第八章 安全模型的原则、设计和功能

8.1 使用安全设计原则实施和管理工程过程

项目开发的早起阶段考虑安全是非常重要的

8.1.1 客体和主体

- 主体：请求访问资源的用户或进程
- 客体：用户或进程想要的访问
- 信任传递：A信任B并且B信任C，则A通过信任传递信任C

8.1.2 封闭式系统和开放式系统

- 封闭式系统被设计用于较小范围内的其他系统协调工作，优点：更安全，缺点：缺乏容易集成的特点
- 开放式系统被设计为使用同一的行业标准

8.1.3 用于确保机密性、完整性和可用性的技术

- 限制：软件设计人员使用进程限制来约束程序的操作，限制仅允许进程在确定的内存地址和资源中读取和写入数据
- 界限：为每一个进程都分配一个授权级别，简单的系统仅两个授权级别，用户和内核，每个进程划分内存逻辑区域，操作系统负责实施逻辑界限不准许其他的进程访问，物理界限通过物理方式隔开，物理界限更贵也更安全
- 隔离：进程隔离能够确保任何行为只影响与隔离进程有关的内存和资源

8.1.4 控制

- 控制使用访问规则来限制主体对客体的访问
- 两种控制：强制访问控制(MAC)和自主访问控制(DAC)
- 自主访问控制与强制访问控制的不同之处在意，主体具有一些定义访问客体的能力
- 访问控制目的：通过组织授权或未经授权的主体的未授权访问，从而确保数据的机密性和完整性

8.1.5 信任与保证

- 安全原则、控制和机制设计和开发之前及期间考虑

8.2 理解安全模型的基本概念

8.2.1 可信计算基（Trusted Computing Base TCB）

硬件、软件和控制方法的组合，形成实施安全控制的可信基准

1. 安全边界
    - 假象的界限，将TCB于系统的其他部分隔开
    - 可信路径：安全边界必须建立安全的通道，被称为可信路径
2. 引用监视器和内核
    - 在准许访问请求之前验证对每种资源的访问的这部分TCB被称为引用监视器
    - 共同工作从而实现引用监视器的TCB中组件的集合被称为安全内核
    - 安全内核的目的是使用适当的组件实施引用监视器的功能和抵抗所有已知的攻击

8.2.2 状态机模型

- 状态机模型描述了一个无论处于何种状态下重是安全的系统
- 安全状态机模型是许多安全模型的基础

8.2.3 信息流模型（BIBA、BLP）

- 信息流模型关注信息流
- Bell-LaPadula的目的是防止信息从高安全级别向点低安全级别流动（上写下读）
- Biba是防止信息从低级别向高安全级别流动（上读下写）
- 信息流模型被设计用于避免未授权的、不安全的或受限的信息流

8.2.4 无干扰模型

- 无干扰模型建立在信息流模型的基础上，关注位于安全级别的主体的动作如何影响系统状态，更高的安全级别上发生的任何操作不会影响在较低级别上发生的操作。

8.2.5 Take-Grant模型

- 采用有向图指示权限如何从一个主体传递至另一个主体或者如何从一个主体传递至一个客体

8.2.6 访问控制矩阵

- 访问控制矩阵：由主体和客体组成的表，表示每个主体可以对每个客体执行的动作或功能

8.2.7 Bell-LaPadula模型（解决机密性问题，下读上写）

- Bell-LaPadula模型防止分类信息泄露或传输至较低的安全许可级别
- Bell-LaPadula专注维护客体的机密性

- Bell-LaPadula模型已状态机概念和信息流模型为基础，采用强制访问控制和格子型概念
- Bell-LaPadula 的三种属性：
  i. 简单安全属性：规定主体不能读取位于较高敏感度级别的信息
  ii. *安全属性，规定主体不能在位于较低敏感度级别的客体上写入信息
  iii. 自主访问控制，规定系统使用访问控制矩阵来实施自主访问控制

