BEZPIECZEŃSTWO BAZ DANYCH

I. Podstawowe informacje

Termin bezpieczeństwo bazy danych odnosi się
do zabezpieczenia bazy danych przed zagrożeniem ,
zarówno celowym, jak i przypadkowym.

Należy przeciwdziałać takim zagrożeniom jak:

- kradzież , defraudacja, zniszczenie danych;
- utrata poufności (tajności);
- utrata prywatności; utrata prywatności;
- brak integralności;
- uniemożliwienie dostępu.

Przeciwdziałanie zagrożeniom polega na:

- zabezpieczeniu SZBD (Systemu zarządzania bazą danych)
- zabezpieczeniu całej bazy danych,
- zabezpieczeniu środowiska bazy
- zabezpieczeniu sprzętu,
- zabezpieczeniu oprogramowania,
- ograniczeniu dostępu niepowołanym osobom,

II. Stosowane metody zabezpieczeń

1) Zabezpieczenia systemowe (System Security Policy)
2) Zabezpieczenie danych (Data Security Policy)
3) Zarządzanie użytkownikami (User Security Policy)
4) Zarządzanie hasłami (Password Management Policy)
5) Monitorowanie systemu (Auditing Policy)

1. **Zabezpieczenia systemowe** (System Security Policy)

a) dostęp do bazy
b) perspektywy
c) kopiowanie i odtwarzanie
d) więzy integralności
e) szyfrowanie
f) technologia RAID

a) dostęp do bazy

uwierzytelnianie (autentykacja, identyfikacja) - proces polegający na zweryfikowaniu zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych

Metody uwierzytelniania:

- fizyczne metody – na przykład tokeny, karty magnetyczne lub metody biometryczne
- procedury użytkownika
- podanie nazwy użytkownika i hasła użytkownika
- pytania i odpowiedzi
- uwierzytelnianie tożsamości komputera
- procedura przywitania - wykonanie przez użytkownika poprawnie jakiegoś algorytmu. Metoda ta ma wyższy stopień bezpieczeństwa, brak jej jawności ale jest czasochłonna i żmudna dla użytkownik

Uwierzytelnianie może być dokonane w wielu warstwach, na przykład uwierzytelnianie przez SZBD, system operacyjny, usługę sieciową. Uwierzytelnianie na kilku poziomach jednocześnie podnosi bezpieczeństwo wymiany danych.

autoryzacja - kontrola dostępu do zasobu, upoważnienie do korzystania z zasobu

Uprawnienia SQL nadawane są na dwóch poziomach:
- poziom użytkownika (schematu)
- poziom relacji (obiektu)

Uprawnienia dla SQL i Oracla znajdują się w rozdziale III.

b) perspektywy

Perspektywa (widok) to logiczna struktura, wirtualna tabela wyliczana w locie, określona przez zapytanie SQL, umożliwia dostęp do podzbioru kolumn i wierszy tabeli lub tabel. Przy pobieraniu wyników do perspektywy odwołujemy się identycznie jak do tabeli. Operacje wstawiania, modyfikowania oraz usuwania rekordów nie zawsze są możliwe a w przypadku niektórych SZBD perspektywa służy tylko i wyłącznie do pobierania wyników i ograniczania dostępu do danych.

c) kopiowanie i odtwarzanie

Kopiowanie narażonych danych zabezpiecza je skutecznie przed utratą. Wadą jest jednak dodatkowe użycie zasobów na kopiowanie, przechowywanie i odtwarzanie danych

- Każda transakcja zatwierdzona przed wystąpieniem awarii nie może być utracona
- Każda transakcja niezatwierdzona przed wystąpieniem awarii musi być wycofana

