数据库安全性概述

数据库安全性概述

总述

内容：数据库管理系统提供统一的数据保护功能来保证数据的安全可靠和正确有效。学习数据库安全性控制的基本概念。

数据库安全性概述

一、安全性定义及标准

二、数据库存取控制

三、安全性和完整性的关系

一、安全性定义及标准

数据库的一大特点是数据可以共享，数据共享必然带来数据库的安全性问题。数据库系统中的数据共享不能是无条件的共享，例如军事秘密、国家机密、新产品实验数据、市场需求分析、市场营销策略、销售计划、客户档案、医疗档案、银行储蓄数据等都有数据安全性问题。

一、安全性定义及标准

数据库的安全性是指保护数据库以防止不合法的使用所造成的数据泄露、更改或破坏。对数据库不合法的使用称为数据库的滥用。数据库的滥用可分为无意的和恶意的两类。

在事务处理时，无意的滥用容易发生系统故障，并发访问数据库时引起异常现象以及违反数据完整性约束等逻辑错误。

恶意的滥用主要指未经授权的读取数据（即窃取信息）和未经授权的修改数据（即破坏数据）。

一、安全性定义及标准

安全性不是数据库系统独有的，计算机系统都有安全性问题。（硬件、软件、数据）

计算机系统安全性级别包括：

（1）环境级，如机房重地；

（2）职员级，不同权限；

（3）OS级，设口令、密码；

（4）网络级，防火墙；

（5）数据库系统级，不同权限。

一、安全性定义及标准

数据安全的级别

1985年，美国颁布(可信计算机系统安全评测标准)TCSEC(Trusted Computer System Evaluation Criteria)，把数据安全级别划分为四类七级：

安全级别	定　　义
D	最小保护
C1	自主安全保护
C2	受控的存取保护
B1√	标记安全保护
B2	结构化保护
B3	安全域
A1	验证设计

一、安全性定义及标准

TCSEC标准数据安全级别的划分

无保护级
- D级，最低安全性（OS）；

自主保护级
- C1级，主客体分离、身份鉴别、数据完整性、自主存取控制;
- C2级，审计；

强制保护级
- B1级，强制存取控制（MAC - 可信系统(安全系统);
- B2级，良好的结构化设计、形式化安全模型；
- B3级，全面的访问控制、可信恢复；

验证保护级
- A1级，形式化认证。

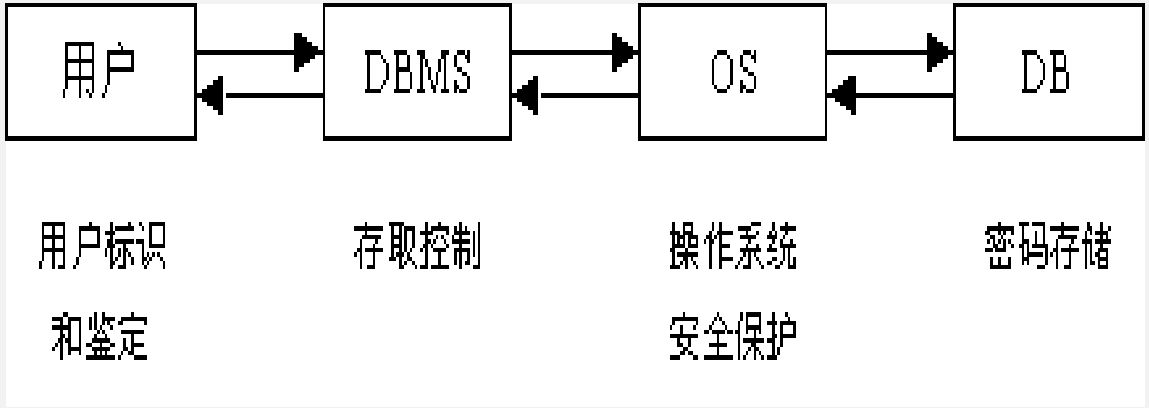
一、安全性定义及标准

为解决各自独立的标准中概念和技术上的差异而制定的一个各国都能接受的通用的信息安全产品和系统的安全性评估准则，称为CC标准。

	TCSEC	评估保证级
		EAL1功能测试
	C1	EAL2结构测试
	C2	EAL3系统地测试和检查
	B1	EAL4系统地设计、测试和复查
	B2	EAL5半形式化设计和测试
	B3	EAL6半形式化验证的设计和测试
	A1	EAL7形式化验证的设计和测试