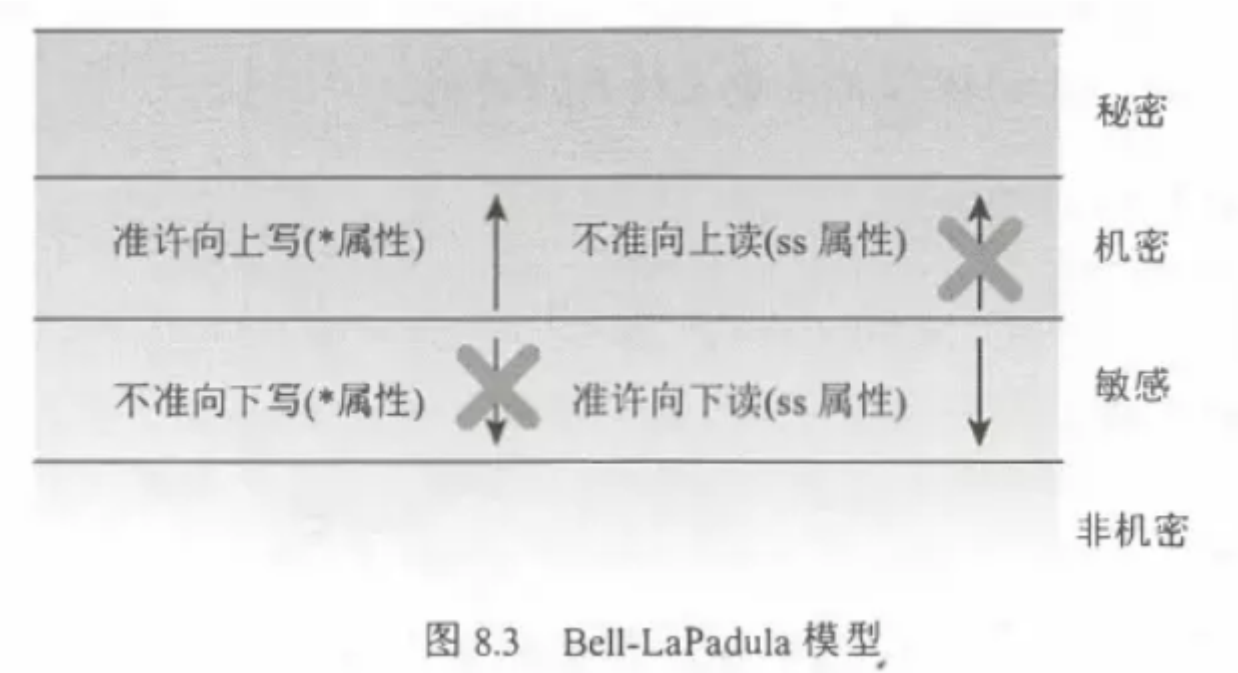
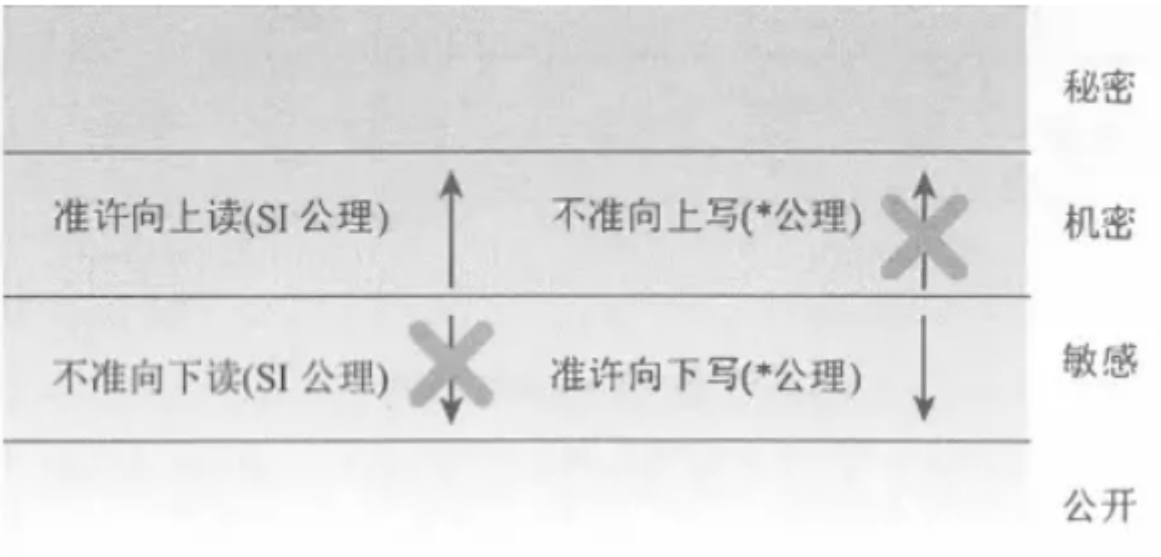


