Bazy Danych

Andrzej M. Borzyszkowski
Instytut Informatyki

Uniwersytetu Gdańskiego

materiały dostępne elektronicznie
http://inf.ug.edu.pl/~amb

Bezpieczeństwo w bazach danych

© Andrzej M. Borzyszkowski
Bazy Danych

Zagrożenia i przeciwdziałanie zagrożeniom

- Rodzaje zagrożeń
  - utrata spójności danych
    - spowodowana przypadkiem lub celowo (złośliwie)
    - prowadzi do błędów i nadużyć
  - utrata dostępu do danych
  - utrata poufności
- Rozwiązania
  - zarządzanie dostępem do bazy danych (*access control*)
  - zarządzanie wnioskowaniem (*inference control*)
  - zarządzanie przepływem danych (*flow control*)
  - szyfrowanie

© Andrzej M. Borzyszkowski
Bazy Danych

Zarządzanie dostępem

- Użytkownicy/konta
  - klasy użytkowników z różnymi uprawnieniami
- Uprawnienia
  - uznaniowe (*discretionary*)
    - możliwość zmiany przez użytkownika
  - stałe (*mandatory*)
    - związane na stałe z kontem
- Administrator bazy danych
  - tworzy/usuwa użytkowników
  - zarządza uprawnieniami
  - analizuje pliki log

© Andrzej M. Borzyszkowski
Bazy Danych

Użytkownicy

- NIE są to użytkownicy systemu operacyjnego
  - użytkownik s.o. może utworzyć wielu różnych użytkowników bazy danych
  - użytkownik bazy danych może mieć dostęp jedynie zdalny i w ogóle nie być użytkownikiem s.o. w którym działa baza
  - użytkownikiem może być program korzystający z bazy danych (serwer aplikacji w architekturze trójwarstwowej)
- polecenia SQL:
  - CREATE USER “nowy” WITH PASSWORD '...' NOCREATEDB NOCREATEUSER VALID UNTIL '2999-9-9'
  - DROP USER stary (tylko jeśli nie jest właścicielem bazy)
  - ALTER USER inny .....
  - PostgreSQL: istnieją wersje poleceń dostępne z powłoki uniksa: createuser, dropuser

Uwierzytelnianie

- Sposoby uwierzytelniania
  - brak (zakładamy, że kto ma w ogóle dostęp jest uprawniony)
  - hasło (różne sposoby przechowywania hasła na serwerze)
  - system Kerberos
  - uwierzytelnienie przez serwer na którym działa i użytkownik i serwer bazodanowy
  - certyfikaty X.509
  - inne sposoby

Uprawnienia uznaniowe

- Poziom uprawnień
  - uprawnienia dla użytkownika w bazie danych
  - uprawnienia związane z tabelą
- Uprawnienia dla użytkownika
  - prawo tworzenia/usuwania innych użytkowników
  - prawo tworzenia/usuwania baz, tabel i perspektyw
  - ogólne prawo do modyfikacji i czytania tabel
- Uprawnienia dla tabel
  - rodzaje: SELECT, INSERT, DELETE, UPDATE, RULE, TRIGGER
  - mogą być podane na poziomie poszczególnych atrybutów (ale nie w PostgreSQL, trzeba używać perspektyw)
  - pojęcie właściciela tabeli (głównie twórca tabeli)
  - macierz dostępu: użytkownik X ma prawo Z do tabeli/atrybutu Y

Propagowanie uprawnień

- GRANT SELECT ON moja_tabela TO PUBLIC
  - GRANT UPDATE ON moja_tabela(atrybut) TO moj_kolega
  - GRANT INSERT ON moja_tabela TO moj_kolega WITH GRANT OPTION
  - odbiorca uprawnienia może być upoważniony do dalszego udzielania uprawnień
- REVOKE ALL ON moja_tabela FROM ten_obcy CASCADE
  - odbiera uprawnienia również udzielone dalej
  - użytkownik może mieć uprawnienia z kilku źródeł
- Ograniczenia propagowania
  - nie są częścią standardu SQL
  - ograniczenia liczby udzielonych uprawnień
  - ograniczenia głębokości udzielonych uprawnień

Perspektywy (widoki, *view*) – dlaczego?

