SIGURNOST BAZA PODATAKA 1

Baza podataka - skup podataka koji su pohranjeni i organizirani tako da mogu zadovoljiti zahtjeve korisnika.

Sustav za upravljanje bazama podataka SUBP je programski sustav koji:

- može istovremeno upravljati s više baza podataka
- više korisnika/aplikacija uz osiguravanje sigurnosti i integriteta baze podataka
- temelji se na odabranom modelu podataka (hijerarhijski, mrežni, relacijski, objektno-relacijski, objektno-orijentirani, ...)

Zadaće SUBP-a

- trajna pohrana podataka (persistent storage)
- osiguravanje programskog sučelja (programming interface
    - DDL - Data Definition Language
    - DML - Data Manipulation Language
- optimiranje metoda pristupa podacima
- zaštita podataka
    - integritet podataka (integrity)
    - pristup podacima - autorizacija, sigurnost (security)
    - potpora za upravljanje transakcijama
        - upravljanje istodobnim pristupom (concurrency control)
        - obnova u slučaju razrušenja (recovery)

različite skupine korisnika:

- korisnici koji često koriste programirana sučelja (npr. službenici u banci)
- korisnici koji povremeno pristupaju bazi koristeći upitni jezik
- sofisticirani korisnici koriste je na složeniji način (npr. inženjeri, znanstvenici)
- Administratori
    - administrator poslužitelja baze podataka (database server administrator – DBSA)
        - instaliranje i nadogradnja SUBP-a; kreiranje novog korisnika; autorizacija na razini SUBP-a
    - administrator baze podataka (database administrator - DBA)
        - autorizacija na razini baze podataka (provođenje sigurnosne politike)
        - dodjeljivanje i ukidanje ovlasti korisniku baze podataka
        - dodjeljivanje sigurnosne klasifikacijske razine korisniku u višerazinskom sigurnosnom sustavu, u skladu s politikom organizacije

Oblici narušavanja sigurnosti baze podataka su:

- neovlašteno čitanje,
- izmjena
- uništavanje podataka

Posljedice:

- krađa ili prijevara
- gubitak tajnosti
- gubitak privatnosti
- gubitak raspoloživosti

sigurnost baze podataka se osigurava zaštitom na nekoliko razina:

- na razini SUBP
- na razini operacijskog sustava
    - spriječiti pristup radnoj memoriji računala ili datotekama u kojima SUBP pohranjuje podatke
- na razini računalne mreže
- fizička zaštita
- na razini korisnika

Defense-in-depth strategija

- zaštita u više slojeva
- proboj jednog sloja ne mora značiti i narušavanje sigurnosti podataka iz baze podataka
- nužna zaštita unutar baze podataka, čak i ako je implementiran poseban sustav zaštite baze podataka izvan baze podataka
- Svaki pokušaj neovlaštenog pristupa sustavu mora biti automatski zabilježen korisničkim imenom, datumom i vremenom, a ako je to moguće i mjestom s kojeg je takav pristup pokušan.

neki od postupaka kojima je bazu podataka moguće učiniti sigurnijom:

- ograničiti pristup važnim resursima - vatrozidi; upravljanje pristupom; antivirusna zaštita
    - patches
    - sustavi za otkrivanje i sprječavanje upada
- onemogućiti nepotrebne komponente i servise sustava za upravljanje bazama podataka
- ukloniti/onemogućiti nepotrebne korisničke račune i lozinke
- izvoditi procese baze podataka pod namjenskim, neprivilegiranim korisničkim računom

Aspekti zaštite podataka

- zakonski, socijalni i etički aspekt
    - ima li vlasnik baze podataka zakonsko pravo na prikupljanje i korištenje podataka
- strategijski aspekt
    - tko definira pravila pristupa
- operativni aspekt
    - kako osigurati poštivanje pravila

GDPR - General Data Protection Regulation

načelo najmanje ovlasti (least privilege)

- korisnik ima minimalan skup dozvola koje su neophodne za njegov trenutni zadatak
- pojedinac ima različite razine ovlasti u različito vrijeme, ovisno o zadaći ili funkciji koju obavlja

razdvajanje dužnosti (separation of duty - SoD)