二、数据库存取控制

在一般计算机系统中，安全措施是一级一级层层设置的。例如可以有如下的模型：



二、数据库存取控制

在数据库系统中，实现安全性的最主要的方法就是存取控制机制，即只允许有权限的用户访问数据库。根据预先定义好的用户权限进行存取控制，保证用户只能存取他有权存取的数据，这是数据库系统存取控制机制的主要功能。

二、数据库存取控制

常用存取控制方法有自主存取控制和强制存取控制两类方法。

（1）自主存取控制

- 不同用户对不同数据库对象有不同权限，通过 SQL 的 GRANT 语句和 REVOKE 语句实现权限管理。
- 用户定义存取权限，DBMS检查存取权限。用户权限定义和合法权限检查机制一起组成了DBMS的安全子系统

二、数据库存取控制

（2）强制存取控制

- 系统为保证更高程度的安全性，对系统控制下的所有主客体实施强制存取控制。
- 主体是用户,客体是文件、表、索引、视图等。
- 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。
- 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,提供了更高级别的安全性。

三、安全性和完整性的关系

安全性是保护数据库防止恶意的破坏和非法的存取。

完整性是为了防止数据库中存在不符合语义的数据，防止错误信息的输入和输出，即所谓“垃圾进垃圾出”所造成的无效操作和错误结果。

安全性和完整性是密切相关的，特别从系统实现的方法来看，某一种机制常常既可用于安全性保护亦可用于完整性保证。

练习

SQL 的 GRANT 语句和 REVOKE 语句可以用来实现（　　）。

A. 自主存取控制

B. 强制存取控制

C. 数据库角色创建

D. 数据库审计

解答

SQL 的 GRANT 语句和 REVOKE 语句可以用来实现（ A ）。

A. 自主存取控制

B. 强制存取控制

C. 数据库角色创建

D. 数据库审计

小结

非授权用户对数据库的恶意存取和破坏、数据库中重要或敏感数据被泄漏以及脆弱的安全环境是对数据库安全性产生威胁的主要因素。完善的安全标准可以规范和指导数据库产品的生产，加强系统的安全性保证。

数据存取控制是实现数据库安全性控制的主要办法。大多数DBMS都实现了自主存取控制，B1级的数据库管理系统支持强制存取控制，强制存取控制提供了更高级别的安全性。


谢谢！

存取控制机制

存取控制机制

总述

内容：数据库管理系统提供统一的数据保护功能来保证数据的安全可靠和正确有效。学习数据库管理系统通过权限进行存取控制的机制。

存取控制机制

一、权限

二、存取控制子系统功能

存取控制机制

一、权限

用户权限是指不同的用户对于不同的数据对象允许执行的操作权限，它由数据对象和操作类型两部分组成。

在数据库系统中，为了保证数据的安全性，用户对数据的操作必须首先从DBA处获得权限，才能进行对数据的操作。同时数据库系统也允许用户将获得的权限转授给其他用户，也允许把已授给其他用户的权限再回收上来。

存取控制机制

一、权限

不同对象类型允许的操作权限

对象	对象类型	操作权限
属性列	TABLE	SELET、INSERT、UPDATE、DELETE、ALL PRIVILEGES
视图	TABLE	SELET、INSERT、UPDATE、DELETE、ALL PRIVILEGES
基本表	TABLE	SELET、INSERT、UPDATE、DELETE、ALL PRIVILEGES、ALTER、INDEX
数据库	DATABASE	CREATE（建表权）

二、存取控制子系统功能

DBMS安全子系统包括定义用户权限和合法权限检查两大功能。

（1）定义用户权限：用户把授权和回收权力的决定告诉系统，授权和回收权限的结果存入数据字典；

（2）合法权限检查：当用户提出操作请求时，根据字典中的授权情况进行检查，以决定是否执行操作请求。

二、存取控制子系统功能

SQLSERVER的权限表

	Owner	Object	Grantee	Grantor	ProtectType	Action	Column
1	dbo	s	u_aa	dbo	Grant	Delete	.
2	dbo	s	u_aa	dbo	Grant	Insert	.
3	dbo	s	u_aa	dbo	Grant	References	(All+New)
4	dbo	s	u_aa	dbo	Grant	Select	(All+New)
5	dbo	s	u_aa	dbo	Grant	Update	(All+New)
6	.	.	u_aa	dbo	Grant	CONNECT	.

