

# 第4章 数据库的安全性

# 本章目标

## ■ 完成本章的学习，你应该能够

- 了解什么是计算机系统安全性问题，什么是数据库的安全性问题，威胁数据库安全性的因素有哪些
- 牢固掌握TCSEC和CC标准的主要内容。C2级DBMS、B1级DBMS的主要特征。DBMS提供的安全措施：用户身份鉴别、自主存取控制和强制存取控制技术、视图技术和审计技术、数据加密存储和加密传输
- 熟练掌握使用SQL中的GRANT和REVOKE语句实现自主存取控制
- 深刻理解强制存取控制中的存取规则

# 大纲

- **数据库安全性概述**
- 数据库安全性控制
- 视图机制
- 审计(Audit)
- 数据加密
- 其他安全性保护
- 本章小结

# 安全问题无处无时不在!



Blackmail



Cyberattack real-time map

# 数据库安全性概述

- 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，数据库中数据的共享是在DBMS统一的严格的控制之下的共享，即只允许有合法使用权限的用户访问允许他存取的数据。
  - 例：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



**数据库安全性**

# 数据库安全性

- 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。
- 系统安全保护措施是否有效是数据库系统主要的性能指标之一。
- 安全性问题不是数据库系统所独有的，所有计算机系统都有这个问题。
  - OS，网络系统，应用程序，硬件，系统架构，移动安全

# 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（Hacker）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。
  - DBMS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。



<https://www.cert.org.cn/>



<http://www.cverc.org.cn/>

## ■ 数据库中重要或敏感的数据被泄露

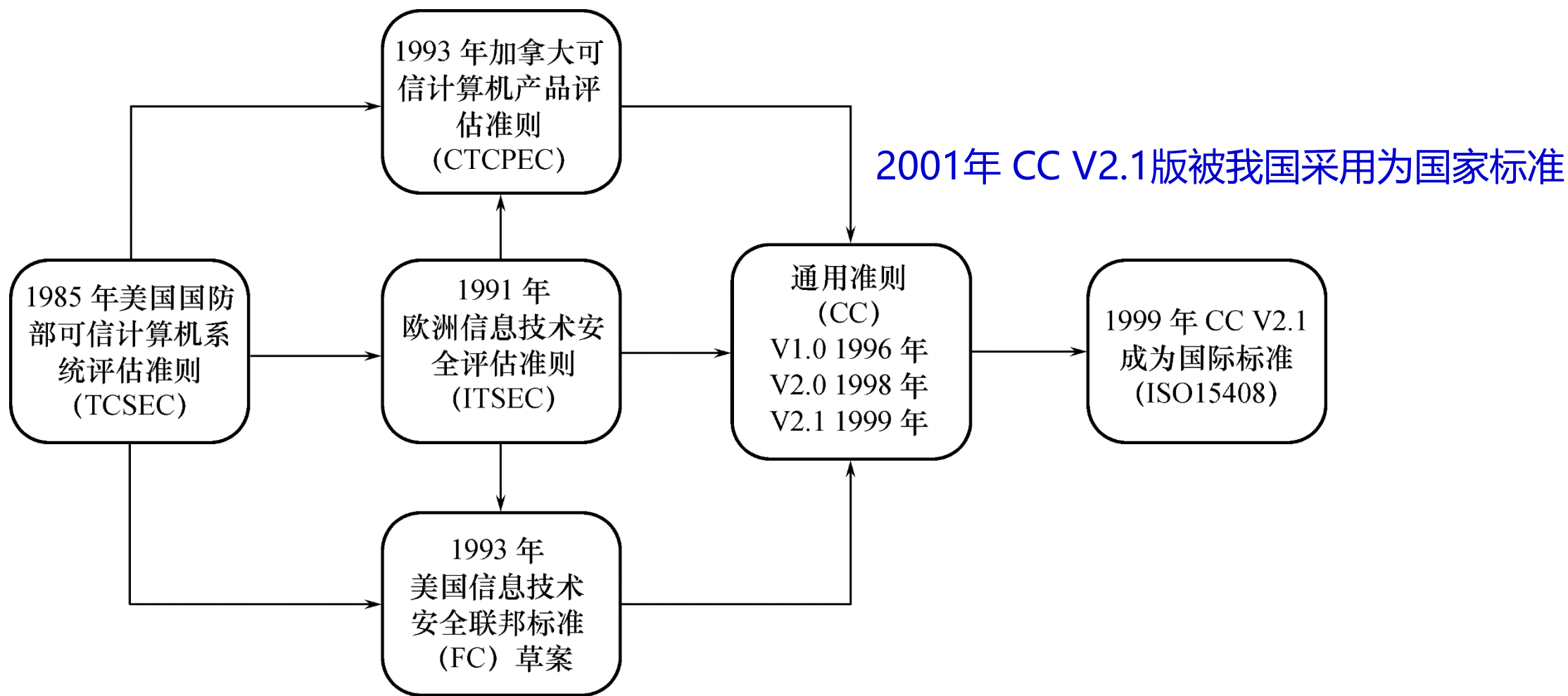
- 黑客和敌对分子千方百计盗窃数据库中的重要数据，一些机密信息被暴露。
- DBMS提供的主要技术有强制存取控制、数据加密存储和加密传输等。
- 审计日志分析
  - 对安全性要求较高的部门提供审计功能：对非授权用户的入侵行为及信息破坏情况进行跟踪，防止对数据库安全责任的否认。

