操作系统安全

2-2 操作系统安全模型

中国科学院大学
网络空间安全学院
2018/4/13

中国科学院大学
University of Chinese Academy of Sciences

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

安全策略和安全模型

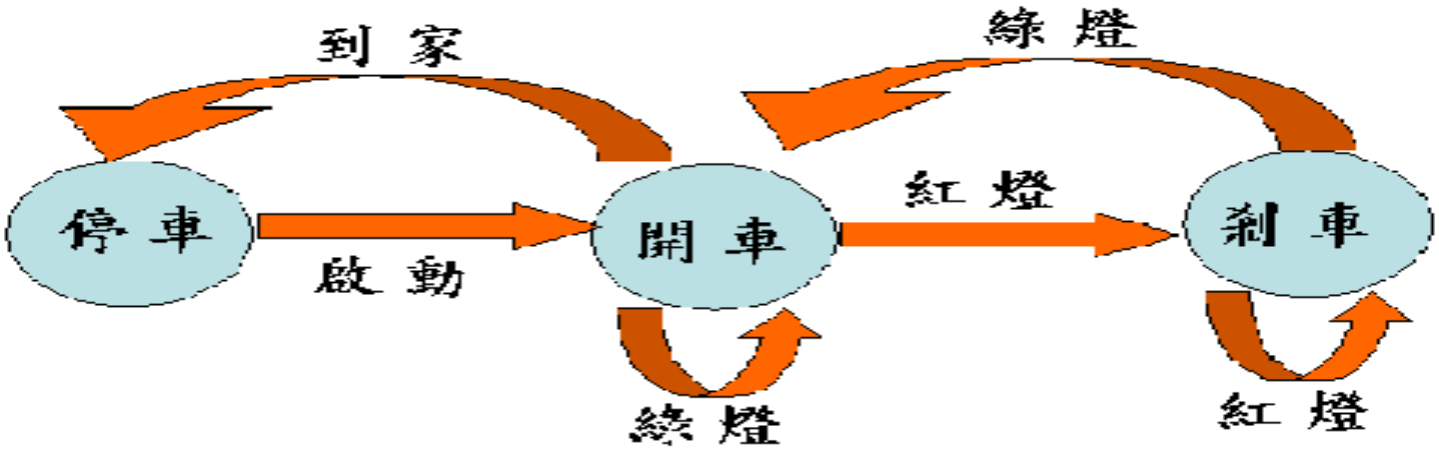
- 安全需求：机密性、完整性、可追究性和可用性
- 安全策略：访问控制策略和访问支持策略
- 安全模型：简单、抽象和无歧义的描述
- 安全模型的目标：明确表达安全需求，为设计开发安全系统提供方针

安全模型的概念及特点

- 安全模型：是对安全策略所表达的安全需求的简单、抽象和无歧义的描述。
- 安全模型的特点：
  - 简单的、清晰的，只描述安全策略，对具体实现的细节不作要求
  - 抽象的、本质的
  - 精确的、没有歧义的
- 安全模型的验证
  - 现有的安全模型大多采用**状态机模拟系统**
  - 形式化方法

