2026年春季学期

数据库系统概论

An Introduction to Database Systems

第四章 数据库安全性

中国科学技术大学
人工智能与数据科学学院

黄振亚，huangzhy@ustc.edu.cn

计算机系统的安全性

- 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，以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。
    - 技术安全类
    - 管理安全类
    - 政策法律类

复习：数据由DBMS统一管理和控制

- **DBMS提供的数据控制功能**
  - **1. 数据的安全性（Security）保护 （第4章）**

    保护数据，以防止不合法的使用造成的数据的泄密和破坏
  - **2. 数据的完整性（Integrity）检查 （第5章）**

    将数据控制在有效的范围内，或保证数据之间满足一定的关系
  - **3. 数据库恢复（Recovery） （第10章）**

    将数据库从错误状态恢复到某一已知的正确状态
  - **4. 并发（Concurrency）控制 （第11章）**

    对多用户的并发操作加以控制和协调，防止相互干扰而得到错误的结果

数据库安全性

- 问题的提出
  - 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
    - 共享 与 安全
  - 数据库系统中的数据共享不能是无条件的共享

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

第四章 数据库安全性

4.1 数据库安全性概述

4.1.1 数据库不安全因素

4.1.2 安全标准简介

4.1.1 数据库不安全因素

- 对数据库安全性产生威胁的主要因素
  - 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的数据被泄露
  - 安全环境的脆弱
    - 计算机硬件、操作系统、网络系统等

4.1.1 数据库不安全因素

- 1. 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。
  - 数据库管理系统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。

4.1.1 数据库不安全因素

- 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。
  - 数据库管理系统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
- 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