## ■ 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。
  - 计算机硬件、操作系统、网络系统等的安全性
- 建立一套可信(Trusted)计算机系统的概念和标准。



# 安全标准简介



信息安全标准的发展历史

# TCSEC标准

- 1991年4月美国NCSC(国家计算机安全中心)颁布了《可信计算机系统评估标准关于可信数据库系统的解释》(TDI)。
  - TDI又称紫皮书。它将TCSEC扩展到数据库管理系统。
  - TDI中定义了数据库管理系统的设计与实现中需满足和用以进行安全性级别评估的标准。

# TCSEC标准

- TCSEC/TDI标准的基本内容。
  - TCSEC/TDI, 从四个方面来描述安全性级别划分的指标
    - 安全策略
    - 责任
    - 保证
    - 文档

# TCSEC/TDI安全级别划分

高  
↑  
低

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)

# 四组七个等级

- D
  - C (C1,C2)
  - B (B1,B2,B3)
  - A (A1)
- 各安全级别之间具有一种偏序向下兼容的关系，即较高安全级别提供的安全保护要包含较低级别的所有保护要求，同时提供更多或更完善的保护能力。

## ■ D级

- 将一切不符合更高标准的系统均归于D组。
- 典型例子：DOS是安全标准为D的操作系统
- DOS在安全性方面几乎没有什么专门的机制来保障

## ■ C1级

- 非常初级的自主安全保护。
- 能够实现对用户和数据的分离，进行自主存取控制 (DAC)，保护或限制用户权限的传播。
- 现有的商业系统稍作改进即可满足

## ■ C2级

- 安全产品的最低档次。
- 提供受控的存取保护，将C1级的DAC进一步细化，以个人身份注册负责，并实施审计和资源隔离。
- 达到C2级的产品在其名称中往往不突出“安全”(Security)这一特色。
- 典型例子: Windows 2000, Oracle 7

## ■ B1级

- 标记安全保护。“安全”或“可信的”(Trusted)产品。
- 对系统的数据加以标记，对标记的主体和客体实施强制存取控制 (MAC)、审计等安全机制。

## ■ B2级

- 结构化保护
- 建立形式化的安全策略模型并对系统内的所有主体和客体实施DAC和MAC

## ■ B3级

- 安全域
- 该级的TCB必须满足访问监控器的要求，审计跟踪能力更强，并提供系统恢复过程

## ■ A1级

- 验证设计，即提供B3级保护的同时给出系统的形式化设计说明和验证以确信各安全保护真正实现



- CC是在上述各评估准则及具体实践的基础上通过相互总结和互补发展而来的。
  - CC提出了目前国际上公认的表述信息技术安全性的结构：
    - 安全功能要求
      - 用以规范产品和系统的安全行为
    - 安全保证要求
      - 要求解决如何正确有效地实施这些功能
- 都以“类-子类-组件”的结构表述
- 组件是安全要求的最小构件块
- CC的文本组成
  - 简介和一般模型；安全功能要求；安全保证要求。