图 8.3 Bell-LaPadula 模型

8.2.7 Biba模型（解决完整性问题，上读下写）

- Biba模型解决完整性问题
- 简单完整性属性：规定主体不能读取位于较低完整性级别的客体(不能向下读)
- *完整性属性，规定主体不能更改位于较高完整性级别的客体（不能向上写）
- Biba模型解决问题：
  - 防止未授权的主体对可以的修改
  - 防止已授权的主体对客体进行未授权的修改
  - 保持内部和外部客体的一致性
- Biba模型的缺陷：
  - 没有解决机密性和可用性问题
  - 没有解决内部威胁
  - 没有说明访问控制管理，也没有提供分配和改变主体或客体分类的方法
  - 没有防止隐蔽通道



8.2.9 Clark-Wilson模型（解决完整性问题）

- 主体 - 程序 - 客体，客体只能通过程序进行访问，通过使用格子良好的事物处理和职责分离提供保护完整性的有效方法
- Clark的优势：
  - 任何用户都不能未授权的修改数据
  - 实现职责分离

8.2.10 Brewer and Nash模型（Chinese Wall）（根据用户行为动态改变访问控制方式、防止利益冲突）

- 准许访问控制基于用户以前的活动而改变

8.2.11 Goguen-Mesegure 模型（预设域或客体列表）

- 基于主体可以访问的预设的域或客体列表

8.2.12 Sutherland模型（解决完整性问题）

- 一个完整性模型，预防对完整性支持的干扰