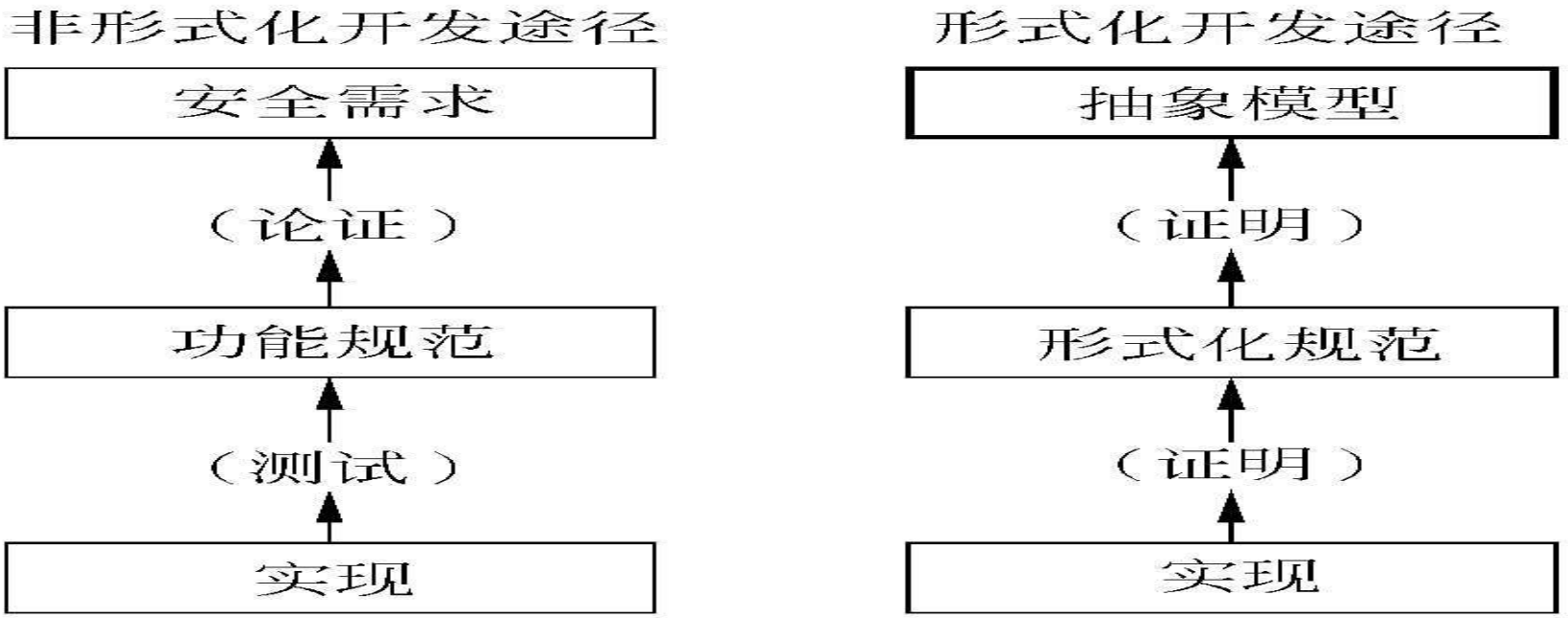
状态机模型

- 状态变量表示系统的状态
- 转换函数或操作规则用以描述状态变量的变化过程
- 可以正确描述状态可以怎样变化和不可以怎样变化



安全模型的开发和验证

- 形式化安全模型：使用数学模型，精确地描述安全性及其在系统中使用的情况
- 非形式化安全模型：仅模拟系统的安全功能，没有严格的数学验证

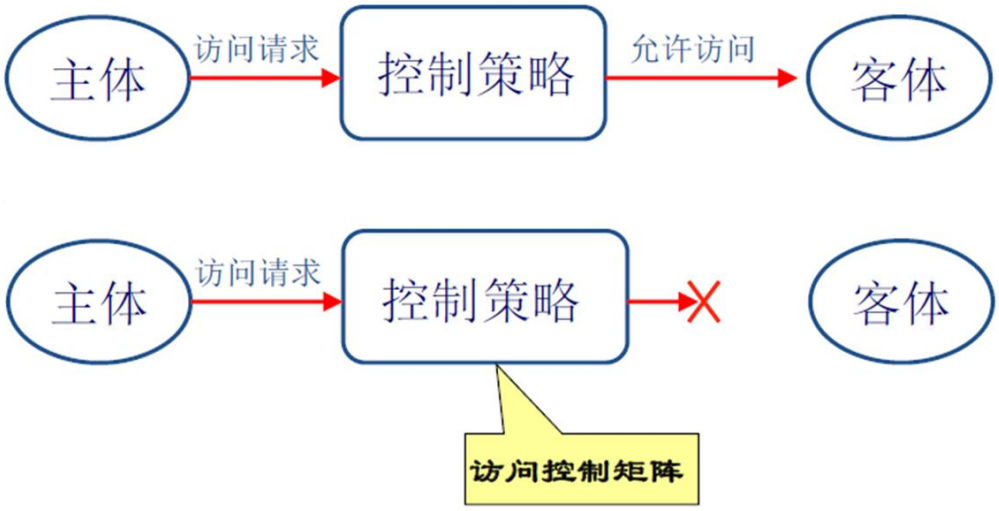


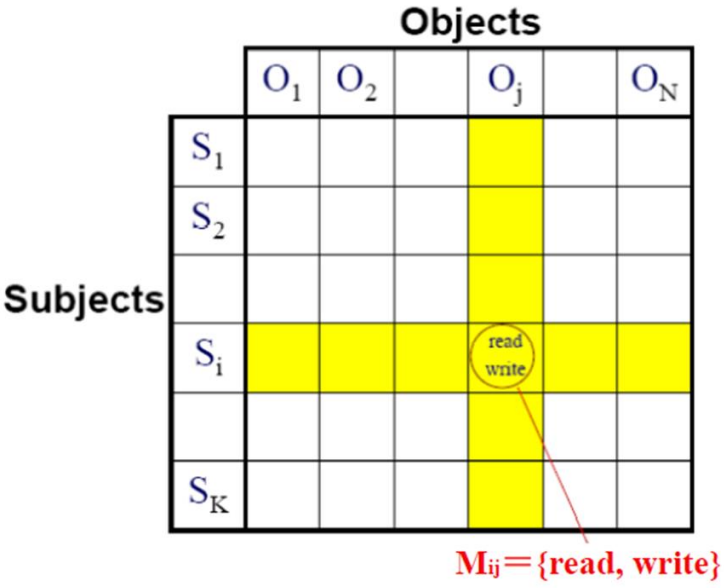
安全模型的分类

- 按实现的方法分类：
  - 访问控制模型
  - 信息流模型