- Wygoda użytkownika, zapamiętanie częstych zapytań
- Perspektywa jest tworzona na podstawie innych tabel/perspektyw
  - może zawierać atrybuty pochodne: obliczane/ zagregowane (tabela zawiera atrybut daty urodzenia, perspektywa zawiera również/zamiast bieżący wiek, albo wynik skomplikowanych obliczeń: suma zamówień klienta)
  - może zawierać tylko wybrane wiersze (obcięcie)
  - albo tylko wybrane atrybuty (rzut)
- Podział na danych na różne tabele w celu ułatwienia współbieżności:
  - osobne tabele dla towarów i dla ich stanu magazynowego, perspektywa łączy jakby była to jedna tabela

Perspektywy w zarządzaniu dostępem

- Uprawnienia do czytania
  - ograniczają dostęp do oryginalnych danych
  - np. wszyscy użytkownicy mogą czytać nazwiska z tabeli pracowników
  - a tylko wybrani ich płace
  - podział tabeli, osobna tabela z płacami, perspektywa łącząca tabele pozwalająca operować jak na jednej tabeli
  - perspektywa może też mieć ograniczenia na wiersze

Perspektywy, operacje

- PostgreSQL do wersji 9.2 nie przewidywał operacji dla perspektyw
  - od wersji 9.3 dla szczególnie prostych perspektyw można używać operacje **INSERT**, **DELETE i UPDATE**
  - od wersji 9.4 dostępne są szersze możliwości operowania na perspektywach
  - dla perspektyw łączących tabele nadal konieczne są procedury wyzwalane do obsługi modyfikacji perspektyw

Zarządzanie dostępem w oparciu o role

- Przydział uprawnień może nastąpić w dwu krokach
  - utworzenie roli (CREATE ROLE) oraz przydział uprawnień do roli
  - przydział roli do użytkownika (wszystkie zasady uwierzytelniania pozostają w mocy)
  - użytkownik może zmieniać rolę w trakcie sesji (SET ROLE ...)
  - użytkownik może występować w wielu rolach w trakcje jednej sesji

Zarządzanie dostępem w oparciu o role

- Przykłady zastosowań
  - jednoczesne udzielenie/odwołanie uprawnień grupie użytkowników
  - uprawnienia o ograniczonym czasie
  - jeśli prawo udzielania uprawnień należy do roli, to każdy z członków może je wykonywać
  - np. jeden z administratorów nadał komuś uprawnienie, a inny odebrał

Dane statystyczne

- Zezwolenie na ujawnianie danych zbiorczych (funkcje agregujące)
  - problem wielkości populacji

    SELECT avg(pensja) FROM personel WHERE .....
  - warunek, że wielkość populacji przekracza próg
  - ale nadal różnica dwóch populacji może być bardzo mała
  - inne rozwiązanie: celowe fałszowanie odpowiedzi
    - w połączeniu z dużą populacją wniosek indywidualny jest bezwartościowy
    - ale nie wolno wielokrotnie udzielać odpowiedzi

Szyfrowanie

- Zajmuje się tym system operacyjny, serwer bazodanowy działa jakby szyfrowania nie było
- Szyfrowanie dysku, na którym przechowywane są dane
  - wówczas dane przesyłane po sieci nie są szyfrowane
  - chyba, że niezależnie dbamy o szyfrowanie komunikacji
- Szyfrowanie na poziomie serwera bazodanowego
  - dane w pamięci operacyjnej nie są zaszyfrowane
- Szyfrowanie na poziomie aplikacji
  - wówczas wyłącznie aplikacja ma dostęp do oryginalnych danych
  - można szyfrować wybrane atrybuty