4.1 数据库安全性概述

4.1.1 数据库不安全因素

4.1.2 安全标准简介

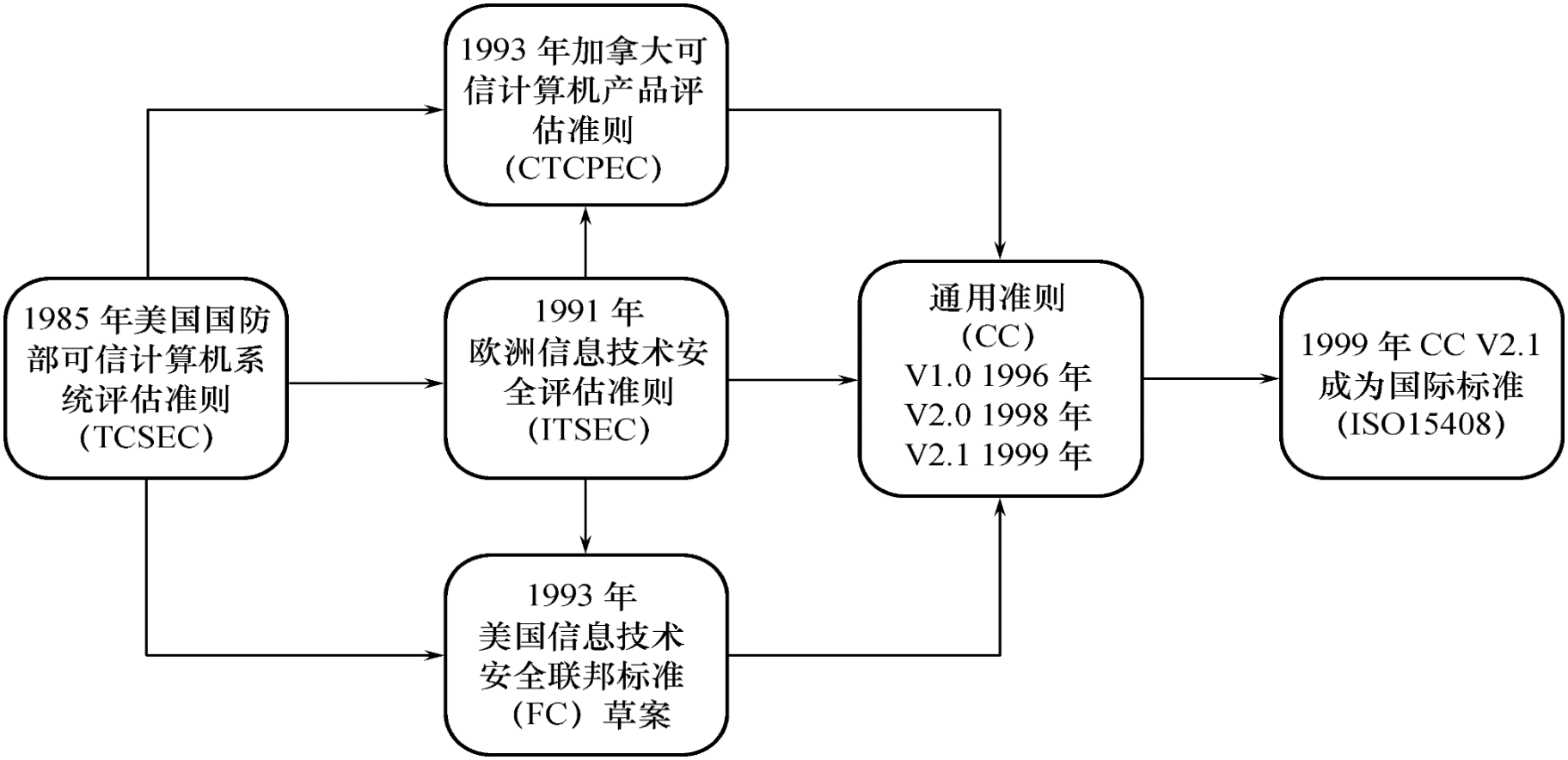
4.1.2 安全标准简介

- 1985年美国国防部（DoD）正式颁布《DoD可信计算机系统评估准则》（简称TCSEC或DoD85）
- 不同国家建立在TCSEC概念上的评估准则
  - 欧洲的信息技术安全评估准则（ITSEC）
  - 加拿大的可信计算机产品评估准则（CTCPEC）
  - 美国的信息技术安全联邦标准（FC）

4.1.2 安全标准简介

- 1993年，CTCPEC、FC、TCSEC和ITSEC联合行动，解决原标准中概念和技术上的差异，称为CC（Common Criteria）项目
- 1999年 CC V2.1版被ISO采用为国际标准
- 2001年 CC V2.1版被我国采用为国家标准
- 目前CC已基本取代了TCSEC，成为评估信息产品安全性的主要标准。

安全标准简介



信息安全标准的发展历史

安全标准简介

- **TCSEC标准**
  - 美国国防部可信计算机系统评估准则
  - 1985年颁布
- **CC标准**
  - 通用准则
  - 2001年成为我国标准

安全标准简介（续）

- **TCSEC/TDI** (Trusted Database Interpretation)**标准的基本内容**
  - 可信计算机系统评估准则关于数据库系统的解释
  - **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

TCSEC/TDI安全级别划分

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）

按系统可靠或可信程度逐渐增高

各安全级别之间：偏序向下兼容

TCSEC/TDI安全级别划分（续）

- 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

TCSEC/TDI安全级别划分（续）

- 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

TCSEC/TDI安全级别划分（续）

- B1级：真正意义上的安全产品
  - 标记安全保护。“安全”（Security）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
  - B1级典型例子
    - 操作系统
      - 惠普公司的HP-UX BLS release 9.09+
    - 数据库
      - Oracle公司的Trusted Oracle 7
      - Sybase公司的Secure SQL Server version 11.0.6

TCSEC/TDI安全级别划分（续）

- B2以上的系统
  - 处于理论研究阶段
  - 应用多限于一些特殊的部门，如军队等
  - 美国正在大力发展安全产品，试图将目前仅限于少数领域应用的B2安全级别下放到商业应用中来，并逐步成为新的商业标准