练习

为了实现数据库的（　　），数据库管理系统提供授权功能以控制用户访问数据的权限。

A. 一致性

B. 完整性

C. 安全性

D. 可靠性

存取控制机制

解答

为了实现数据库的（ C ），数据库管理系统提供授权功能以控制用户访问数据的权限。

A. 一致性

B. 完整性

C. 安全性

D. 可靠性

小结

授权机制可以保证用户只能进行其权限范围内的操作。DBA拥有对数据库中所有对象的所有权限，并根据需要将不同的权限授予不同的用户。


谢谢！

授权和回收权限

授权和回收权限

总述

内容：数据库管理系统采用存取控制机制来保证数据的安全可靠。学习SQL中用户授权和回收权限的方法。

授权和回收权限

一、授予权限

二、回收权限

三、角色

授权和回收权限

一、授予权限

授权是通过SQL语言的Grant语句实现的。

Grant语句的一般格式为：

Grant <权限>[,<权限>]… [on <对象类型><对象名>] to <用户>[,<用户>]…

[With Grant Option];

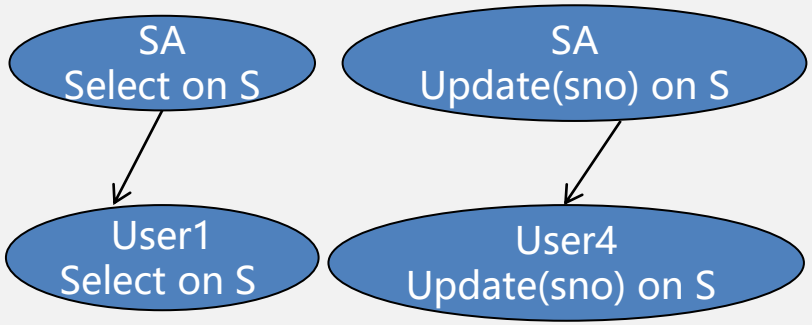
★ 用户可以是多个用户，也可以是PUBLIC。

★ 指定With Grant Option子句，则获得权限的用户还可以将此权限授予给其他用户。

授权和回收权限

一、授予权限

例1：Grant Select
on Table S
to User1；



例2：Grant ALL PRIVILEGES
on Table S，C
to User1，User2；

例3：Grant Update(sno)，Select
on Table S
to User4；

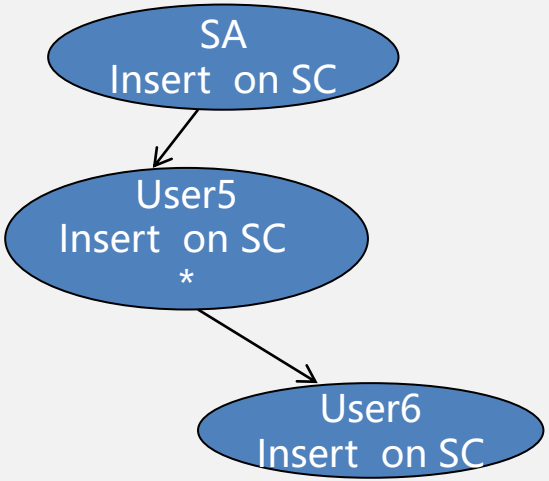
授权和回收权限

一、授予权限

例4：Grant Insert
on Table SC
to User5
With Grant Option；

User5又可以将SC表上的Insert权限授予其他用户User6

例5：Grant Insert
on Table SC
to User6



二、回收权限

授予的权限可以由DBA或其他授权者用Revoke语句收回。Revoke语句的一般格式为：

Revoke <权限>[,<权限>]… [on <对象类型><对象名>] From <用户>[,<用户>]… ；

★ 回收操作级联收回。

二、回收权限

例6：Revoke Select
on Table S
From PUBLIC;

例7：Revoke Update(sno)
on Table S
From User4;

二、回收权限

例8：Revoke Insert on Table SC
From User5;