CC官网: <https://www.commoncriteriaportal.org/>

## ■ CC评估保证级(EAL)划分

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

# 大纲

- 数据库安全性概述
- **数据库安全性控制**
- 视图机制
- 审计 (Audit)
- 数据加密
- 其他安全性保护
- 本章小结

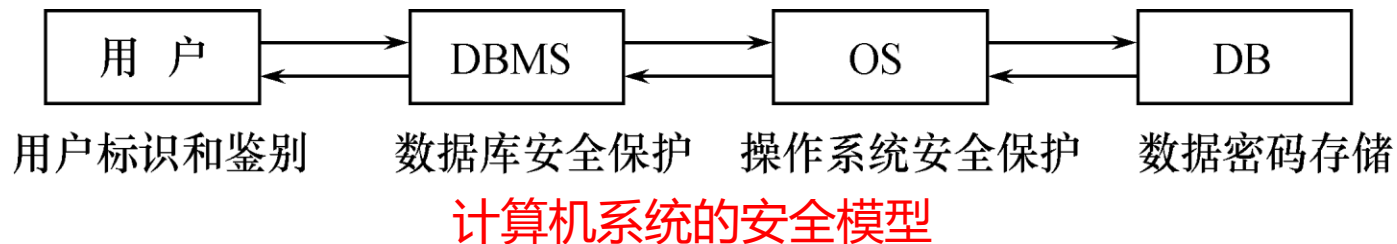
# 数据库安全性控制

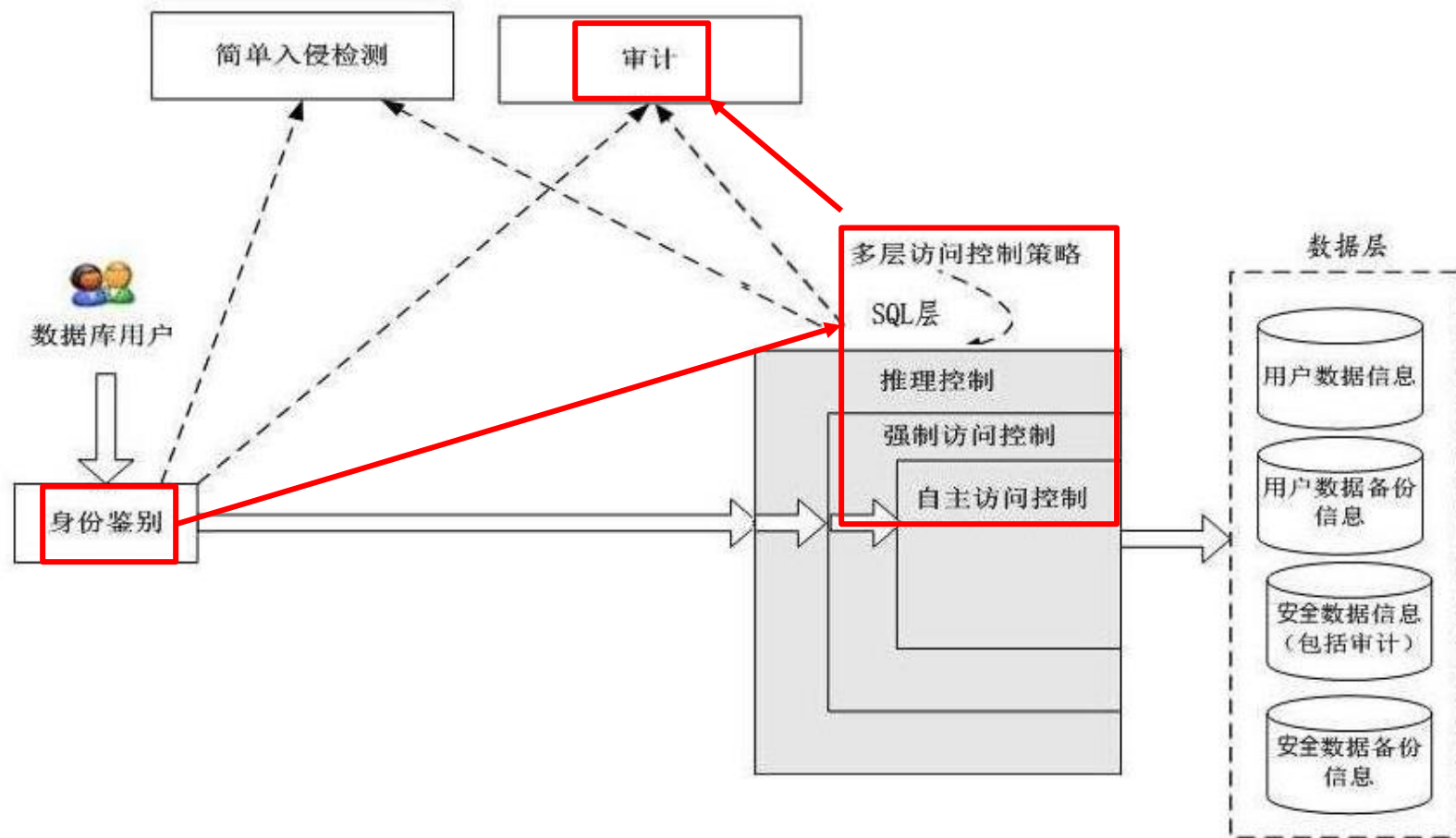
## ■ 非法使用数据库的情况：

- 编写合法程序绕过DBMS及其授权机制
- 直接或编写应用程序执行非授权操作
- 通过多次合法查询数据库从中推导出一些保密数据

## ■ 计算机系统中，安全措施是一级一级层层设置

- 系统根据用户标识鉴定用户身份，合法用户才准许进入计算机系统
- 数据库管理系统还要进行存取控制，只允许用户执行合法操作
- 操作系统有自己的保护措施
- 数据以密码形式存储到数据库中





图：数据库管理系统安全性控制模型

• 存取控制流程：

- ① 首先，数据库管理系统对提出SQL访问请求的数据库用户进行身份鉴别，防止不可信用户使用系统。
- ② 然后，在SQL处理层进行自主存取控制和强制存取控制，进一步可以进行推理控制。
- ③ 还可以对用户访问行为和系统关键操作进行审计，对异常用户行为进行简单入侵检测。

# 数据库安全性控制的常用方法

- **用户标识和鉴别**
- 存取控制
- 视图
- 审计
- 数据加密

# 用户标识和鉴别

- 用户身份鉴别(Identification & Authentication)

- 系统提供的最外层安全保护措施。
- 用户标识：由用户名(user name)和用户标识号(UID)组成。
- 用户标识号在系统整个生命周期内唯一

- 用户身份鉴别方法

- 静态口令鉴别
- 动态口令鉴别
- 生物特征鉴别
- 智能卡鉴别

# 数据库安全性控制的常用方法

- 用户标识和鉴别
- **存取控制**
- 视图
- 审计
- 数据加密



# 存取控制

- 存取控制(Access Control)

- 数据库系统的存取控制机制用于确保只授权给有资格的用户访问数据库的权限，令所有未被授权的人员无法接近数据。

- 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，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(privilege)。
  - 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
  - 用户发出存取数据库操作请求；
  - DBMS查找数据字典，进行合法权限检查

- 用户权限定义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。
- 常用存取控制系统方法：
  - 自主存取控制(Discretionary Access Control , 简称DAC), C2级
    - 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
    - 用户还可以将其拥有的存取权限转授给其他用户
  - 强制存取控制(Mandatory Access Control , 简称MAC), B1级
    - 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

