16. Сигурност

Лекционен курс “Бази от данни”

Под сигурност разбираме защита на данните срещу неоторизирано:

- Търсене
- Промяна
- Изтриване

Сигурността включва осигуряване на потребителите да извършат позволените операции с БД.

Общи бележки

Съществуват различни аспекти на проблема със сигурността:

- Правни, социални и етични;
- Физически контрол – различни видове физически защити;
- Организационни проблеми – кой има право на достъп?
- Операционни проблеми – как да се запази в тайна схемата на използване на пароли?
- Хардуерен контрол;
- Сигурност на операционната система;
- Специфични въпроси на сигурността, засягащи самата СУБД.

Модерните СУБД обикновено поддържат два подхода за сигурност на данните:

- Discretionary (предоставяне на изрични права) – потребителите имат различни права за достъп до различните обекти или до един и същ обект;
- Mandatory (задължителен):
  - На всеки обект от данни е зададено определено класификационно ниво;
  - На всеки потребител е дадено някакво ниво за получаване на контролирана информация (clearance);
  - Достъпът до обектите се разрешава в зависимост от степента на двете нива.

Независимо от избраната схема всички решения на следните проблеми:

- Какви права за достъп?
- До кои обекти?
- На кои потребители?

са от организационен характер, а не от технически.

Като такива те са извън юристдикцията на СУБД – единственото, което може да направи СУБД, е да ги прилага.

От тези разсъждения следва следната схема за работа:

- Резултатите от организационните решения:
  - Трябва да станат познати на системата – в термините на подходящ език за дефиниции;
  - Трябва да бъдат запомнени от системата – в каталога на БД под формата на правила за сигурност (security rules), наричат се също така авторизираща подсистема (authorization subsystem).

- Трябва да съществуват средства за контролиране на достъпа според правилата за сигурност;
- За да може системата да реши кои правила за сигурност за коя заявка са приложими тя трябва да може да разпознава източника на заявката - това се постига чрез:
  - Потребителски идентификатори (user IDs) – за да кажат кои са (потребителите могат също така да се групират);
  - Пароли (passwords) – за контрол дали наистина са те.

Discretionary контрол за достъп

Това е по-често използваният вид контрол.

Понеже е необходим някакъв език за дефиниции – ще използваме мета-език (хипотетичен език).

```
CREATE SECURITY RULE SR3
        GRANT RETRIEVE (F#, NAME, YEAR),
                DELETE
        ON      ST  WHERE ST.YEAR = 'Inf-III'
        TO      Ivan, Georgi, Maria
        ON ATTEMPTED VIOLATION REJECT ;
```

Правилата за сигурност трябва да имат следните компоненти:

- Име (SR3) – под това име се регистрира в каталога на СУБД;
- Една или повече привилегии (privileges):
  - Специфицират се посредством GRANT клаузата;
  - За примера правата са за търсене и извличане (RETRIEVE) на посочените атрибути и изтриване (DELETE).

- Област (scope), за която може да се приложи правилото:
  - Специфицира се посредством ON клаузата;
  - В случая за Inf-III.
- За кои потребители:
  - User Ids - в примера Ivan, Georgi, Maria.
- Казва на системата какво да прави ако се направи опит за нарушаване на правилото:
  - В случая се отхвърля заявката.

Правилата могат да бъдат изтривани от каталога на СУБД:

DESTROY SECURITY RULE SR3

Mandatory контрол за достъп

Този вид контрол се прилага обикновено за БД, където данните имат предимно статична и твърда класификационна структура – напр., военни и държавни БД.

Както казахме – поддържат се две нива за достъп:
- Класификационно ниво;
- Ниво за получаване на контролирана информация.

Основни правила за функциониране на този контрол:
- Потребител X може да види обект Y само ако нивото за получаване на информация на X е по-голямо или равно на класификационното ниво на Y;
- Потребител X може да модифицира обект Y само ако нивото за получаване на информация на X е равно на класификационното ниво на Y.

Към тези правила се разработват различни класификационни схеми за различните групи потребители.

Напр., за Пентагона съществуват:
- Оранжева книга (Orange Book)
- Бледо-лилавата книга (Lavender Book)

Кодиране на данни

Досега предполагахме, че няма да се нарушават нормалните средства за достъп до БД.
Въпреки всичко, съществуват възможности за неправомерен достъп до БД.

Една възможност за справяне с този проблем – кодиране на съществените и важните данни.

Понятия:

- Обикновен текст (plaintext) – оригиналните данни;
- Кодират се посредством кодиращ алгоритъм;
- С помощта на кодиращ ключ;
- Резултат – шифрован текст (cipheredtext).