Operacijski sistemi

Upravljanje z uporabniki

Jurij Mihelič, FRI, Uni LJ

Vsebina

- Varnost in zaščita
- Uporabniki
- Prijava v sistem
- Uporabniki v Linux

Varnosti in zaščita

- Zaščita
  - je mehanizem za nadzor dostopa do virov
    - programi (oz. uporabniki) uporabljajo vire
    - ščiti pred nedovoljeno uporabo virov
  - pravila uporabe, politika (policy)
    - pravila delovanja mehanizma in uporabe virov
    - npr. različne vrste dostopov (read, write, execute)
  - naloga OS
    - OS je odgovoren za vzpostavljanje zaščite virov, ki jih upravlja

Varnosti in zaščita

- Varnost
  - mera zaupanja v ohranjanje integritete sistema
    - posledica zaščite na različnih nivojih
  - varnost sistema vključuje tudi okolje
  - zaščita virov s strani OS
    - zaščita pred omrežnim dostopom (npr. požarni zidovi)
    - zaščita pred fizičnim dostopom (npr. poseben prostor)
    - uporabniška ozaveščenost (npr. dobra gesla)

Varnosti in zaščita

- Načela načrtovanja varnosti
  - mehanizem zaščite mora biti javen
    - predpostavljanje, da napadalec ne pozna mehanizma samo zavaja načrtovalce
  - privzeto dovoljenje naj bo „ni dostopa“
    - legitimni dostop zavrnjen lažje odkrijemo
      - uporabnik se pritoži administratorju
    - neavtoriziran dostop odobren težje odkrijemo
      - napadalec navadno ne razglaša svojih dejanj
  - sprotno preverjanje dovoljenj
    - aktualna dovoljenja naj se preverijo ob dejanju
    - spreminjanje dovoljenj tako ne povzroči težav
      - npr. datoteka, ki je v uporabi dlje časa

Varnosti in zaščita

- Načela načrtovanja varnosti
  - procesi naj imajo najmanjše možne privilegije
    - npr. program naj ima dovoljenje spreminjanja le tistih podatkov, ki jih nujno mora
  - mehanizem zaščite naj bo:
    - preprost, celovit in vgrajen v najnižje sloje OS
    - nadgradnja ne-varnih sistemov se ne obnese
  - shema varnosti naj bo uporabniško prijazna
    - prezapleteni mehanizmi se ne bodo uporabljali
    - premalo zaščite bo povzročilo pritožbe

Uporabniški račun

- Uporabnik
  - oseba, ki uporablja računalniški system
  - različni nameni uporabe
    - navadna uporaba, zabava, informiranje, delo
    - programiranje, urejanje slik in videa
    - vzdrževanje sistema
  - prekiravanje dejavnosti in uporabljanih podatkov
    - različne osebe lahko podatke delijo ali ne
    - privatnost podatkov

Uporabniški račun

- Vrste uporabnikov
  - navaden uporabnik
    - za običajno uporabo računalnika
  - administrator, root
    - vzdrževalec sistema, ima več ali vse pravice
  - superuser, sudoer
    - običajen uporabnik, ki lahko začasno dvigne svoje pravice
  - gost
    - anonimen običajen uporabnik
    - njegove nastavitve in datoteke se navadno ne hranijo

Uporabniški račun

- Število uporabnikov OSa
  - brezuporabniški (enouporabniški) OS
    - ni razlikovanja med uporabniki
    - ni nadzora nad uporabo virov
  - večuporabniški OS
    - razlikovanje in razpoznavanje uporabnikov
    - sočasna uporaba sistema s strani več uporabnikov
    - lastništvo virov
    - nadzor uporabe virov

Uporabniški račun

- Uporabniški račun
  - mehanizem, ki omogoča
    - razlikovanje med uporabniki
    - prijavo v sistem
    - ločevanje virov med uporabniki
  - skupek podatkov o uporabniku
    - osebni podatki
      - uporabniška številka, ime in priimek, dodatne informacije
    - podatki za prijavo v sistem
      - uporabniško ime in geslo
      - domači imenik, prijavna lupina
    - podatki za mehanizem zaščite
      - uporabnikove skupine

Prijava v sistem

- Prijava v sistem
  - **identifikacija**
    - ugotavljanje, kdo je dani uporabnik
    - npr.: uporabniško ime
  - **avtentikacija**
    - preverjanje istovetnosti danih podatkov
    - potrjevanje identitete
      - Ali je uporabniki res tisti, za katerega se izdaja?
      - npr. z geslom preverimo uporabniško ime
    - več faktorska avtentikacija
      - geslo + pin (telefon), bančna kartica + pin