- 按实现的策略分类:
  - ✓ 保密性模型：注重防止信息的非授权泄漏，主要应用于军事（BLP模型）
  - ✓ 完整性模型：注重信息完整性（Biba和Wilson模型）
  - ✓ 混合策略模型：兼顾保密性和完整性（中国墙模型）

访问控制模型

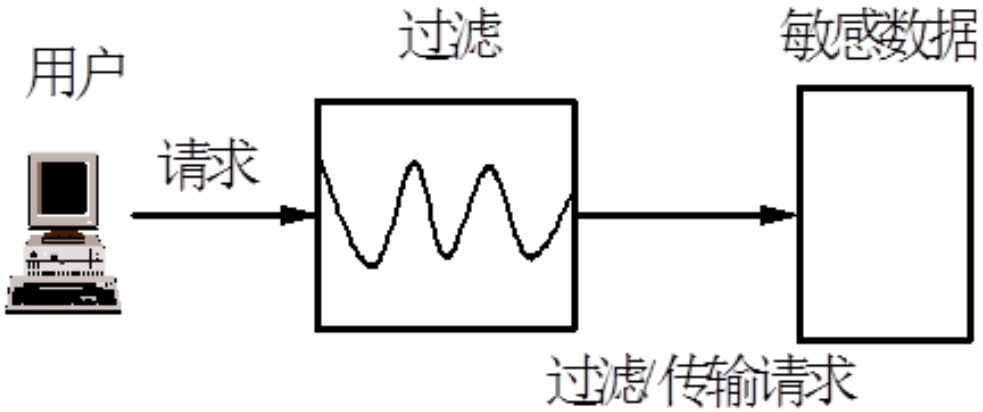
- 访问矩阵模型三要素:
  - 主体：可以对其他实体施加动作的主动实体，简记为S
  - 客体：是主体行为的对象，简记为O
  - 访问权限：访问权限有限集A={ 读，写，执行，追加 }
- 控制策略：主体对客体的操作行为集和约束条件集
- 访问矩阵：主体用行表示，客体用列表示，交叉项表示该主体对该客体所拥有的访问权限