# 自主存取控制之SQL实现(重点)

- 通过 SQL 的GRANT语句和REVOKE语句实现。
- 用户权限组成：
  - 数据对象
  - 操作类型
- 定义用户存取权限：
  - 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

## ■ 关系数据库系统中存取控制对象

关系数据库系统中的存取权限表

对象类型	对象	操 作 类 型
数据库  模式	模式	CREATE SCHEMA
	基本表	CREATE TABLE, ALTER TABLE
	视图	CREATE VIEW
	索引	CREATE INDEX
数据	基本表和视图	SELECT, INSERT, UPDATE, DELETE, REFERENCES, ALL PRIVILEGES
	属性列	SELECT, INSERT, UPDATE, REFERENCES, ALL PRIVILEGES

# 授权：授予与回收

- 权限的授予(Grant)
- 权限的回收(Revoke)

# 1.GRANT命令

## ■ GRANT命令格式:

```
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];
```

– 语义: 将对指定操作对象的指定操作权限授予指定的用户

### 谁能够发出GRANT语句?

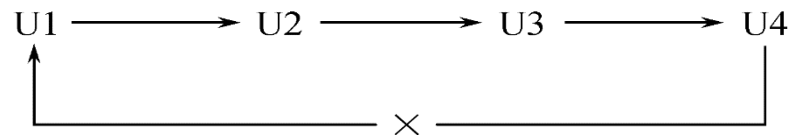
- DBA; 数据库对象创建者(即属主owner);
- 拥有该权限的用户

### 接收权限的用户:

- 一个或多个具体用户;
- PUBLIC(即全体用户)

### WITH GRANT OPTION子句

- 指定了该子句, 则获得权限的用户可以把这种权限再授予其他用户
- 没有指定, 则不能传播已获得的权限
- SQL标准规定不允许循环授权



[例4.1] 把查询Student表权限授给用户U1。

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

[例4.2] 把对Student表和Course表的全部权限授予用户U2和U3。

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

[例4.3] 把对表SC的查询权限授予所有用户。

```
GRANT SELECT ON TABLE SC TO PUBLIC;
```

[例4.4] 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;
```



对属性列的授权时必须明确指出相应属性列名

[例4.5] 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;
```

- 执行例4.5后，U5不仅拥有了对表SC的INSERT权限，还可以传播此权限

[例4.6] U5用户发布以下命令将得到的权限转授给U6。

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

- U6还可以转授该权限给U7

[例4.7] U6转授该权限给U7，但U7不能再传播该权限给其他用户。

```
GRANT INSERT ON TABLE SC TO U7;
```



■ 执行了例4.1~例4.7语句后学生-课程数据库中的用户权限定义表

授权用户名	被授权用户名	数据库对象名	允许的操作类型	能否转授权
DBA	U1	关系Student	SELECT	不能
DBA	U2	关系Student	ALL	不能
DBA	U2	关系Course	ALL	不能
DBA	U3	关系Student	ALL	不能
DBA	U3	关系Course	ALL	不能
DBA	PUBLIC	关系SC	SELECT	不能
DBA	U4	关系Student	SELECT	不能
DBA	U4	属性列Student.Sno	UPDATE	不能
DBA	U5	关系SC	INSERT	能
U5	U6	关系SC	INSERT	能
U6	U7	关系SC	INSERT	不能

