第5章 操作系统安全

本章学习要点：

- ✓ 了解安全操作系统的安全策略与模型。
- ✓ 了解安全操作系统的访问控制机制。
- ✓ 了解安全操作系统的评测方法与准则。

5.1 安全操作系统概述

1. 定义及术语

- ✓ 可信计算基（Trusted Computing Base，TCB）：计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体。
- ✓ 自主访问控制（Discretionary Access Control，DAC）：用来决定一个用户是否有权限访问此客体的一种访问约束机制，该客体的所有者可以按照自己的意愿指定系统中的其他用户对此客体的访问权。

- ✓ 敏感标记（Sensitivity Label）：用以表示客体安全级别并描述客体数据敏感性的一组信息，在可信计算基中把敏感标记作为强制访问控制决策的依据。
- ✓ 强制访问控制（Mandatory Access Control，MAC）：用于将系统中的信息分密级和类进行管理，以保证每个用户只能够访问那些被标明可以由他访问的信息的一种访问约束机制。
- ✓ 角色（Role）：系统中一类访问权限的集合。
- ✓ 隐蔽信道（Covert Channel）：允许进程以危害系统安全策略的方式传输信息的信道。
- ✓ 客体重用（Object Reuse）：对曾经包含一个或几个客体的存贮介质（如页框、盘扇面、磁带）重新分配和重用。

- ✓ 可信通路（Trusted Path）：终端人员能借以直接同可信计算基通信的一种机制。该机制只能由有关终端操作人员或可信计算基启动，并且不能被不可信软件模仿。
- ✓ 多级安全（MultiLevel Secure，MLS）：一类包含不同等级敏感信息的系统，它既可供具有不同安全许可的用户同时进行合法访问，又能阻止用户去访问其未被授权的信息。
- ✓ 安全操作系统（Secure Operating System）：能对所管理的数据与资源提供适当的保护级、有效地控制硬件与软件功能的操作系统。
- ✓ 多级安全操作系统（Multilevel Secure Operating System）：实现了多级安全策略的安全操作系统，比如符合美国TCSEC B1级以上的安全操作系统。

2.安全操作系统

- ✓ 从安全角度来看，操作系统软件的配置是很困难的，配置时一个很小的错误就可能导致一系列安全漏洞。每一个与安全相关的漏洞都会使整个系统的安全机制变得毫无价值。
- ✓ 从计算机信息系统的角度分析，操作系统、数据库管理系统与网络系统的安全问题是核心。
- ✓ 操作系统的安全性在计算机信息系统的整体安全性中具有至关重要的作用。

5.2 安全策略与安全模型

5.2.1安全策略

- ✓ 安全策略是指有关管理、保护和发布敏感信息的法律、规定和实施细则。
- ✓ 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。
- ✓ 进行安全操作系统的设计和开发时，也要围绕一个给定的安全策略进行。
- ✓ 安全策略由一整套严密的规则组成，这些确定授权访问的规则是决定访问控制的基础

1.军事安全策略

- ✓ 军事安全策略是基于保护机密信息的策略。每条信息被标识为一个特定的等级，如公开、受限制、秘密、机密和绝密。这些等级构成了一个层次结构。

2.商业安全策略

- ✓ 一个大的机构，如一家公司或一所大学，可能会被分成许多个组或者部门，他们各自负责不同的项目。当然，还可能存在一些机构级的职责，比如财务或者人事。位于不同级别的数据项具有不同的安全等级，例如：公共的、专有的或内部的。
- ✓ 商业信息安全和军事信息安全有两个很显著的区别
  - ➢ 第一，通常没有正式的“许可”概念
  - ➢ 第二，允许访问的规则不太规范

（1）Clark-Wilson商业安全策略

- ✓ 为良构事务（Well-Formed Transaction）提供的策略
- ✓ 考虑这样一个例子：一家公司预订货物，然后付款。典型的流程如下所示：
  - ➢ 采购员先做一张供应订单，并把订单同时发给供货方和收货部门。
  - ➢ 供货方将货物运到收货部门。接收员检查货物，确保收到货物的种类和数量是正确的，然后在送货单上签字。送货单和原始订单再交给财务部门。
  - ➢ 供货方将发票送到账务部门。财务人员将发票同原始订单进行校对（校对价格和其他条款）和将发票同送货单进行校对（校对数量和品种），然后开支票给供货方。
- ✓ 用受约束数据项来表达策略，受约束数据项由转变程序（Transformation Procedure）进行处理。
- ✓ 将策略定义为访问三元组（Access Triples） $< Userid，Tpi，\{Cdij，Cdik，...\} >$