8.2.13 Graham-Denning模型（主体和客体在创建和删除时的安全性）

- 关注主体和客体在创建和删除时的安全性

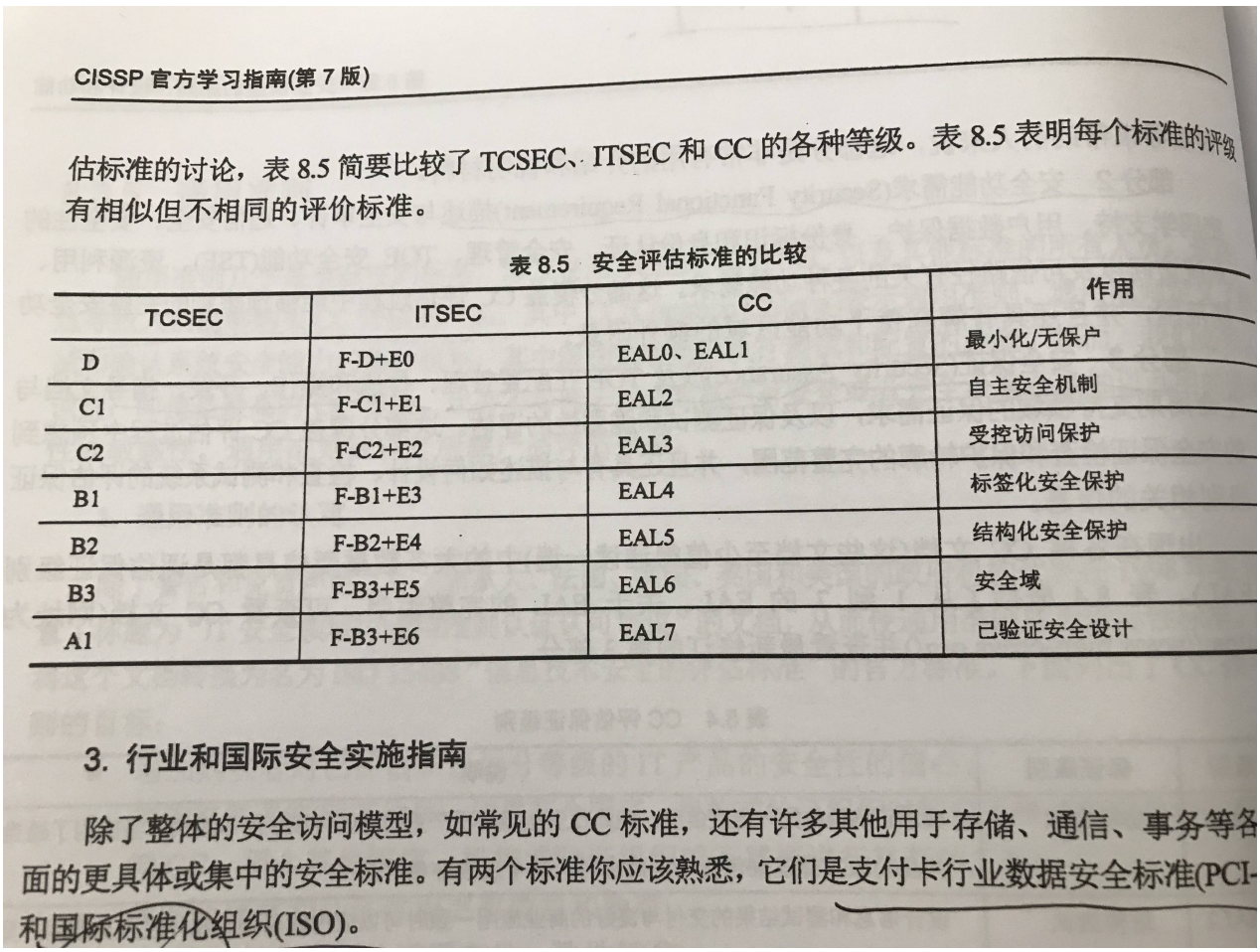
8.3 基于系统安全评估模型选择控制和对策

8.3.1 彩虹系列

- 出现可信计算机系统评估标准（TCSEC），因为封面被称为彩虹系列

8.3.2 TCSEC（橙皮书）分类和所需功能

- TCSEC将系统挺的功能性和机密性保护等级保证组合成4个主要类别
  - 已验证保护，最高的安全级别
  - 强制性保护
  - 自主性保护
  - 最小化保护
- 保护分类（B3与A1是最高级级别，理解为强访问控制）：
  i. 自主性安全保护（C1） 通过用户ID或用户组实现访问控制，对客体访问采取一些控制措施
  ii. 受控访问保护（C2）：用户必须被单独表示后才能获得访问客体的权限，必须实施介质清除措施，限制无效或未授权用户访问的严格登录措施
  iii. 标签式安全（B1）：每个主体和客体都有安全标签，通过匹配主体和客体的安全标签比较他们的权限兼容性
  iv. 结构化保护（B2）：确保不存在隐蔽通道，操作者和管理员职责分离，进程隔离
  v. 安全域（B3）：进一步增加无关进程的分离和隔离，系统关注点转移到简易信，从而减少暴露出来的脆弱性
  vi. 已验证保护（A1）：与B3的差距在于开发周期，开发周期每个阶段都使用正式的方法进行控制



CISSP 官方学习指南(第 7 版)

