第四章 数据库安全性

4.1 计算机安全性概述

4.2 数据库安全性控制（重点）

4.3 视图机制

4.4 审计（自学）

4.5 数据加密（自学）

4.6 统计数据库安全性（自学）

4.1 计算机安全性概述

问题的提出

- 数据库的一大特点是数据可以共享
- 但数据共享必然带来**数据库的安全性**问题

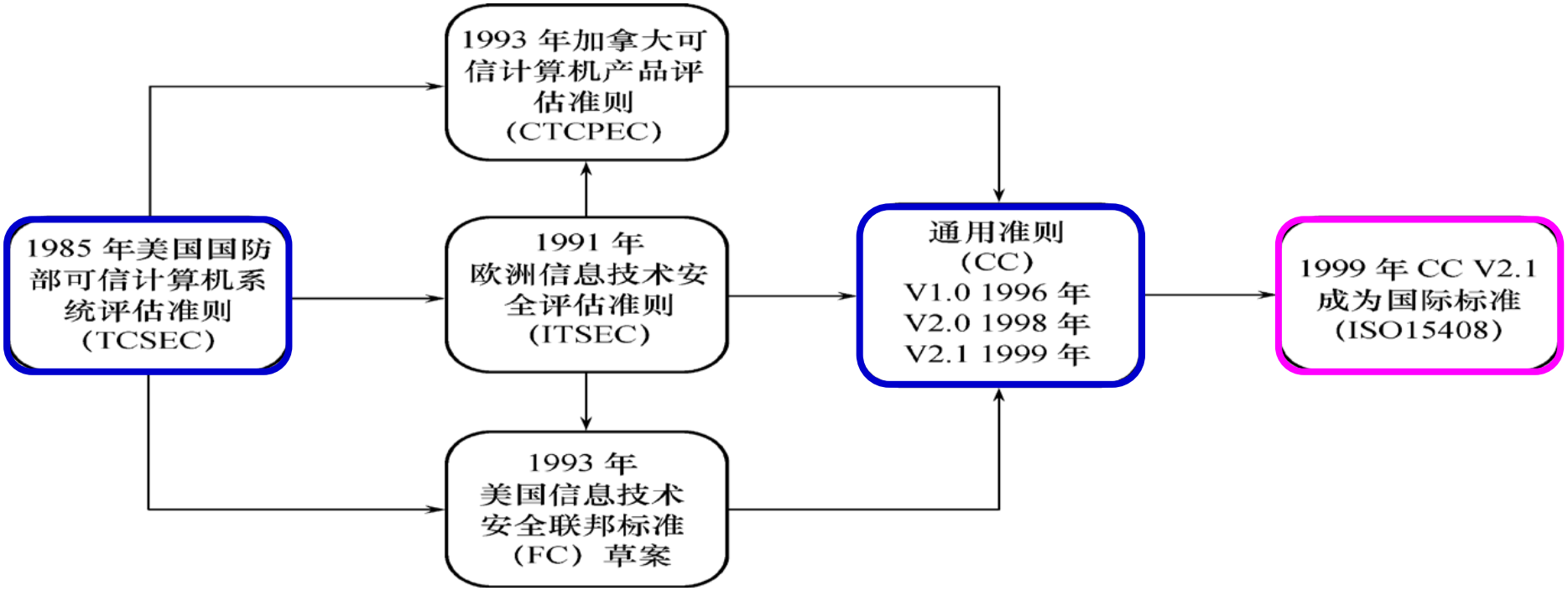
什么是数据库的安全性

- 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。

4.1.2 安全标准简介（了解）

- 计算机系统安全性
  - 为计算机系统建立和采取的各种安全保护措施，保护计算机系统中的**硬件、软件及数据**，防止其因偶然或恶意的原因使系统遭到破坏，数据遭到更改或泄露等。
- 为降低进而消除对系统的安全攻击，各国引用或制定了一系列安全标准。

