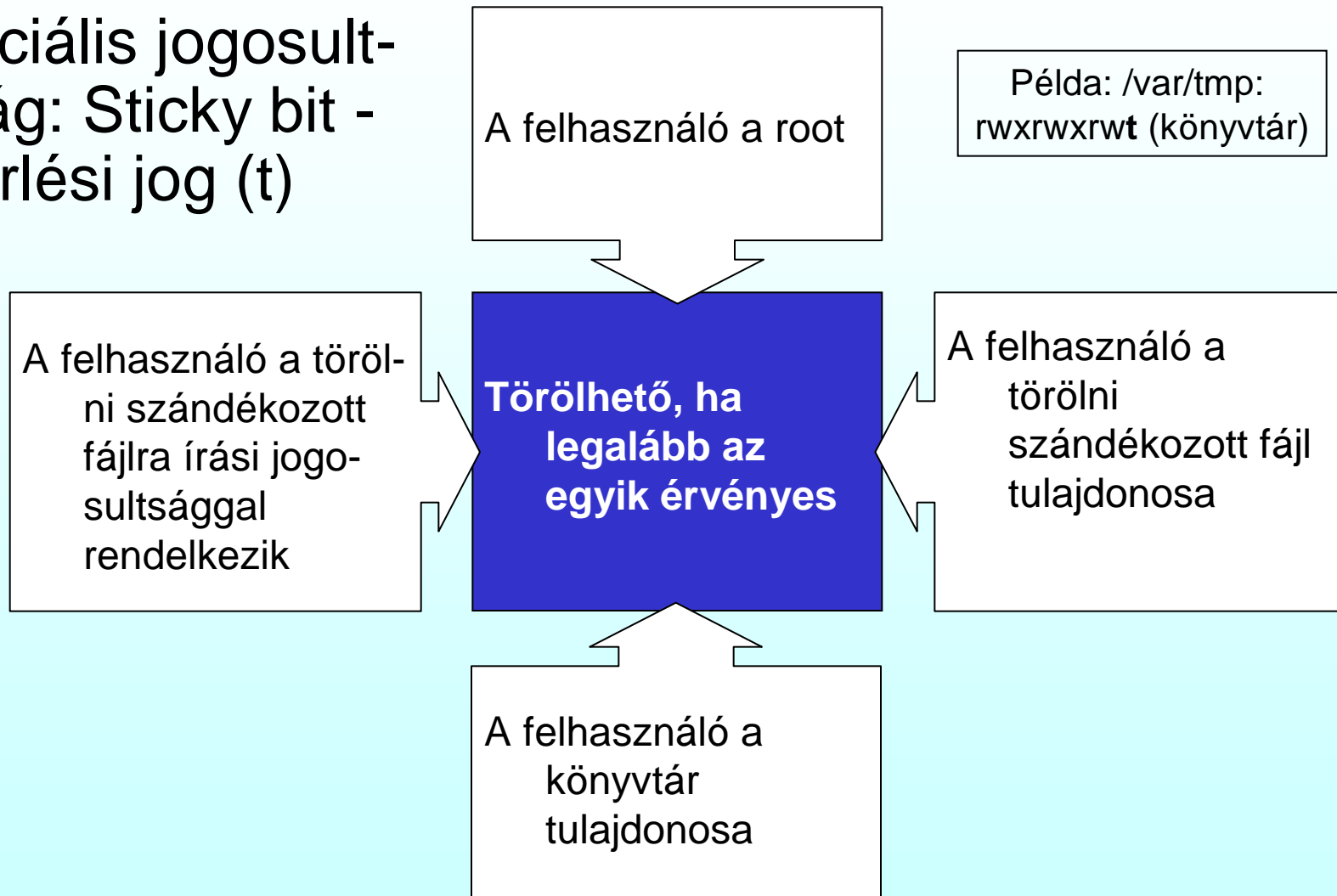
- /usr/bin/passwd – setuid bit érvényes
- /usr/bin/passwd - tulajdonosa a root, emiatt a userek beírhatnak a jelszavakat tartalmazó fájlba (/etc/shadow)

– setgid – csoportokra hasonlóan

Otthoni gépen rootként létrehozott cdrom???