注意：回收操作的级联，系统只回收直接或间接从User5处获得的权限。

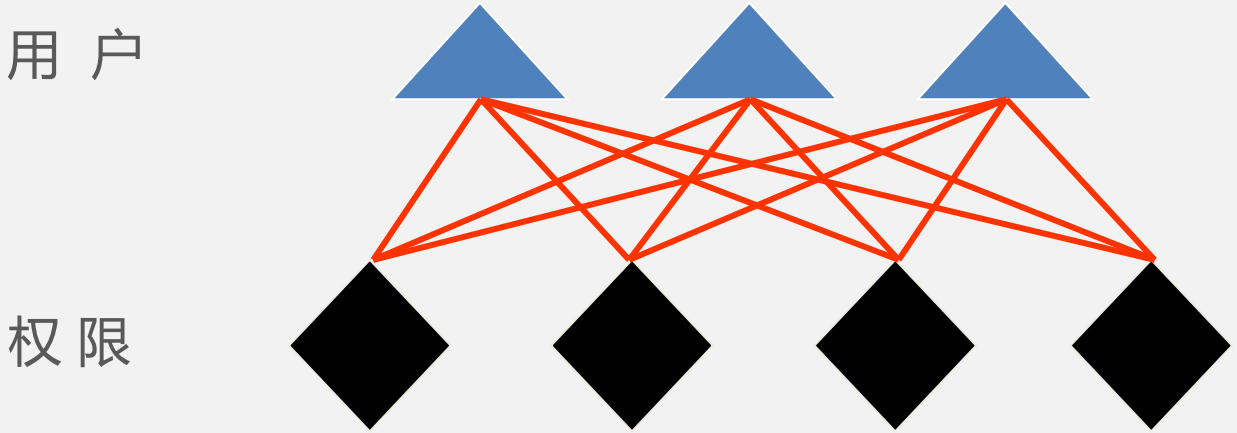
三、角色

如果用户数量非常多，流动也大，权限管理会非常复杂。使用角色可以把很多用户统一成一个整体以方便管理，简化授权的过程。

角色是一组数据库权限的集合，可以为一组具有相同权限的用户创建一个角色。

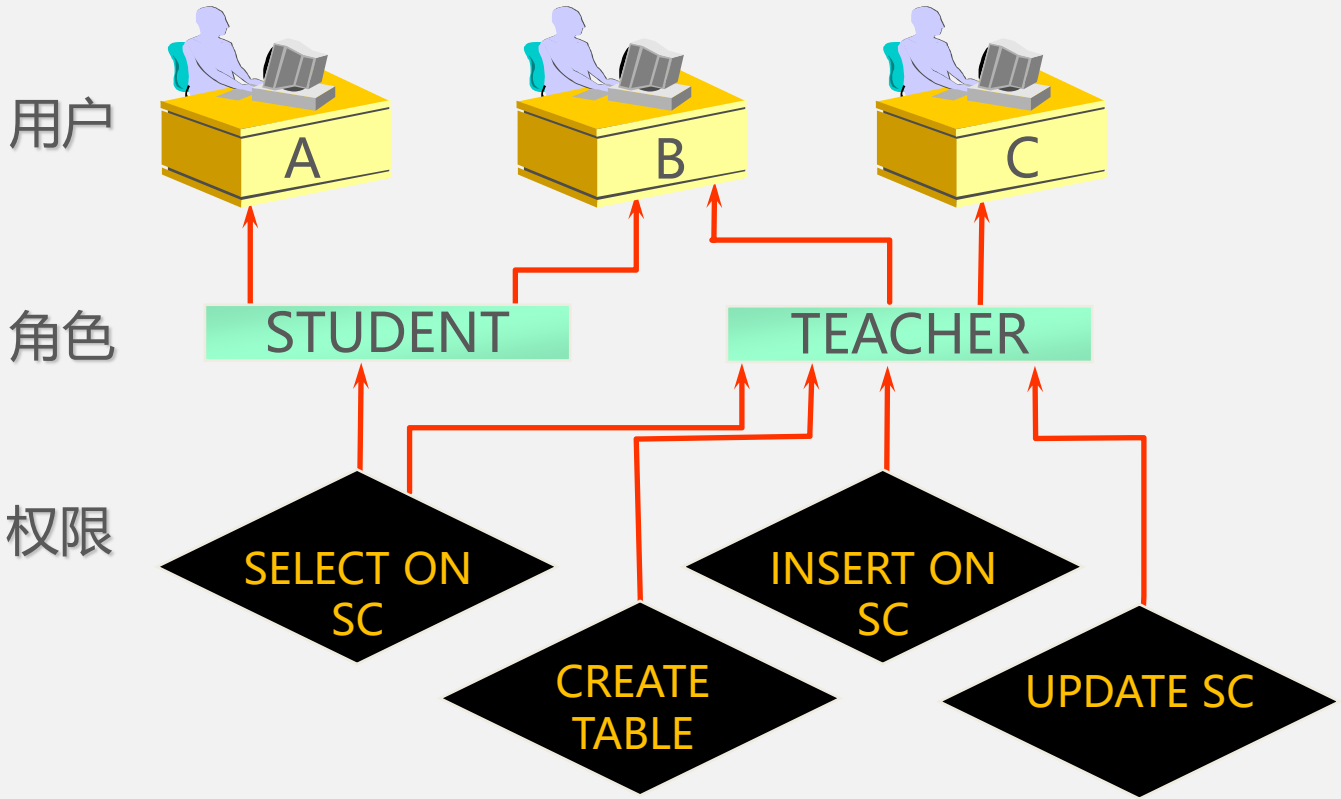
三、角色

无角色管理的授权示意图



授权和回收权限

三、角色


用户
A
B
C
角色
STUDENT
TEACHER
权限
SELECT ON SC
CREATE TABLE
INSERT ON SC
UPDATE SC

三、角色

SQL中的角色命令

（1）创建角色(标准)

Create Role r1

（2）给角色授权

Grant Select on Table S to r1

（3）将角色授予用户

Grant r1 to user1

（4）收回角色权限

Revoke r1 From user1

授权和回收权限

练习

SQL中对于授予的权限可以由DBA或其他授权者用（　　）语句收回。

A. DROP

B. REVOKE

C. REMOVE

D. DELETE

授权和回收权限

练习

SQL中对于授予的权限可以由DBA或其他授权者用（ B ）语句收回。

A. DROP

B. REVOKE

C. REMOVE

D. DELETE

小结

DBA拥有对数据库中所有对象的所有权限，并根据需要将不同的权限授予不同的用户。用户对自己建立的基本表和视图拥有全部的操作权限，并可将这些权限授予给别人。授予用户的权限可由DBA或其他授权者收回。

为了使自主授权的执行更加灵活方便，一些DBMS引入角色来简化授权的过程。通过角色对用户分组，可以授予同类用户同样的访问权限。


谢谢！

视图技术和审计

总述

内容：数据库管理系统提供统一的数据保护功能来保证数据的安全可靠和正确有效。数据库的主要安全措施包括用户身份鉴别、存取控制、视图机制和审计等，学习视图机制和审计。

视图技术和审计

一、视图技术

二、审计

一、视图技术