## 2.REVOKE命令

### ■ REVOKE命令格式:

```
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];
```

– 语义：由数据库管理员或其他授权者收回已授予的权限

[例4.8] 把用户U4修改学生学号的权限收回。

```
REVOKE UPDATE(SnO) ON TABLE Student FROM U4;
```

[例4.9] 收回所有用户对表SC的查询权限。

```
REVOKE SELECT ON TABLE SC FROM PUBLIC;
```

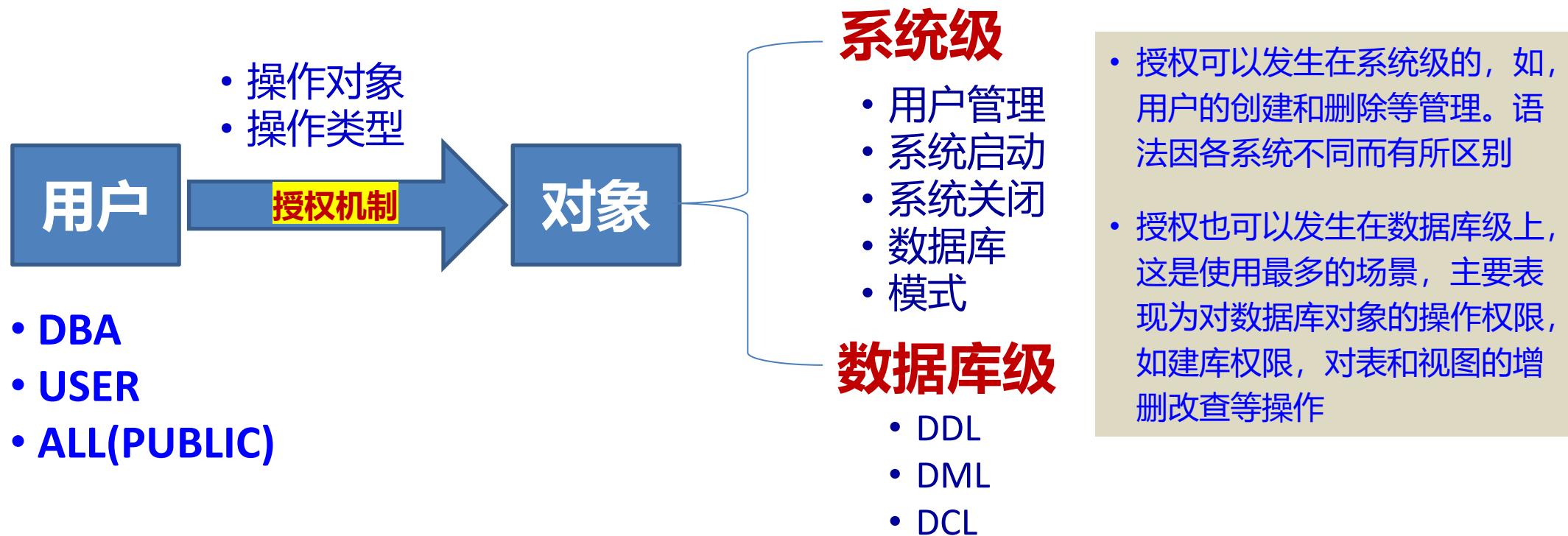
**[例4.10]** 把用户U5对SC表的INSERT权限收回。

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

- 将用户U5的INSERT权限收回的时候应该使用CASCADE，否则拒绝执行该语句
- 如果U6或U7还从其他用户处获得对SC表的INSERT权限，则他们仍具有此权限，系统只收回直接或间接从U5处获得的权限
- **执行例4.8~4.10语句后学生-课程数据库中的用户权限定义表**

授权用户名	被授权用户名	数据库对象名	允许的操作类型	能否转授权
DBA	U1	关系Student	SELECT	不能
DBA	U2	关系Student	ALL	不能
DBA	U2	关系Course	ALL	不能
DBA	U3	关系Student	ALL	不能
DBA	U3	关系Course	ALL	不能
DBA	U4	关系Student	SELECT	不能

# SQL授权小结



- 被授权的用户如果具有“继续授权”的许可，可以把获得的权限再授予其他用户。
- 所有授予出去的权限在必要时又都可用REVOKE语句收回。

## ■ 权限与可执行的操作对照表

拥有的权限	可否执行的操作			
	CREATE USER	CREATE SCHEMA	CREATE TABLE	登录数据库，执行数据查询和操纵
DBA	可以	可以	可以	可以
RESOURCE	不可以	不可以	可以	可以
CONNECT	不可以	不可以	不可以	可以，但必须拥有相应权限

# 数据库角色

- 数据库角色(Role)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
  - 可以为一组具有相同权限的用户创建一个角色
  - 简化授权过程

- 角色创建命令:

CREATE ROLE <角色名>;

- 给角色授权:

GRANT <权限>[,<权限>]... ON <对象类型>对象名 TO <角色>[,<角色>]...;