估标准的讨论，表 8.5 简要比较了 TCSEC、ITSEC 和 CC 的各种等级。表 8.5 表明每个标准的评级有相似但不相同的评价标准。

表 8.5 安全评估标准的比较

TCSEC	ITSEC	CC	作用
D	F-D+E0	EAL0、EAL1	最小化/无保户
C1	F-C1+E1	EAL2	自主安全机制
C2	F-C2+E2	EAL3	受控访问保护
B1	F-B1+E3	EAL4	标签化安全保护
B2	F-B2+E4	EAL5	结构化安全保护
B3	F-B3+E5	EAL6	安全域
A1	F-B3+E6	EAL7	已验证安全设计

3. 行业和国际安全实施指南

除了整体的安全访问模型，如常见的 CC 标准，还有许多其他用于存储、通信、事务等各面的更具体或集中的安全标准。有两个标准你应该熟悉，它们是支付卡行业数据安全标准(PCI-和国际标准化组织(ISO)。

8.3.3 彩虹系列的其他颜色

- 红皮书：应用于为连接网络的独立计算机
- 绿皮书：提供创建和管理密码的指导原则

8.3.4 ITSEC类别与所需的保证和功能性

- TCSEC几乎只关注机密性，ITSEC除了机密性外还关注完整性和可用性
- ITSEC并不依赖TCB的概念，不要求系统的安全组件在TCB内是隔离的
- TCSEC要求发生任何变化的系统都要重新评估

8.3.5 通用准则

通用准则(CC)全球性的标准，定义了测试和确定系统安全能力的各个级别

- 通用准则的认可，**保护轮廓和安全目标**：
  - 保护轮廓PP：指定被评估产品的安全需求和保护。满足特定的消费者需求的，独立于实现的一组安全要求。PP回答“需要什么？”，而不涉及“如何实现？”
  - 安全目标ST：指定通硬伤在TOE内构成的安全申明。依赖于实现的一组安全要求和说明，ST回答“提供什么？”、“如何实现？”
  - 评估目标TOE：IT产品或系统 + 相关的管理指南和用户指南文档。TOE是Common Criteria评估的对象
- 通用准则的结构
  - 部分1：介绍和一般模型描述用于评估IT安全性和指定评估目标设计的一般概念和基础模型
  - 部分2：安全功能描述
  - 部分3：安全保证
- 行业和国际安全实施指南
  - 常见安全标准： CC标准，PCI-DSS（支付行业数据安全标准），国际化标准组织（ISO）

8.3.6 认证和鉴定

- 认证
  - 对IT系统的技术和非技术安全特性以及其他防护措施的综合评估
  - 评估完所有的因素和确定系统的安全级别之后，认证阶段就完成了
- 鉴定
  - 领导层认可，测试和记录具有特定配置的系统的安全能力，认证和鉴定是一个不断重复的过程
- 认证和鉴定系统
  - 认证和鉴定过程的4个阶段：
    a. 定义：项目人员分配、项目需求的记录以及指导整个认证和鉴定过程的同安全许可协议的注册、协商和创建

b. 验证：包括细化SSAA、系统开发活动以及认证分析
c. 确定：细化SSAA，集成系统的认证评估、DAA建议的开发以及DAA的鉴定结果
d. 后鉴定：维护SSAA、系统操作、变更管理以及遵从性验证

8.4 理解信息系统的安全功能

8.4.1 内存保护

- 内存保护是一个核心安全组件，必须对它进行设计和在操作系统中加以实现

8.4.2 虚拟化

- 虚拟化技术被用于在单一系统的内存中运行 一个或多个操作系统

8.4.3 可信平台模块

- 可信平台模块：及时对主板上加密处理芯片的描述，同时也是描述实施的通用名称
- HSM（硬件安全模块）：用于管理/存储数字加密秘钥、加速加密操作、支持更快的数字签名，以及提高身份认证的速度

8.4.4 接口

- 约束接口的目的是限制或制止授权和未经授权用户的行为，是Clark-Wilson安全模型的一种实践

8.4.5 容错

- 容错能力时指系统遭受故障，但持续运行的能力，容错是添加冗余组件