Sigurnost baza podataka, 2. dio

Upravljanje pristupom ovisno o sadržaju i kontekstu

upravljanje pristupom ovisno o sadržaju

- pristup objektu na temelju sadržaja jedne ili više njegovih komponenata

upravljanje pristupom ovisno o kontekstu

- pristup objektu ovisi o trenutnom kontekstu - u obzir uzima predikate sustava (vrijeme, lokacija …), trenutnog korisnika

Kako to implementirati?

1. definiranje virtualnih tablica koje odabiru objekt čiji sadržaj zadovoljava dani uvjet te dodjeljivanje dozvola na virtualne tablice, umjesto na temeljne tablice
2. povezivanje predikata (ili logičke kombinacije predikata) s autorizacijama
    - predikat izražava uvjet nad sadržajem objekta koji mora biti zadovoljen kako bi pristup bio dozvoljen

Zašto su virtualne tablice korisne?

➔ omogućavaju prikaz samo onih informacija koje su korisniku potrebne:
➔ zbirne informacije i/ili samo neki atributi tablice i/ili samo neke n-torke iz tablice korisniku se dodjeljuju ovlasti nad virtualnom tablicom

Pohranjene procedure/funkcije

➔ pohranjena procedura/funkcija je potprogram koji je pohranjen u rječniku podataka i koji se izvršava u kontekstu sustava za upravljanje bazama podataka
    - **procedura** je potprogram koji u pozivajući program ne vraća rezultat
    - **funkcija** je potprogram koji u pozivajući program vraća rezultat
➔ implementirane su kao SQL procedure ili kao vanjske procedure
➔ pohranjena je kao objekt u rječniku baze podataka
➔ postiže se veća produktivnost programera i smanjuje mogućnost pogreške zbog toga što se programski kôd potreban za obavljanje nekog postupka koji čini logičku cjelinu implementira i testira na samo jednom mjestu

pohranjena procedura omogućuje zaštitu podataka od neovlaštene uporabe na razini funkcija

- korisniku se pridijeli dozvola za obavljanje definirane procedure, umjesto dozvole za pristup podacima

- precizno određen način na koji korisnik smije obaviti operacije nad podacima

Mandatno upravljanje pristupom

- sigurnosna politika na razini sustava određuje tko ima pravo pristupa, a ne vlasnik objekata
- primjenjiva u sustavima u kojima se dozvole dodjeljuju ovisno o poziciji korisnika u hijerarhiji neke organizacije (vojska, državna uprava, ...)
- svaki objekt dobiva oznaku klasifikacijske razine (classification level), npr. povjerljivo, tajno, ...
- svakom korisniku dodjeljuje se oznaka razine ovlasti te tada korisnici mogu obavljati operacije nad onim objektima za koje imaju odgovarajuću razinu ovlasti

Višerazinska mandatna politika pristupa

! najčešći oblik mandatne politike pristupa

klasa pristupa se sastoji od dvije komponente:

1. sigurnosna razina – element hijerarhijski uređenog skupa, npr. TS > S > C > U (Top Secret, Secret, Confidential, Unclassified
2. skup kategorija – podskup neuređenog skupa elemenata (funkcionalna područja ili područja kompetentnosti), npr: { Nuclear, Army }

klasa pristupa c1 dominantna je klasi pristupa c2 , tj. $c1 \geq c2$ ako je

- sigurnosna razina klase pristupa c1 >= sigurnosne razine klase pristupa c2
- kategorije klase pristupa c1 uključuju one od c2

klase pristupa c1 i c2 su neusporedive ako niti $c1 \geq c2$ niti $c2 \geq c1$

>> korisnik se može prijaviti na sustav u svakoj klasi pristupa kojoj je njegova klasa pristupa dominantna

BLP model (**Bell – La Padula Security Model**)

cilj: spriječiti tijek informacije od subjekata/objekata više razine prema subjektima/objektima nižih (ili neusporedivih) razina

Načela:

simple property (no-read-up) - subjektu je dozvoljeno čitanje iz objekta samo ako je klasa pristupa subjekta dominantna klasi pristupa objekta (tj. može čitati iz onih objekata kojima je njegova klasa pristupa dominantna)

***-property (star-property, no-write-down):** subjektu je dozvoljeno pisanje u objekt samo ako je klasa pristupa objekta dominantna klasi pristupa subjekta

- nije moguće pisati u objekte koje mogu pročitati subjekti s nižom razinom - spriječeno propuštanje informacija

Zajednička primjena DAC i MAC politike

DAC i MAC politike **nisu međusobno isključive** i mogu biti primijenjene zajedno

diskrecijska politika djeluje unutar granica mandatne politike i može samo spriječiti neki pristup koji bi uz primjenu samo MAC politike bio dozvoljen

Mandatna politika pristupa u bazama podataka

- **simple property** (no-read-up)
- **strong-star-property (umjesto *-property)**: korisnik može pisati **isključivo na svojoj razini** (radi sprječavanja uništenja npr. S-podataka od strane U-korisnika)
- subjekti na različitim razinama imaju različite poglede na relaciju

Upravljanje pristupom temeljeno na ulogama

PROBLEM: svakom nastavniku treba dodijeliti dozvole posebno, ako imamo 150 nastavnika to je 150x isti proces

Osnovne postavke

1. podaci vlasništvo poduzeća
2. odluke o pristupu temeljene na ulogama korisnika kao dijela organizacije
3. Korisnici ne mogu svoje ovlasti prosljeđivati drugim korisnicima

Glavni principi:

