Operacijski sistemi

Varnost in nadzor dostopa

Jurij Mihelič, FRI, Uni LJ

Vsebina

- Varnost
- Občutljivost podatkov
- Načela snovanja varnosti
- Nadzor dostopa
- Zaščita datotek
- Zagon programov

Varnost

- Vrste varnosti
  - Informacijska varnost
  - Kibernetska varnost
    - računalniška varnost, IT varnost, digitalna varnost
  - Omrežna, internetna in spletna varnost
  - Oblačna, aplikacijska in programska varnost
  - Varnost infrastrukture, podatkovnih baz, računalniških sistemov, operacijskih sistemov

Varnost

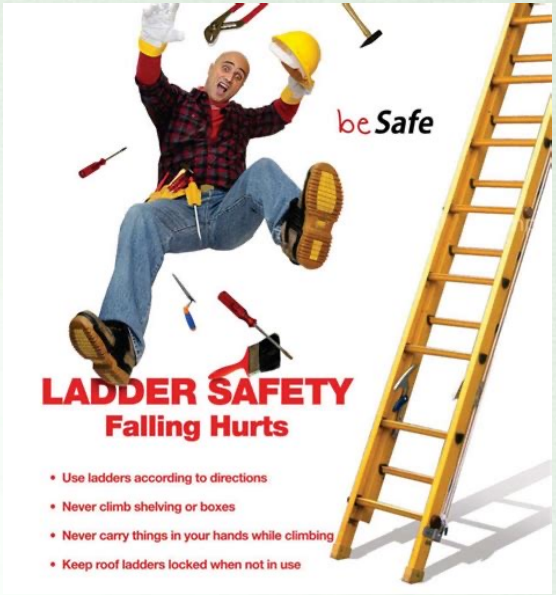
- Informacijska varnost – InfoSec
  - veda o varovanju informacij in sistemov
  - varovanje **občutljivih informacij**
    - **tajnost**, skrivanje (secrecy)
      - skrivanje informacij pred ogledom s strani neželnih oseb
    - **zasebnost** (privacy)
      - zasebne in javne informacije
      - pravica do tajnosti osebnih informacij (nerazkritje javnosti)
  - varovanje **informacijskih sistemov**
    - zagotavljanej želenega oz. pravilnega delovanja

Varnost

- **Ranljivost sistema** (system vulnerability)
  - lastnost sistema, da je izpostavljen možnosti neželene uporabe

- **Varnostna pretnja** (security threat)
  - potencialna negativna aktivnost, katere posledica je lahko neželeno delovanje sistema

Varnost



- **Varstvo / varnost** (safety)
  - **zagotavljanje želenega** delovanja sistema
  - varovanje pred škodo zaradi **nenamernih** negativnih aktivnosti
    - človeške napake, naravne sile
    - požar, orkan, sevanje, fizične okvare
  - funkcionalna varnost, pravilnost

- **Varnost** (security)
  - **izogibanje neželenemu** delovanju sistema
  - varovanje pred škodo zaradi **namernih** negativnih aktivnosti
    - kriminal, vdiranje v sisteme

Varnost

- Cilji varovanja
  - **preprečiti** oz. zmanjšati verjetnost **nepooblaščenega** oz. neprimernega **dostopa** do podatkov in sistemov
    - nezakonita uporaba, nezaželjena uporaba, razkritje,
    - uničenje, okvara, sprememba, pregled,
    - snemanje, kopiranje, razvrednotenje itd.
  - vzpostaviti oz. ohraniti **zaupanje** v želeno delovanje sistema
  - celostno varovanje
    - varovanja na različnih nivojih
    - vključuje tudi okolje varovanega sistema
    - vključuje tudi uporabniško ozaveščenost