信息流模型

- 控制客体之间的信息传输过程
- 通过分析信息流向**可以发现系统中存在的隐蔽通道**
- 安全规则:在系统状态转换时，信息流只能从访问级别低的状态流向访问级别高的状态
- 信息流模型是基于事件或足迹的模型，注重系统用户可见的行为



机密性模型-BLP

- Bell-LaPadula模型是Bell和LaPadula于1973年提出的对应于军事类型安全密级分类的计算机操作系统模型；
- 是第一个可证明的安全系统的数学模型，实际上是一个形式化的状态机模型；
- 包括有两部分安全策略：自主安全策略和强制安全策略；
- BLP模型采用线性排列安全许可的分类形式来保证信息的保密性
  - ✓ 每个主体都有个安全许可，等级越高，可访问的信息就越敏感
  - ✓ 每个客体都有个安全密级，密级越高，客体信息越敏感
- 基本原理：系统由主体（进程）和客体（数据、文件）组成，主体对客体的访问分为只读（R）、读写（W）、只写（A）、执行（X）及控制（C）几种访问模式，C指主体授予或撤消另一主体对某一客体访问权限的能力。

机密性模型-BLP

- BLP安全模型
  - 敏感标记：指主体或客体的安全标记，是系统进行保密性访问控制的依据，包括等级分类和非等级类别两部分。其中，等级分类指主体或客体的密级，由一个整数代表；非等级类别指主体可以访问的客体范围，由一个集合表示。
  - 权限：指主体对客体的访问操作，比如读写执行等。
  - 属性：指模型的安全性质。
  - 规则：描述模型状态之间的状态转换规则。

机密性模型-BLP

- BLP安全模型的特性
  - 简单安全特性(ss-特性）：如果（主体，客体，可读）是当前访问，那么一定有：

    level（主体）>=level（客体）

    - 其中，level表示安全级别。这个特性表示的是主体只能读取自己的敏感标记可以支配其敏感标记的客体，也就是不上读的特性。

机密性模型-BLP

- BLP安全模型的特性
  - 星号安全特性(*-特性）：在任意状态，如果（主体，客体，方式）是当前访问，那么一定有：
    - 若方式是a，则：level（客体）>=current-level（主体）
    - 若方式是w，则：level（客体）=current-level（主体）
    - 若方式是r，则：current-level（主体）>=level（客体）
  - 其中，current-level表示当前安全级别。它表示的是主体只能写敏感标记支配自己的敏感标记的客体，也就是不下写的特性。

机密性模型-BLP

- BLP安全模型的特性
  - 自主安全特性(ds-特性）：如果（主体-i，客体-j，方式-x）是当前访问，那么，方式-x一定在访问控制矩阵M的元素Mij中。
  - 与ds-特性处理自主访问控制相对应，ss-特性和*-特性处理的是强制访问控制。自主访问控制的权限由客体的属主自主确定，强制访问控制的权限由特定的安全管理员确定，由系统强制实施。

机密性模型-BLP

- BLP安全模型
  - 基本安全定理：如果系统状态的每一次变化都能满足ss-特性、*-特性和ds-特性的要求，那么，在系统的整个状态变化过程汇总，系统的安全性是不会被破坏的。

机密性模型-BLP

- BLP安全模型（下读上写）
  - 依据Bell-Lapadula安全模型所制定的原则是利用不上读/不下写来保证数据的机密性。即不允许低信任级别的用户读高敏感度的信息，也不允许高敏感度的信息写入低敏感度区域，禁止信息从高级别流向低级别。强制访问控制通过这种梯度安全标签实现信息的单向流通。

