数据库原理及应用

Principle and Application of Database

华东交通大学
喻佳



存取控制

- 自主存取控制
- 强制存取控制

4.2.2 数据库安全性控制

----- 强制存取控制方法

一、存取控制

管理的方式不同就形成不同的访问控制方式。

自主发出的安全控制-----自主存取控制（Discretionary Access Control——DAC）

由安全策略管理员集中控制-----强制存取控制（Mandatory Access Control——MAC）

一、存取控制

管理的方式不同就形成不同的访问控制方式。

自主存取控制-----商用

强制存取控制-----军用

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）

TCSEC/TDI安全级别划分

安全级别	定　　义
A1	
B3	
B2	
B1	tection）
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）

自主存储控制

商用标准

TCSEC/TDI安全级别划分

安全级别	定　　义
A1	
B3	
B2	
B1	tection）
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）

强制存储控制

军用、政府等标准

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）

尚未实现

强制存取控制(MAC)方法

- MAC----系统为保证更高程度的安全性，按照TDI/TCSEC标准中安全策略的要求，所采取的强制存取检查手段。



- 具体实现方法？

强制存取控制(MAC)方法

1、分类

2、敏感度级别

3、遵循规则

强制存取控制(MAC)方法

1、分类

2、敏感度级别

3、遵循规则

分 类

在MAC中，DBMS所管理的全部实体被分为

主体和客体两大类。

分类

- 主体
- 客体

分类

主体 系统中的活动实体

客体

分类

主体 系统中的活动实体

客体 系统中的被动实体，是受主体操纵的

分类

主体 系统中的活动实体

- 既包括DBMS所管理的实际用户
- 也包括代表用户的各进程

客体 系统中的被动实体，是受主体操纵的

分类

主体 系统中的活动实体

- 既包括DBMS所管理的实际用户
- 也包括代表用户的各进程

客体 系统中的被动实体，是受主体操纵的

- 文件
- 基表
- 索引
- 视图

强制存取控制(MAC)方法

1、分类

2、敏感度级别

3、遵循规则

敏感度级别

敏感度标记被分成若干级别：

绝密(Top Secret)、
机密(Secret)、
可信(Confidential)、
公开(Public)

敏感度级别

敏感度标记被分成若干级别：

绝密(Top Secret)、
机密(Secret)、
可信(Confidential)、
公开(Public)

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）

强制存取控制(MAC)方法

1、分类

2、敏感度级别

3、遵循规则

遵循规则

(1)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。

(2)仅当主体的许可证级别**等于**客体的密级时，该主体才能**写**相应的客体。

规则的**特点**

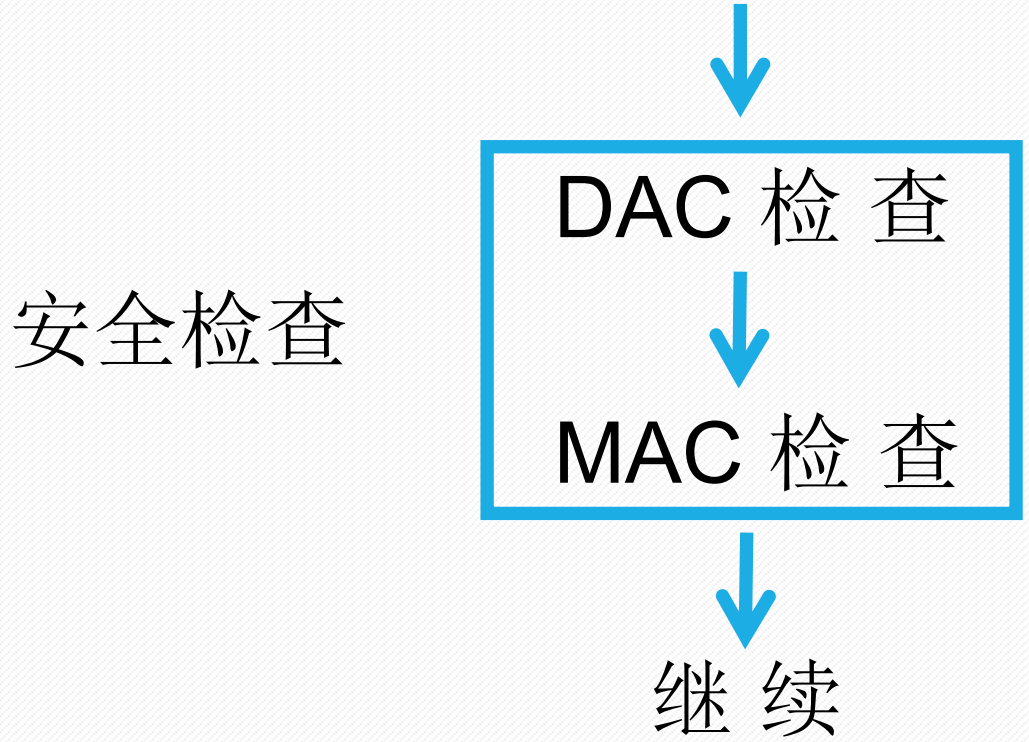
禁止了拥有高许可证级别的主体更新低密级的数据对象

强制存取控制MAC

DAC + MAC安全检查示意图

自主存取控制

SQL语法分析 & 语义检查



小结:强制存取控制MAC

MAC通常用于多级安全军事系统。但对通用、大型系统并不是那么有效。一般强制控制采用以下几种方法：

1、限制控制访问

2、过程控制

3、系统限制

THANK YOU FOR YOUR WATCHING

