第4章 数据库安全性

> 计科2201zzy友情分享😎😋

概述

- 数据库的安全性：是指保护数据库以防止不合法使用所造成的数据泄露、更改和破坏。
- 评估信息产品安全性的安全标准
  - 可信计算机系统评估准则(TCSEC标准)
  - 通用准则(Common Criteria,CC)

数据库安全性控制

- 数据库安全性主要包括用户身份鉴别、多层存取控制、审计、视图和数据加密等安全技术。 *（容易考简答题）*

用户身份鉴别

- 用户身份鉴别是数据库管理系统提供的最外层安全保护措施
- 由系统提供一定的方式让用户表示自己的名字或身份。每次用户要求进入系统时由系统进行核对，通过鉴定后才提供使用权限。
- 每个用户都有一个用户标识，用户标识由用户名(user name)和用户标识号(UID)两部分组成。

多层存取控制

存取控制的概念

- 存取控制
  - 存取控制机制主要包括定义用户权限和合法权限检查两部分
    - 定义用户权限
      - 权限指用户对某一数据对象的操作权力。
      - 这一功能确保用户能在规定的范围内形式权限。
      - 用户权限可以由适当的语言来定义，存储在数据字典中，被称作安全规则或授权规则。
    - 合法权限检查
      - DBMS根据安全规则进行合法权限检查，若用户的操作请求超出了定义的权限，则拒绝执行。
  - 定义用户权限和合法权限检查机制一起组成了数据库管理系统的存取控制子系统。
  - C2级别的DBMS支持自主存取控制(DAC)，B1级别的DBMS支持强制存取控制(MAC)

- 自主存取控制方法
  - 概念：
    - 用户对于不同的数据库对象有不同的存取权限，不同的用户对同一对象也有不同的权限
    - 用户可以将其拥有的存取权限转授给其他用户，相对更灵活
  - SQL标准中主要通过 `GRANT` 和 `REVOKE` 语句来实现，详见下方“授权”。
- 强制存取控制方法
  - 概念：
    - 每一个数据库对象被标以一定的密级，每一个用户也被授予某一个级别的许可证。
    - 对于任意一个对象，只有具有合法许可证的用户才可以存取，相对更严格。
  - 强制存取控制是对数据本身进行密级标记，无论数据如何复制，标记和数据是一个不可分的整体，只有符合密级标记要求的用户才可以操纵数据，从而提供了更高级别的安全性。
  - 详解：
    - 在强制存取控制中，全部实体被分为主体(用户、代表用户的操作进程等)和客体(文件、基本表等)。
    - 每一个实体都被指派一个敏感度标记(label)，主体的label称为许可证级别，客体的label称为密级。
    - 密级的次序是
      $$\text{绝密}(TopSecret, TS) \geq \text{机密}(Secret, S) \geq \text{可信}(Confidential, C) \geq \text{公开}(Public, P)$$
    - 系统要求主体对客体的存取必须遵循如下规则：
      - 仅当主体的许可证级别大于等于客体的密级时，主体才能读取对应的客体
      - 仅当主体的许可证级别小于等于客体的密级时，主体才能写入对应的客体

授权

- 授权：用户权限由数据库对象和操作类型两要素构成；定义存取权限称为授权。
- SQL中使用 `GRANT` 和 `REVOKE` 语句向用户授予或收回对数据的操作权限。
- 数据库角色：数据库角色是被命名的一组与数据库操作相关的权限，角色是权限的集合。SQL中可通过 `GRANT` 语句将权限授予给角色，也可将一个角色授予给用户/其他的角色

GRANT语句

```
GRANT <权限> [,<权限>]...
ON <对象类型> <对象名> [,<对象类型> <对象名>]...
TO <用户> [,<用户>]...
[WITH GRANT OPTION];
```

- 注意：不要漏了 `ON` 后面的 `TABLE`.

- 注意：对操作单独某一属性的权限的修改，加在具体权限后而不是表后。如 `UPDATE(Sno)`.

REVOKE语句

```
REVOKE <权限> [,<权限>]...
ON <对象类型> <对象名> [,<对象类型> <对象名>]...
FROM <用户> [,<用户>]...
[CASCADE | RESTRICT];
```

- 注意 `TO` 变成了 `FROM`.

视图机制

- 视图机制将用户可以访问的数据对象限制在一定的范围内，把要保密的数据对无权存取的用户隐藏起来，从而自动对数据提供一定程度的安全保护。

审计

- 审计功能把用户对数据库的所有操作自动记录下来放入审计日志，审计员可以利用审计日志监控数据库中的各种行为，重现导致数据库现有状态的一系列事件，找出非法存取数据的人、时间和内容等。

数据加密

- 加密的基本思想：根据一定的算法将原始数据(明文, plain text)变换为不可直接识别的格式(密文, cipher text)，从而使得不知道解密算法的人无法获知数据的内容
- 数据加密主要包括存储加密和传输加密。