CC

- **CC (Common Criteria)**
  - **提出国际公认的表述信息技术安全性的结构**
    - **结构开放、表达方式通用**
  - **把信息产品的安全要求分为**
    - **安全功能要求**
      - 信息技术的安全机制所要达到的功能和目的
    - **安全保证要求**
      - 确保安全功能有效并正确实现的措施与手段

CC（续）

- CC文本组成
  - 简介和一般模型
    - 介绍CC中有关的术语、基本概念和一般模型以及与评估有关的框架
  - 安全功能要求
    - 列出了一系列类（11个）、子类（66个）和组件（135个）。
  - 安全保证要求
    - 列出了保证类（11个）、子类（26个）和组件（74个），提出了评估保证级(EAL)

CC（续）

CC评估保证级划分

评估保证级	定　　义	TCSEC安全级别（近似相当）
EAL1	功能测试（functionally tested）	
EAL2	结构测试（structurally tested）	C1
EAL3	系统地测试和检查（methodically tested and checked）	C2
EAL4	系统地设计、测试和复查（methodically designed， tested，and reviewed）	B1
EAL5	半形式化设计和测试（semiformally designed and tested）	B2
EAL6	半形式化验证的设计和测试（semiformally verified design and tested）	B3
EAL7	形式化验证的设计和测试（formally verified design and tested）	A1