Struktury wykorzystywane do odtwarzania bazy danych
- Dziennik powtórzeń
- Segmenty wycofania
- Pliki kontrolne
- Kopie bezpieczeństwa danych

d) więzy integralności

Więzy integralności są warunkami, które powinny być spełnione przez określony podzbiór danych z bazy. Spełnienie tych warunków świadczy o tym, że baza danych jest w stanie spójnym. Istnieją dwa sposoby sprawdzania reguł integralnościowych:
- deklaratywne - dotyczą wszystkich operacji, wszystkich wierszy (statyczne), wykonywane przez DBMS, na przykład NOT NULL, PRIMARY KEY
- proceduralne - dotyczą tylko zmienianych danych (dynamiczne), są to procedury wykonywane przez DBMS lub przez aplikację (dotyczą wtedy tylko operacji tej aplikacji)

Więzy integralności (większość z nich definiuje się w instrukcjach CREATE oraz ALTER TABLE języka SQL):
- **Integralność encji** (entity integrity): odnosi się do pojedynczej tabeli, w której powinien istnieć klucz pierwotny. Jeżeli danej kolumnie nałożyliśmy warunek PRIMARY KEY, DBMS automatycznie nałoży jej warunki NOT NULL i UNIQUE.
- **Integralność krotki**: zakłada się, że każda krotka opisuje jeden obiekt świata rzeczywistego a wartość krotki powinna odpowiadać elementowi świata rzeczywistego. Na wartości przyjmowane przez krotki można nałożyć niezależne więzy, które muszą być spełnione przez wszystkie krotki niezależnie. Więzy te to:
  - zawężenie dziedziny atrybutu poprzez podanie przedziału wartości, listy możliwych wartości (np. płeć VARCHAR(1) NOT NULL CHECK (płeć IN ('M','F')))

- podanie zależności pomiędzy wartościami różnych atrybutów w krotce,
- podanie formatu wartości (imię VARCHAR(20))
- zadeklarowanie konieczności występowania jakiejś wartości (NOT NULL)
- zdefiniowanie niepowtarzalnych wartości atrybutu (UNIQUE)

- **Więzy wewnętrzne relacji**: sprawdzane są wartości występujących w krotkach w ramach tej samej relacji
- **Więzy zbioru krotek**: sprawdzane są wartości atrybutów w różnych relacjach

e) szyfrowanie

Podstawowe pojęcia i oznaczenia :

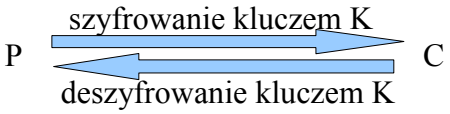
- Tekst jawny [ozn.: P]
- Tekst zaszyfrowany [ozn.: C]
- Klucz [ozn.: K]
- Klucz jawny (publiczny)
- Klucz prywatny
- Kryptogram (Tekst zaszyfrowany) [ozn.: EK(P)]
- Tekst jawny uzyskany z kryptogramu [ozn.: DK(C)]

Metody szyfrowania :

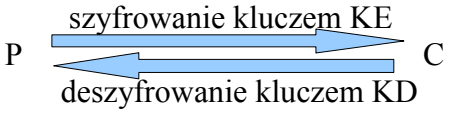
- podstawieniowa – szyfrowanie opiera się na podstawianiu pod znaki alfabetu jawnego znaków alfabetu szyfrowego.
- przestawieniowa - w zaszyfrowanym tekście występują wszystkie znaki z tekstu jawnego, ale w innej kolejności

Rodzaje szyfrowania :

- **blokowe** – tekst jawny dzielony jest na bloki określonej długości, po czym bloki są szyfrowane niezależnie
- **strumieniowe** - szyfr symetryczny, który koduje generując potencjalnie nieskończony strumień szyfrujący (keystream) i XOR-ując go z wiadomością. Odszyfrowywanie zakodowanej wiadomości odbywa się w identyczny sposób – generujemy strumień szyfrujący i XOR-ujemy go z szyfrogramem
- **symetryczne** – szyfrowanie i odszyfrowanie odbywa się za pomocą tego samego klucza