Security – file security

Speciális jogosultság: Sticky bit - törlési jog (t)



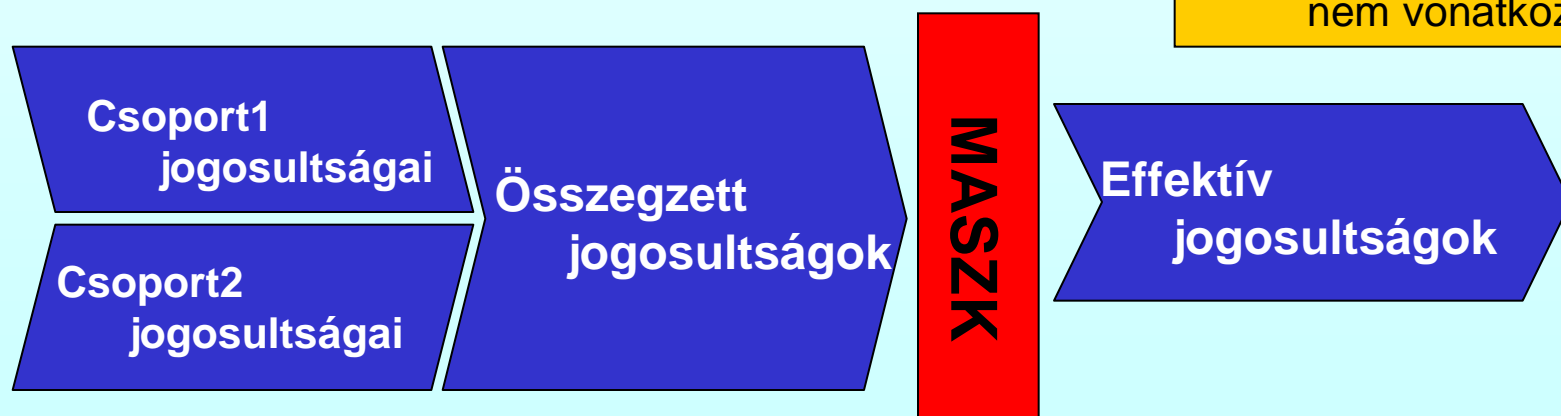
Security – file security

ACL – Access Control List

- Nemcsak a tulajdonos és egy csoport, hanem tetszőleges userok és tetszőleges csoportok is kaphatnak jogosultságokat
- setfacl, getfacl
- A kapott jogok összegződnek
- Mask szükséges!
 - A fájlhoz tartozik
 - Meghatározza a maximális (effektív) jogokat.

Az ACL mask és az umask között semmiféle kapcsolat nincs!

A mask a tulajdonosra nem vonatkozik



Security – user security

Multiuseres működés

Felhasználó név

- Általában publikus
- Többnyire meghatározott szabályok szerint képezik

Jelszó

- Titkos!
- Meghatározott szabályok vonatkoznak a kezelésére
 - „Írott” szabályok
 - „Íratlan” szabályok
- Titkosított tárolás
- Titkosított átvitel

Döntés: beléphet-e?