- svaki pristup podatkovnim objektima i resursima, potreban korisniku za obavljanje njegova zadatka, obavlja se kroz uloge
- **uloga** predstavlja **poslovnu funkciju** unutar organizacije
- ovlasti nad podatkovnim objektima i resursima potrebnim za obavljanje zadatka dodijeljene su ulogama umjesto pojedinim korisnicima
- korisnik je ovlašten za obavljanje odgovarajuće uloge

Šifriranje podataka

- dodatna razina zaštite ako neovlašteni korisnik uspije doći do podataka iz baze podataka

Šifriranje se može koristiti kao **zadnji sloj obrane** radi zaštite osjetljivih i vrlo povjerljivih informacija **!!!** nije zamjena za ostale tehnike zaštite podataka, npr. za upravljanje pristupom

šifriranje/dešifriranje podataka u **prijenosu** događa se u krajnjim točkama komunikacije između klijenta i poslužitelja

- specifične mogućnosti određenog SUBP-a (npr. Oracle Advanced Security)
- Connection-based methods (npr. korištenje Secure Sockets Layer [SSL])
- Secure tunnels (npr. korištenje Secure Shell [SSH] tunela)
- mogućnosti koje podržava operacijski sustav (npr. IPSec)

prijenos šifriranih podataka temelji se na industrijskim standardima i ne ovisi o proizvođaču baze podataka - većina metoda šifrira cijeli komunikacijski tok

Pohrana šifriranih podataka

šifriranje/dešifriranje moguće je obaviti na razini:

- aplikacije
- datotečnog sustava
- sustava za upravljanje bazama podataka

podaci su neupotrebljivi dok se ne dešifriraju

- SUBP ne može obaviti učinkovita uspoređivanja vrijednosti i temeljne operacije nad šifratima

Nedostaci:

- neizbježan pad performanci, ovisno o opsegu šifriranja i korištenim algoritmima
- šifrirani podaci zauzimaju više prostora od originalnog teksta

Zbog toga treba:

- šifrirati selektivno - samo iznimno osjetljive informacije
- ne šifrirati atribute koji se koriste kao ključevi ili indeksi

Upravljanje ključevima za šifriranje

kompromitirani ključevi - mogućnost otkrivanja informacije

izgubljeni ključevi - gubitak informacija

pohrana ključeva

- u bazi podataka, u operacijskom sustavu
- alati koji nude cjelovita rješenja vezana uz upravljanje ključem
- korisnici upravljaju vlastitim ključevima za šifriranje
- korištenje transparentnog šifriranja baze podataka

Transparentno šifriranje podataka

šifriranje/dešifriranje podataka obavlja SUBP prilikom pohrane/dohvata podatka

➔ nije potrebno koristiti posebne funkcije
➔ transparentno za korisnike baze podataka
➔ nije potrebna izmjena aplikacija radi rukovanja šifriranim podacima
➔ poslovi upravljanja ključem su automatizirani

Praćenje rada korisnika

- prijava/odjava za rad s bazom podataka
- neuspjeli pokušaji prijave
- obavljanje DDL naredbi
- pogreške koje dojavljuje sustav za upravljanje bazama podataka
- promjene definicija pohranjenih procedura i okidača
- promjene podataka o korisnicima, njihovim dozvolama i ostalih sigurnosnih atributa
- promjene osjetljivih podataka
- dohvat osjetljivih podataka
- izmjene definicija snimanja traga i snimljenih podataka

! evidentirati svaki pristup osjetljivim podacima u posebnoj datoteci za praćenje radakorisnika (Audit Trail)

tipičan zapis datoteke sadrži sljedeće informacije (*ispitno pitanje):

- SQL naredba koja se izvršava (statement source)
- mjesto s kojeg je upućen zahtjev (terminal, IP adresa računala)
- identifikator korisnika koji je pokrenuo operaciju
- datum i vrijeme operacije
- n-torke, atributi na koje se zahtjev odnosi
- stara vrijednost n-torke
- nova vrijednost n-torke

Selektivno praćenje

➔ nužnost selektivnog praćenja DML aktivnosti zbog mogućnosti stvaranja goleme količine podataka - praćenje aktivnosti na podskupu tablica baze podataka

Implementacija praćenja rada korisnika

1. **mehanizmi sustava za upravljanje baze podataka**

- okidači - implementacija vlastitih rješenja praćenja rada korisnika
- proširenja funkcionalnosti: DB2 - praćenje tragova; SQL Server - trace functions; Sybase- native auditing

2. **vanjski sustavi za praćenje rada korisnika**

- Imperva - Database Activity Monitoring
- DAS-DBAuditor: Database Auditor
- Ambeo - Activity Tracker, Usage Tracker, NetServer

3. **usporedba shema**

- periodičko prikupljanje sheme (obično jednom dnevno) i usporedba s prethodnom shemom (diff)

Zaštita i privatnost podataka -> Opća uredba o zaštiti podataka EU - 25.5.2018.

- Uredbom se utvrđuju pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka.

Opća uredba o zaštiti podataka EU - obaveze:

- Klijent mora moći dati izričit pristanak na korištenje svojih podataka,
- Mora moći biti obaviješten kada, u kojem obliku (izvorno, anonimizirani, ili pseudo-anonimizirani) i od strane koga se koriste njegovi podaci, za koju namjenu, i koliko dugo će biti pohranjeni;
- Omogućiti klijentima uvid u njihove osobne podatke i omogućiti ispravak nepravilnosti;
- Jamčiti da nema prijenosa podataka u zemlji izvan EU-a koji ima nedovoljnu zaštitu podataka;
- Ispuniti "pravo na zaborav" – obrisati osobne podatke klijenta na njegov zahtjev, ako su ispunjeni propisani uvjeti.