数据库系统概论

An Introduction to Database System

第四章 数据库安全性

中国人民大学信息学院

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
  - 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

数据库安全性（续）

- 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。

第四章 数据库安全性

4.1 数据库安全性概述

4.1.1 数据库的不安全因素

4.1.2 安全标准简介

4.1.1 数据库的不安全因素

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。

数据库的不安全因素（续）

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

数据库的不安全因素（续）

3.安全环境的脆弱性

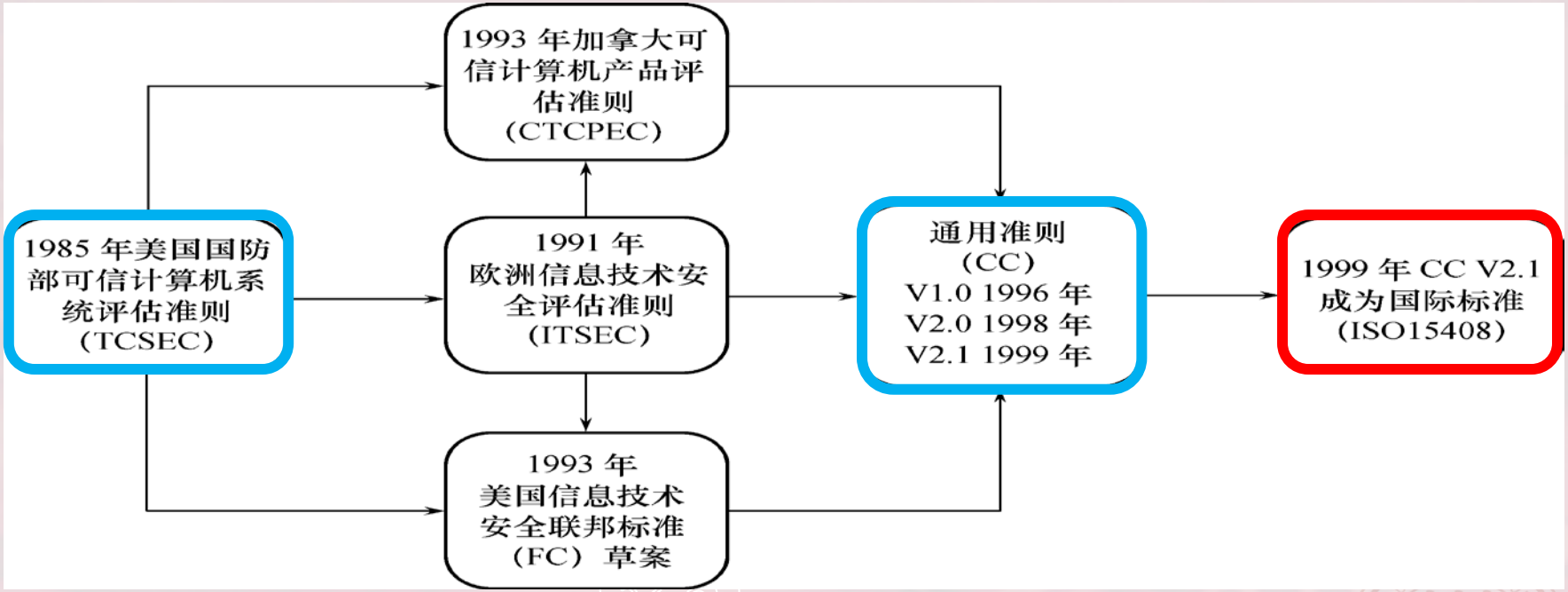
- 数据库的安全性与计算机系统的安全性紧密联系
  - 计算机硬件、操作系统、网络系统等的安全性
- 建立一套可信（Trusted）计算机系统的概念和标准

4.1 数据库安全性概述

4.1.1 数据库的不安全因素

4.1.2 安全标准简介

安全标准简介



信息安全标准的发展历史

安全标准简介（续）

- TCSEC标准
- CC标准

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》（Trusted Database Interpretation 简称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（续）

- **TCSEC/TDI标准的基本内容**
  - 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）

系统可靠或可信程度逐渐增高

TCSEC/TDI安全级别划分（续）

- 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

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
  - 是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 11g

TCSEC/TDI安全级别划分（续）

- B1级
  - 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
      - Sybase公司的Secure SQL Server version 11.0.6

TCSEC/TDI安全级别划分（续）

- 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

TCSEC/TDI安全级别划分（续）

- **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

❖ CC

- 提出国际公认的表述信息技术安全性的结构
- 把信息产品的安全要求分为
  - 安全功能要求
  - 安全保证要求

CC（续）

❖ CC评估保证级（EAL）划分

保证程度逐渐增高

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

小结

- 数据库的不安全因素
  1. 非授权用户对数据库的恶意存取和破坏
  2. 数据库中重要或敏感的数据被泄露
  3. 安全环境的脆弱性
- 安全标准简介
  1. TCSEC标准
  2. CC标准