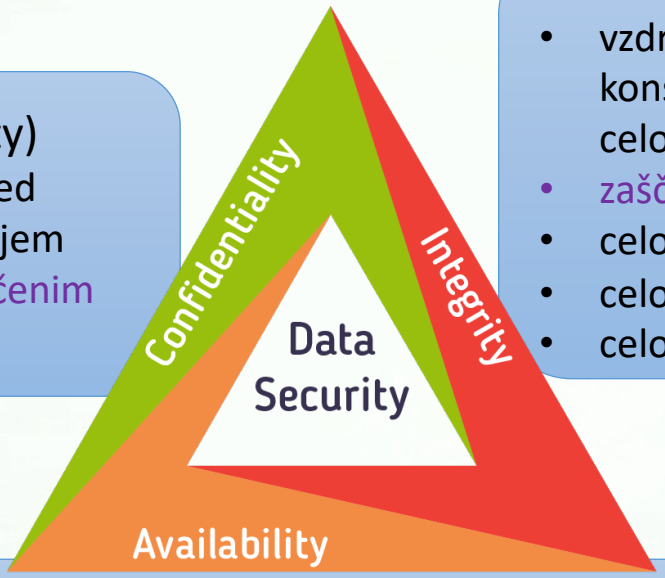
Varnost

- Vloga operacijskega sistema
  - ponuditi mehanizme za zaščito (protection) oz. varovanje
  - pravila uporabe oz. **varnostna politika** (policy)
    - pravila delovanja mehanizma in uporabe virov
    - npr. različne vrste dostopov (read, write, execute)
  - OS vzpostavlja **nadzor dostopa do virov**
    - programi (oz. uporabniki) uporabljajo vire
    - ščiti pred nedovoljeno uporabo virov
    - preverjanje, ali se sme nek vir zaseči
    - sestoji iz identifikacije, overitve in avtorizacije

Občutljivost podatkov

- Triada CIA, NIST, 1977
  - **C**onfidentiality, **I**ntegrity, **A**vailability

Zaupnost (confidentiality)
- varovanje informacij pred nepooblaščenim razkritjem
- zaščita pred nepooblaščenim **branjem**



Celovitost (integrity)
- vzdrževanje natančnosti, celovitosti in konsistentnosti podatkov skozi njihov celoten življenski cikel
- zaščita pred nepooblaščenim **pisanjem**
- celovitost podatkov
- celovitost sistema
- celovitost ljudi

Razpoložljivost (availability)
- informacije so na voljo, ko jih potrebujemo
- pravilno in nemoteno delovanje sistema
- preprečevanje DoS napadov

Občutljivost podatkov

- Je CIA triada zadostna / zadovoljiva
  - OECD, 1992, 2002
    - 9 načel: awareness, responsibility, ethics, ...
  - Parkerjeva heksada, 1998
    - *confidentiality*, possession, *integrity*, authenticity, *availability*, utility
  - NIST, 2004
    - 33 načel na osnovi OECD
  - Open Group, 2011
    - 5 ključnih konceptov

Občutljivost podatkov

- Pristnost, avtentičnost (authenticity)
  - dokaz izvora sporočila za prejemnika
- Neovrgljivost, nazatajljivost (non-repudability)
  - dokaz dostave sporočila za pošiljatelja
- . . .

Varnost in zaščita

- Načela načrtovanja varnih sistemov
  - ekonomičnost mehanizma
    - naj bo preprost in nezapleten
    - vgrajen v najnižji mogoči sloj sistema
    - nadgradnja ne-varnih se ne izplača
  - odprta zasnova
    - mehanizem naj bo javen
    - predpostavi, da napadalec pozna vse podrobnosti, a mehanizem kljub temu omogoča varovanje
    - predpostavljanje, da napadalec ne pozna mehanizma samo zavaja načrtovalce

Varnost in zaščita

- Načela načrtovanja varnih sistemov
  - varne privzete nastavitve
    - 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
  - popolno in sprotno preverjanje
    - aktualna dovoljenja naj se preverijo ob dejanju
    - sprememba dovoljenj tako ne povzroči težav
      - npr. datoteka, ki je v uporabi dlje časa