- 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];
```

- 角色权限的授权语句：把角色授予某用户，或授予另一个角色
- 授予者是角色的创建者或拥有在这个角色上的ADMIN OPTION
- 指定了WITH ADMIN OPTION则获得某种权限的角色或用户还可以把这种权限授予其他角色
- 一个角色的权限：直接授予这个角色的全部权限加上其他角色授予这个角色的全部权限

## ■ 角色权限的回收:

REVOKE <权限>[,<权限>]... ON <对象类型>对象名 FROM <角色>[,<角色>]...;

- 用户可以回收角色的权限，从而修改角色拥有的权限
- REVOKE执行者是
  - 角色的创建者
  - 拥有在这个(些)角色上的ADMIN OPTION

## ■ 角色的删除:

DROP ROLE <角色名>;



## [例4.11] 通过角色来实现将一组权限授予一个用户

– 实现步骤:

- CREATE ROLE R1;
- GRANT SELECT, UPDATE, INSERT ON TABLE Student TO R1;
- GRANT R1 TO 王平,张明,赵玲;
- REVOKE R1 FROM 王平;

## [例4.12] 角色权限的修改: 增加权限

GRANT DELETE ON TABLE STUDENT TO R1;

## [例4.13] 角色权限的修改: 收回权限

REVOKE SELECT ON TABLE STUDENT FROM R1;

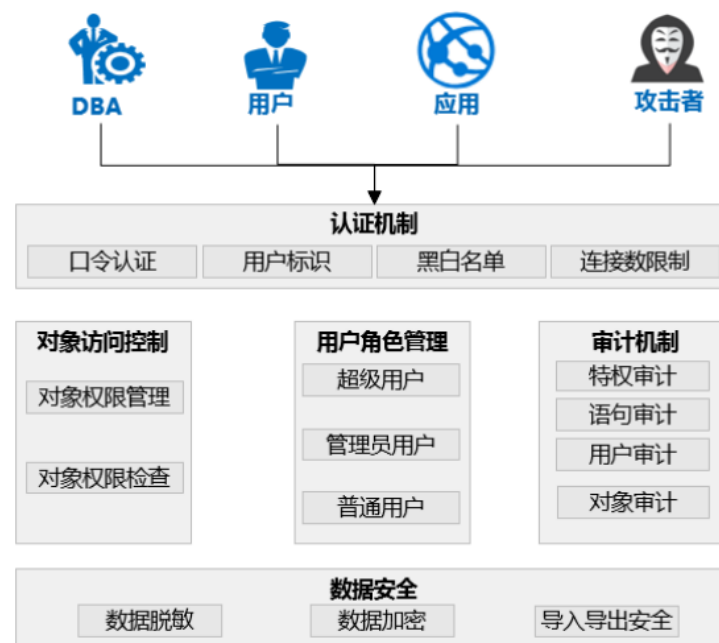
# openGauss的安全机制

## ■ 官网：

<https://www.opengauss.org/zh/docs/3.1.0/docs/CharacteristicDescription/%E6%95%B0%E6%8D%AE%E5%BA%93%E5%AE%89%E5%85%A8.html>

## ■ 网络：

<https://baijiahao.baidu.com/s?id=1722802793849324928>



# openGauss权限的授予与回收

- openGauss支持Grant和Revoke命令实现权限的授予和回收。
- 具体用法详见《openGauss开发者指南》16.13和16.14节。

- **SELECT**

允许对指定的表、视图、序列执行SELECT命令，update或删除时也需要对应字段上的select权限。

- **INSERT**

允许对指定的表执行INSERT命令。

- **UPDATE**

允许对声明的表中任意字段执行UPDATE命令。通常，update命令也需要select权限来查询出哪些行需要更新。SELECT... FOR UPDATE和SELECT... FOR SHARE除了需要SELECT权限外，还需要UPDATE权限。

- **DELETE**

允许执行DELETE命令删除指定表中的数据。通常，delete命令也需要select权限来查询出哪些行需要删除。

## 权限及说明

# 强制存取控制方法

- 自主存取控制缺点：

- 可能存在数据的“无意泄露”。
- **原因**：这种机制仅仅通过对数据的存取权限来进行安全控制，而数据本身并无安全性标记。
- **解决思路**：对系统控制下的所有主客体实施强制存取控制策略。

- 强制存取控制(MAC)

- 保证更高层次的安全性。
- 用户不能直接感知或进行控制。
- 适用于对数据有严格而固定密级分类的部门。

- 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	客体
<u>系统中的活动实体</u> <ul style="list-style-type: none"><li>• DBMS管理的实际用户</li><li>• 代表用户的各进程</li></ul>	<u>系统中的被动实体，受主体操纵</u> <ul style="list-style-type: none"><li>• 文件</li><li>• 基本表、索引、视图</li></ul>

## ■ 敏感度标记(Label)

– 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：

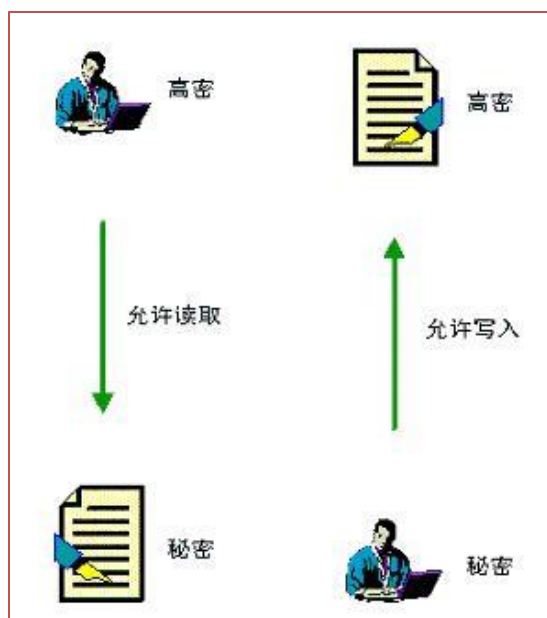
- 绝密(Top Secret, TS)
- 机密(Secret, S)
- 可信(Confidential, C)
- 公开(Public, P)
- $TS \geq S \geq C \geq P$



– 主体的敏感度标记称为**许可证级别**(Clearance Level)

– 客体的敏感度标记称为**密级**(Classification Level)

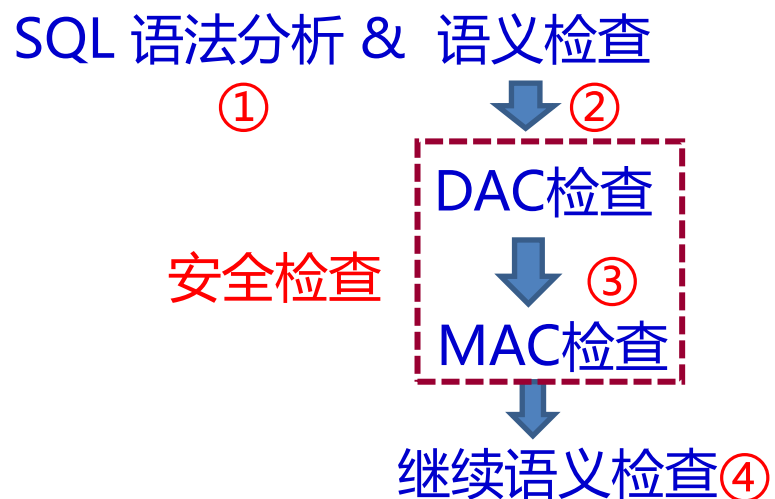
- **Bell-LaPadula(BLP)保密性模型**是第一个能够提供分级别数据机密性保障的安全策略模型，一般应用于军事用途。
- **强制存取控制规则**(课本上介绍的即为BLP保密模型)
  - **上读**：仅当主体的许可证级别大于或等于客体的密级时，该主体才能读取相应的客体
  - **下写**：仅当主体的许可证级别小于或等于客体的密级时，该主体才能写相应的客体



假如一个用户，他的安全级别为“高密”，想要访问安全级别为“秘密”的文档，他将能够成功读取该文件，但不能写入；而安全级别为“秘密”的用户访问安全级别为“高密”的文档，则会读取失败，但他能够写入。这样，文档的**保密性**就得到了保障

参考：<https://blog.csdn.net/ajian005/article/details/8490082>

- 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。
  - 原因: 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
- **DAC+MAC共同构成数据库管理系统的安全机制**



只有通过MAC检查的数据对象方可存取



# 大纲

- 数据库安全性概述
- 数据库安全性控制
- **视图机制**
- 审计(Audit)
- 数据加密
- 其他安全性保护
- 本章小结

# 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

**[例4.14]** 建立计算机系学生的视图，把对该视图的SELECT权限授于王平，把该视图上的所有操作权限授于张明。