- osjetljive zadatke u cijelosti ne može obaviti samo jedan korisnik

Mehanizmi zaštite na razini SUBP

- identifikacija i dokazivanje autentičnosti
- upravljanje pristupom
- šifriranje podataka
- praćenje pristupa podacima

- maskiranje podataka

Integritet baze podataka (database integrity) - operacije nad podacima koje korisnici obavljaju su ispravne (tj. uvijek rezultiraju konzistentnim stanjem baze podataka) • "podaci se štite od ovlaštenih korisnika„

Sigurnost baze podataka (database security) - korisnici koji obavljaju operacije nad podacima su ovlašteni za obavljanje tih operacija • "podaci se štite od neovlaštenih korisnika"

U oba slučaja: •

- moraju biti definirana pravila koja korisnici ne smiju narušiti •
- pravila se pohranjuju u rječnik podataka •
- SUBP nadgleda rad korisnika i osigurava poštivanje pravila

administrator sustava **omogućuje korisniku pristup sustavu** definiranjem jedinstvenog identifikatora korisnika (user name, user ID, login ID) i pripadne lozinke (password)

SQL-sjednica (SQL-session) je kontekst u kojem jedan korisnik obavlja niz SQL naredbi putem jedne veze (SQL-Connection) prema sustavu za upravljanje bazama podataka

- SQL-sjednica započinje kada korisnik ostvari vezu sa SUBP
- SQL-sjednica završava kada korisnik prekine vezu

```
CREATE USER name [ [ WITH ] option [ ... ] ]
where option can be:
      SUPERUSER | NOSUPERUSER
    | CREATEDB | NOCREATEDB
    | CREATEUSER | NOCREATEUSER
    | [ ENCRYPTED | UNENCRYPTED ] PASSWORD 'password'
    | INHERIT | NOINHERIT
    |...
```

Upravljanje pristupom - niz postupaka kojima se utvrđuje i evidentira pokušaj pristupa, te odobrava ili odbija pristup na temelju unaprijed utvrđenih pravila

sigurnosna politika - pravila pristupa na visokoj razini (zakonski, socijalni, etički aspekt)

- temeljena na načelu treba-znati (need-to-know), kompetentnosti, nadležnosti, sukobu interesa…
- na nju mogu utjecati zakonska i etička pitanja, politike na državnoj ili korporativnoj razini …•
- dinamična - mijenja se u skladu s promjenama poslovnih faktora, regulativa i uvjeta u okruženju•
- problem preslikavanja nejasnih i dvosmislenih zahtjeva u dobro definirana i jednoznačna pravila

sigurnosni model - formalni prikaz sigurnosne politike (strategijski aspekt)

sigurnosni mehanizam - (operativni aspekt) funkcije kojima je implementirano upravljanje pristupom

reference monitor - komponenta koja upravlja svakim pokušajem pristupa i utvrđuje je li u skladu sa sigurnosnom politikom

autorizacija - postupak evidentiranja pravila pristupa

Elementi sustava za upravljanje pristupom

- korisnik – entitet koji koristi računalni sustav (osoba, uređaj)
    - sjednica (session) - instanca dijaloga korisnika sa sustavom
- subjekt – aktivni entitet koji može inicirati zahtjev za obavljanje operacija na objektima
    - proces koji djeluje u ime korisnika
    - korisnik može imati više aktivnih subjekata
- objekt - entitet sustava na kojem može biti obavljena operacija
- operacija - aktivan proces pozvan od strane subjekta, koji nakon poziva izvršava funkcije
- dozvola (pravo pristupa, ovlast) određenog načina pristupa objektu u sustavu
    - kombinacija objekta i operacije
    - pozitivna dozvola - ako ne postoji, zatraženi pristup je odbijen
    - negativna dozvola (tj. zabrana) - ako postoji, zatraženi pristup je odbijen

klasični pristupi upravljanja pristupom:

