操作系统安全

Operating System Security

[第2次课]安全操作系统理论

授课教师：涂碧波

授课时间：2024年3月8日

引题


女性
起居：晚12点-早7点
喜欢瑜伽/常慢跑
居住地 北京
家有孩子 幼儿期
80后 白领
常看电影
常去星巴克
喜欢 兰蔻
常去上海
爱打扮
宾馆：中高档
炒股
中国移动4G 高流量用户
使用银行：工行
喜欢海淘常手机支付
自有住房/还贷中
喜欢做菜
爱看美剧
在学车
关注时尚
关注可穿戴设备
作息规律
注重品质
生活健康
爱尝试新鲜事物
小资

安全操作系统理论

- 安全基础
  - 基本概念
  - 安全设计
- 安全模型
  - 安全模型的概念
  - 安全模型的分类
- 安全测评
  - 操作系统安全测评概念及技术
  - 安全测评的标准
    - TCSEC
    - CC
    - 等保
- 安全体系结构
  - 安全体系结构
  - Flask安全体系结构
  - 权能体系结构
  - 可信计算体系结构
- 安全机制
  - 标识与鉴别
  - 访问控制
  - 安全审计
  - 可信路径

[第2次课]安全操作系统理论

内容概要

01 安全基础

02 安全模型

03 安全测评

安全操作系统的基本概念

- 可信定义
  - 安全流派(Trusted Computing)：一个实体是可信的，如果它的行为总是以所期望的方式，达到预期的目标
  - 容错流派(Dependable Computing):从用户的角度看，计算机系统所提供的服务是可信赖的，而且这种可信赖是可论证的。
  - 微软流派(Trustworthy Computing)：一种可以随时获得的可靠安全的计算，并包括人类信任计算机的程度，就像使用电力系统、电话那样自由、安全。

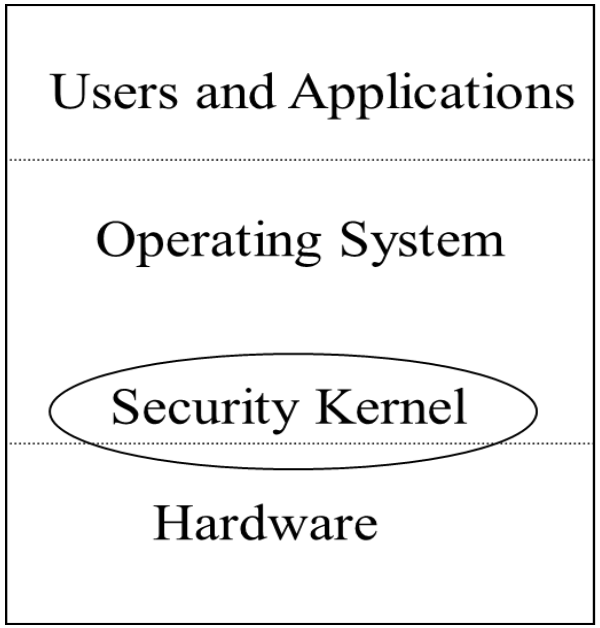
- **可信≈安全+可靠**
- 可信计算机系统是能够提供可信计算服务的计算机软硬件实体，它能够提供系统的可靠性、可用性、主体行为与信息的安全性。

安全操作系统的基本概念

- **系统**：实施计算和通信环境的全体
  - 系统安全的范畴？
- **系统边界**：系统内部得到保护
  - 攻击面
  - 安全威胁模型
  - 边界安全：FW/IDS/GW
- **安全周界**
  - 系统内部安全功能组件与非安全功能组件的边界

安全操作系统基本概念

- 安全内核
  - 指系统中与安全性实现有关的部分：引用监控器
  - 引用验证机制、访问控制机制、授权机制、授权管理机制



- 可信计算基（Trust Computing Base）
  - 组成：操作系统安全内核，具有特权的程序和命令、处理敏感信息的程序、与TCB实施安全策略有关的文件

安全操作系统的基本概念

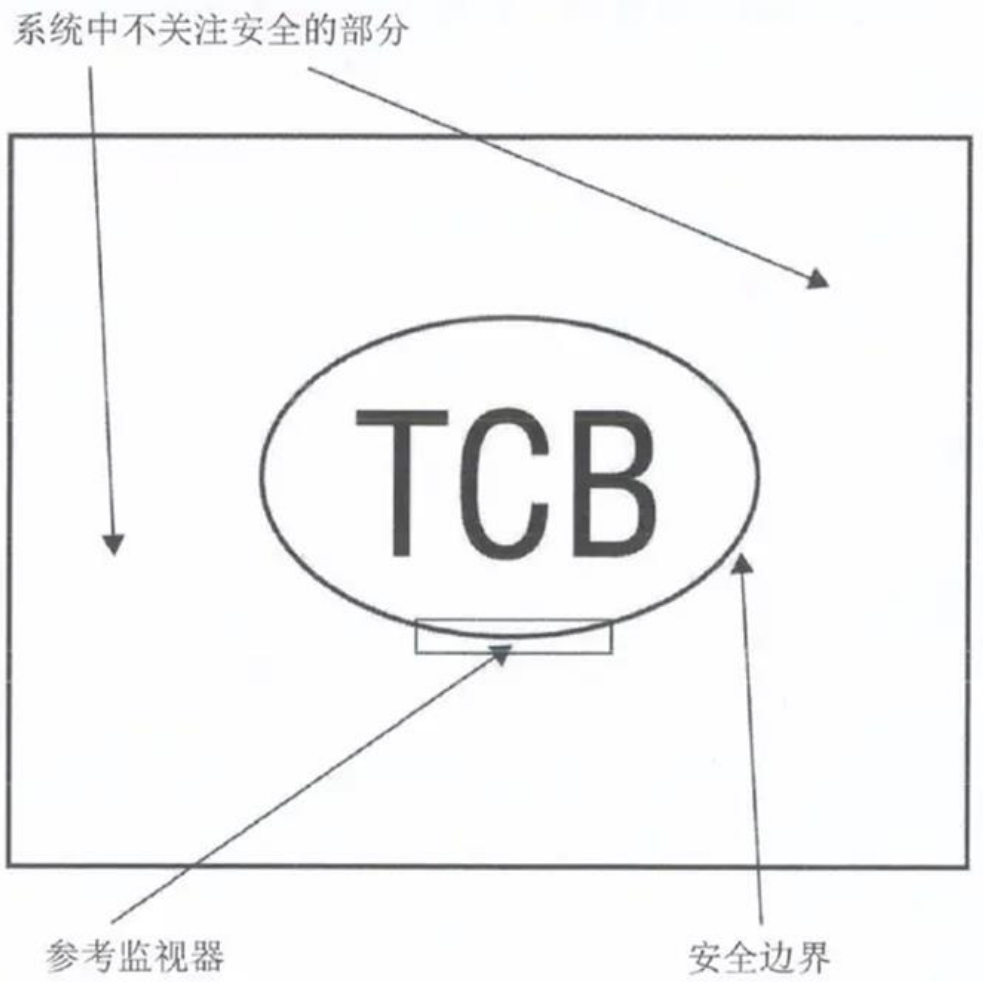
- 主体与客体：操作系统中，每一个实体组件都必须或者是主体、或者是客体，或者既是主体又是客体。
- 主体（Subject）：一个主动的实体
- 客体（Object）：一个被动的实体

安全操作系统的基本概念

- 安全功能与安全保证：**安全性的两个要素**
  - 安全功能：应对威胁、风险的操作系统提供安全功能（安全策略和安全机制的体现）
  - 安全保证：安全功能的确信度
  - 安全强度：？

思考

- 引用监控器、安全内核、可信基
- 可信基、可信软件



安全目标

- 安全操作系统的主要目标：
  - 标识系统中的用户并进行身份鉴别；
  - 依据系统安全策略对用户的操作进行存取控制，防止用户对计算机资源的非法存取；
  - 监督系统运行的安全性；
  - 保证系统自身的安全性和完整性。

构建安全的基本要素

策略: 描述安全
做什么?