信息安全标准的发展历史



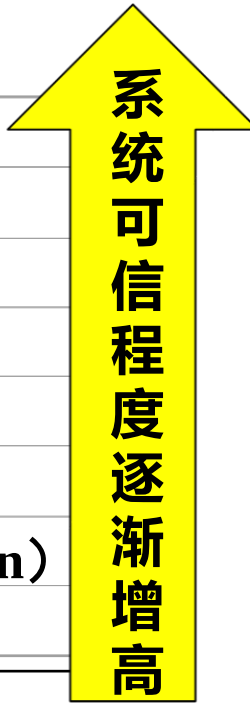
2001年，CC被我国采用为国家标准

4.1.2 安全标准简介

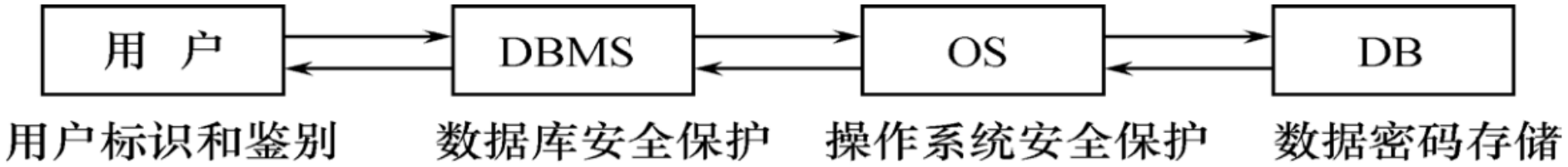
- 1991年美国NCSC（国家计算机安全中心）颁布《可信计算机系统评估标准关于可信数据库系统的解释》(TDI)
  - TDI又称紫皮书。它将TCSEC扩展到数据库管理系统。
  - 定义了数据库管理系统的设计与实现中需满足和用以进行安全性级别评估的标准。

TCSEC/TDI安全级别划分（四组七个等级）

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）



在计算机系统中，安全措施是分层设置的：



计算机系统的安全模型

- 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

4.2.1 用户标识与鉴别

系统提供的最外层安全保护措施

用户标识：用户名

用户鉴别：

① 只有用户知道的信息；

② 只有用户具有的物品；

③ 个人特征。

最常见的用户鉴别：口令，要求长度/不回显

4.2.2 存取控制

□存取控制机制的组成

- ■定义用户权限
  - 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组成了DBMS 的存取控制子系统

4.2.4 授权与回收

关系数据库系统中存取控制对象

对象类型	对象	操作类型
数据	属性列	SELECT，INSERT，UPDATE，REFERENCES，ALL PRIVILEGES
	基本表和视图	SELECT，INSERT，UPDATE，DELETE，REFERENCES，ALL PRIVILEGES
数据库	基本表、视图和索引	CREATE TABLE，ALTER TABLE，CREATE VIEW，CREATE INDEX

4.2.3 自主存取控制（DAC）方法

一、授权

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]

可再转授权限

1.将一种权限授予一个用户

例1.把查询Student表权限授给用户U1。

GRANT SELECT ON TABLE Student TO U1

2.将多种同类对象的权限授予多个用户

例2.把Student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

4.2.4 授权与回收

特殊角色，数据库合法用户都属于该角色

例3.把对SC表的查询权限授予全部用户。

GRANT SELECT ON TABLE SC TO PUBLIC

3.一次完成不同对象的授权

例4.把修改学生学号和查询Student的权限授给用户U2 。

GRANT UPDATE(Sno),SELECT ON TABLE Student TO U2

例5. 把对表SC的INSERT权限授予U5用户，并允许其将此权限授予其他用户。

GRANT INSERT ON TABLE SC TO U5 WITH GRANT OPTION

执行例5后，U5不仅拥有表SC 的INSERT 权限，还可传播此权限

Grant Insert On Table SC To U6 With Grant Option

同样U6可将此权限授予U7

Grant Insert On Table SC To U7

U7不能再传播此权限

二、回收

```
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]
```

例6 将用户U2修改学生学号的权限收回。

```
REVOKE UPDATE(Sno) ON TABLE Student FROM U2
```

例7 收回所有用户对表SC的查询权限 。

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

例8 把用户U5对SC的INSERT权限收回。

级联回收

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

4.2.5 数据库角色

口 自主存取控制方法的缺点

- 可能存在数据的“无意泄露”
- 原因：DAC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：对系统控制下的所有主客体实施强制存取控制策略

如何授予用户查询某些行的权限?

- 为不同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这些数据的用户隐藏起来。

例：假定王平老师只能检索计算机系学生的信息。

（1）建立计算机系学生的视图

```
Create View CS_Student
As Select * From Student Where Sdept='CS'
```

（2）把对该视图的检索权限授予王平

```
Grant Select On CS_Student To 王平
```

作业

《数据库系统概论》P155

7题 第（3）题不做：使用GRANT语句

8题 第（3）题不做：使用REVOKE语句