- **asymetryczne** - występują 2 klucze – klucz publiczny służący do szyfrowania, oraz klucz prywatny służący do deszyfrowania. Ponieważ nie ma potrzeby rozpowszechniania klucza prywatnego, bardzo małe są szanse, że wpadnie on w niepowołane ręce. Opierają się na trudnościach w rozwiązywaniu niektórych problemów matematycznych na współczesnych komputerach



- **Kaskadowe** tzn. szyfrowanie danych po kolei kilkoma algorytmami

Wybrane zastosowania szyfrowania

- Ochrona danych przed niepowołanym odczytem
  - szyfrowanie danych na nośnikach
  - zabezpieczenie komunikacji
- Uwierzytelnianie dokumentów (podpis elektroniczny)
- Ochrona prywatności poczty elektronicznej
- Elektroniczny notariusz (certyfikaty)

Wybrane algorytmy szyfrujące

- **DES** (Data Encryption Standard) - symetryczny szyfr blokowy
- **Triple-DES** – polega na zaszyfrowaniu wiadomości algorytmem DES trzy razy
- **RC4** – symetryczny szyfr strumieniowy używany między innymi w SSL oraz WEP
- **RSA** (Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman) – algorytm z kluczem publicznym
- **ElGamal** – jeden z najważniejszych algorytmów kryptografii asymetrycznej obok RSA
- **AES** (Advanced Encryption Standard) - symetryczny szyfr blokowy znany też pod nazwą Rijndael. Opracowany z powodu niewystarczającej siły algorytmu DES

f) technologia RAID

RAID (Redundant Array of Independent Disks) – rozwiązanie pozwalające łączyć ze sobą dyski celem stworzenia pamięci masowej o dużej pojemności, szybkości i niezawodności. Macierze RAID posiadają kilka odmian różniących się funkcjonalnością. Dobranie odpowiedniego poziomu ma kluczowe znaczenie dla wydajności, bezpieczeństwa i kosztów.

Poziom RAID	Min. liczba dysków	Dostępna przestrzeń	Max. ilość dysków, które mogą ulec awarii bez utraty danych
RAID 0	2	N	0
RAID 1	2	1	N-1
RAID 2	3	N-logN	1
RAID 3	3	N-1	1
RAID 4	3	N-1	1
RAID 5	3	N-1	1
RAID 6	4	N-2	2
RAID 1+0	4+N*2	N/2	1
RAID 0+1	4+N*2	Pojemność pojedynczej części RAID 0	1

Technologia umożliwia:

- zwiększenie niezawodności (odporność na awarie)
- przyspieszenie transmisji danych
- powiększenie przestrzeni dostępnej jako jedna całość

2. Zabezpieczenie danych (Data Security Policy) – bezpieczeństwo danych w sieci www

Przesyłanie informacji gwarantujące:

- tajność – uniemożliwienie dostępu do informacji niepowołanym osobom
- spójność – ochrona informacji przed usunięciem lub jakimikolwiek nieuprawnionymi zmianami
- uwierzytelnianie – zweryfikowanie zadeklarowanej tożsamości osoby
- wysłanie do rzeczywistego odbiorcy
- niekwestionowalność – niepodważalność faktu wysłania wiadomości i jego nadawcy
- przeciwdziałanie ewent. szkodom jeśli informacja zawiera kod wykonywalny

Metody zabezpieczenia transmisji danych:

- Serwery zastępcze (Proxy)
- Zapory (Firewalls)
- Streszczanie komunikatu
- Podpisy cyfrowe
- Certyfikaty cyfrowe
- Protokoły zabezpieczające komunikację (Kerberos)
- Protokoły szyfrowania (SSL, S-HTTP)

III. Bezpieczeństwo danych w SQL i systemach Oracle

1) SQL : Przydzielanie uprawnień obiektowych

- **przydzielenie wszystkich uprawnień dla wybranej tabeli wybranym użytkownikom**

