Bezpieczeństwo Systemów Komputerowych

Projekt nr 2

Implementacja mechanizmów kontroli dostępu do baz danych

Wersja 1.0, Gdańsk, 2018

Wymagania stawiane studentom:

- umiejętność uruchamiania programów w środowisku Windows / Unix-Linux,
- umiejętność programowania w języku C / C++ / C#,
- umiejętność zaprojektowania i wykonania graficznego interfejsu użytkownika,
- podstawowa znajomość systemów zarządzania bazami danych MySQL, Postgress, MS-SQL, Oracle, DB2 Informix

Główne zadania projektowe:

- analiza wymagań postawionych przez prowadzącego zajęcia,
- projekt struktury bazy danych,
- projekt interfejsu użytkownika,
- wybór techniki zarządzania użytkownikami i uprawnieniami,
- implementacja aplikacji i testy,
- przygotowanie raportu końcowego.

1. Cel zajęć projektowych i zasady oceniania

Główny celem niniejszego projektu jest utrwalenie przez studenta wiedzy związanej z zagadnieniami tworzenia aplikacji baz danych – począwszy od pomysłu bazy danych, poprzez jej model do implementacji w SZBD w postaci kodu SQL aż do implementacji interfejsu oraz typowych manipulacji na danych.

Wykonany projekt zostanie oceniony według następujących zasad:

- Poprawna i terminowa realizacja zadań projektowych – 12 pkt.
- Funkcjonalność interfejsu użytkownika – 2,5 pkt.
- Dokumentacja techniczna – 2,5 pkt.
- Przedstawienie projektu interfejsu użytkownika – 1,5 pkt. (I termin kontrolny)
- Przedstawienie częściowo działającej aplikacji – 1,5 pkt. (II termin kontrolny)

Terminy kontrolne oraz termin zaliczenia projektu zostaną ogłoszone na wykładzie.

W przypadku oddania projektu po wyznaczonym końcowym terminie zaliczenia uzyskana ocena będzie pomniejszana o 10 pkt.

Termin ostatecznego zaliczenia wyznaczono na dzień 22.06.2018. Po tym terminie jedynie kompletne projekty będą oceniane na 1 pkt z wyjątkiem usprawiedliwionych sytuacji szczególnych (zwolnienia lekarskie, przypadki losowe).

2. Zadania do wykonania

Głównym zadaniem jest zaprojektowanie i implementacja w wytworzonej bazie danych wybranego modelu autoryzacji i kontroli dostępu według następujących reguł:

- dowolna technologia wykonania, ale ograniczona możliwościami dostępnego DBMS,
- baza danych powinna być prosta – kilka, najwyżej kilkanaście relacji, np. wypożyczalnia płyt DVD, gabinet lekarski, ogłoszenia, członkowie stowarzyszeń, itp,
- powinna być zaimplementowana pełna funkcjonalność modelu kontroli dostępu z uwzględnieniem podstawowych operacji SQL na obiektach (tablicach),
- dostęp do bazy danych powinien być zasadniczo zrealizowany przez przeglądarkę i tunel SSL. Dopuszczalne są także dedykowane aplikacje klienckie
- w przypadku modelu DAC z delegacją uprawnień należy kontrolować (eliminować) obecność cykli w grafie delegacji uprawnień, a także eliminować możliwość nadawania tego samego uprawnienia do tego samego obiektu przez więcej jak jednego dawcę. Ponadto dla uprawnienia *przejmij* należy przyjąć, że posiadane dotychczas uprawnienia przejmującego zostają skasowane i zastąpione uprawnieniami przejętymi od dawcy, natomiast dawca jest pozbawiany absolutnie wszystkich posiadanych uprawnień - nawet gdy przekazuje tylko jedno przejmującemu,
- w przypadku modelu MAC (Jajodia-Sadhu) należy pamiętać o zasadach kontroli przepływu danych (zasada: no-read-up, no-write-down),
- w przypadku modelu RBAC należy uwzględnić statyczną separację ról podczas pracy, tzn. w czasie trwania sesji można pełnić tylko jedną rolę (posiadając ich wiele), pomimo otwarcia np. wielu połączeń z bazą danych i z użyciem różnych przeglądarek.

Projektowanie aplikacji relacyjnej bazy danych wygodnie jest podzielić na cztery podstawowe etapy:

- zdefiniowanie problemu – w tym miejscu należy zebrać możliwe jak najwięcej informacji na temat bazy danych, którą chcemy zaprojektować. Jeśli to jest wymagane, należy zgromadzić wymagania na warunki pracy aplikacji oraz

założenia jej towarzyszące. W ramach projektu każda grupa studentów będzie miała odrębny problem do analizy i opracowania,

- zamodelowanie rozwiązania problemu przy użyciu diagramów związków encji. Wynikiem działania powinien być diagram uwzględniający wszystkie relacje w bazie danych oraz powiązania pomiędzy nimi. Do tego celu należy wykorzystać narzędzia graficzne do zobrazowania wyników pracy analitycznej. Na tym etapie należy podjąć równolegle prace nad postacią interfejsu użytkownika,
- opracowanie diagramu relacyjnego, wygenerowanie kodu zakładającego poszczególne tabele, wprowadzenie danych inicjalnych (zapełnienie bazy danych) w dość dużej ilości, ocena spójności; rejestracja użytkowników z różnymi uprawnieniami,
- ostatnim etapem tworzenia aplikacji bazy danych jest zaprojektowanie i skonstruowanie ewentualnych (niekoniecznie) zapytań biznesowych i manipulacji na danych, a następnie przeprowadzenie testów aplikacji z uwzględnieniem kontroli poprawności z punktu widzenia posiadanych przez użytkownika uprawnień.

Przykładowa baza danych może zostać zaprojektowana dla magazynu produkcyjnego (bez określenia branży). Wydania magazynowego dokonuje się pracownikowi tejże firmy. Jedno wydanie może się składać z wielu pozycji, każda z nich ma przypisaną grupę produktową i ilość lub liczbę sztuk danego asortymentu. W analogiczny sposób wygląda zapełnienie magazynu. W tym przypadku wpisu na stan magazynu dokonuje jeden z magazynierów.

Wybór metody kontroli dostępu jest narzucony warunkami projektu. Grupa projektowa powinna zaimplementować pełną funkcjonalność tego modelu.