Varnost in zaščita

- Načela načrtovanja varnosti
  - najmanjši privilegiji
    - uporabniki naj imajo najmanjše še možne privilegije, za izvedbo želenih dejanj
    - npr. program naj ima dovoljenje spreminjanja le tistih podatkov, ki jih nujno mora
  - ločevanje privilegijev
    - kritična dejanja naj zahtevajo potrditev s strani več uporabnikov
    - več-dejavniška overitev

Varnost in zaščita

- Načela načrtovanja varnosti
  - najmanjši skupni mehanizem
    - za različne uporabnike ali proces uporabi ločene podatkovne strukture ali mehanizme
  - shema varnosti naj bo uporabniško prijazna
    - prezapleteni mehanizmi se ne bodo uporabljali
    - premalo zaščite bo povzročilo pritožbe

Nadzor dostopa

- Nadzor dostopa do datoteke
  - določa **kdo** lahko **kaj** počne **s čim**
  - **kdo? subjekt**
    - uporabnik, skupina, proces, območja zaščite
    - npr. lastnik datoteke, skupina datoteke, ostali
  - **kaj? dovoljenje**
    - dovoljenja za operacije nad datoteko
    - npr. nič, preverjanje obstoja, izvajanje, branje, dodajanje, pisanje, spreminjanje zaščite, brisanje
  - **s čim? objekt, vir**
    - objekti zaščite so navadno datoteke, vendar lahko tudi naprave, pomnilnik itd.

Nadzor dostopa

- Ključni pojmi
  - **identifikacija**
    - glej prosojnice "Uporabniki"
  - **overitev** / avtentikacija
    - glej prosojnice "Uporabniki"
  - **avtorizacija** (authorization)
    - postopek preverjanja, s katerim uporabnik pridobi dovoljenja za uporabo vira
    - dovoljenja za uporabo vira
  - beleženje (accounting, logging)
  - nadzor (audit)

Nadzor dostopa

- **Matrika nadzora dostopa**
  - stolpci: objekti nadzora dostopa
  - vrstice: subjekti, ki dostopajo
  - elementi: način dostopa (npr. nabor dovoljenj)

	Datoteka 1	Datoteka 2	Datoteka 3	Datoteka 4
Uporabnik A	lastnik R, W	R, X	lastnik R	
Uporabnik B		lastnik R, W, X	R	
Uporabnik C	W			lastnik R

Nadzor dostopa

- **Nadzorni seznam dostopa** (access control list)
  - vsak vir ima svoj seznam dostopa
  - seznam vsebuje ACL vnose (ACL entry)
  - vnos podaja dovoljenja za posamezne subjekte

	Datoteka 1	Datoteka 2	Datoteka 3	Datoteka 4
Uporabnik A	lastnik R, W	R, X	lastnik R	
Uporabnik B		lastnik R, W, X	R	
Uporabnik C	W			lastnik R

dekompozicija matrike dostopa po stolpcih

Datoteka 1: (A, lastnik, R, W), (C, W)
Datoteka 2: (A, R, X), (B, lastnik, R, W, X)
Datoteka 3: (A, lastnik, R), (B, R)
Datoteka 4: (C, lastnik, R)

Nadzor dostopa

- **Seznam zmožnosti** (capabillities list)
  - vsak subjekt ima svoj seznam zmožnosti
  - zmožnost podaja dovoljenja uporabe virov
  - zmožnost je ne-poneverljiv objekt