视图是从一个或几个基本表导出的表，是虚表，视图定义后可以像基本表一样用于查询和删除。

视图机制使系统具有三个优点： 数据安全性、数据独立性、操作简便性。

视图机制把用户可以使用的数据定义在视图中，这样用户就不能使用视图定义外的其他数据，从而保证了数据库的安全性。

一、视图技术

例1：建立计算机系学生的视图，用户王平和张明可以使用该视图访问计算机系学生的信息。

实际中，视图机制与授权机制配合使用：

- 首先用视图机制屏蔽掉一部分保密数据；
- 视图上面再进一步定义存取权限。

例如，对于已经建立的计算机系学生的视图，把对该视图的查询权限授于王平，把该视图上的所有操作权限授于张明。

二、审计

将用户对数据库的所有操作记录在审计日志（Audit Log）中，DBA利用审计日志找出非法存取数据的人、时间和内容。

审计功能是DBMS达到C2以上安全级别必不可少的一项指标。

二、审计

审计通常是很费时间和空间的，DBMS将其作为可选特征，允许DBA根据应用对安全性的要求，灵活地打开或关闭审计功能。

SQL提供AUDIT和NOAUDIT语句，AUDIT语句用来设置审计功能， NOAUDIT语句取消审计功能。

二、审计

例2：对修改SC表结构或数据的操作进行审计。

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

例3：取消对SC表的审计。

```
NOAUDIT ALTER,UPDATE
ON SC;
```

练习

数据库管理系统提供的安全措施中不包括下面的哪一个技术（　）。

A. 加密技术

B. 审计技术

C. 图技术

D. 强制存取控制技术

解答

数据库管理系统提供的安全措施中不包括下面的哪一个技术（C）。

A. 加密技术

B. 审计技术

C. 图技术

D. 强制存取控制技术

小结

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。

数据库审计功能提供了一种事后检查定责的安全机制，能够约束用户可能的恶意操作，监督并发现潜在风险，建立黑白用户名单。

对于高度敏感性数据，还可以采取数据加密技术进一步保证数据的安全。


谢谢！