**SIGURNOST I INTEGRITET**

**Sigurnost** - zaštita podataka od neautorizovanih korisnika (zaštita protiv neautorizovanog pristupa, promene ili uništenja)

**Integritet** – zaštita podataka protiv autorizovanih korisnika (obezbeđenje ispravnosti I korektnosti podataka)

**Uvod**

**Sličnosti između sigurnosti I integriteta**

* Sistem mora da bude svestan izvesnih ograničenja koje korisnici ne smeju da prekrše
* Ograničenja moraju da budu zadata (od strane DBA) u nekom jeziku
* Ograničenja moraju da budu evidentirana u sistemskom katalogu (rečniku podataka)
* SUBP mora da vrši nadzor nad operacijama korisnika

**Sigurnost**

Aspekti problema sigurnosti :

* Pravni, socijalni i etički (npr. uvid u stanje računa korisnika)
* Fizička kontrola (npr. fizičko obezbeđenje računarske sale)
* Politička pitanja (odlučivanje ko i čemu sme da pristupi)
* Operativni problemi (npr. kako obezbediti tajnost lozinki)
* Hardverska kontrola (npr. da li CPU ima mogućnost hardverske zaštite programa)
* Podrška operativnog sistema (npr. da li OS briše sadržaj memorije I diskova po završetku rada programa)
* Problemi vezane za same baze podataka (npr. da li postoji koncept valsnika podataka)

Jedinice podataka na koje se osigurava:

* baza podataka
* relvar
* pojedinačna torka ili vrednost atributa
* alijasi
* sheme
* indeksi
* paketi
* prostori za čuvanje tabela

**Sigurnost u SQL-u**

Sigurnost se obično zapisuje preko kontrolne matrice pristupa

* Predstavljanje po korisnicima
* Predstavljanje po objektima
* Predstavljanje po dozvoli za pristup

Postoje dva mehanizma koji su, nezavisno jedan od drugog uključeni u sistem zaštite

1. **pogledi**, koji mogu da se korsite za sakrivanje osetljivih podataka od neautorizovanih korisnika
2. **podsistem za autorizaciju**, koji dopušta korisniku sa određenim pravima pristupa da ta prava selektivno i dinamički prenosi na druge korisnike, i/ili da preneta prava povuče

**Podsistem za autorizaciju**

Da bi korisnik izvršio bilo kakvu operaciju nad nekim objektom on mora da poseduje dozvolu (ili autorizaciju) za tu operaciju nad tim objektom. Tipovi i vrste dozvola nisu isti kod svih SUBP.

**Sistemski administrator** (SYSADM nivo autorizacije) je inicijalni vlasnik svih dozvola.

Davanje dozvola se vrši **GRANT** naredbom, a povlačenje **REVOKE** naredbom.

**GRANT naredba**

Sintaksa za dozvole nad pogledima ili tabelama:

GRANT dozvola [ON [tip] objekat] TO korisnik;

* dozvola – lista jedne ili više dozvola, razdvojene zarezima ili fraza *ALL PRIVILEGES ili ALL* koja označava sve privilegije koje se mogu dati GRANT naredbom
* korisnik – je lista korisnika razdvojenih zarezima ili *PUBLIC* (svi korisnici)
* tip – označava tip objekata. podrazumevano *TABLE*
* objekat – lista imena jednog ili više objekta (koji su svi istog tipa) razdvojeni zarezima
* ON se ne upotrebljava kada se daje dozvola za sistemske privilegije

Dozvole koje se odnosne na osnovne tabele i poglede:

* CONTROL
* INSERT
* DELETE  
  SELECT
* UPDATE (MOGU da se navedu pojedinačne kolone)

Dozvole koje se odnose samo na osnovne tabele:

* ALTER – dozvola sa izvršavanje naredbe ALTER nad tabelom
* INDEX – dozvola za izvršavanje naredbe CREATE INDEX nad tabelom
* REFERENCES – dozvola za formiranje/brisanje spoljašnjeg ključa koji referiše tu tabelu kao roditelj tabelu

**Primeri**:

GRANT SELECT ON TABLE DOSIJE TO KORISNIK01;

GRANT SELECT, UPDATE (SIFRA, NAZIV) ON TABLE PREDMET TO KORISNIK02, KORISNIK03, KORISNIK009;

GRANT ALL PRIVILEGES ON TABLE DOSIJE, PREDMET, ISPIT TO KORISNIK76, KORISNIK77;

GRANT SELECT ON TABLE DOSIJE TO PUBLIC;

GRANT DELETE ON ISPITNI\_ROK TO KORISNIK99;

**GRANT naredba – WITH GRANT OPTION**

Ako korisnik K1 želi da prenese dozvolu D korisniku K2, to može da uradi naredbom:

* GRANT dozvola ...
* GRANT dozvola ... WITH GRANT OPTION čime omogućuje korisniku K2 da dalje distribuira dozvolu koja mu je preneta

**Primeri**:

Neka je dato:

Korisnik K1:

GRANT SELECT ON TABLE DOSIJE TO K2 WITH GRANT OPTION;

Korisnik K2:

GRANT SELECT ON TABLE DOSIJE TO K3 WITH GRANT OPTION;

Korisnik K3:

GRANT SELECT ON TABLE DOSIJE TO K4 WITH GRANT OPTION;

Korisnik K4: ….

Tada povlačenje dozvole: REVOKE SELECT ON TABLE DOSIJE FROM K2

prouzrokuje lančano povlačenje dozvola za K3, K4…

**REVOKE naredba**

Sintaksa za dozvole nad tabelama ili pogledima:

REVOKE dozvola [ON [tip] OBJEKAT] FROM korisnik [BY ALL];

Povlačenje dozvole za nekog korisnika uzrokuje da svi planovi/paketi zasnovani na toj dozvoli postanu neispravni i uzrokuje automatsko vezivanje/ponovno vezivanje prilikom pozivanja takvog plana/paketa.

NIJE moguće ukinuti UPDATE dozvolu samo za pojedine kolone!

**Ostali aspekti sigurnosti**

* Kompletan sistem treba da bude zaštićen
* Ne prespostavljati da je sistem zaštite savršen
* Voditi evidenciju o prijavljivanju na bazu