第四章 数据库安全性

4.1 数据库安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计（Audit）

4.5 数据加密

4.6 其它安全性保护

4.7 小结

4.2 数据库安全性控制概述

- 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
  - 大数据安全：从数据模型中推导保密数据

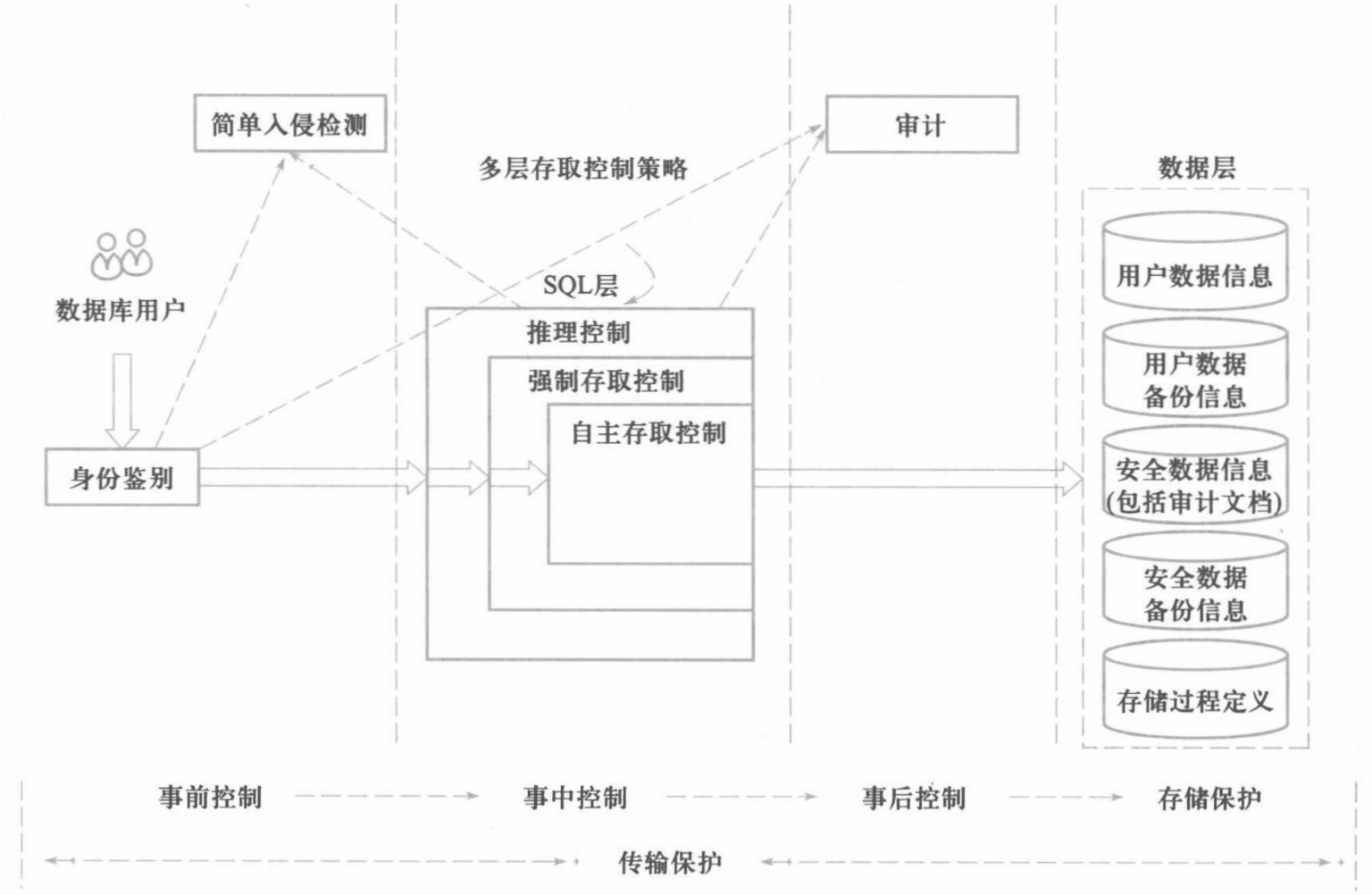
数据库安全性控制概述（续）

- 计算机系统中，安全措施一级一级层层设置

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

数据库安全性控制概述（续）



数据库管理系统安全性控制模型

数据库安全性控制概述（续）

- 存取控制流程
  - 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。
  - 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。
  - 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。

数据库安全性控制概述（续）

- 数据库安全性控制的常用方法
  - 用户身份鉴定
  - 存取控制
  - 视图
  - 审计
  - 密码存储

4.2 数据库安全性控制

4.2.1 用户身份鉴定

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权与收回

4.2.5 数据库角色

4.2.6 强制存取控制方法

4.2.1 用户身份鉴定

- 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：由用户名和用户标识号组成

    （用户标识号在系统整个生命周期内唯一）

用户身份鉴定（续）

- 用户身份鉴别的方法
  - 1.静态口令鉴别
    - 静态口令一般由用户自己设定，这些口令是静态不变的
  - 2.动态口令鉴别
    - 口令是动态变化的，每次鉴别时均需使用动态产生的新口令登录数据库管理系统，即采用一次一密的方法
  - 3.生物特征鉴别
    - 通过生物特征进行认证的技术，生物特征如指纹、虹膜和掌纹等
  - 4.智能卡鉴别
    - 智能卡是一种不可复制的硬件，内置集成电路的芯片，具有硬件加密功能