机制: 实现安全
怎样去做?

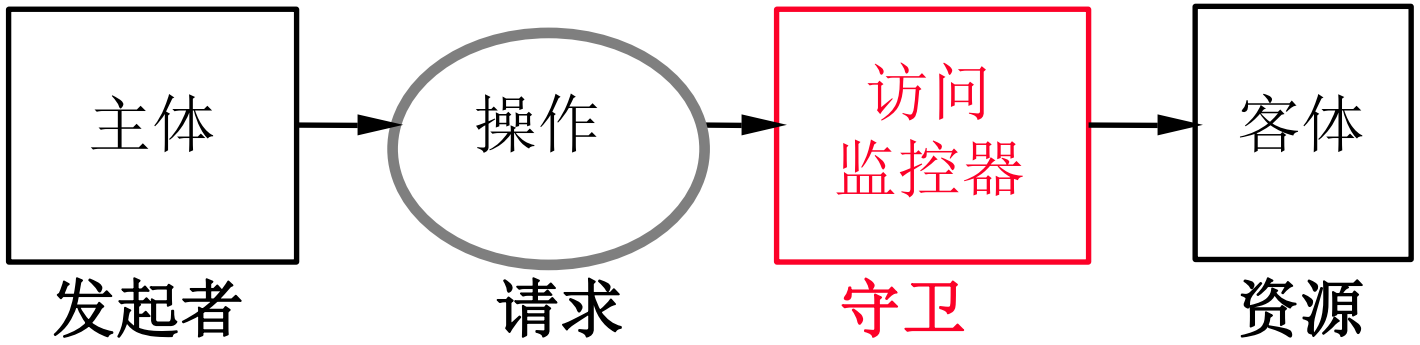
保证: 安全的正确性
是否有效?

为了实现这些目标，需要建立相应的安全机制，包括硬件安全机制、标识与鉴别、存取控制、最小特权管理、可信路径和安全审计等

安全操作系统一般包括两层意思：一是操作系统在设计时通过权限访问控制、信息加密性保护、完整性鉴定等一些机制实现的安全；二是操作系统在使用中通过一系列的配置，保证操作系统尽量避免由于实现时的缺陷或是应用环境因素产生的不安因素。只有通过这两方面的同时努力，才能最大可能地建立安全的操作环境。

策略：访问控制模型

- 守卫控制对有用资源的访问.



机制：通用准则（4A）

Account

鉴别/认证 Authentication

授权 Authorization

审计 Auditing

保证 Assurance

可信计算基

保证:使安全发挥作用

- 可信计算基（Trusted Computing Base，TCB）
  - 规定为确保安全什么必须工作
    - 理想状态下 TCB小且简
  - 包括硬件和软件
  - 还包括配置, 常被忽略
    - 什么软件有特权
    - 用户、口令、特权、组等的数据库
    - 网络信息 (可信主机, ...)
    - 对系统资源的访问控制
    - . . .

安全机制设计原则

- 经济性原则（Economy of Mechanism）：安全机制设计尽可能简单短小，从而在排查缺陷、检测漏洞时代码更容易处理
- 默认拒绝原则（Fail-Safe Defaults）：只要没有授权的信息就不允许访问，不能出现本该允许的请求被拒绝，与本该拒绝的请求被允许
- 完全仲裁原则（Complete Mediation）：授权检查覆盖任何一个访问操作，安全机制有能力标识每一个访问操作请求的所有源头
- 开放设计原则（Open Design）：不将安全机制的设计作为秘密，不将系统安全性寄托在保守安全机制设计秘密的基础上
- 特权分离原则（Separation of Privilege）：细分特权，分配给多个主体，减少每个特权拥有者的权利：
- 最小特权原则（Least Privilege）：每个程序和每个用户应该只拥有完成工作所需特权的最小集合限制由意外或错误所引起的破坏将特权程序之间的潜在交互数降低到正确操作所需的最小值，尽量避免非经意、不必要、不恰当的使用特权
- 最少公共机制原则（Least Common Mechanism）：将多个用户公用或被全体用户依赖的机制数量降到最少
- 心理可接受原则（Psychological Acceptability）：安全机制的良好交互性、安全机制、安全目标的吻合性

出处：https://blog.csdn.net/AIMINdeCSDN/article/details/105011561

内容概要

01 安全基础

02 安全模型

03 安全测评

安全策略和安全模型

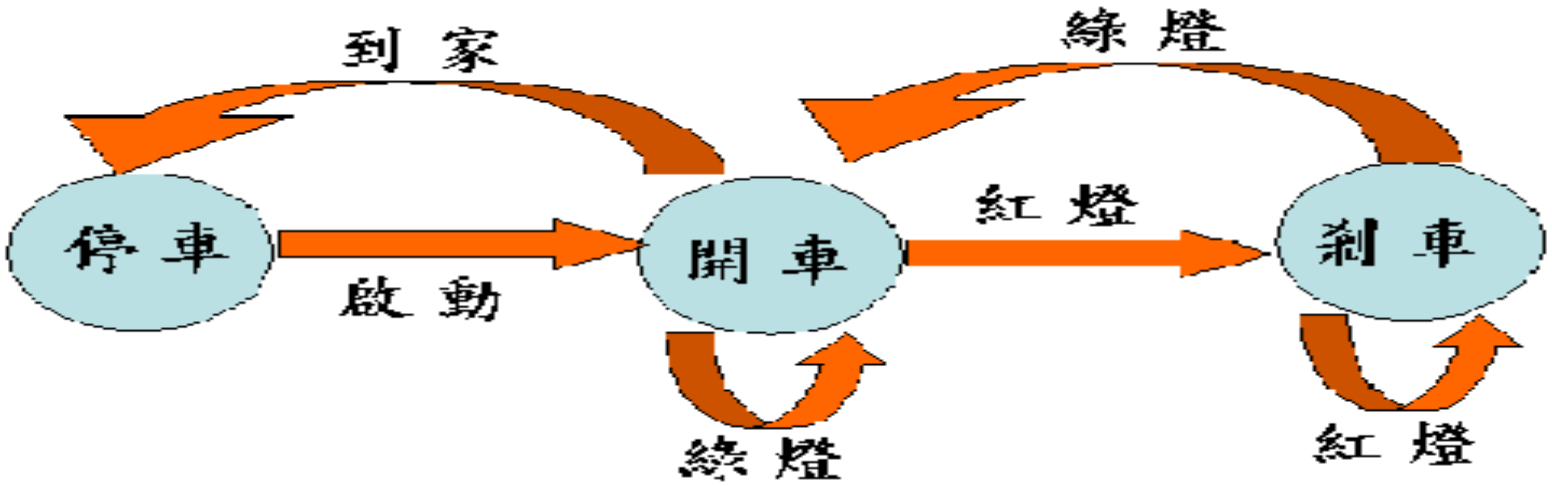
- 安全需求：机密性、完整性、可追究性和可用性
- 安全策略：访问控制策略和访问支持策略
- 安全模型：简单、抽象和无歧义的描述
- 安全模型的目标：明确表达安全需求，为设计开发安全系统提供方针