Security – user security

User adatbázis fájlok

/etc/passwd

login_name:x:UID:GID:comment:home_dir:login_shell

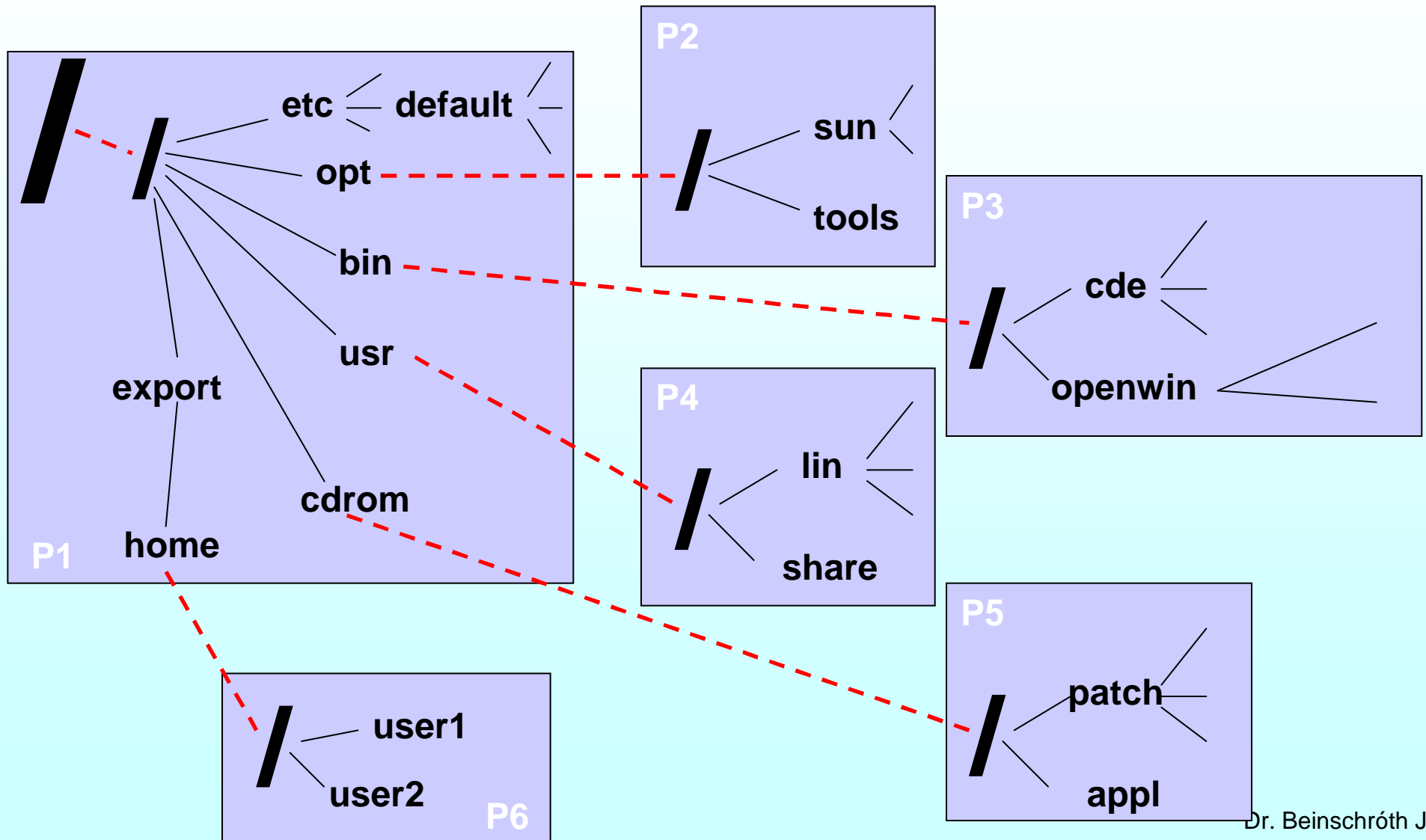
/etc/shadow

login_name:passwd:lastchg:min:max:warn:inactive:expire

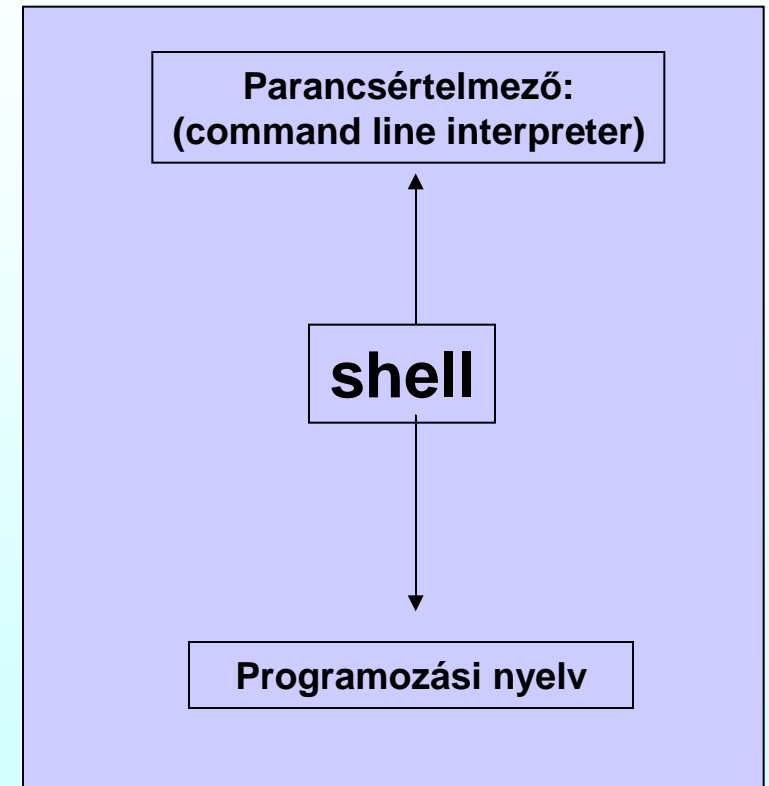
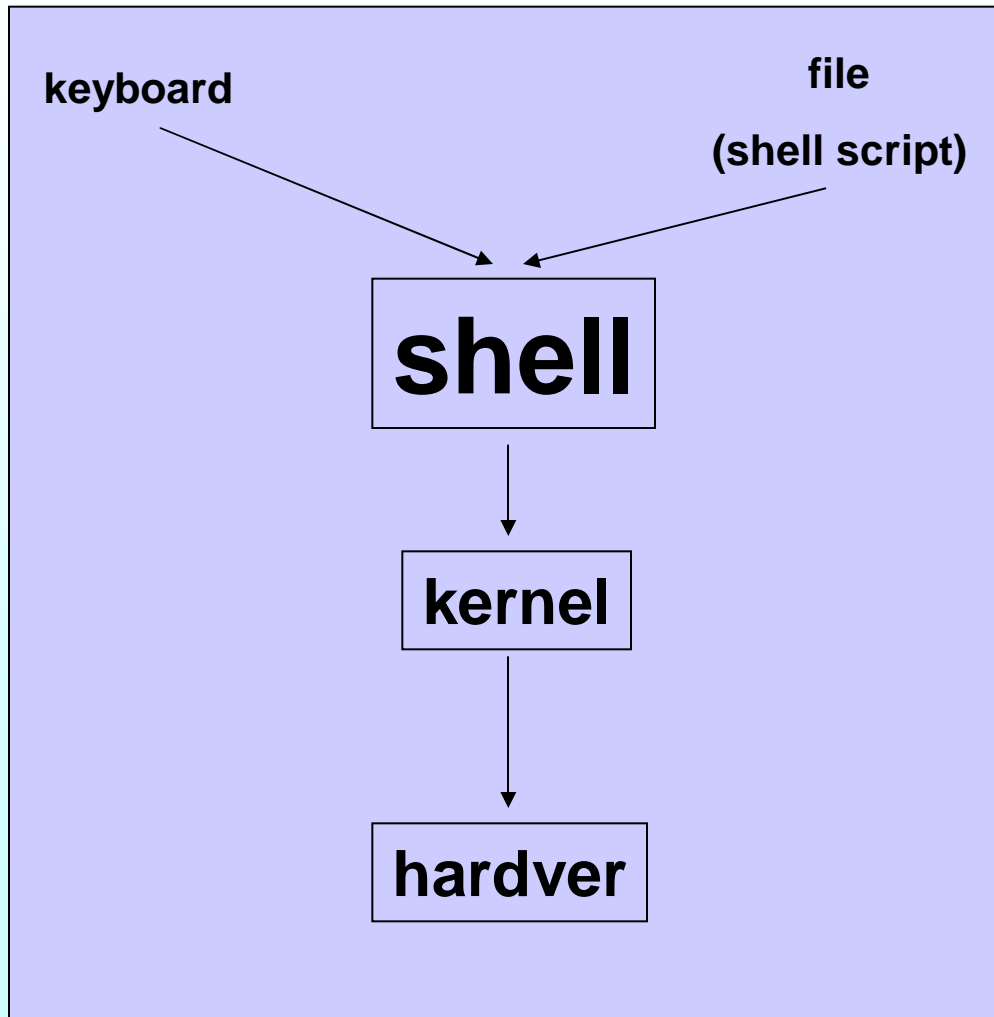
/etc/group

group_name:(passwd):GID: userlist

Mountolás



Shell (parancsértelmező)



Speciális unix tulajdonság: a shell nincs beépítve a kernelbe, így többféle shell is használható!

Shell (parancsértelmező)

A felhasználók és az op. rendszer közötti interfész a shell!

Bourne shell

- /bin/sh
- tradicionális shell
- Parancsvisszahívás hiányzik
- Alias mechanizmus hiányzik