用户身份鉴定（补充）

- **SQL注入：Web应用最常见的攻击方式之一**

SQL Injection

学校：你好，这里是你儿子的学校，我们遇到了一些计算机问题

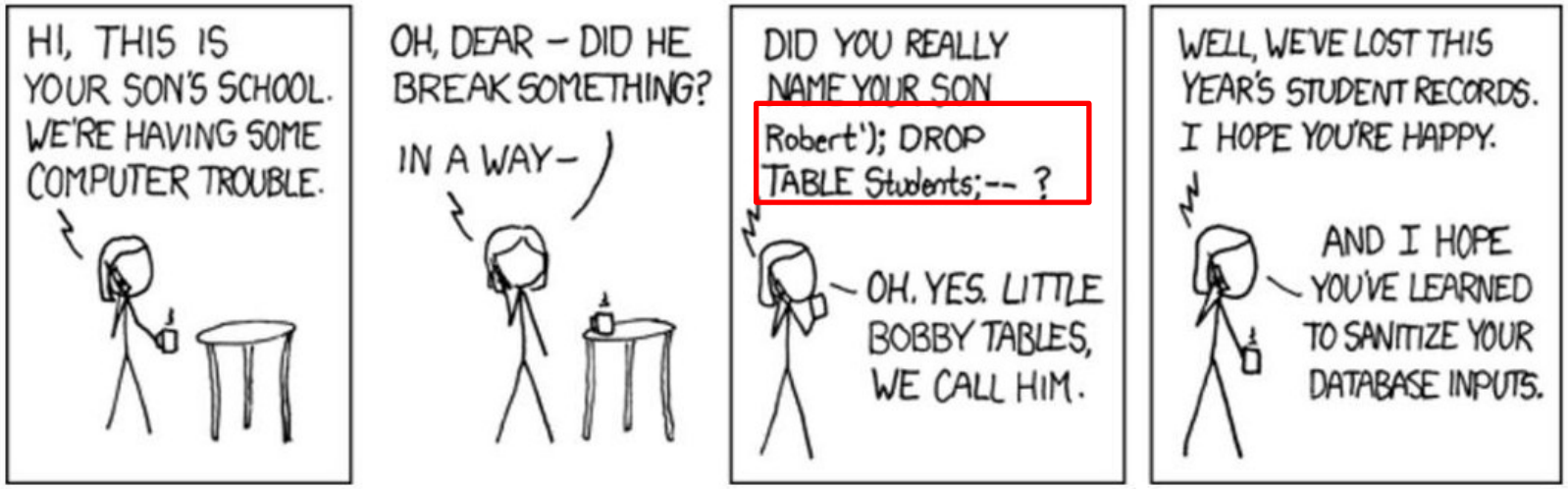
家长：啊这？他搞坏了什么嘛？

学校：你真的给你儿子起名字叫”Robert'); DROP TABLE Student;--”

家长：啊对对对，我们都叫他波比桌子。

学校：好吧，我们丢失了所有的学生数据

家长：希望你们能学会清洗数据库输入



用户身份鉴定（补充）

- 发生什么事了？

绑定$name

Username: Robert Submit

原SQL语句：
SELECT * FROM users WHERE name='{$name}'

$name = "Robert"
SELECT * FROM users WHERE name='Robert'

正常

$name = "Robert'; DROP TABLE Student;--"
SELECT * FROM users WHERE name='Robert' ;
DROP TABLE Student;--'

SQL注入：删库

用户身份鉴定（补充）

- **SQL注入：Web应用最常见的攻击方式之一**
  - **1.思想：**
    - **利用Web应用对用户输入数据的合法性没有判断或过滤不严，在预定义好的查询语句后添加一段数据库查询代码，获得想得知的数据**
  - **2.漏洞在哪？**
    - **Robert’ ; DROP TABLE Student;--**
      - ’使得原本的‘闭合，--注释了后面的’
  - 分类
    - **联合注入、布尔注入、报错注入、时间注入、堆叠注入、二次注入、宽字节注入、cookie注入**

用户身份鉴定（续）

- **3.防御**
  - **最基本：用户口令的要求**
  - **检查变量数据类型和格式**
    - 日期、时间、邮箱、数字型等严格按照固定格式检查
  - **过滤特殊符号**
    - 过滤’ ” \字符中添加反斜杠转义
      - Robert’; DROP TABLE Student;--
      - Robert\’; DROP TABLE Student;--(SQL语句中’{$name}’两个’无法闭合)
  - **绑定变量，预编译语句**
    - 将传入的特殊SQL语句视为字符串执行(不会再编译SQL)
  - **严格管理数据库帐号权限**
    - 避免普通用户增删改查其他用户的资源