信息系统安全

李涛

目录
CONTENTS

01 信息系统安全概述

什么是信息系统?

- 信息系统（Information System）是以提供特定信息处理功能、满足特定业务需要为主要目标的计算即系统
  - 现代化的大型信息系统都是建立在计算机操作系统和计算机网络不断发展的基础上的
  - 一直以来，信息安全的问题都受到操作系统和网络安全特征的影响

信息系统安全的发展

- 随着计算机操作系统和网络的发展，安全问题也在不断变化
- 单机用户时期（20世纪40年代至60年代中期）
  - 一台机器、一个用户、一个或几个进程。不存在计算机安全的问题，只有物理安全的问题
- 单机多用户时期（20世纪60年代末至80年代末）
  - 同一台机器上多用户运行多进程，共用文件系统、CPU等资源。关注文件系统、CPU的安全
  - 由操作系统来保护数据，操作系统进行用户身份认证和访问控制

信息系统安全的发展

- 多机多用户时期（20世纪80年代末至今）
  - 多台机器构建的分布式系统，安全问题更加复杂
  - 出现不同的多个主体（Subject）
  - 服务器、数据库及账户、用户密码等关键数据由机构管理，用户密码及安装在个人计算机上的客户端由客户自己管理并负责
  - 机构要确认用户身份、认证用户权限，实施访问控制
  - 用户担心机构系统的不安全
- 由于计算机网络和分布式系统的发展，信息安全内涵扩大，不仅是计算机安全、信息技术的问题，而是扩展为组织安全、业务安全的等管理的问题

安全需求的来源

- 根据数据自身性质（Information Type）确定其安全需求
- 安全保护措施被破坏时，信息系统和拥有该信息系统的机构将遭受不同程度的负面影响
- 安全需求分类：根据数据安全保护被破坏时造成的影响对数据进行分类
- 如何具体保障安全需求?
  - 机密性、完整性、真实性、抗抵赖性等基本属性
  - 安全需求的目标：确保信息系统由足够的保护措施达到这些基本属性

安全需求的来源

- 机构根据自身需要，在安全风险和系统成本之间做出平衡
  - 不同的组织机构（部门）因为业务特点对某些安全属性更为重视
  - 从属不同机构的信息系统很可能有不一样的安全目标
  - 一般企业的电子商务系统 VS 国家部门的电子政务系统

安全需求的来源

- 构建一个安全信息系统前，首先分析机构对安全的理解和安全需求，然后具体实现安全标准和安全技术
  - 机构的管理人员一般不是安全专家，如何获取和分析安全需求?
  - 如何让来自不同领域的人员对安全目标达成共识?
  - 如果对安全需求是否实现进行评估和跟踪?
- 理解机构的业务目标、信息需求、技术环境、解决方案等信息，实现安全信息系统的构建

信息系统安全问题的困境

- 监听和篡改，系统内的数据易受监听和篡改
  - 现代网络的开放性和缺少集中式的管理
- 假冒身份和擅自泄露信息
  - 不同的机器有不同的管理人员、身份认证机制和安全策略
- 程序模块运行在不同机器上，信息必须在开放网络间传输
  - 信息通过网络来传输，加剧了安全隐患
- 系统资源由特定的服务器管理
  - 数据存储在一台机器，又由另一台机器上的进程来处理；身份认证在一台机器开始，却在另一台机器上进行验证

信息系统安全问题的困境

- 对所有的网络数据包进行加密，双向身份认证，强有力的安全保护策略……
- 安全需求：
  - 信息不能被恶意篡改
  - 不能向未经授权方泄露信息
  - 信息传输双方的身份认证和可行
- 安全服务：机密性、身份认证、完整性、不可抵赖性
  - 这四个方面不等于安全本身，仅仅是安全的服务
- 信息系统的安全需求是一个管理与技术需求的平衡，很大程度上收到机构的治理、业务、成本和风险等因素影响

信息系统安全基本概念

- 安全：国家标准（GB/T 28001）对“安全“给出的定义是”免除了不可接受的损害风险的状态”，也就是防备危害和其它损害。
- 信息安全：
  - 美国国家安全系统委员会（CNSS）：“信息安全就是保护信息及其关键要素，包括使用、存储以及传输信息的系统和硬件”。基础是CIA：机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）
  - ISO/IEC 27000:2005《信息安全管理体系原理与术语》：“保护、维持信息的机密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质
  - 从具体需求分析，信息安全可以涉及物理安全、操作安全、通信安全、系统安全、网络安全、数据安全、安全管理等多个方面

信息系统安全基本概念

- 信息系统安全
  - 最终目标是为了支持、促进所属机构的长远发展
  - 信息系统是否满足机构自身的发展目的或使命要求?
  - 信息系统是否能为机构的长远发展提供安全方面的保障?
  - 机构在信心安全方面所投入的成本与所保护的信息价值是否平衡?
  - 什么程度的信息系统安全保障在给定的系统环境下能保护的最大价值是多少?
  - 信息系统如何达到有效地实现安全保障?