The Clark-Wilson Model

- Rather than dealing with document confidentiality and/or integrity, the **Clark-Wilson (CW)** model deals with *systems that perform transactions*.
- It describes mechanisms for *assuring that the integrity of such a system is preserved across the execution of a transaction*. Key components of the CW model include the following:
  - **Integrity constraints** that express relationships among objects that must be satisfied for the system state to be valid. A classic example of an integrity constraint is the relationship stating that the final balance of a bank account after a withdrawal transaction must be equal to the initial balance minus the amount withdrawn.
  - **Certification methods** that verify that transactions meet given integrity constraints. Once the program for a transaction is certified, the integrity constraints do not need to be verified at each execution of the transaction.
  - **Separation of duty rules** that prevent a user that executes transaction from certifying it. In general, each transaction is assigned disjoint sets of users that can certify and execute it, respectively.

（2）中国墙安全策略

- ✓ 反映了对信息访问保护的某种商业需求。
- ✓ 安全策略建立在三个抽象等级上：
  - ➢ 对象（Object）：位于最低等级，比如文件。每个文件只包含一个公司的信息。
  - ➢ 公司群体（Company Group）：位于第二个等级，由与一家特定公司相关的所有对象组成。
  - ➢ 冲突类（Conflict Class）：位于最高等级，相互竞争的公司的所有对象集合。
- ✓ 和其他的商业策略不同，中国墙策略注重完整性。

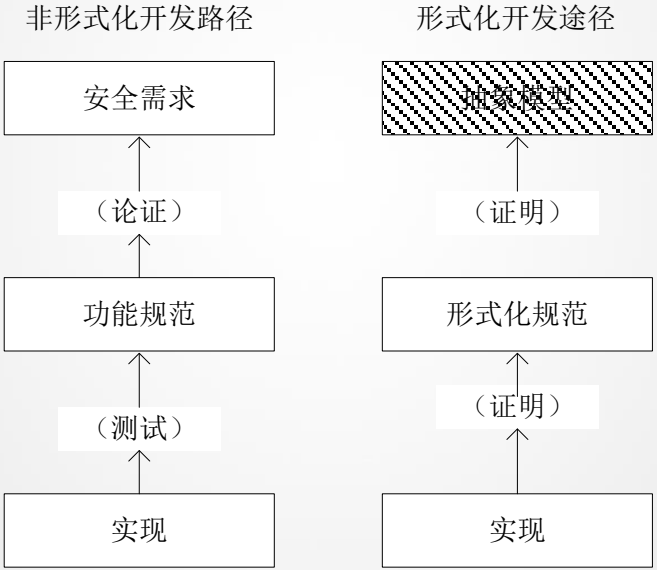
The Chinese Wall Model

- The **Brewer and Nash model,** commonly referred to as the **Chinese wall model,** is designed for use in the commercial sector to eliminate the possibility of conflicts of interest.
- To achieve this, the model groups resources into “conflict of interest classes.”
- The model enforces the restriction that each user can only access one resource from each conflict of interest class.
  - In the financial world, such a model might be used, for instance, to prevent market analysts from receiving insider information from one company and using that information to provide advice to that company’s competitor.
- Such a policy might be implemented on computer systems to regulate users’ access to sensitive or proprietary data.

5.2.2安全模型

- ✓ 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，它为安全策略和安全策略实现机制的关联提供了一种框架。
- ✓ 要开发安全系统首先必须建立系统的安全模型。
- ✓ 安全模型有以下几个特点：
  - ➢ 它是精确的、无歧义的；
  - ➢ 它是简易和抽象的，所以容易理解；
  - ➢ 它是一般性的：只涉及安全性质，而不过度地牵扯系统的功能或其实现；
  - ➢ 它是安全策略的明显表现。
- ✓ 安全模型一般分为两种：形式化的安全模型和非形式化的安全模型。

- ✓ 形式化的安全模型是设计开发高级别安全系统的前提。形式化安全模型使用数学模型，精确描述安全性及其在系统中使用的情况。
- ✓ 如果是用非形式化的开发路径，修改一个现有的操作系统以改进它的安全性能，则只能达到中等的安全级别。