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

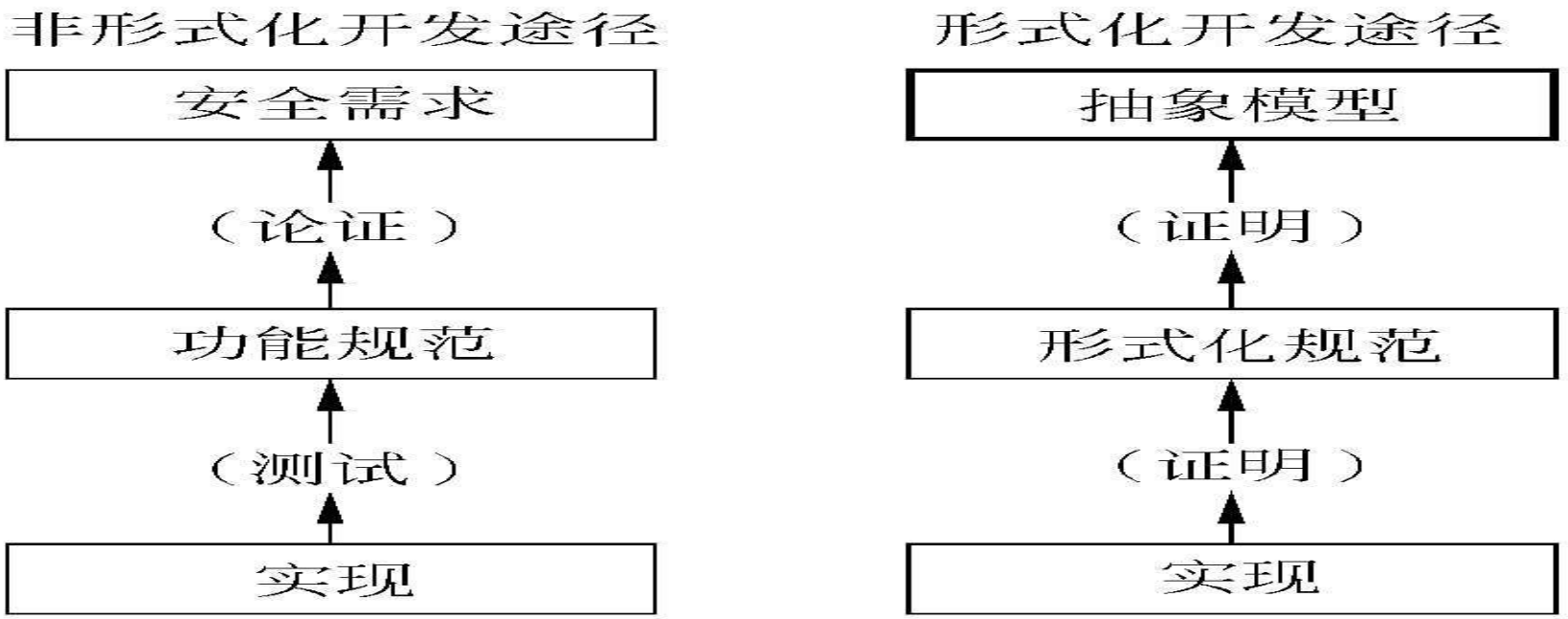
状态机模型

- 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

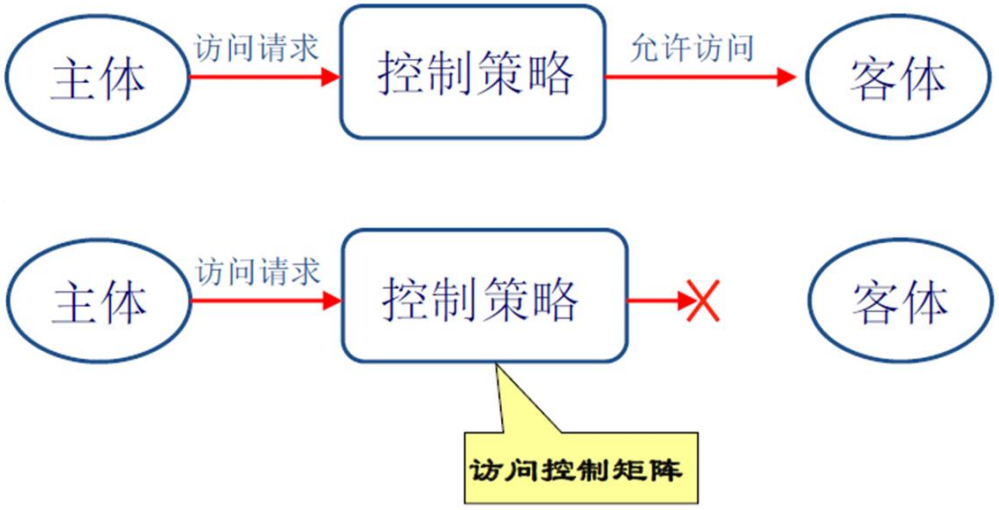


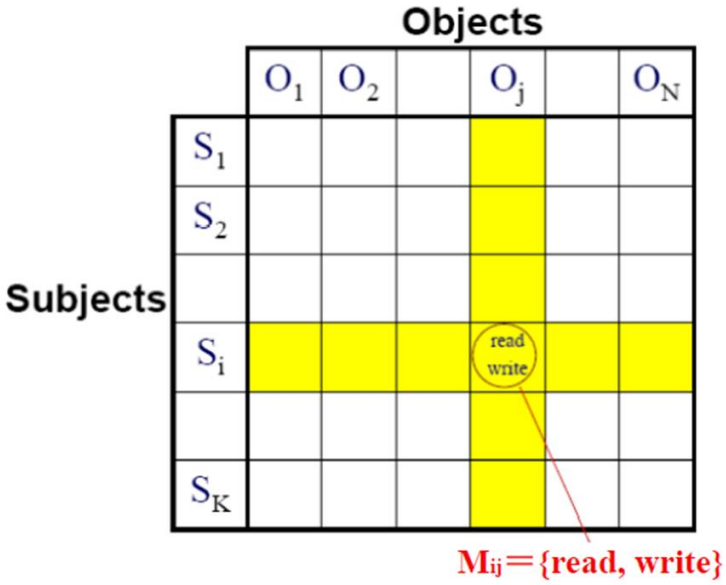
安全模型的分类

- 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:
  - 机密性模型：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：兼顾机密性和完整性（中国墙模型）