```
CREATE VIEW CS_Student  
AS  
SELECT *  
FROM Student  
WHERE Sdept='CS';
```

```
GRANT SELECT ON CS_Student TO 王平;
```

```
GRANT ALL PRIVILEGES ON CS_Student TO 张明;
```

# 大纲

- 数据库安全性概述
- 数据库安全性控制
- 视图机制
- **审计(Audit)**
- 数据加密
- 其他安全性保护
- 本章小结

# 审计

## ■ 什么是审计(Audit)

- 启用一个专用的审计日志，将用户对数据库的所有操作记录在上面
- 审计员利用审计日志，监控数据库中的各种行为，找出非法存取数据的人、时间和内容
- 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

## ■ 审计事件

### — 服务器事件

- 审计数据库服务器发生的事件

### — 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以及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

## ■ 审计功能

### — 基本功能

- 提供多种审计查阅方式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

## ■ Audit和Noaudit语句

- AUDIT语句：设置审计功能
- NOAUDIT语句：取消审计功能

## ■ 用户级审计

- 任何用户可设置的审计
- 主要是用户针对自己创建的数据库表和视图进行审计

## ■ 系统级审计

- 只能由数据库管理员设置
- 监测成功或失败的登录要求、监测授权和收回操作以及其它数据库级权限下的操作

[例4.15] 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;
```

[例4.16] 取消对SC表的一切审计。

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



# 大纲

- 数据库安全性概述
- 数据库安全性控制
- 视图机制
- 审计(Audit)
- **数据加密**
- 其他安全性保护
- 本章小结

# 数据加密

- 数据加密

- 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

- 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)