图：BLP安全模型

机密性模型-BLP

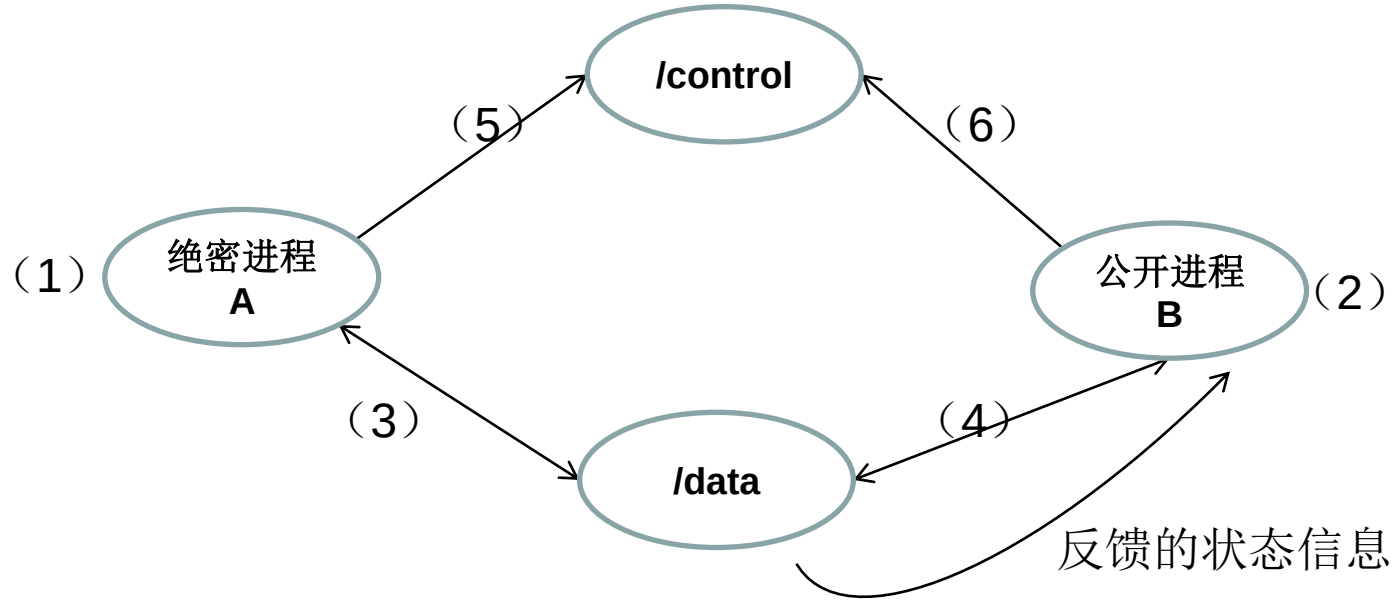
- BLP模型存在的问题
  - 只涉及机密性，而没有涉及完整性
  - 没有解决访问控制的管理问题
  - 包含隐蔽通道

机密性模型-BLP

- 隐蔽通道
  - 隐蔽通道是一个不受安全机制控制的信息流；它违反MAC策略，从高安全等级的主体向低安全等级的主体泄露信息。
    - 隐蔽通道设计两个程序，其中一个必须是特洛伊木马
    - 隐蔽通道通常具有复杂的机制，实现较困难
    - 隐蔽通道利用共享资源作为通信通路。这要求空间共享或时间共享。隐蔽存储通道使用共享资源的属性。隐蔽定时通道使用在对共享资源访问中的时态或排序关系

