第四章 数据库安全性

4.1 数据库安全性概述

4.1.1 数据库的不安全因素

- 非授权用户对数据库的恶意存取和破坏
  - 一些黑客和犯罪分子在用户存取数据库时猎取用户名和用户口令，然后假冒合法用户偷取、修改甚至破坏用户数据
  - 数据库管理系统提供的安全措施主要包括用户身份鉴别、存取控制和视图等技术
- 数据库中重要或敏感的数据被泄露
  - 黑客和敌对分子千方百计盗窃数据库中的重要数据，一些机密信息被暴露
  - 数据库管理系统提供的主要技术有强制存取控制、数据加密存储和加密传输等
  - 审计日志分析
- 安全环境的脆弱性
  - 数据库的安全性与计算机系统的安全性紧密联系
  - 建立一套可信计算机系统的概念和标准

4.1.2 安全标准简介

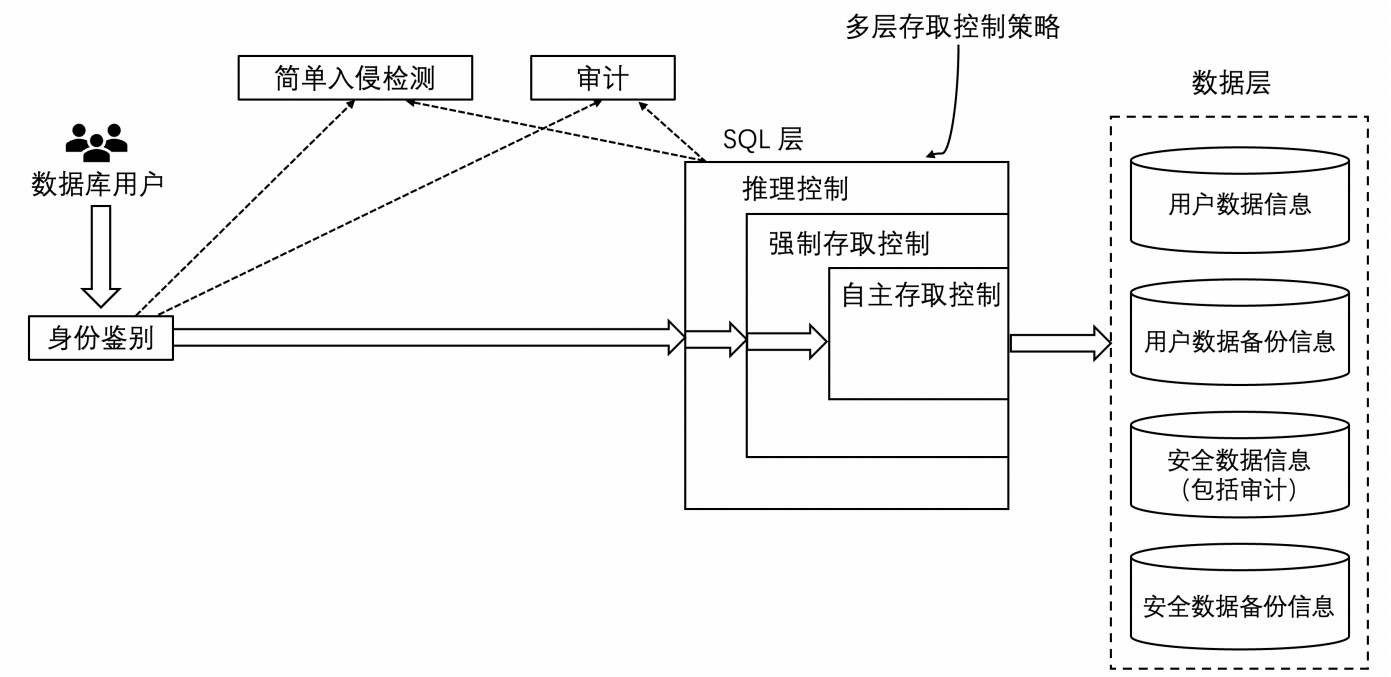
- TCSEC/TDI 安全级别划分
  - 按系统可靠或可信程度逐渐增高
  - 各安全级别之间具有一种偏序向下兼容的关系

安全级别	定义
A1	验证设计（Verified Design）
B3	安全域（Security Domains）
B2	结构化保护（Structural Protection）
B1	标记安全保护（Labeled Security Protection）
C2	受控的存取保护（Controlled Access Protection）
C1	自主安全保护（Discretionary Security Protection）
D	最小保护（Minimal Protection）

- CC 评估保证级（EAL）划分

评估保证级	定义	TCSEC安全级别（近似相当）
EAL1	功能测试（functionally tested）	
EAL2	结构测试（structurally tested）	C1
EAL3	系统地测试和检查（methodically tested and checked）	C2
EAL4	系统地设计、测试和复查（methodically designed，tested，and reviewed）	B1
EAL5	半形式化设计和测试（semiformally designed and tested）	B2
EAL6	半形式化验证的设计和测试（semiformally verified design and tested）	B3
EAL7	形式化验证的设计和测试（formally verified design and tested）	A1

4.2 数据库安全性控制



4.2.1 用户身份鉴别

- 静态口令鉴别
- 动态口令鉴别
- 生物特征鉴别
- 智能卡鉴别

4.2.2 存取控制

- 定义用户权限，并将用户权限登记到数据字典中
  - 用户对某一数据对象的操作权力称为权限
  - DBMS 提供适当的语言来定义用户权限，存放在数据字典中，称做安全规则或授权规则
- 合法权限检查
- 用户权限定义和合法权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 级的数据库管理系统支持自主存取控制（Discretionary Access Control，DAC），B1 级的数据库管理系统支持强制存取控制（Mandatory Access Control，MAC）
  - 在自主存取控制方法中，用户对不同的数据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，而且用户还可将其拥有的存取权限转授给其他用户
  - 在强制存取控制方法中，每一个数据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