访问控制模型

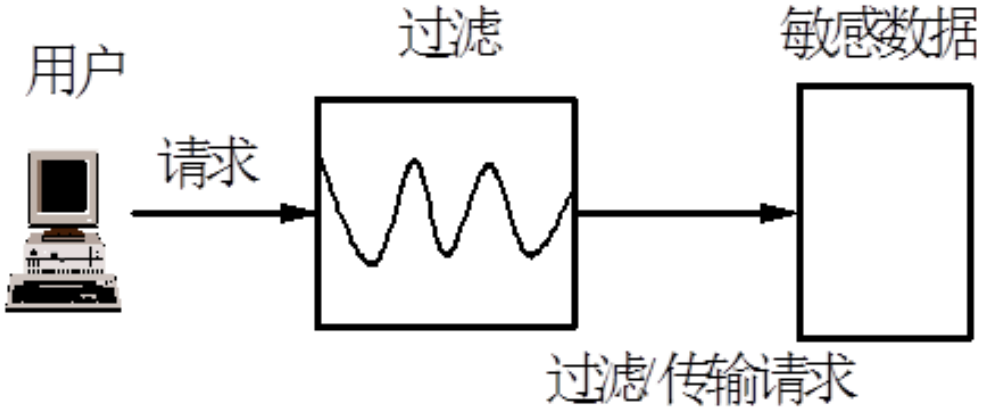
- 访问矩阵模型三要素:
  - 主体：可以对其他实体施加动作的主动实体，简记为S
  - 客体：是主体行为的对象，简记为O
  - 访问权限：访问权限有限集A={ 读，写，执行，追加 }
- 控制策略：主体对客体的操作行为集和约束条件集
- 访问矩阵：主体用行表示，客体用列表示，交叉项表示该主体对该客体所拥有的访问权限





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（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。

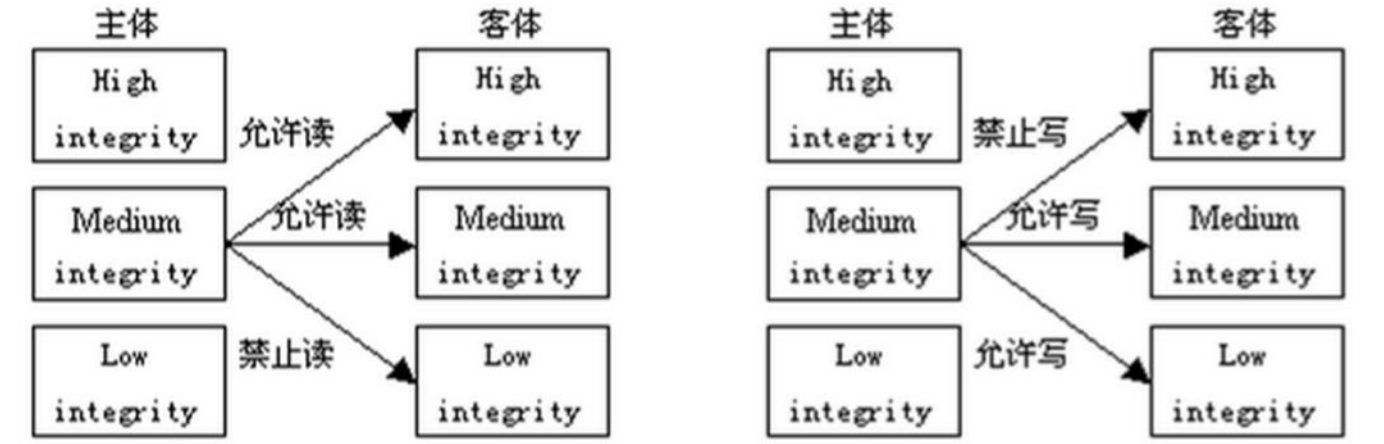
图：BLP安全模型

完整性模型-Biba

- Biba安全模型
  - 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（上读下写）
  - 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。

[第2次课]安全操作系统理论

内容概要

01 安全基础

02 安全模型

03 安全测评

安全操作系统测评

- 怎样才能确保你的计算机系统是充分安全的呢？
  - 你可以信赖你的软件提供商
  - 你可以自行测试系统，此时用户必须是一个安全专家
  - 你可以依靠独立机构的公正的安全评估
- 大多数的用户并不是安全专家，因此某种安全评估是信任一种安全产品的唯一选择
- 1980年以来，安全评估方案取得长足发展；当前，共同标准(Common Criteria)已成为国际标准ISO 15048

- 我们说一个操作系统是安全的，是指它满足某一给定的安全策略。一个操作系统的安全性是与设计密切相关的，只有有效保证从设计者到用户都相信设计准确地表达了模型，而代码准确地表达了设计时，该操作系统才可以说是安全的。

安全操作系统评测

- 评测操作系统安全性的技术有三种：
  - 入侵测试
  - 形式化验证
  - 非形式化确认

- 操作系统安全性保证手段
  - 漏洞扫描评估
  - 系统安全性评测

安全操作系统评测技术：入侵测试

- 操作系统在某一次入侵测试中失效，则说明它内部有错。相反地，操作系统在某一次入侵测试中不失效，并不能保证系统中没有任何错误。入侵测试在确定错误存在方面是非常有用的。
- 一般来说，评价一个计算机系统安全性能的高低，应从如下两个方面进行。
  (1) 安全功能: 系统具有哪些安全功能。
  (2) 可信性: 安全功能在系统中得以实现的可被信任的程度。通常通过文档规范、系统测试、形式化验证等安全保证来说明。

安全操作系统评测技术：形式化验证

- 分析操作系统安全性最精确的方法是形式化验证。在形式化验证中，安全操作系统被简化为一个要证明的“定理”。定理断言该安全操作系统是正确的，即它提供了所应提供的安全特性。但是证明整个安全操作系统正确性的工作量是巨大的。
- 另外，形式化验证也是一个复杂的过程，对于某些大的实用系统，试图描述及验证它都是十分困难的，特别是那些在设计时并未考虑形式化验证的系统更是如此。

安全操作系统评测技术：非形式化确认

- 确认是比验证更为普遍的术语。它包括验证，但它也包括其他一些不太严格的让人们相信程序正确性的方法。完成一个安全操作系统的确认有如下几种不同的方法。

(1) 安全需求检查：通过源代码或系统运行时所表现的安全功能，交叉检查操作系统的每个安全需求。其目标是认证系统所做的每件事是否都在功能需求表中列出，这一过程有助于说明系统仅作了它应该做的每件事。但是这一过程并不能保证系统没有做它不应该做的事情。