- zatvorena politika - dozvoljen pristup za koji postoji (pozitivna) dozvola
- otvorena politika - uskraćen pristup za koji postoji zabrana (tj. “negativna dozvola”) •
    - ako zabrana ne postoji, pristup je dozvoljen

problemi kod kombiniranog korištenja pozitivnih i negativnih dozvola:

- nepotpunost - za pristup nije specificirana dozvola • može se izbjeći definiranjem pretpostavljene politike
- nekonzistentnost - za pristup postoji i negativna i pozitivna dozvola • može se izbjeći definiranjem politike razrješavanja konflikata

Diskrecijsko upravljanje pristupom

- upravljanje pristupom na temelju:
    - identiteta korisnika koji zahtijeva pristup i
    - eksplicitnih pravila pristupa koja utvrđuju tko može izvesti koje akcije na kojim objektom sustava
- koncept vlasništva nad objektom vlasnik objekta određuje kome se dozvoljava pristup
- određenom korisniku potrebno je eksplicitno dodijeliti dozvolu za obavljanje određene operacije nad određenim objektom (autorizacija)
- dozvole su opisane trojkama <korisnik, objekt, vrsta operacije>
- podaci o dodijeljenim dozvolama pohranjuju se u rječnik podataka
- prije obavljanja svake operacije, SUBP provjerava ima li korisnik dozvolu za obavljanje operacije nad objektom (upravljanje pristupom)

Upravljanje pristupom u SQL-u

Mehanizmi upravljanja pristupom

- naredbe za dodjeljivanje (GRANT) i ukidanje dozvola (REVOKE)
- virtualne tablice (view)
- pohranjene procedure
- modifikacija upita

Objekti

- tablica (table)
- atribut (stupac tablice, column)
- virtualna tablica (pogled, view)
- pohranjena procedura
- baza podataka (neki sustavi, npr. IBM Informix)

Vlasnik objekta - implicitno dobiva dozvole za obavljanje svih vrsta operacija nad objektom

SHEME

PostgreSQL:

- Baza podataka sadrži jednu ili više shema
- Sheme sadrže tablice, virtualne tablice (, funkcije, …)
- Različite sheme mogu sadržavati istoimene tablice
- Sheme analogne s: •
    - Mapama u datotečnom sustavu (s tim da se ne mogu gnijezditi) •
    - Imenskim područjima (namespaces) u programskim jezicima

- Stvaranje:

```
CREATE SCHEMA student;

CREATE TABLE student.postavke (
          username TEXT primary key,
          cm_skin  TEXT not null
);
```

- Pristup:

```
-- schema.table
-- database.schema.table
SELECT * FROM student.postavke
```

- Brisanje:

```
DROP SCHEMA student;
-- cannot drop schema student because
-- other objects depend on it
DROP SCHEMA student CASCADE;
-- obrisani i sadržani objekti!!
```

Trenutne postavke za SSP se mogu dobiti sljedećom naredbom:

```
SHOW search_path;
```

search_path
"$user", public

- Kao trenutnu shemu PostgreSQL će odrediti shemu "$user", ako takva postoji
- Ako ne postoji, trenutna shema postaje public

Ako je CURRENT_USER npr. tibor, tada je "$user" shema koja se zove tibor

Vrste dozvola u SQL-u na razini baze podataka - dbPrivilege

- CONNECT – spajanje na bazu
- CREATE – stvaranje shema

Vrste dozvola u SQL-u na razini sheme - (schemaPrivilege

- USAGE - Nužan preduvjet za pristupanje objektima sadržanima u shemi.
- CREATE - Dozvoljava stvaranje novih objekata (tablice, funkcije, …) u shemi.
- Korisnik nema dozvolu pristupa nijednom objektu sheme kojoj nije vlasnik

Vrste dozvola u SQL-u na razini [virtualne] tablice - (tablePrivilege)

- **SELECT, UPDATE, INSERT, DELETE, ALL PRIVILEGES(sve)**

SQL naredbe za dodjeljivanje i ukidanje dozvola

- GRANT/REVOKE {privilegija} ON {db/schema/table} {ime} TO/FROM {korisnik}