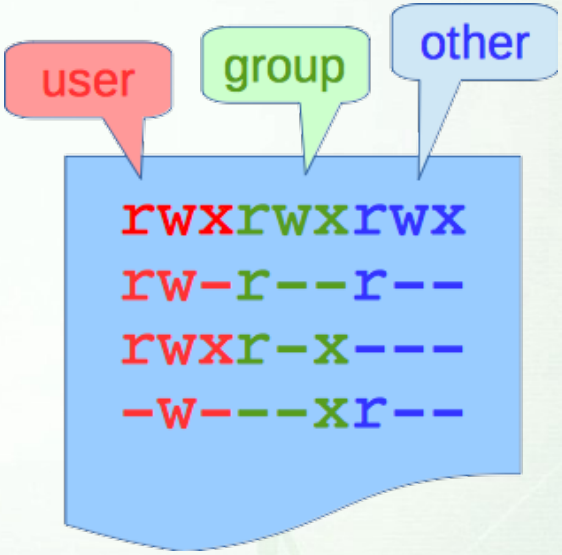
	Datoteka 1	Datoteka 2	Datoteka 3	Datoteka 4
Uporabnik A	lastnik R, W	R, X	lastnik R	
Uporabnik B		lastnik R, W, X	R	
Uporabnik C	W			lastnik R

dekompozicija matrike dostopa po vrsticah

Uporabnik A: (1, lastnik, R, W), (2, R, X), (3, lastnik, R)
Uporabnik B: (2, lastnik, R, W, X), (3, R)
Uporabnik C: (1, W), (4, lastnik, R)

Zaščita datotek

- Osnovna zaščita datotek
  - **vrste dovoljenj**
    - `r` – **r**ead, `w` – **w**rite
    - `x` – e**x**ecute, `-` – prazno
  - **sklopi uporabnikov**
    - `u` – user (lastnik)
    - `g` – group (skupina)
    - `o` – other (ostali)
    - `a` – all (vsi)



Zaščita datotek

- Osnovna zaščita datotek
  - **pomen dovoljenj glede na tip datoteke**

znak	datoteka	imenik
`r`	branje datoteke	izpis vsebine imenika, npr. ukaz `ls`
`w`	pisanje oz. spreminjanje datoteke	spreminajanje imenika (ustvarjanje in brisanje imeniških vnosov)
`x`	izvajanje oz. datoteke je izvršljiva	vstop v imenik, npr. ukaz `cd`

Zaščita datotek

- Kdo lahko pobriše datoteko?
  - običajna zmota: njen lastnik
  - brisanje datoteke = brisanje imeniškega vnosa
  - torej: kdor ima dovoljenje pisanja v imenik, kjer je datoteka
    - podobno velja za ustvarjanje novih datotek

```
drwxrwxr-x zala devops  ./
drwxr-x--- sef  boss   ../
-rwxr-x--- vid  tester  brisi.me
```

Kdo lahko pobriše datoteko `brisi.me`?

Zaščita datotek

- Omejeno brisanje (restricted deletion)
  - bit oz. oznaka t – omejeno brisanje
    - sprememba privzetega delovanja
    - datoteko v imeniku lahko odstrani lastnik datoteke
  - uporaba
    - imenik `/tmp` za začasne datoteke

```
drwxrwxrwt root root tmp
```

Zagon programov

- Zagon programa
  - nastali proces dobi dovoljenja trenutnega uporabnika in skupine
  - Kako lahko torej ukaz `passwd` spremeni datoteko `/etc/shadow`?

```
-rwsr-xr-x root root     /usr/bin/chage
-rwsr-xr-x root root     /usr/bin/crontab
-rwsr-xr-x root root     /usr/bin/passwd
-rwsr-xr-x root root     /usr/bin/su
---s--x--x root root     /usr/bin/sudo
-rwxr-sr-x root postdrop /usr/sbin/postdrop
-rwxr-sr-x root postdrop /usr/sbin/postqueue
```

Zagon programov

- Bit setuid, oznaka `u+s`
  - zagnani program dobi dovoljenja lastnika
- Bit setgid, oznaka `g+s`
  - zagnani program dobi dovoljenja skupine

Sistemski klici

- `getuid()` … UID lastnika procesa
- `getgid()` … GID skupine, kateri pripada proces

- `geteuid()` … aktualni (effective) UID lastnika procesa
- `getegid()` … aktualni (effective) GID skupine, kateri pripada proces