《数据库系统》作业-第四章

姓名：任宇 学号：33920212204567

1. 什么是数据库的安全性？
答：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、更改或破坏。

2. 举例说明对数据库安全性产生威胁的因素。
答：（1）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。
（2）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。
（3）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，包括计算机硬件、操作系统、网络系统等的安全性是紧密联系的。操作系统安全的脆弱，网络协议安全保障的不足等都会造成数据库安全性的破坏。

4. 试述实现数据库安全性控制常用方法和技术。
常用方法和技术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。
（1） 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。常用的用户身份鉴别方法有：静态口令鉴别、动态口令鉴别、生物特征鉴别、智能卡鉴别等。
（2） 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。
（3） 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，审计员可以利用审计日志监控数据库中的各种行为，重视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。
（4） 视图机制：为不同的用户定义不同的视图，通过视图机制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。
（5） 数据加密：加密的基本思想是根据一定的算法将原始数据变换为不可直接识别的格式—密文，从而使得不知道解密算法的人无法获取数据的内容，数据加密包括存储加密和传输加密。

5. 什么是数据库中的自主存取控制方法和强制存取控制方法？
（1） 在自主存取控制方法中，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，而且用户可将其拥有的权限转授给其他用户。因此自主存取控制非常灵活。
（2） 在强制存取控制方法中，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。因此，强制存取控制相对比较严格。

6. 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：

（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） 将对班级表查看权限授予所有用户。

（4） 将对学生表的查询、更新权限授予角色 R1。

（5） 将角色 R1 授予用户 R1，并且 U1 可继续授权给其他角色。

答：

```
（1）GRANT ALL PRIVILEGES
     ON TABLE 学生，班级
     TO U1
     WITH GRANT OPTION;
（2）GRANT SELECT，UPDATE（家庭住址）ON TABLE 学生 TO U2;
（3）GRANT SELECT ON TABLE 班级 TO PUBLIC;
（4）CREATE ROLE R1;
    GRANT SELECT, UPDATE ON TABLE 学生 TO R1;
（5）GRANT R1 TO U1 WITH ADMIN OPTION;
```

7. 今有以下两个关系模式：

职工（职工号，姓名，年龄，职务，工资，部门号）

部门（部门号，名称，经理名，地址，电话号）

请用 SQL 语句中的 GRANT 和 REVOKE 语句（加上视图机制）完成以下授权定义或存取控制功能；

（1） 用户王明对两个表有 SELECT 权限。

（2） 用户李勇对两个表有 INSERT 和 DELETE 权限。

（3） 每个职工只对自己的记录有 SELECT 权限。

（4） 用户刘星对职工表有 SELECT 权限，对工资字段具有更新权限。

（5） 用户张新剧有修改这两个表的结构的权限。

（6） 用户周平具有对两个表的所有权限，并具有给其他用户授权的权限。

（7） 用户杨兰具有从每个部门职工中 SELECT 最高工资、最低工资、平均工资的权限，他不能查看每个人的工资。

答：

```
（1）GRANT SELECT ON TABLE 职工,部门 TO 王明;
（2）GRANT INSERT,DELETE ON TABLE 职工,部门 TO 李勇;
（3）GRANT SELECT ON TABLE 职工 WHEN USER()=NAME TO ALL;
（4）GRANT SELECT,UPDATE(工资) ON TABLE 职工 TO 刘星;
（5）GRANT ALTER TABLE ON TABLE 职工,部门 TO 张新;
（6）GRANT ALL PRIVILEGES ON TABLE 职工,部门 TO 周平 WITH GRANT OPTION;
（7）CREATE VIEW 部门工资 AS
```

```
 SELECT 部门，名称，MAX（工资），MIN（工资），AVG（工资）
FROM 职工，部门
WHERE 职工.部门号＝部门.部门号
GROUP BY 职工.部门号;
GRANT SELECT ON 部门工资 TO 杨兰;
```

8. 针对习题 7 中（1）-（7）的每一种情况，撤销各用户所授予的权限。
答：

```
（1）REVOKE SELECT ON TABLE 职工,部门 FROM 王明;
（2）REVOKE INSERT,DELETE ON TABLE 职工,部门 FROM 李勇;
（3）REVOKE SELECT ON TABLE 职工 WHEN USER()=NAME FROM ALL;
（4）REVOKE SELECT,UPDATE(工资) ON TABLE 职工 FROM 刘星;
（5）REVOKE ALTER TABLE ON TABLE 职工,部门 FROM 张新;
（6）REVOKE ALL PRIVILEGES ON TABLE 职工,部门 FROM 周平;
（7）REVOKE SELECT ON 部门工资 FROM 杨兰;
 DROP VIEW 部门工资;
```

9. 解释强制存取控制机制中主体、个体、敏感度标记的含义。
答：主体是系统中的活动实体，既包括数据库管理系统所管理的实际用户，也包括代表用户的各进程。客体是系统中的被动实体，是受主体操纵的，包括文件、基本表、索引、视图等。对于主体和客体，数据库管理系统为它们每个实例（值）指派一个敏感度标记，敏感度标记被分成若干级别，例如绝密、机密、可信、公开等。

10. 举例说明强制存取控制机制是如何确定主体能否存取客体的。
答：强制存取控制机制通过对比主题的敏感度标记和客体的敏感度标记，最终确定主题是否能够存取客体，遵循以下两条规则：
（1）仅当主体的许可证级别大于或等于客体的密级时，该主体才能读取对应的客体。
（2）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。
例如：
假设有一家银行拥有一个客户信息数据库。对于该数据库中的每个数据对象，银行将其分为三个安全级别：公开、可信和机密。同时，高层管理人员的安全级别为“机密级别”，普通的行政人员的安全级别为“可信级别”，而保洁人员的安全级别则为“公开级别”。
则保洁人员不能获取可信和机密级别的数据对象，普通的行政人员可以写机密级别，但不能获取机密级别的数据对象，而高层管理人员则可以获取机密级别的数据对象。

11. 什么是数据库的审计功能，为什么要提供审计功能？
答：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，审计员可以利用审计日志监控数据库中的各种行为，重视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。

因为任何系统的安全保护措施都不是完美无缺的，蓄意盗窃、破坏数据的人总是想法设法打破控制。