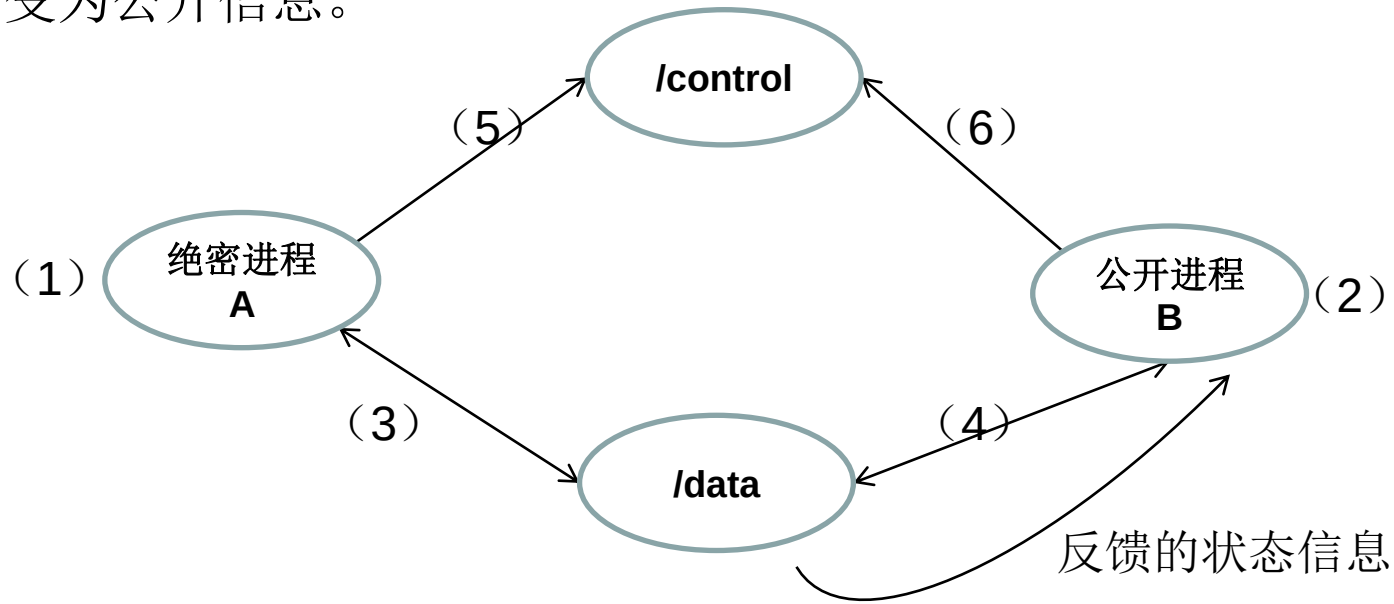
机密性模型-BLP

- BLP安全模型中隐蔽通道举例
  - （1）进程A创建绝密信息文件/data
  - （2）进程B打开文件/control，并写入一个字节。同时进程A一直监控文件/control
  - （3）进程A改变文件/data的DAC存取模式。例若允许进程B写该文件，意味着进程A发送二进制编码1，否则进程要发送二进制编码0



机密性模型-BLP

- BLP安全模型中隐蔽通道举例
  - （4）进程B试图写打开文件/data，则它将得到成功或失败两种结果信息。如果得到的是成功的结果信息，则代表接收了二进制编码1，得到的是失败的信息，则代表接收了二进制编码0
  - （5）进程B每当接收一个二进制编码信息，则将其写入文件/control，进程A则通过检查文件/control的内容，知道信息传递是否正确
  - （6）反复（3）-（5）的动作，直到绝密信息全部从进程A传给进程B，变为公开信息。