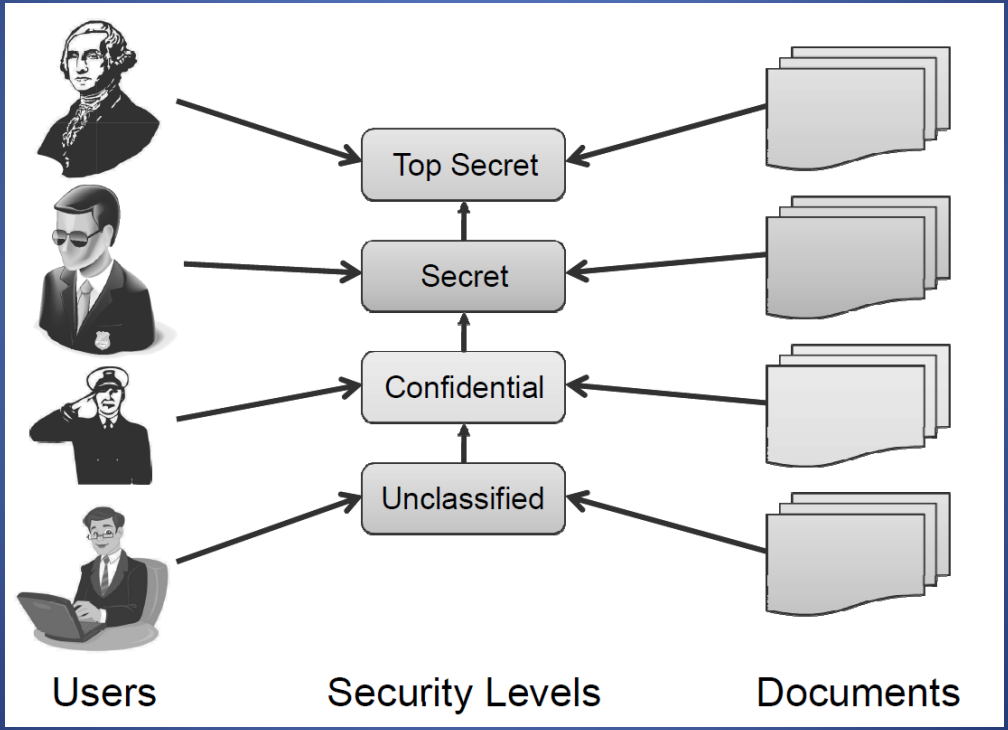
3.主要安全模型介绍

BLP机密性安全模型、Biba完整性安全模型和RBAC安全模型。此外，还有Clark-Wilson完整性安全模型、信息流模型、DTE安全模型和无干扰安全模型等。

（1）Bell-Lapadula模型

- ✓ 一种适用于军事安全策略的安全模型
- ✓ 将主体定义为能够发起行为的实体，将客体定义为被动的主体行为承担者
- ✓ 是一个状态机模型，对于一个系统而言，如果它的初始状态是安全的，并且所经过的一系列规则转换都保持安全，那么可以证明该系统的终止也是安全的。
- ✓ 但随着计算机安全理论和技术的发展，BLP模型已不足以描述各种各样的安全需求。

The Bell-La Padula Model



How the BLP Model Works

- Each object, x, is assigned to a security level, L(x). Similarly, each user, u, is assigned to a security level, L(u). Access to objects by users is controlled by the following two rules:
  - **Simple security property.** A user u can read an object x only if
    $$L(x) \leq L(u).$$
  - ***-property.** A user u can write (create, edit, or append to) an object x only if
    $$L(u) \leq L(x).$$
- The simple security property is also called the "no read up" rule, as it prevents users from viewing objects with security levels higher than their own.
- The *-property is also called the "no write down" rule. It is meant to prevent propagation of information to users with a lower security level.

（2）Biba模型

- ✓ 第一个完整性安全模型
- ✓ 也是基于主体、客体以及它们的级别概念
- ✓ 与BLP模型完全相反的模型
- ✓ 优势在于其简单性以及和BLP模型相结合的可能性
- ✓ 不足之处在于以下：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。仅在Multics和VAX等少数几个系统中实现。难以满足实际系统真正的需求。

The Biba Model

- The **Biba model** has a similar structure to the BLP model, but it addresses **integrity** rather than confidentiality.
- Objects and users are assigned **integrity levels** that form a partial order, similar to the BLP model.
- The integrity levels in the Biba model indicate *degrees of trustworthiness, or accuracy*, for objects and users, rather than levels for determining confidentiality.
  - For example, a file stored on a machine in a closely monitored data center would be assigned a higher integrity level than a file stored on a laptop.
  - In general, a data-center computer is less likely to be compromised than a random laptop computer. Likewise, when it comes to users, a senior employee with years of experience would have a higher integrity level than an intern.