信息系统安全基本概念

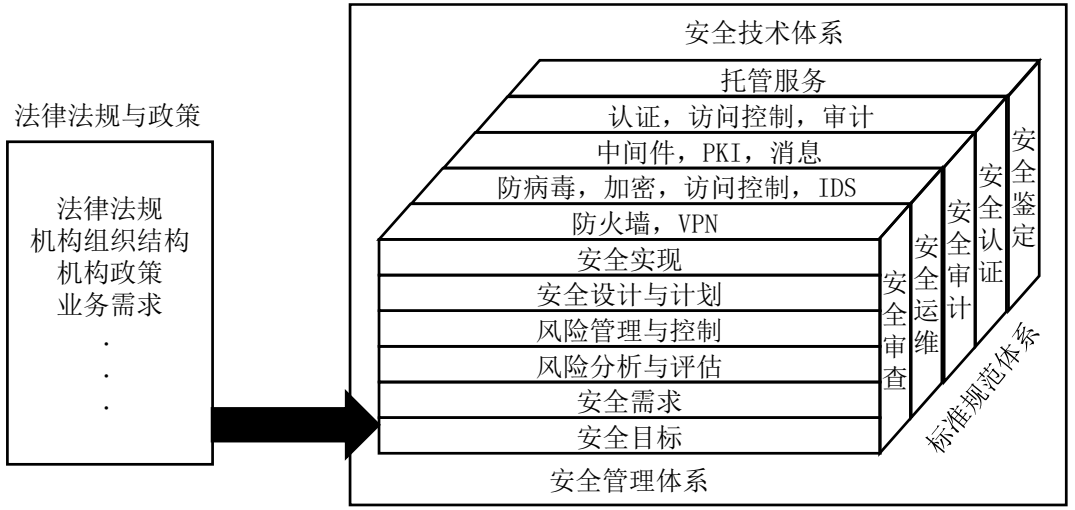
- 信息系统是以提供特定信息处理能力、满足特定业务需要为主要目标的计算机应用系统
- 典型的信息系统都属于分布式系统中的一种：一个硬件或软件组件分布在网络计算机上，通过消息传递进行业务处理和操作协调的系统
  - 物理分布
  - 环境多变
  - 分布式管理

信息系统安全体系概述

- 信息系统安全体系：为了实现安全目标，信息系统需要部署与安全相关的物理组件和逻辑组件。这些与安全相关的组件构成了信息系统安全体系（Information Systems Security Architecture, ISSA)
  - 信息系统安全技术体系
  - 信息系统安全管理体系
  - 信息系统安全标准体系
  - 信息系统安全法律体系

信息系统安全体系

- 信息系统安全体系框架



信息系统安全技术体系

- 信息系统安全技术体系是对实现安全信息系统所采用的安全技术的构建框架，包括：
  - 信息系统安全的基本属性
  - 信息系统安全的组成与相互关系
  - 信息系统安全等级划分
  - 信息系统安全保障的基本框架
  - 信息系统风险控制手段及其技术框架
  - ……

信息系统安全技术体系

- 从具体的应用软件构建划分，信息系统安全技术体系分为传输安全、系统安全、应用程序安全和软件安全
- 根据涉及技术的不同，可将信息系统安全技术体系粗略分为：
  - 信息系统硬件安全
  - 操作系统安全
  - 密码算法技术
  - 安全协议技术
  - 访问控制管理
  - 安全通信技术
  - 应用程序安全
  - 身份识别和认证管理技术
  - 入侵检测技术
  - 防火墙技术等安全信息系统的构建技术

信息系统安全管理体系

- 从机构的安全目标出发，利用机构体系结构这一工具分析并理解机构自身的管理运行架构，并纳入安全管理理念，对实现信息系统安全所采用的安全管理措施进行描述
- 包括信息系统的安全目标、安全需求、风险评估、工程管理、运行控制和管理、系统监督检查和管理等方面
- 期望在整个信息系统开发生命周期内实现机构的全面可持续的安全目标

信息系统安全管理体系

- 信息系统安全管理体系范围广泛，主要包括以下内容：
  - 安全目标确定
  - 安全需求获取与分类
  - 风险分析有评估
  - 风险管理与控制
  - 安全计划制定
  - 安全策略与机制实现
  - 安全措施实施

信息系统安全管理体系

- 信息系统安全管理体系各组成部分的关系：
  - 信息系统的安全目标由与国家安全相关的法律法规、机构组织结构、结构的业务需求等因素确定
  - 将安全目标细化、规范化为安全需求，安全需求再按照信息资产（如业务功能、数据）的不同安全属性和重要性进行分类
  - 安全需求分类后，要分析系统可能受到的安全威胁和面临的各种风险，并对风险的影响和可能性进行评估，得出风险评估结果
  - 根据风险评估结果，选择不同的应对措施和策略，以便管理和控制风险
  - 制定安全计划
  - 设定安全策略和相应的实现策略的机制
  - 实施安全措施

