数据库原理及应用

Principle and Application of Database

华东交通大学
喻佳



数据库安全性指保护数据库以防止不合法使用所造成的数据泄露、更改或破坏。

常用的数据库安全性控制方法

用户身份鉴别

A

存取控制

B

视图机制

C

审计

D

加密存储

E

存取控制

- 自主存取控制
- 强制存取控制

4.2 数据库安全性控制

----- 自主存取控制方法


教务综合管理系统
主页
个人课表
教学任务书
成绩录入
监考安排
退出
信息查询
班级名单 专业培养方案
教师任务书 班级任务书
平时成绩登记表 学生成绩
班级选课情况 学分统计
素质拓展学分 实验大纲
学生考试安排 学生评教情况
课表/考试
班级课表 教师课表 空教室
教师周历 教室信息 空班级
我的课表 教师监考
调课申请 教室申请
成绩录入
学生成绩 补考成绩
辅修成绩 辅修补考成绩
实践教学
主页 / 成绩录入 / 学生成绩录入
2018年6月5日 星期二
学期: 2017-2018 第二学期
成绩录入结束时间: 2018年06月30日
学期
总学时
主讲教师
成绩录入
2017.2
2
分班录入
授 权
数据库对象
操作类型
定义用户存取权限

一、自主存取控制

大型数据库管理系统都支持自主存取控制。

SQL标准也对自主存取控制提供支持，主要通过SQL的GRANT（授权）和REVOKE（回收授权）语句来实现。

示例数据库

学生-课程数据库

- 学生表：Student(Sno，Sname，Ssex，Sage，Sdept)
- 课程表：Course(Cno，Cname，Cpno，Ccredit)
- 学生选课表：SC(Sno，Cno，Grade)

学 号 Sno	姓 名 Sname	性 别 Ssex	年 龄 Sage	所在系 Sdept
201815121	李勇	男	20	CS
201815122	刘晨	女	19	CS
201815123	王敏	女	18	MA
201815125	张立	男	19	IS

Student表

学 号 Sno	课程号 Cno	成绩 Grade
201815121	1	92
201815121	2	85
201815121	3	88
201815122	2	90
201815122	3	80

SC表

课程号 Cno	课程名 Cname	先行课 Cpno	学分 Ccredit
1	数据库	5	4
2	数学		2
3	信息系统	1	4
4	操作系统	6	3
5	数据结构	7	4
6	数据处理		2
7	PASCAL语言	6	4

Course表

1、GRANT

- GRANT语句的一般格式：

  GRANT <权限>[,<权限>]...

  [**ON** <对象类型> <对象名>]

  TO <用户>[,<用户>]...

  [WITH GRANT OPTION];

- 语义：将对指定操作对象的指定操作权限授予指定的用户

- 发出GRANT：
  - DBA
  - 数据库对象创建者（即属主Owner）
  - 拥有该权限的用户
- 按受权限的用户
  - 一个或多个具体用户
  - PUBLIC（全体用户）

1、GRANT举例

[例1] 把查询Student表权限授给用户U1

```
GRANT   SELECT
ON      TABLE   Student
TO      U1;
```

[例2] 把对Student表和Course表的全部权限授予用户U2和U3

```
GRANT   ALL PRIVILIGES
ON      TABLE Student, Course
TO      U2, U3;
```

1、GRANT举例

[例3] 把对表SC的INSERT权限授予U5用户并允许他再将此权限授予其他用户.

```
GRANT INSERT
ON TABLE SC
TO U5
WITH GRANT OPTION;
```

[例4] 执行例3后，U5不仅拥有了对表SC的INSERT权限，还可以**传播**此权限：

```
GRANT INSERT
ON TABLE SC TO U6
WITH GRANT OPTION;
```


REVOKE

2、REVOKE

[例3] 把对表SC的INSERT权限授予U5用户，并允许他再将此权限授予其他用户.

```
GRANT INSERT
ON TABLE SC
TO U5
WITH GRANT OPTION;
```

[例5]把用户U5对SC表的INSERT权限收回

```
REVOKE  INSERT
ON      TABLE SC
FROM    U5  CASCADE ;
```

将用户U5的INSERT权限收回的时候必须级联（CASCADE）收回

系统只收回直接或间接从U5处获得的权限

小结:SQL灵活的授权机制

- DBA：拥有所有对象的所有权限
  - 不同的权限授予不同的用户
- 用户：拥有自己建立的对象的全部的操作权限
  - GRANT：授予其他用户
- 被授权的用户
  - “继续授权”许可：再授予
- 所有授予出去的权力在必要时又都可用REVOKE语句收回

思考题

对下列两个关系模式：

学生（学号，姓名，年龄，性别，家庭住址，班级号）

班级（班级号，班级名，班主任，班长）

使用GRANT语句完成下列授权功能，再用REVOKE把所有权限回收：

（1）授予用户U1对两个表的所有权限，并可给其他用户授权；

（2）授予用户U2对学生表具有查看权限，对家庭住址具有更新权限；

（3）将对班级表的查看权限授予所有用户。

THANK YOU FOR YOUR WATCHING