4.2.3 自主存取控制方法

- 通过 SQL 的 `GRANT` 语句和 `REVOKE` 语句实现
- 用户权限由数据库对象和操作类型两个要素组成
- 定义一个用户的存取权限就是要定义用户可以在哪些数据库对象上进行哪些类型的操作
- 定义存取权限称为授权

4.2.4 授权：授予与收回

1. `GRANT`

`GRANT` 语句的一般格式为

```
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];
```

如果指定 `WITH GRANT OPTION` 子句，则获得某种权限的用户还可以把这种权限再授予其他的用户

> 例：把查询Student表和修改学生学号的权限授给用户U4

```
GRANT UPDATE(Sno), SELECT
ON TABLE Student
TO U4;
```

2. `REVOKE`

`REVOKE` 语句的一般格式为

```
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];
```

4.2.5 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

1. 角色的创建

```
CREATE ROLE <角色名>
```

2. 给角色授权

```
GRANT <权限>[,<权限>]…
ON <对象类型>对象名
TO <角色>[,<角色>]…
```

3. 将一个角色授予其他的角色或用户

```
GRANT <角色1>[,<角色2>]…
TO <角色3>[,<用户1>]…
[WITH ADMIN OPTION]
```

4. 角色权限的收回

```
REVOKE <权限>[,<权限>]…
ON <对象类型> <对象名>
FROM <角色>[,<角色>]…
```

4.2.6 强制存取控制方法

- 在强制存取控制中，数据库管理系统所管理的全部实体被分为**主体**和**客体**两大类
- 主体是系统中的活动实体：数据库管理系统所管理的实际用户，代表用户的各进程
- 客体是系统中的被动实体，受主体操纵：文件、基本表、索引、视图
- 对于主体和客体，DBMS 为它们每个实例（值）指派一个**敏感度标记**，敏感度标记分成若干级别，例如绝密（TS）、机密（S）、可信（C）和公开（P）等
- 主体的敏感度标记称为许可证级别，客体的敏感度标记称为密级
- 强制存取控制规则
  - 仅当主体的许可证级别大于或等于客体的密级时，该主体才能读取相应的客体
  - 仅当主体的许可证级别小于或等于客体的密级时，该主体才能写相应的客体
- 强制存取控制（MAC）是对数据本身进行密级标记，无论数据如何复制，标记与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

- 实现强制存取控制时要首先实现自主存取控制，因为较高安全性级别提供的安全保护要包含较低级别的所有保护

4.3 视图机制

- 把要保密的数据对无权存取这些数据的用户隐藏起来，对数据提供一定程度的安全保护
- 间接地实现支持存取谓词的用户权限定义

4.4 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中
- 审计员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况的一系列事件，找出非法存取数据的人、时间和内容等
- C2 以上安全级别的 DBMS 必须具有审计功能
- 审计功能的可选性
    - 审计很费时间和空间
    - DBA 可以根据应用对安全性的要求，灵活地打开或关闭审计功能
    - 审计功能主要用于安全性要求较高的部门

1. 审计事件

审计事件一般有多个类别，例如

- 服务器事件：审计数据库服务器发生的事件，包括数据库服务器的启动、停止、数据库服务器配置文件的重新加载
- 系统权限：对系统拥有的结构或模式对象进行操作的审计，要求该操作的权限是通过系统权限获得的
- 语句事件：对 SQL 语句，如 DDL、DML、DQL 及 DCL 语句的审计
- 模式对象事件：对特定模式对象上进行的 SELECT 或 DML 操作的审计

2. 审计功能

审计功能主要包括以下几个方面的内容：

- 基本功能，提供多种审计查阅方式
- 多套审计规则，一般在初始化设定
- 提供审计分析和报表功能
- 审计日志管理功能
    - 防止审计员误删审计记录，审计日志必须先转储后删除
    - 对转储的审计记录文件提供完整性和保密性保护
    - 只允许审计员查阅和转储审计记录，不允许任何用户新增和修改审计记录等
- 提供查询审计设置及审计记录信息的专门视图

3. `AUDIT` 语句和 `NOAUDIT` 语句

`AUDIT` 语句用来设置审计功能，`NOAUDIT` 语句取消审计功能

> 例：对修改 SC 表结构或修改 SC 表数据的操作进行审计

```
AUDIT ALTER,UPDATE
ON  SC;
```

4.5 数据加密

- 数据加密是防止数据库中数据在存储和传输中失密的有效手段
- 加密的基本思想是根据一定的算法将原始数据——明文变换为不可直接识别的格式——密文
- 加密方法
  - 存储加密
    - 透明存储加密
      - 内核级加密保护方式，对用户完全透明
      - 将数据在写到磁盘时对数据进行加密，授权用户读取数据时再对其进行解密
      - 数据库的应用程序不需要做任何修改，只需在创建表语句中说明需加密的字段即可
      - 内核级加密方法：性能较好，安全完备性较高
    - 非透明存储加密
      - 通过多个加密函数实现
  - 传输加密
    - 链路加密
      - 在链路层进行加密
      - 传输信息由报头和报文两部分组成
      - 报文和报头均加密
    - 端到端加密
      - 在发送端加密，接收端解密
      - 只加密报文不加密报头
      - 所需密码设备数量相对较少，容易被非法监听者发现并从中获取敏感信息

4.6 其他安全性保护

- 推理控制：避免用户利用能够访问的数据推知更高密级的数据
- 隐蔽信道：间接数据传递
- 数据隐私保护：描述个人控制其不愿他人知道或他人不便知道的个人数据的能力