The Biba Model Rules

- The access-control rules for Biba are the reverse of those for BLP. That is, Biba does not allow reading from lower levels and writing to upper levels.
- If we let I(u) denote the integrity level of a user u and I(x) denote the integrity level for an object, x, we have the following rules in the Biba model:
  - A user u can read an object x only if
    $$I(u) \leq I(x).$$
  - A user u can write (create, edit or append to) an object x only if
    $$I(x) \leq I(u).$$
- Thus, the Biba rules express the principle that information can only *flow down*, going from higher integrity levels to lower integrity levels.

（3）基于角色的访问控制（RBAC）模型

- ✓ 提供了一种强制访问控制机制
- ✓ 由系统管理员负责管理系统的角色集合和访问权限集合，并将这些权限（不同类别和级别）通过相应的角色分别赋予承担不同工作职责的终端用户，而且还可以随时根据业务的要求或变化对角色的访问权限集和用户所拥有的角色集进行调整。
- ✓ 明确区分权限（Authority）和职责（Responsibility）这两个概念
- ✓ 功能相当强大，适用于许多类型（从政府机构到商业应用）的用户需求
- ✓ Netware、Windows NT、Solaris和Selinux等操作系统中都采用了类似的RBAC技术作为访问控制手段。

Role-Based Access Control

- The **role-based access control (RBAC)** model can be viewed as an evolution of the notion of group-based permissions in file systems.
- An RBAC system is defined with respect to an organization, such as company, a set of resources, such as documents, print services, and network services, and a set of users, such as employees, suppliers, and customers.

RBAC Components

- A **user** is an entity that wishes to access resources of the organization to perform a task. Usually, users are actual human users, but a user can also be a machine or application.
- A **role** is defined as a collection of users with similar functions and responsibilities in the organization. Examples of roles in a university may include “student,” “alum,” “faculty,” “dean,” “staff,” and “contractor.” In general, a user may have multiple roles.
  - Roles and their functions are often specified in the written documents of the organization.
  - The assignment of users to roles follows resolutions by the organization, such as employment actions (e.g., hiring and resignation) and academic actions (e.g., admission and graduation).
- A **permission** describes an allowed method of access to a resource.
  - More specifically, a permission consists of an operation performed on an object, such as “read a file” or “open a network connection.” Each role has an associated set of permissions.
- A **session** consists of the activation of a subset of the roles of a user for the purpose of performing a certain task.
  - For example, a laptop user may create a session with the administrator role to install a new program.
  - Sessions support the principle of least privilege.