- 加密方法

- 存储加密
  - 传输加密

## ■ 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

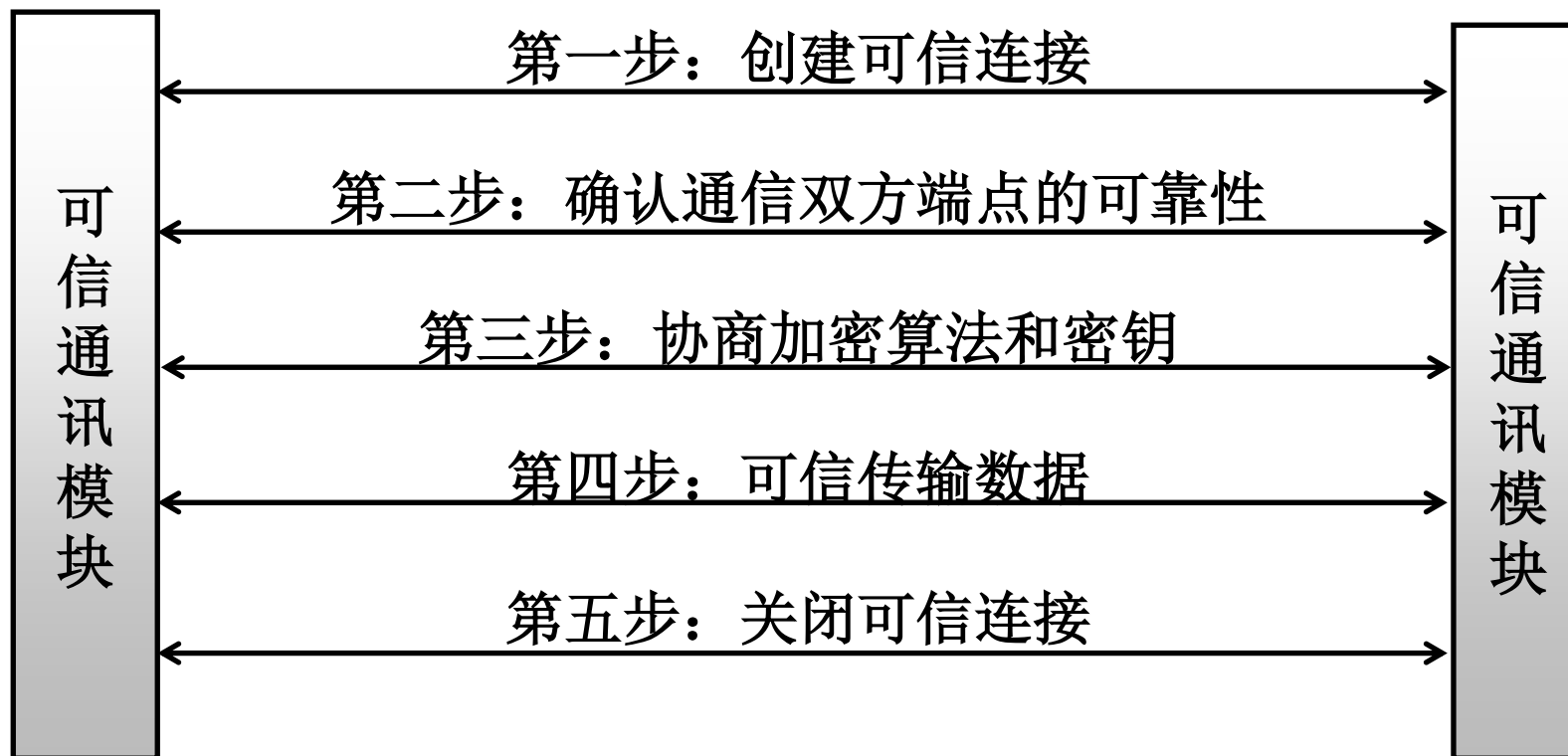
- 在链路层进行加密
- 传输信息由报头和报文两部分组成
- 报文和报头均加密

### — 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



用户



数据库服务器

数据库管理系统可信传输示意图

## ■ 基于安全套接层协议SSL传输方案的实现思路：

### — 确认通信双方端点的可靠性

- 采用基于数字证书的服务器和客户端认证方式
- 通信时均首先向对方提供己方证书，然后使用本地的CA 信任列表和证书撤销列表对接收到的对方证书进行验证

### — 协商加密算法和密钥

- 确认双方端点的可靠性后，通信双方协商本次会话的加密算法与密钥

### — 可信数据传输

- 业务数据在被发送之前将被用某一组特定的密钥进行加密和消息摘要计算，以密文形式在网络上传输
- 当业务数据被接收的时候，需用相同一组特定的密钥进行解密和摘要计算

# openGauss管理数据库的安全

- openGauss管理数据库的安全详见《openGauss开发者指南》第7章。

- 7 管理数据库安全
  - 7.1 客户端接入认证
  - 7.2 管理用户及权限
    - 7.2.1 默认权限机制
    - 7.2.2 管理员
    - 7.2.3 三权分立
    - 7.2.4 用户
    - 7.2.5 角色
    - 7.2.6 Schema
    - 7.2.7 用户权限设置
    - 7.2.8 行级访问控制
    - 7.2.9 设置安全策略
  - 7.3 设置数据库审计
    - 7.3.1 审计概述
    - 7.3.2 查看审计结果
    - 7.3.3 维护审计日志
    - 7.3.4 设置文件权限安全策略
    - 7.3.5 统一审计策略概述
  - 7.4 设置密态等值查询
    - 7.4.1 密态等值查询概述
    - 7.4.2 使用gsq操作密态数据库
    - 7.4.3 使用JDBC操作密态数据库
    - 7.4.4 密态支持函数/存储过程
  - 7.5 设置账本数据库

# 大纲

- 数据库安全性概述
- 数据库安全性控制
- 视图机制
- 审计(Audit)
- 数据加密
- **其他安全性保护**
- 本章小结



# 其它安全性保护

## ■ 推理控制

- 处理强制存取控制未解决的问题。
- 避免用户利用能够访问的数据推知更高密级的数据。
- 常用方法
  - 基于函数依赖的推理控制
  - 基于敏感关联的推理控制

## ■ 隐蔽信道

- 处理强制存取控制未解决的问题

## ■ 数据隐私

- 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。
- 范围很广：数据收集、数据存储、数据处理和数据发布各个阶段

# 本章小结

- 数据的共享日益加强，数据的安全保密越来越重要。
- 数据库管理系统是管理数据的核心，因而其自身必须具有一整套完整而有效的安全性机制。
- 实现数据库系统安全性的技术和方法
  - 用户身份鉴别
  - 存取控制技术：自主存取控制和强制存取控制
  - 视图技术
  - 审计技术
  - 数据加密存储和加密传输

# 课堂练习

- 强制存取控制策略是TCSEC/TDI哪一级安全级别的特色( )  
A.C1                  B. C2                  C. B1                  D. B2
- SQL的GRANT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
- 在MAC机制中，当主体的许可证级别等于客体的密级时，主体可以对客体进行如下操作( )  
A.读取                  B.写入                  C.不可操作                  D.读取、写入
- 在数据库的安全性控制中，授权的数据对象的\_\_\_\_，授权子系统就越灵活。  
A. 范围越小      B. 约束越细致      C.范围越大      D.约束范围大

- 关于DBMS的安全机制，下列说法不正确的是\_\_\_\_\_。
  - A. 强制安全性机制是通过对数据和用户强制分类，从而使得不同类别用户能够访问不同级别的数据
  - B. 当有对DB访问操作时，任何人都被允许访问
  - C. 自主安全性是通过授权机制来实现的
  - D. 推断控制机制是防止通过历史信息或统计信息，推断出不该被其知道的信息，防止通过公开信息推断出私密信息
- 在对用户授予列INSERT权限时，一定要包含对\_\_\_\_\_的INSERT权限，否则用户的插入会因为空值而被拒绝。除了授权的列，其他列的值或者取\_\_\_\_\_, 或者为\_\_\_\_\_。

# 本章作业

- 教材第四章习题：1, 2, 4-11.