完整性模型-Biba

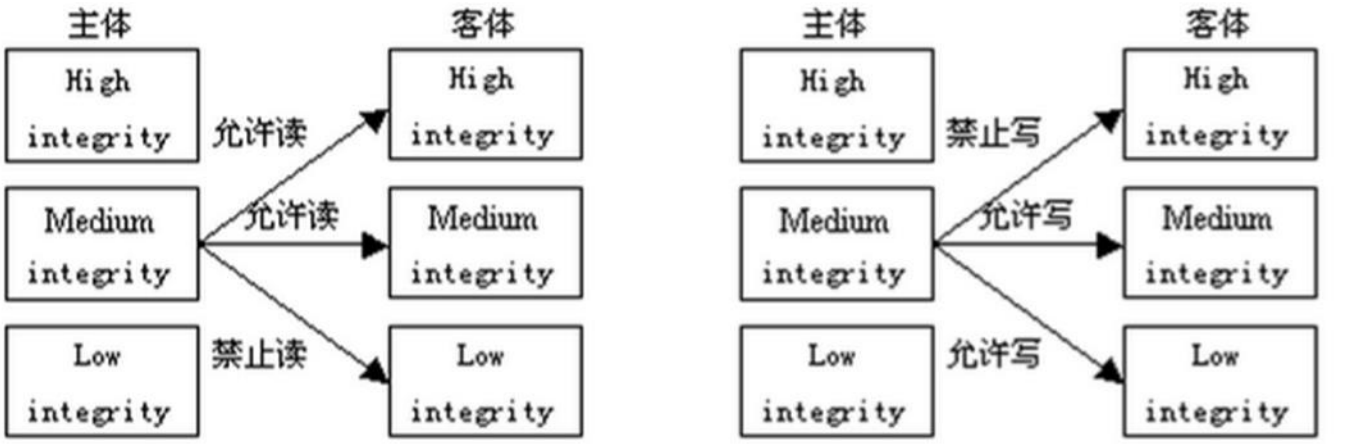
- Biba安全模型（不下读不上写）
  - Biba模型是K.J.Biba于1977年提出的，该模型是第一个涉及到计算机系统中完整性问题的模型。该模型是以完整性级别的有序格为基础的。它支持的是信息的完整性。Biba模型的基本概念就是不允许低完整性的信息流动到高完整性的对象中，只允许信息流以相反的方向流动。
  - 安全策略分为非自主策略与自主策略

完整性模型-Biba

- Biba安全模型（不下读不上写）
  - Biba模型提出了5种不同的用于完整性目的的强制访问控制策略
    - 面向主体的低水标策略
    - 面向客体的低水标策略
    - 低水标完整性审计策略
    - 环策略
    - 严格完整性策略
  - 优点：简单、可能可以和BLP模型相结合
  - 不足之处：
    - 完整标签确定的困难性；
    - 在有效保护数据一致性方面是不充分的；
    - 不能抵御病毒攻击，难以适应复杂应用

完整性模型-Biba

- Biba安全模型（不下读不上写）
  - 依据Biba安全模型所制定的原则是利用不下读/不上写来保证数据的完整性。在实际应用中，完整性保护主要是为了避免应用程序修改某些重要的系统程序或系统数据库。



图：Biba安全模型

完整性模型-Clark-Wilson

- Clark-Wilson完整性模型
  - 1987年David Clark和David Wilson提出的**具有里程碑意义的数据完整性模型**；
  - 核心：良构事务（well-formal transaction）和任务分离机制
    - 良构事务处理机制：用户不能任意处理数据，而必须以确保数据完整性的受限方式来对数据进行处理
    - 任务分离机制：将任务分成多个子集，不同的子集由不同的人来完成。
  - 优点
    - 能有效表达完整性的3个目标
    - 久经考验的商业方法；
  - 局限性
    - 性能问题；
    - 不利于把对数据的控制策略从数据项中分离；
    - 没有形式化；

多安全策略模型

- 中国墙模型：1989年，D.Brewer和M.Nash提出的同等考虑保密性与完整性的安全策略模型，主要用于用于解决商业中的利益冲突；
- 基于角色的存取控制（RBAC）模型提供一种强制存取控制机制；经过发展，已经形成了RBAC0-RBAC3的家族系列；
- DTE（Domain and type enforcement）模型由域定义表和域交互表组成，依据主体域和客体类型来决定访问权限。

谢谢！