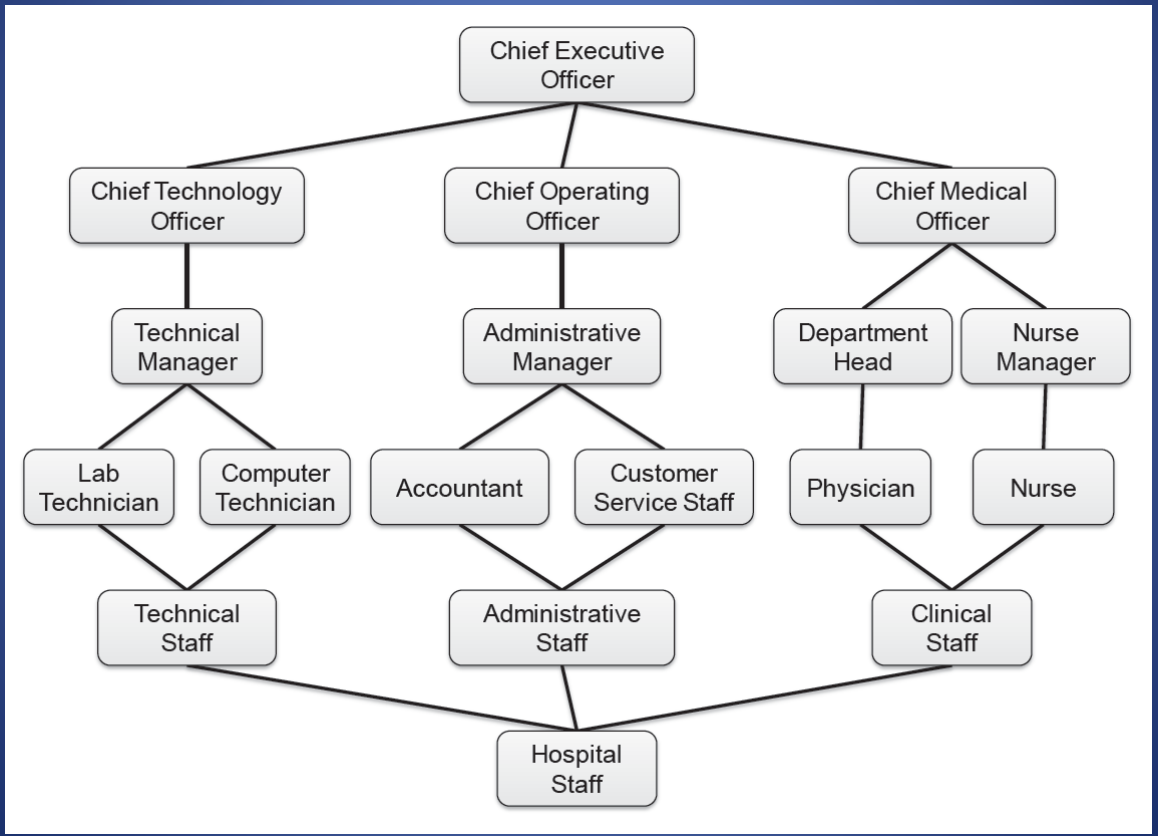
Hierarchical RBAC

- In the role-based access control model, roles can be structured in a hierarchy similar to an organization chart.
- More formally, we define a *partial order among roles* by saying that a role R1 **inherits role R2,** which is denoted

  $$R1 \geq R2,$$

  if R1 includes all permissions of R2 and R2 includes all users of R1.
- When $R1 \geq R2$, we also say that role R1 is **senior** to role R2 and that role R2 is **junior** to role R1.
  - For example, in a company, the role "manager" inherits the role "employee" and the role "vice president" inherits the role "manager."
  - Also, in a university, the roles "undergraduate student" and "graduate student" inherit the role "student."

Visualizing Role Hierarchy



5.3 访问控制

- 在计算机系统中，安全机制的主要内容是访问控制，包括以下3个任务：
  - 授权，即确定可给予哪些主体访问客体的权力；
  - 确定访问权限（读、写、执行、删除、追加等访问方式的组合）；
  - 实施访问权限。
- 这里，“访问控制”仅适用于计算机系统内的主体和客体，而不包括外界对系统的访问。控制外界对系统访问的技术是标识与鉴别。
- 主要讲述自主访问控制、强制访问控制和基于角色的访问控制三种形式

5.3.1自主访问控制

1.基本概念

- ✓ 最常用的一类访问控制机制，是用来决定一个用户是否有权访问一些特定客体的一种访问约束机制。
- ✓ 目前在操作系统中实现的DAC机制是基于矩阵的行或列表达访问控制信息。

(1) 基于行的自主访问控制机制

- ✓ 在每个主体上都附加一个该主体可访问的客体明细表

(2) 基于列的自主访问控制机制

- ✓ 在每个客体上都附加一个可访问它的主体明细表，它有两种形式，即保护位和访问控制表。

Discretionary Access Control

- **Discretionary access control,** or **DAC,** refers to a scheme where users are given the ability to determine the permissions governing access to their own files.
  - DAC typically features the concept of both users and groups, and allows users to set access-control measures in terms of these categories.
  - In addition, DAC schemes allow users to grant privileges on resources to other users on the same system.

客体file1:	ID1.rx	ID2.r	ID3.x	…	IDn.rwx

- 对于客体file1，主体ID1对它只具有读（r）和运行（x）的权力，主体ID2只具有读权力，主体ID3只具有运行的权力，而主体IDn则对它同时具有读、写和运行的权力。
- 但在实际应用中，当对某客体可访问的主体很多时，访问控制表将会变得很长。
- 访问控制表必须简化，如把用户按其所属或其工作性质进行分类，构成相应的组（group），并设置一个通配符（wild card）“*”，代表任何组名或主体标识符，如图5-4所示。