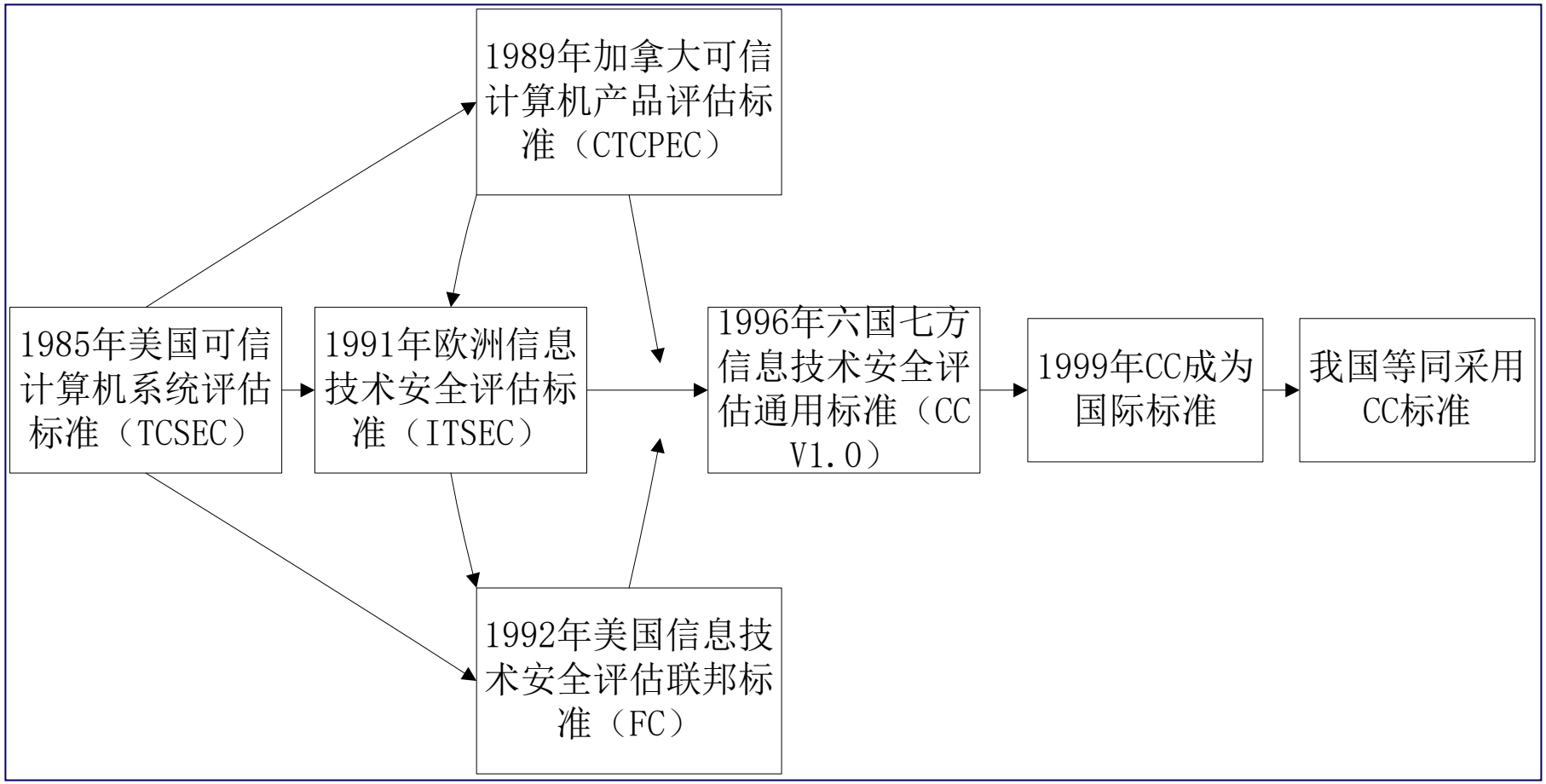
(2) 设计及代码检查：设计者及程序员在系统开发时通过仔细检查系统设计或代码，试图发现设计或编程错误。例如不正确的假设、不一致的动作或错误的逻辑等。这种检查的有效性依赖于检查的严格程度。

(3) 模块及系统测试：在程序开发期间，程序员或独立测试小组挑选数据检查操作系统的安全性。必须组织测试数据以便检查每条运行路线、每个条件语句、所产生的每种类型的报表、每个变量的更改等。在这个测试过程中要求以一种有条不紊的方式检查所有的实体。

安全操作系统保证技术：操作系统漏洞扫描

- 操作系统安全漏洞扫描的主要目的是：自动评估由于操作系统的固有缺陷或配置方式不当所导致的安全漏洞。
- 扫描软件在每台机器上运行，通过一系列测试手段来探查每一台机器，发现潜在的安全缺陷。它从操作系统的角度评估单机的安全环境并生成所发现的安全漏洞的详细报告。我们可以使用扫描软件对安全策略和实际实施进行比较，并给出建议采取相应措施来堵塞安全漏洞。

安全操作系统保证技术：安全评测发展历程



安全操作系统保证技术：安全评测发展历程

标准名称	颁布的国家和组织	颁布年份
美国TCSEC、修订版	美国国防部	1983、85
德国标准	西德	1988
英国标准	英国	1989
加拿大标准	加拿大	1989
欧洲ITSEC标准	西欧四国	1991
联邦标准草案（FC）	美国	1992
加拿大标准V3	加拿大	1993
CC V1.0、2.0	美、荷、法、德、英、加	1996、97
中国军标GJB2646-96	中国国防科学技术委员会	1996
ISO/IEC 15408	国际标准组织	1999
GB17859-1999、GB/T18336-2001	中国国家质量技术监督局	99、2001

安全评测发展历程：TCSEC

- 为了对现有计算机系统的安全性进行统一的评价，为计算机系统制造商提供一个有权威的系统安全性标准，需要有一个计算机系统安全评测准则。
- 美国国防部于1983年推出了历史上第一个计算机安全评价标准《可信计算机系统评测准则（Trusted Computer System Evaluation Criteria，TCSEC）》，又称橘皮书。
- TCSEC将计算机操作系统安全分为四大类（A、B、C、D），D、C1、C2、B1、B2、B3和A1七个级别。

安全评测发展历程：加拿大标准

- 加拿大政府设计开发了自己的可信任计算机标准——加拿大可信计算机产品评估标准（Canadian Trusted Computer Product Evaluation Criteria, CTCPEC）。
- CTCPEC提出了在开发或评估过程中产品的功能（functionality）和保证（assurance）。功能包括机密（confidentiality）、完整性（integrity）、可用性（availability）和可追究性（accountability）。保证说明安全产品实现安全策略的可信程度。

安全评测发展历程：通用安全评价准则CC

- 美国联合荷、法、德、英、加等国，于1991年1月宣布了制定通用安全评价准则（Common Criteria for IT Security Evaluation，CC）的计划。1996年1月发布了CC的1.0版。它的基础是欧洲的ITSEC、美国的TCSEC、加拿大的CTCPEC，以及国际标准化组织ISO SC27 WG3的安全评价标准。1999年7月，国际标准化组织ISO将CC 2.0作为国际标准——ISO/IEC 15408公布。
- CC标准提出了“保护轮廓”，将评估过程分为“功能”和“保证”两部分，是目前最全面的信息技术安全评估标准。