  GRANT ALL [PRIVILEGES] ON Tabela
  TO user1, user2, ... [WITH GRANT OPTION] ;

  np.
  GRANT ALL PRIVILEGES ON Zamówienia
  TO Księgowy WITH GRANT OPTION;

  WITH GRANT OPTION – oznacza że odtąd użytkownik będzie mógł samemu przydzielać uprawnienia

- **przydzielenie wszystkich uprawnień dla wybranej tabeli wszystkim użytkownikom**

  GRANT ALL [PRIVILEGES] ON Tabela TO PUBLIC ;

  np.
  GRANT ALL PRIVILEGES ON Książki TO PUBLIC ;

- **przydzielenie wybranych uprawnień dla wybranej tabeli wybranym użytkownikom**

  GRANT [SELECT] [INSERT] [DELETE] [UPDATE [(Lista kolumn)]]
  ON Tabela TO ....

  np.
  GRANT SELECT, UPDATE (Cena, NumerDost) ON Książki
  TO Maria, Marek, Jan;

2) SQL: Odbieranie uprawnień

- **odbieranie wybranych uprawnień dla wybranej tabeli wybranym użytkownikom**
  REVOKE [SELECT] [INSERT] [DELETE] [UPDATE [(Lista kolumn)]]
  ON Tabela FROM user1, user2, ... ;

  np.
  REVOKE SELECT ON Zamówienia FROM Księgowy CASCADE ;

- **odbieranie wszystkich uprawnień dla wybranej tabeli wybranym użytkownikom**
  REVOKE ALL [PRIVILEGES] ON Tabela
  FROM user1, user2, ... ;

  np.
  REVOKE ALL ON Dostawcy
  FROM Jan, Maria ;

3) Oracle

- dostęp do bazy np.: przez podanie nazwy użytkownika i hasła
- 2 rodzaje uprawnień :
  - systemowe
  - obiektowe
- nadawanie uprawnień bezpośrednio lub przez role
- **Oracle roles** – są to nazwane grupy użytkowników. Przykład:

```
CREATE ROLE księgowy
IDENTIFIED BY lubieliczby;
```

Po utworzeniu roli, należy dodać prawa do tej roli używając komendy GRANT:

```
GRANT SELECT, INSERT, UPDATE
ON finanse
TO księgowy;
```

4) Uprawnienia systemowe Oracle

Uprawnienia systemowe – prawa wykonania określonej akcji lub wykonania określonej operacji na wskazanym typie obiektu we wskazanym/dowolnym schemacie bazy danych, na przykład:

- CREATE SESSION – zezwala użytkownikowi na przyłączenie się do bazy danych
- CREATE TABLE – zezwala użytkownikowi na tworzenie relacji w jego własnym schemacie
- SELECT ANY TABLE
- INSERT ANY TABLE
- DROP ANY VIEW

nadawanie uprawnień systemowych:

```
GRANT <lista_uprawnień_systemowych>
TO <lista_użytkowników> | PUBLIC
[WITH ADMIN OPTION];
```

np.

```
GRANT CREATE SESSION, SELECT ANY TABLE TO student;
```

odbieranie uprawnień systemowych:

```
REVOKE <lista_przywilejów>
FROM <lista_użytkowników> | PUBLIC;
```

np.

```
REVOKE SELECT ANY TABLE FROM student ;
```

5) Uprawnienia obiektowe Oracle

Uprawnienia obiektowe zezwalają użytkownikowi na wykonanie określonych operacji na konkretnym obiekcie bazy danych, na przykład SELECT, INSERT, DELETE

- **nadawanie uprawnień obiektowych**

```
GRANT ALL [ PRIVILEGES ] | uprawnienie [ , uprawnienie, ... ]
ON obiekt
TO PUBLIC | rola [ , rola, ... ] | użytkownik [ , użytkownik, ... ]
[ WITH GRANT OPTION ];
```