文件ALPHA		
Jones	CRYPTO	rwx
*	CRYPTO	r_x
Green	*	---
*	*	r__

- ✓ CRYPTO组中的用户Jones对文件ALPHA拥有rwx访问权限。CRYPTO同组中的其他用户拥有rx权限。Green如果不在CRYPTO同组中，就没有任何权限。其他用户拥有r权限。
- ✓ 通过简化，访问控制表大大缩小，效率提高，并且也能够满足自主访问控制的需要。

2.实现举例

(1) 拥有者/同组用户/其他用户模式

- ✓ UNIX、Linux、VMS等系统中，在每个文件上附加一段有关访问控制信息的二进制位

r w x	r w x	r w x
拥有者	同组用户	其他用户

- ✓ 这些二进制位反映了不同类别用户的访问方式，他们是文件的拥有者，与文件拥有者同组的用户及其他用户（一般称为9比特位模式）。即:
  - owner的3位反映此客体的拥有者对它的访问权限；
  - group的3位反映owner同组用户对此客体的访问权限；
  - other的3位反映其他用户对此客体的访问权限。
- ✓ 缺点是客体的拥有者不能够精确控制某个用户对其客体的访问权。

(2) 访问控制表（ACL）和“拥有者/同组用户/其他用户”相结合的模式

- ✓ 安全操作系统UNIX SVR 4.1ES采用了该方法
- ✓ 访问控制表只对“拥有者/同组/其他用户”无法分组的用户才使用
- ✓ 既保持了与原系统的兼容性，又将用户控制粒度细化到系统中的单个用户
- ✓ UNIX SVR 4.1ES在文件系统中，针对文件的索引结构开发ACL项及相关信息项，使每个文件对应一个ACL。在IPC的索引结构中开发ACL项及相关信息项，使每个消息队列、每个信号量集合、每个共享存储区对应一个ACL。

- ✓ 虽然这种自主性为用户提供了很大的灵活性，但缺乏高安全等级所需的高安全性。系统需要采取更强的访问控制手段，这就是强制访问控制。

5.3.2强制访问控制

1.基本概念

- ✓ 系统中的每个进程、每个文件、每个IPC客体(消息队列、信号量集合和共享存储区)都被赋予了相应的安全属性，这些安全属性是不能改变的，它由管理部门或由操作系统自动地按照严格的规则来设置，不像访问控制表那样由用户或他们的程序直接或间接地修改。
- ✓ 强制访问控制用于将系统中的信息分密级和类进行管理，适用于政府部门、军事和金融等领域。
- ✓ 一般将强制访问控制和多级安全体系相提并论。
- ✓ 多级安全（又称MLS）是军事安全策略的数学描述，是计算机能实现的形式定义。

Mandatory Access Control

- **Mandatory access control** is a more restrictive scheme that does not allow users to define permissions on files, regardless of ownership. Instead, security decisions are made by a central policy administrator.
  - Each security rule consists of a **subject,** which represents the party attempting to gain access, an **object,** referring to the resource being accessed, and a series of permissions that define the extent to which that resource can be accessed.
- **Security-Enhanced Linux (SELinux)** incorporates mandatory access control.

(1) 军事安全策略

- 安全级由两方面的内容构成。
  - 1) 保密级别（或敏感级别或级别）。
  - 2) 范畴集。
- 实际上范畴集常常是空的，而且很少有几个范畴名。
- 在安全级中保密级别是线性排列的。两个安全级之间的关系有以下几种。
  - 第一安全级支配第二安全级。
  - 第一安全级支配于第二安全级，或第二安全级支配第一安全级。
  - 第一安全级等于第二安全级。
  - 两个安全级无关。

(2) 多级安全规则与BLP模型

- ✓ BLP模型的目标就是详细说明计算机的多级操作规则。对军事安全策略的精确描述被称作是多级安全策略。
- ✓ BLP模型有两条基本的规则。
  - ➢ 简单安全特性规则。一个主体对客体进行读访问的必要条件是主体的安全级支配客体的安全级，即主体的保密级别不小于客体的保密级别，主体的范畴集合包含客体的全部范畴。即主体只能向下读，不能向上读。
  - ➢ *特性规则。一个主体对客体进行写访问的必要条件是客体的安全级支配主体的安全级，即客体的保密级别不小于主体的保密级别，客体的范畴集合包含主体的全部范畴。即主体只能向上写，不能向下写。