C shell

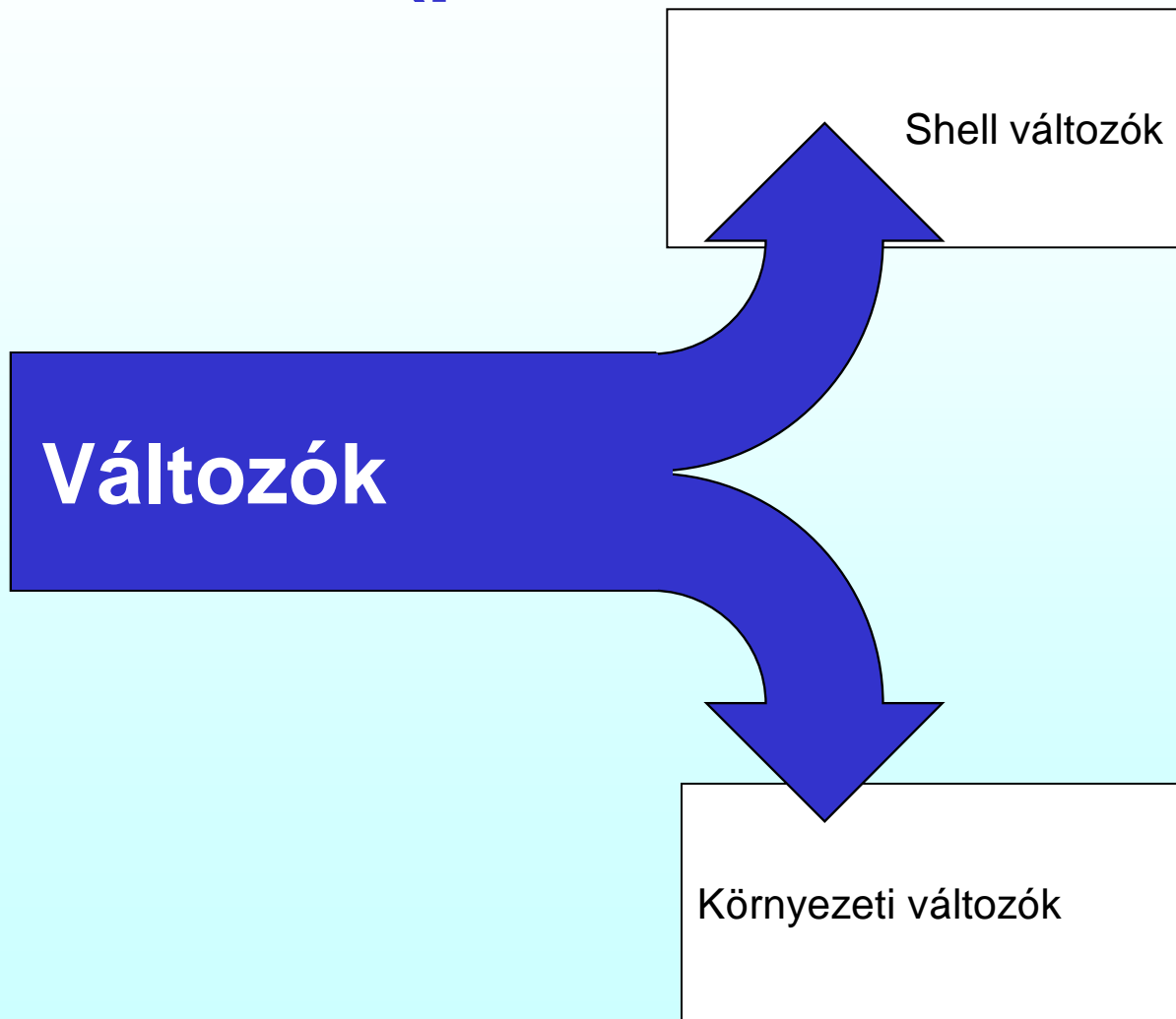
- /bin/csh
- Nem kompatibilis a Bourne shelllel
- Szintaxisa a C nyelvet követi
- Parancsvisszahívás és automatikus parancskiegészítés használható
- Alias mechanizmus használható
- Interaktív feladatok megoldásához optimalizált

Korn shell

- A Bourne shelllel felülről kompatibilis
- Parancsvisszahívás használható
- Alias mechanizmus használható
- Job kezelés lehetséges

További shellek is léteznek: pl. bash

Shell (parancsértelmező)



Korn shell:

Shell változó
értékkadás:

VÁLTOZÓ=érték

Környezeti változó
értékkadás:

VÁLTOZÓ=érték

export VÁLTOZÓ

Változó értékre
hivatkozás:

\$VÁLTOZÓ

Shell (parancsértelmező)

Shell inicializálás

Login shell
(Elsődleges
shell belépés
után)

1. /etc/profile
2. \$HOME/.profile
3. Az ENV változó határozza meg

**Nem login
shell**

1. Az ENV változó határozza meg

**A shell
elindul**

Shell (parancsértelmező)

Speciális karakterek idézése

- **A shell számára speciális karakterek:**
* ? | [] < > ; ' " ` \ \$ &
- \ elrejt az utána következő karaktert
- " " elrejt a közöttük levő karaktereket (kivéve: \$)
- ' ' elrejt a közöttük levő karaktereket
- ` ` parancs behelyettesítés!

Alias parancsok

- A parancsokra a felhasználók saját maguk által adott névvel hivatkozhatnak
- Az aliasok a felhasználói környezethez tartoznak
- **Létrehozás:**
 - alias alias_parancs=már_meglevő_parancs
- **Átmeneti megszüntetés:**
 - \alias_parancs
- **Végleges megszüntetés:**
 - unalias alias_parancs