安全评测标准

- TCSEC
- CC
- 等保

美国国家计算机中心于1983年发表了著名的“可信任计算机标准评价准则”（Trusted Computer Standards Evaluation Criteria，简称TCSEC），指出了可信任计算机系统的六项基本需求，其中四项涉及信息的访问控制，两项涉及安全保障。

TCSEC：基本需求

该六项基本需求为：

1）安全策略。系统必须提供一个明确和良好定义的安全策略。对于识别出的主体和客体，系统必须有一个规则集决定指定的主体是否能访问指定的客体。计算机系统必须实施强制访问控制，有效地实现对敏感信息（如分级信息等）访问规则的处理。此外，还需建立自主访问控制机制，确保只有选中的用户或组才能访问指定数据。

2）标记。访问控制标签必须与对应的客体相联系。为了控制对存储在计算机中信息的访问，必须按强制访问控制规则，合理地为每个客体加一个标签，可靠地标识该对象的敏感级别，以及与可能访问该客体的主体相符的访问方式。

3）标识。每个主体都必须被标识。每次访问信息，都必须确定是谁在访问，以及授权访问信息的级别。身份和授权信息必须由计算机系统安全地维护。

TCSEC：基本需求

该六项基本需求为：

4）审计。必须记录和保存审计信息，以便在影响安全的行为发生时，能追踪到责任人。一个可信任的系统必须有能力将与安全有关的事件记录到审计记录中。必须有能力选择所记录的审计事件，减少审计开销。必须保护审计数据，以免遭到修改、破坏或非法访问。

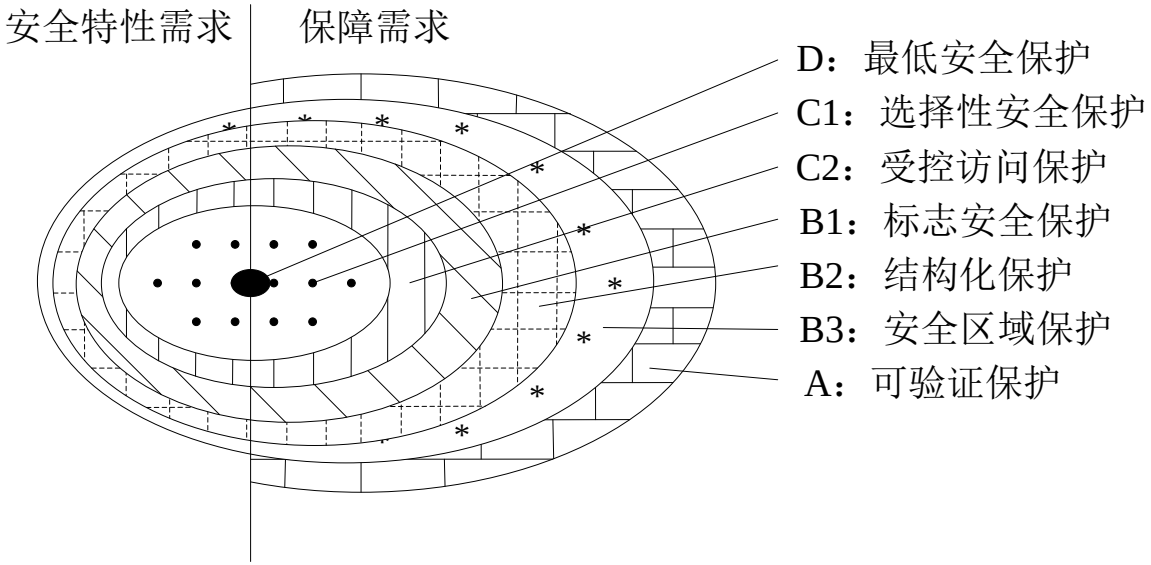
5）保证。计算机系统软件机制，能提供充分的保证正确实施以上必须包含硬件项基本需求。这些机制在典型情况下，被嵌入在操作系统中，并被设计成以安全方式执行所赋予的任务。

6）持续保护。实现这些基本需求的可信任机制必须得到持续保护，避免篡改和非授权改变。如果实现安全策略的基本硬件和软件机制本身受到非授权的修改或破坏，则这样的计算机系统不能被认为是真正安全的。持续保护需要在整个计算机系统生命周期中均有意义。

TCSEC：安全等级划分

可信系统评价标准（TCSEC）

TCSEC标准将计算机系统的安全性分为以下四个等级（A、B、C、D）八个级别，其结构如下图所示。



TCSEC的构成与等级结构

TCSEC：安全等级划分

安全级别	描述
D	最低的级别。如MS-DOS计算机，没有安全性可言。
C1	灵活的安全保护。系统不需要区分用户，可提供基本的访问控制。
C2	灵活的访问安全性。系统不仅要识别用户还要考虑唯一性。系统级的保护主要存在于资源、数据、文件和操作上。Windows NT属于C2级。
B1	标记安全保护。系统提供更多的保护措施包括各式的安全级别。如AT&T的SYSTEM V UNIX with MLS 以及IBM MVS/ESA。
B2	结构化保护。支持硬件保护。内容区被虚拟分割并严格保护，如Trusted XENIX和Honeywell MULTICS。
B3	安全域。提出数据隐藏和分层，阻止层之间的交往，如Honeywell XTS-200。
A	校验级设计。需要严格准确的证明系统不会被危害，而且提供所有低级别的安全，如Honeywell SCOMP。

TCSEC安全等级划分：D类安全等级

- **D类：无保护**
  - 最低安全性，无任何安全保护，不再分级。 不满足任何较高安全可信性的系统全部划入D级。该级别说明整个系统都是不可信任的，对硬件来说，没有任何保护作用，操作系统容易受到损害，不提供身份验证和访问控制。例如，MS-DOS、Macintosh System 7.x等操作系统属于这个级别。

TCSEC安全等级划分：C类安全等级

- **C类：自主式保护**
  - **该等级具有一定的保护能力，采用自主访问控制和审计跟踪的措施。该类的安全特点在于系统的对象（如文件、目录）可由其主体（如系统管理员、用户、应用程序）自定义访问权。自主保护类依据安全从低到高又分为C1、C2两个安全等级。**
    - C1：自主安全保护，主存取控制。
    - C2：自主访问保护，较完善的自主存取控制（DAC）、审计。

TCSEC安全等级划分：C类安全等级

- 又称自主安全保护（discretionary security protection）系统，实际上描述了一个典型的UNIX系统上可用的安全评测级别。
- 对硬件来说，存在某种程度的保护。用户必须通过用户注册名和口令系统识别，这种组合用来确定每个用户对程序和信息拥有什么样的访问权限。具体地说，这些访问权限是文件和目录的许可权限（permission）。
- 存在一定的自主存取控制机制（DAC），这些自主存取控制使得文件和目录的拥有者或者系统管理员，能够阻止某个人或几组人访问哪些程序或信息。UNIX的“owner/group/other”存取控制机制，即是一种典型的事例。

TCSEC安全等级划分：C类安全等级

- 但是这一级别没有提供阻止系统管理账户行为的方法，结果是不审慎的系统管理员可能在无意中损害了系统的安全。
- 另外，在这一级别中，许多日常系统管理任务只能通过超级用户执行。由于系统无法区分哪个用户以root身份注册系统执行了超级用户命令，因而容易引发信息安全问题，且出了问题以后难以追究责任。