2.实现举例

- ✓ UNIX SVR 4.1ES分别对系统中的主体和客体赋予了相应的安全级，并采用了BLP模型对应的多级安全规则。

(1) 安全级赋值

- ✓ 1) 主体的安全级
- ✓ 2) 客体的安全级
- ✓ 3) 设备的安全级

(2) 强制访问控制规则

这里分别以CLASS(S)、CLASS(O)表示主体与客体的安全级，强制访问控制规则为：

- ✓ if CLASS(S)>=CLASS(O) then Read(S,O) or Execute(S,O)；
- ✓ if CLASS(S)=CLASS(O) then Write(S,O) or Append(S,O)。

3.使用强制访问控制防止特洛伊木马

- ✓ 解决特洛伊木马的一个有效方法是使用强制访问控制机制。
- ✓ 例如在多级安全系统中，*特性能阻止正在机密安全级上运行的进程中的特洛伊木马把机密信息写入一个公开的文件里。
- ✓ 再如一个公司对系统中自己拥有的信息指定强制访问范畴，只有该公司的雇员才可能进入这个范畴。

5.3.3基于角色的访问控制

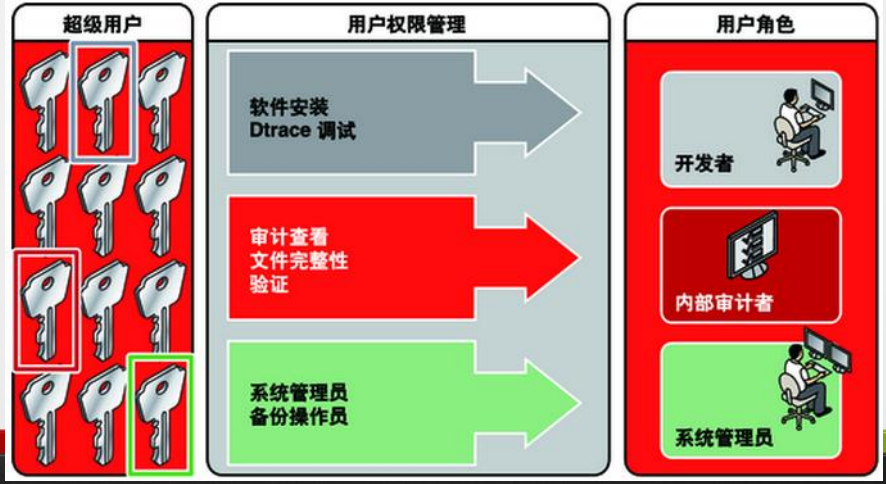
1.基本概念

- ✓ 基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。RBAC从控制主体的角度出发，根据管理中相对稳定的职权和责任来划分角色，将访问权限与角色相联系，这点与传统的MAC和DAC将权限直接授予用户的方式不同；通过给用户分配合适的角色，让用户与访问权限相联系。角色成为访问控制中访问主体和受控对象之间的一座桥梁。
- ✓ 用户即访问计算机资源的主体。角色即一种岗位，代表一种资格、权利和责任。权限即对客体的操作权力。用户分配即将用户与角色关联。权限分配即将角色与权限关联
- ✓ 角色可以看作是一组操作的集合，不同的角色具有不同的操作集，这些操作集由系统管理员分配给角色。

- ✓ 相比较而言，RBAC是实施面向企业安全策略的一种有效访问控制方式，允许组织根据用户或角色的独特需要和要求选择性地向其授予管理权限，从而应用最小特权安全原则，还具有灵活性、方便性和安全性的特点。
- ✓ 角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色。用户与客体无直接联系，他只有通过角色才享有该角色所对应的权限，从而访问相应的客体。因此用户不能自主地将访问权限授给别的用户，这是RBAC与DAC的根本区别所在。
- ✓ RBAC与MAC的区别在于：MAC是基于多级安全需求的，而RBAC则不是。

2.实现举例

- ✓ Oracle Solaris 11的RBAC功能控制用户对通常限于root角色的任务的访问。通过对进程和用户应用安全属性，RBAC可以在多个管理员之间分布管理权限。RBAC组件包括角色、权限配置文件和授权。进程权限管理通过特权实现。与通过超级用户管理系统相比，将特权与RBAC结合使用是一种更为安全的管理方法。



