Sistemsko programiranje

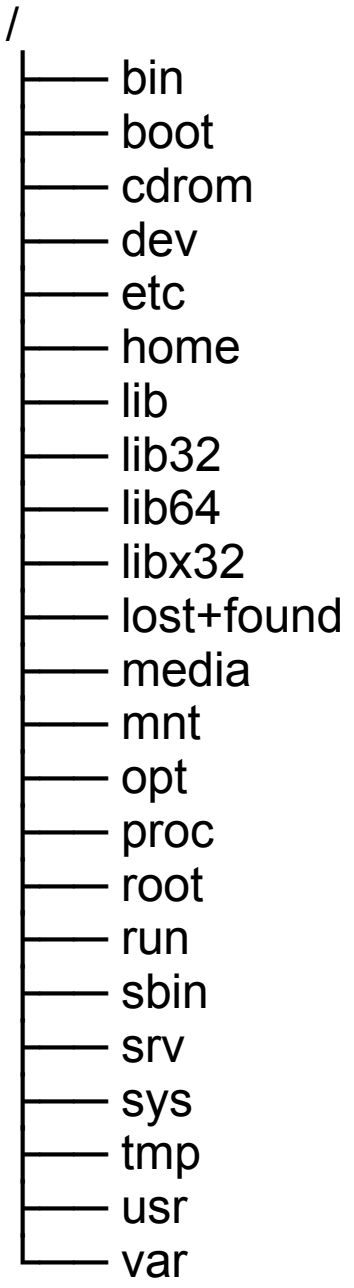
dr.sc. Amer Hasanović

Unix sistem

- Unix kernel stvara jedinstven intefejs i infrastrukturu za:
  - proizvoljan broj korisnika,
  - autorizaciju i sigurnost,
  - paralelizam i koordinaciju (procesi i niti),
  - vezu sa vanjskim uređajima (fajl sistem).
- Aplikacije moguće razvijati upotrebom:
  - direktno kernela (kroz sistemske pozive),
  - ljuski (shell),
  - c bilioteke,
  - ostalih biblioteka.

Unix fajl sistem

- U formi stabla omogućava vezu sa vanjskim uređajima, organizaciju programa i podataka.
- Sačinjen od inode-a koji su asocirani sa stazama.
- Tipovi inode-a:
  - datoteke,
  - direktoriji,
  - uređaji:
    - blok
    - karakter
  - simbolički linkovi,
  - fifo,
  - soketi.



Unix korisnici i grupe

- Unix sistem može da ima proizvoljan broj korisnika koji se organizuju u grupe.
- Korisnici i grupe imaju simboličка imena (user name, group name) i brojčani identifikator (uid i gid)
- Korisnici se definiraju u tekstualnoj datoteci “/etc/passwd”.
- Korisnik je član minimalno jedne grupe koja se zove primarna grupa, a može biti član i sekundarnih grupa (fajl “/etc/group”)
- Sistem obavezno ima root korisnika i root grupu (uid=0 i gid=0).

/etc/passwd i /etc/group

```
root:x:0:0:root:/root:/bin/bash
…
syslog:x:104:110::/home/syslog:/bin/false
…
amer:x:1000:1000:amer,,,:/home/amer:/bin/bash
```

```
root:x:0:
...
adm:x:4:syslog,amer
….
docker:x:132:amer
….
amer:x:1000:
```

Unix autentifikacija

- Svaki proces izvršava se u vlasništvu nekog korisnika i grupe, i ima slijedeće vlasničke kredencije:
  - ruid, rgid → real uid i gid
    - uid i gid korisnika koji je kreirao proces.
  - euid, egid → effective uid i gid
    - uid i gid koji se koristi prilikom autorizacije.
  - suid, sgid → saved uid i gid
    - snimljeni euid i egid
  - sekundarni gid-ovi
- Nakon procesa pokretanja sistema (bootloader → kernel → init → login) korisnik se identificira sistemu kroz login program unošenjem imena i šifre.
  - Po uspješnom logiranju obično se pokreće shell sa ruid, euid i suid postavljenim na id korisnika koji se autentificirao sistemu.

Fajl sistem dozvole

- Svaki inode je u vlasništvu određenog korisnika i grupe, i ima dozvole za pristup spram tri podržane operacije u formi slijedećih bita:
  - r → čitanje za vlasika, grupu i ostale korisnike
  - w → pisanje za vlasnika, grupu i ostale korisnike
  - x → izvršenje za vlasnika, grupu i ostale korisnike.
- Ako proces proba pristupiti nekom inode-u, sistem vrši provjere spram postavljenih fajl sistem dozvola i kredencija procesa, i to:
  - euid,
  - egid,
  - sekundarni gid.

- Dozvole za direktorije
  - W → omogućava kreiranje, promjenu i brisanje linkova iz direktorija.
  - R → omogućava čitanje imena svih linkova u direktoriju.
  - X → omogućava pristup inode-ima koji imaju linkove u direktoriju, pod uslovom da korisnik zna ime linka.

setuid i setgid

- Ove dozvole, ukoliko su postavljene za izvršne datoteke, omogućavaju da euid, egid, suid i sgid procesa, nakon učitavanja izvršne datoteke tj. nakon obavljenog sistemskog poziva exec, budu postavljeni na vlasnika i vlasničku grupu učitanog programa.
  - ruid i rgid ostaju nepromjenjeni.
- setgid, ukoliko je postavljen za direktorij, određuje da vlasnik kreirane datoteke ili poddirektorija unutar tog direktorija bude grupa koja je vlasnik direktorija.

sticky bit i umask

- Ukoliko je sticky bit postavljen za direktorij omogućeno je da samo vlasnik inode-a čiji je link unutar datog direktorija i vlasnik direktorija mogu brisati ili promjeniti ime linka asocirano sa datim inode-om.
- Predstavlja poseban set kontrolnih bita na osnovu kojeg proces postavlja default dozvole za novokreirane inode.