TCSEC安全等级划分：C类安全等级

- 又称受控制的存取控制系统。它具有以用户为单位的DAC机制，且引入了审计机制。
- 除C1包含的安全特征外，C2级还包含其他受控访问环境（controlled-access environment）的安全特征。该环境具有进一步限制用户执行某些命令或访问某些文件的能力，这不仅基于许可权限，而且基于身份验证级别。
- 另外，这种安全级别要求对系统加以审计，包括为系统中发生的每个事件编写一个审计记录。审计用来跟踪记录所有与安全有关的事件，比如那些由系统管理员执行的活动。

TCSEC安全等级划分：B类安全等级

- **B类：强制式保护**

B类为强制保护类（mandatory protection)。该类的安全特点在于由系统强制的安全保护，在强制保护模式中，每个系统对象（如文件、目录等资源）及主体（如系统管理员、用户、应用程序）都有自己的安全标签（security label），系统则依据主体和对象的安全标签赋予访问者对访问对象的存取权限。强制保护类依据安全从低到高又分为B1、B2、B3这3个安全等级。

TCSEC安全等级划分：B1安全等级

- B1级或标记安全保护（labeled security protection）级：B1级要求具有C2级的全部功能，并引入强制型存取控制（MAC）机制，以及相应的主体、客体安全级标记和标记管理。
- B1级是支持多级安全（比如秘密和绝密）的第一个级别，这一级别说明一个处于强制性访问控制之下的对象，不允许文件的拥有者改变其存取许可权限。

TCSEC安全等级划分：B2安全等级

- B2级或结构保护（structured protection）级：B2级要求具有形式化的安全模型、描述式顶层设计说明（DTDS）、更完善的MAC机制、可信通路机制、系统结构化设计、最小特权管理、隐蔽通道分析和处理等安全特征。
- B2级要求计算机系统中所有的对象都加标记，而且给设备（如磁盘、磁带或终端）分配单个或多个安全级别。

TCSEC安全等级划分：B3安全等级

- B3级或安全域（security domain）级：B3级要求具有全面的存取控制（访问监控）机制、严格的系统结构化设计及TCB最小复杂性设计、审计实时报告机制、更好地分析和解决隐蔽通道问题等安全特征。
- B3使用安装硬件的办法增强域的安全性，例如，内存管理硬件用于保护安全域以避免无授权访问或对其他安全域对象的修改。该级别也要求用户的终端通过一条可信任途径连接到系统上。

TCSEC安全等级划分：A1安全等级

- A类为验证保护类（verify design）：A类是当前橘皮书中最高的安全级别，它包含了一个严格的设计、控制和验证过程。与前面提到的各级别一样。这一级包含了较低级别的所有特性。设计必须是从数学上经过验证的，而且必须进行隐蔽通道和可信任分布的分析。
- 可信任分布（trusted distribution）的含义是，硬件和软件在传输过程中已经受到保护，不可能破坏安全系统。验证保护类只有一个安全等级，即A1级。
- A1级要求具有系统形式化顶层设计说明（FTDS），并形式化验证FTDS与形式化模型的一致性，以及用形式化技术解决隐蔽通道问题等。

通用准则CC

- CC作为ISO/IEC 15408信息技术安全评估准则
  - 定义了作为评估信息技术产品和系统安全性的基础准则，面向系统的用户、开发者和评估者；
  - 是目前系统安全认证方面最权威的标准。
- CC的范围
  - 不涉及管理细节、具体的实现算法和评估方法；
  - 适用于硬件和软件实现的信息技术安全措施。
- 1998年1月，来自美国、加拿大、法国、德国以及英国的政府组织签订了历史性的安全评估沪人协议：IT安全领域内CC认可协议，即在协议签署国范围内，在某个国家进行的基于CC的安全评估将在其他国家内得到承认。

CC的目标读者

- CC的目标读者主要包括TOE用户、TOE开发者和TOE评估者。其他读者包括系统管理员和安全管理员、内部和外部审计员、安全规划和设计者、评估发起人和评估机构。
- 用户可以利用评估结果，判断一个系统和产品是否满足他们的安全需求，可以通过评估结果比较不同的系统和产品。CC用保护轮廓为用户提供了一个独立于实现的框架，用户在保护轮廓中可提出对评估对象的特殊IT安全要求。
- 开发者遵照CC对系统和产品进行设计和开发，可以通过安全功能和保证证明TOE实现了特定的安全要求，每个安全要求都包含在安全目标（ST）中。
- 评估者遵照CC对TOE进行评估，判断TOE与安全要求的一致性，可以得到可重复的、客观的评估结果。

CC准则结构

- 第一部分: 简介和一般模型。它定义了IT安全评估的通用概念和原理，提出了评估的通用模型。它还提出了一些概念，这些概念可用来表达IT安全目的，用于选择和定义IT安全要求、书写系统与产品的高层规范。
- 第二部分: 安全功能要求。它建立了一系列功能组件，作为表示TOE功能要求的标准方法。
- 第三部分: 安全保证要求。它建立了一系列保证组件，作为表示TOE保证要求的标准方法。它也定义了保护轮廓（PP）和安全目标（ST）的评估准则，提出了评估保证级别，即评估TOE保证的CC预定义等级。

CC的内容

功能	保证
识别和鉴别 可信路径 安全审计 安全功能调用 用户数据保护 资源利用 可信安全功能保护 秘密通信	开发 测试 脆弱性评估 配置管理 生命周期支持 文档向导 发布和操作

缩略语

EAL: 评估保证级（evaluation assurance level）

IT: 信息技术（information technology）

TOE: 评估对象（target of evaluation）

PP: 保护轮廓（protection profile）

TSP: TOE安全策略（TOE security policy）

SF: 安全功能（security function）

SFP: 安全功能策略（security function policy）

SOF: 功能强度（strength of function）

ST: 安全目标（security target）

TSC: TSF控制范围（TSF scope of control）

什么是等级保护?