5.4 安全操作系统评测

5.4.1操作系统的典型缺陷

很多操作系统中都发现了漏洞。

1.已知的漏洞

- ✓ I/O处理是操作系统最大的薄弱点
- ✓ 第二个突出弱点是访问策略的二义性
- ✓ 第三个潜在的问题是不完全检查
- ✓ 通用性是第四个弱点

2.漏洞利用的例子

- ✓ 第一个例子涉及到用户接口。某些操作系统只在用户操作开始时进行访问权限检查，这就导致了典型的检查时刻到使用时刻的缺陷。
- ✓ 另一个例子涉及程序上的纰漏。某些操作系统为一些安全性软件包的安装保留了一种特殊的管理功能。执行安装时，这个管理调用以特权方式将控制权返回给用户。
- ✓ 检查时刻到使用时刻的不匹配也会引发安全问题。
- ✓ 其他利用多种漏洞的更复杂组合的入侵

总的来说，安全操作系统的安全缺陷是由于复杂情形（例如用户接口）的错误分析造成的，或者是由于安全策略中的二义性或疏忽造成的。利用简单的安全机制实现清楚而完善的安全策略，入侵的数量就会显著减少。

5.4.2评测方法与评估准则

1.评测方法

评测操作系统安全性的方法主要有三种：形式化验证、非形式化确认及入侵分析。这些方法各自可以独立使用，也可以将它们综合起来评估操作系统的安全性。

- ✓ （1）形式化验证：最精确、工作量巨大、复杂、困难
- ✓ （2）非形式化确认：安全需求检查、设计及代码检查、模块及系统测试
- ✓ （3）“老虎”小组入侵测试：应当掌握操作系统典型的安全漏洞，试图发现并利用

2.评估准则

（1）评估准则概况

- ✓ 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）》。TCSEC带动了国际上计算机安全评测的研究，我国也制定了相应的强制性国家标准GB17859-1999《计算机信息系统安全保护等级划分准则》和推荐标准GB/T18336 - 2001《信息技术 安全技术 信息技术安全性评估准则》。表5-1给出了国内外计算机评价标准的概况。

标准名称	颁布的国家或组织	颁布年份
美国TCSEC	美国国防部	1983
美国TCSEC修订版	美国国防部	1985
德国标准	西德	1988
英国标准	英国	1989
加拿大标准V1	加拿大	1989
欧洲ITSEC	西欧四国（英、法、荷、德）	1991
联邦标准草案（FC）	美国	1992
加拿大标准V3	加拿大	1993
CC V1.0	美、荷、法、德、英、加	1996
中国军标GJB2646-96	中国国防科学技术委员会	1996
CC V2.0	美、荷、法、德、英、加	1997
ISO/IEC 15408	国际标准组织	1999
中国GB17859-1999	中国国家质量技术监督局	1999
中国GB/T18336-2001	中国国家质量技术监督局	2001

（2）美国TCSEC

- ✓ 在用户登录、授权管理、访问控制、审计跟踪、隐蔽信道分析、可信通路建立、安全检测、生命周期保障、文档写作等各方面，均提出了规范性要求，
- ✓ 根据所采用的安全策略、系统所具备的安全功能将系统分为四类7个安全级别。亦即：D类、C类、B类和A类，以层次方式排序，最高类A代表安全性最高的系统。其中，C类和B类又有若干子类称为级，级也以层次方式排序，各级别安全可信性依次增高，较高级别包含较低级别的安全性。
- ✓ 在每个级别内，准则分为四个主要部分。前三部分叙述满足安全策略、审计和保证的主要控制目标。第四部分是文档，描述文档的种类，以及编写用户指南、手册、测试文档和设计文档的主要要求。

（3）中国国标GB17859-1999

- 该准则参考了美国TCSEC《可信计算机系统评估准则》和《可信计算机网络系统说明》（NCSC-TG-005），将计算机信息系统安全保护能力划分为5个等级，即：
  - 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。
- GB17859-1999的第四级对应于TCSEC B2级，第五级对应于TCSEC B3级。

（4）国际通用安全评价准则CC

- ✓ 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。
- ✓ CC标准在内容上包括三部分：
  - 一是简介和一般模型，
  - 二是安全功能要求，
  - 三是安全保证要求。

5.5 本章小结

- ✓ 对安全操作系统的概念进行了简单概述；
- ✓ 描述了主要的安全策略和模型，安全策略包括军事安全策略和商业安全策略，安全模型包括具有代表性的BLP机密性安全模型、Biba完整性安全模型和RBAC安全模型；
- ✓ 描述了安全操作系统的访问控制机制；
- ✓ 给出了操作系统的典型缺陷、安全操作系统的评测方法与评估准则。