Prijava v sistem

- Načini avtentikacije
  - **pomnjenje** določenih **podatkov**
    - gesla, osebni podatki, PIN/PUK kode, geste, podpis, izziv-odgovor (npr. skrita formula) itd.
  - **fizične lastnosti** uporabnikov
    - prstni odtis, dolžina prstov, zenica, glas, hoja
  - **fizične naprave**
    - ključ, pametne kartice, RFID ključi

gesla dolžine 8 iz nabora 50 znakov
- št. različnih gesel = 508
- preverjanje 1 gesla = 1 ns
- preverjanje vseh = 39063 s ~ 11h
- hranjenje vseh ~ 285 TiB

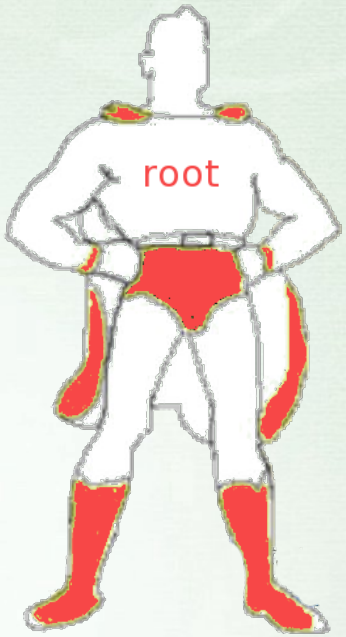
gesla dolžine 10 iz nabora 50 znakov
- preverjanje vseh ~ 3 leta
- hranjenje vseh ~ 694 TiB

So realna gesla naključni nizi znakov?

Prijava v sistem

- Načini dostopa do računalnika
  - **lokalna** prijava / dostop
    - prijava v lokalni računalnik, ki ga fizično uporabljamo
    - uporaba računalnika, ki je neposredno priklopljen na tipkovnico in zaslon
  - **oddaljena** prijava
    - prijava v oddaljeni računalnik preko lokalnega
    - dostop poteka preko omrežja
    - tipkovnica in zaslon lokalnega sta
    - primeri
      - Unix: ssh oz. secure shell
      - Windows: remote desktop connection

Uporabniki v Linuxu



- Administrator
  - uporabniško ime `root`
  - domači imenik `/root`
  - ima vsa dovoljenja in odgovornost
- Ostali uporabniki
  - skoraj poljubno uporabniško ime
  - domači imenik se nahaka v `/home/`*<username>*

Uporabniki v Linuxu

- Uporabniški računi
  - datoteka /etc/passwd
    - vse razen podatkov o geslu

```
root:x:0:0:root:/root:/bin/bash
jure:x:1001:1001:Jure  Mihelic,,,:/home/jure:/bin/bash
student:x:1364:1198:Student:/home/student:/bin/bash
```

ime:x:uid:gid:polno ime:domači imenik:prijavna lupina

  - datoteka /etc/shadow
    - hrani zgoščene vrednosti (hash) gesel

```
jure:$6$G1nqqs54$F0xL1...kZfvMoP1:14630:0:99999:7:::
student:$6$myVOR2Ad$g...AFZckSRj.:14943:0:99999:7:::
```

ime:$**metoda**$**sol**$**koda**:ostalo (rok trajanja gesla itd.)

Uporabniki v Linuxu

- Uporabniški računi
  - soljenje gesel
    - sol: naključni niz dodan geslu pred zgoščanjem
  - namen soljenja
    - enaki gesli + različna sol imata različno zgoščena vrednost
    - onemogočanje napada z mavrično tabelo (rainbow table)

geslo	md5 hash	ae404a1ecbcdc8e96ae4457790025f50
geslo123	md5 hash	211340d1aab430caaadba78431c3e810
geslo456	md5 hash	230859fca4cdc8046ebdde7685391ff1

Uporabniki v Linuxu

- Uporabniške skupine
  - datoteka /etc/group
  - hrani seznam uporabnikov, ki še pripadajo skupini
    - poleg skupine, zapisane v /etc/passwd

ime skupine:x:gid:seznam uporabnikov

```
root:x:0:
cdrom:x:24:jure,luka,ana,tomaz,uros,branka,mitja,metka
audio:x:29:ana,uros,mitja
video:x:44:luka,tomaz,branka
games:x:60:jure,ana,metka
admin:x:115:jure,luka,metka
jure:x:1001:
luka:x:1002:
```

  - datoteka /etc/shadow
    - gesla skupin