网络安全等级保护是指对国家重要信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

等级保护的划分

* 第一级 信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益
* 第二级 信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全
* 第三级 信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害
* 第四级 信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害
* 第五级 信息系统受到破坏后，会对国家安全造成特别严重损害

中国国标GB17859—1999（等保1.0）

- 我国于1999年10月19日发布了《计算机信息系统安全保护等级划分准则》GB17859-1999（Classified criteria for security protection of Computer information system），规定了计算机信息系统安全保护能力的五个等级：
  - 第一级：用户自主保护级
  - 第二级：系统审计保护级
  - 第三级：安全标记保护级
  - 第四级：结构化保护级
  - 第五级：访问验证保护级

中国国标GB17859—1999

- 美国国防部采购的系统要求其安全级别至少达到B类，商业用途的系统也追求达到C类安全级别。但是，国外厂商向我国推销安全功能符合TCSEC B类和以上级别的计算机系统是限制的。因此，自主开发符合TCSEC中B类安全功能的安全操作系统一直是我国近几年来研究的热点。TCSEC从B1到B2的升级，在美国被认为是安全操作系统设计开发中，单级增强最为困难的一个阶段。
- 我国国标基本上是参照美国TCSEC制定的，但将计算机信息系统安全保护能力划分为5个等级，第五级是最高安全等级。一般认为我国GB17859—1999的第四级对应于TCSEC B2级，第五级对应于TCSEC B3级。

第一级：用户自主保护级

- 每个用户对属于自己的客体具有控制权，如不允许其他用户写他的文件而允许其他用户读他的文件。访问控制的权限可基于3个层次：客体的属主、同组用户、其他任何用户。
- 系统中的用户必须用一个注册名和一个口令验证其身份，目的在于标明主体是以某个用户的身份进行工作的，避免非授权用户登录系统。
- 确保非授权用户不能访问和修改“用来控制客体存取的敏感信息”和“用来进行用户身份鉴别的数据”。

第二级：系统审计保护级

- 自主访问控制的粒度更细。
- 审计机制。审计系统中受保护客体被访问的情况（包括增加、删除等），用户身份鉴别机制的使用，系统管理员、系统安全管理员、操作员的对系统的操作，以及其他与系统安全有关的事件。要确保审计日志不被非授权用户访问和破坏。
- TCB对系统中的所有用户进行惟一标识（如id号），系统能通过用户标识号确认相应的用户。
- 客体重用。释放一个客体时，将释放其目前所保存的信息；当它再次分配时，新主体将不能据此获得其原主体的任何信息。

第三级：安全标记保护级

- 强制访问控制机制。
- 在网络环境中，要使用完整性敏感标记确保信息在传送过程中没有受损。
- 系统要提供有关安全策略模型的非形式化描述。
- 在系统中，主体对客体的访问要同时满足强制访问控制检查和自主访问控制检查。
- 在审计记录的内容中，对客体增加和删除事件要包括客体的安全级别。另外，TCB对可读输出记号（如输出文件的安全级标记等）的更改要能审计。

第四级：结构化保护级

- 可信计算基建立于一个明确定义的形式化安全策略模型之上。
- 对系统中的所有主体和客体实行自主访问控制和强制访问控制。
- 进行隐蔽存储信道分析。
- 为用户注册建立可信通路机制。
- TCB必须结构化为关键保护元素和非关键保护元素。TCB的接口定义必须明确，其设计和实现要能经受更充分的测试和更完整的复审。
- 支持系统管理员和操作员的职能划分，提供了可信功能管理。

第四级：结构化保护级

具体内容如下所示。

- 自主访问控制。同第三级“安全标记保护级”。
- 强制访问控制。TCB对外部主体能够直接或间接访问的所有资源实施强制访问控制。
- 身份鉴别。同第三级“安全标记保护级”。
- 客体重用。同第三级“安全标记保护级”。
- 审计。同第三级“安全标记保护级”，但增加了审计隐蔽存储信道事件。
- 隐蔽通道分析。系统开发者应彻底搜索隐蔽存储信道，并确定每一个被标识信道的最大带宽。
- 可信路径。对用户的初始登录（如login），TCB在它与用户之间提供可信通信路径，使用户确信与TCB进行通信。

第五级：访问验证保护级

- TCB满足参照监视器需求，它仲裁主体对客体的全部访问，其本身足够小，能够分析和测试。在构建TCB时，要清除那些对实施安全策略不必要的代码，在设计和实现时，从系统工程角度将其复杂性降低到最小程度。
- 扩充审计机制，当发生与安全相关的事件时能发出信号。
- 系统具有很强的抗渗透能力。

等保2.0

- 等保2.0：
  - 2.0时代：等级保护空前重要
  - 2.0时代：名称的变化
  - 2.0时代：等级保护制度上升为法律
  - 2.0时代：等级保护对象大扩展
  - 2.0时代：等级保护内容大不同
  - 2.0时代：等级保护体系大升级

等级保护空前重要

- 国内：
  - 国家正面临经济社会结构调整和转型，信息技术成为新的引擎
  - 网络和信息系统作为新兴动力的承载者，将构建起整个经济社会神经中枢
  - 等级保护将继续扮演不可替代的重要角色
- 全球：
  - 网络空间已成为与陆地、海洋、天空、太空同等重要的人类活动新领域
  - 随着我国全球地位不断提升，网络空间主权成为了国家主权的一个新维度
  - 等保的核心始终是围绕关键信息基础设施保护，所以，它已经成为了国家网络空间战略的重要组成部分。

等级保护名称的变化

- 将原来的信息系统安全等级保护相关标准名称更改为信息安全等级保护，再更名为网络安全等级保护相关标准，与《中华人民共和国网络安全法》保持一致。

等级保护制度上升为法律

- 《中华人民共和国网络安全法》即将在2017年6月1日施行，作为网络安全基础性法律，在第21条明确规定了“国家实行网络安全等级保护制度，要求网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；第31条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。等级保护制度在今天已上升为法律，并在法律层面确立了其在网络安全领域的基础、核心地位，正如业内所言，不做等保就是违法了。

等级保护对象大扩展

- 随着云计算、移动互联、大数据、物联网、人工智能等新技术不断涌现，计算机信息系统的概念已经不能涵盖全部，特别是互联网快速发展带来大数据价值的凸显，这些都要求等保外延的拓展。新的系统形态、新业态下的应用、新模式背后的服务、以及重要数据和资源统统进入了等保视野。**具体对象则囊括了大型互联网企业、基础网络、重要信息系统、网站、大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等等。**

等级保护内容大不同

- 我们总说等级保护有五个规定动作，即定级、备案、建设整改、等级测评和监督检查，2.0时代，等保的内涵已大为丰富和完善。风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等这些与网络安全密切相关的措施都将全部纳入等级保护制度并加以实施。

等级保护体系大升级

- 等级保护工作一直是在顶层设计下，以体系化的思路逐层展开、分步实施。2.0时代，在现有体系基础上，建立完善等级保护政策体系、标准体系、测评体系、技术体系、服务体系、关键技术研究体系、教育训练体系等。等级保护也将作为核心，围绕它来构建起安全监测、通报预警、快速处置、态势感知、安全防范、精确打击等为一体的国家关键信息基础设施安全保卫体系。

内容大纲对比


结构图
等级保护1.0
等级保护2.0
旧标准
新标准
技术要求
物理安全
网络安全
主机安全
应用安全
数据安全及备份恢复
管理要求
安全管理制度
安全管理机构
人员安全管理
系统建设管理
系统运维管理
物理和环境安全
网络和通信安全
设备和计算安全
应用和数据安全
安全策略和管理制度
安全管理机构和人员
安全建设管理
安全运维管理
技术要求
管理要求

技术指标对比

	原控制点	要求项数		新控制点	要求项数
主机安全	1 身份鉴别	6	设备和计算安全	1 身份鉴别	4
	2 访问控制	7		2 访问控制	7
	3 安全审计	6		3 安全审计	5
	4 剩余信息保护	2		4 入侵防范	5
	5 入侵防范	3		5 恶意代码防范	1
	6 恶意代码防范	3		6 资源控制	4
	7 资源控制	5			

谢谢！