信息系统安全标准体系

- 完整的信息系统安全标准体系，是建立信息系统安全体系的重要组成部分，也是信息系统安全体系实现规范化管理的重要保证
- 信息系统安全标准体系是对信息系统安全技术和安全管理的机制、操作和界面的规范，是从技术和管理方面以标准的形式对有关信息安全的技术、管理、实施等具体操作进行的规范化描述

安全鉴定
安全认证
安全审计
安全运维
安全审查

信息系统安全法律法规

- 所构建的信息系统在设计、实施和管理上必须遵守机构所在国家的信息安全相关的法律法规，以及相关的国家标准和行业标准
- 信息安全从业人员必须理解当前的法律环境，及时了解出台的相关法律、规则

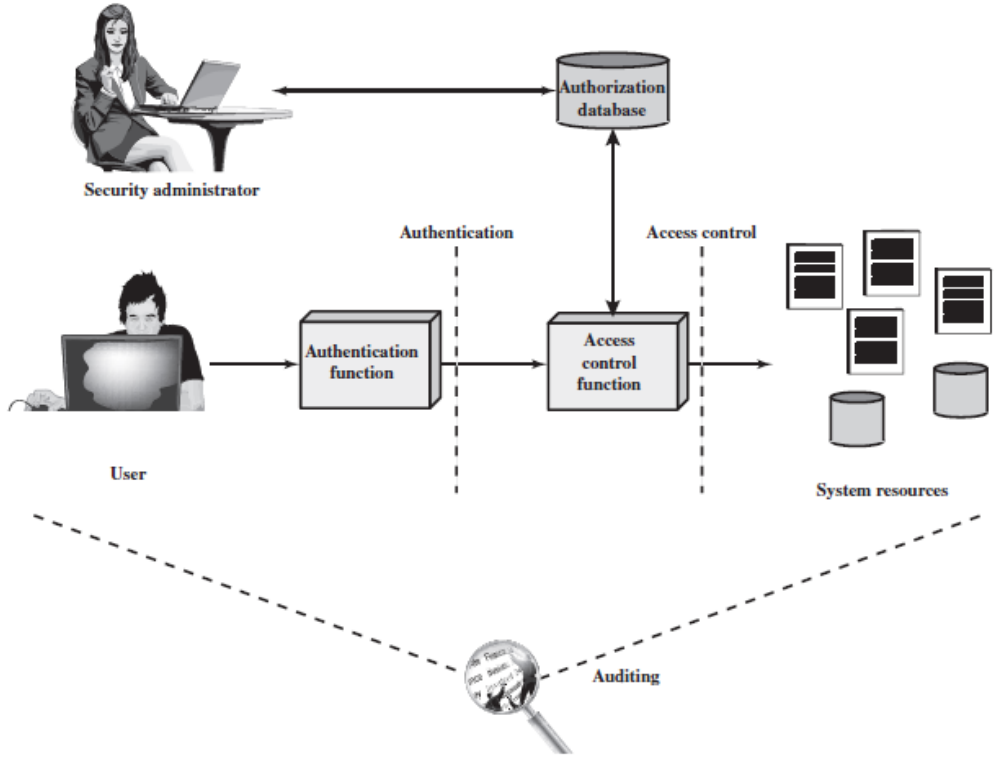
小结

- 以法律法规作为安全目标和安全需求的依据
- 以标准规范体系作为检查、评估和测评的依据
- 以管理体系作为风险分析和控制的理论基础与处理框架
- 以技术体系作为风险控制的手段与安全管理的工具

02 访问控制

访问控制语境

- 访问控制与其他安全功能的关系



访问控制策略

- 基于角色的访问控制(RBAC)
  - 基于用户在系统中所具有的角色和说明各种角色用户享有哪些访问权的规则来控制访问
- 基于属性的访问控制(ABAC)
  - 基于用户、被访问资源及当前环境条件来控制访问
- 自主访问控制(DAC)
  - 基于请求者的身份和访问规则（授权）控制访问，规定规则请求者可以（或不可以）做什么
- 强制访问控制(MAC)
  - 通过比较具有安全许可（表明系统实体有资格访问某种资源）的安全标记（表明系统资源的敏感或关键程度）来控制访问

主体、客体和访问权

- 主体
  - 能够访问客体的实体
  - 三类主体：所有者、组、世界
- 客体
  - 外界对其访问受到控制的资源
  - 用来包含或接收信息的实体
- 访问权
  - 描述了主体可以访问客体的方式
  - 可以包括:
    - 读，写，执行
    - 删除，创建，搜索

自主访问控制

- 一个实体可以被授权按其自己的意志使另一个实体能够访问某些资源

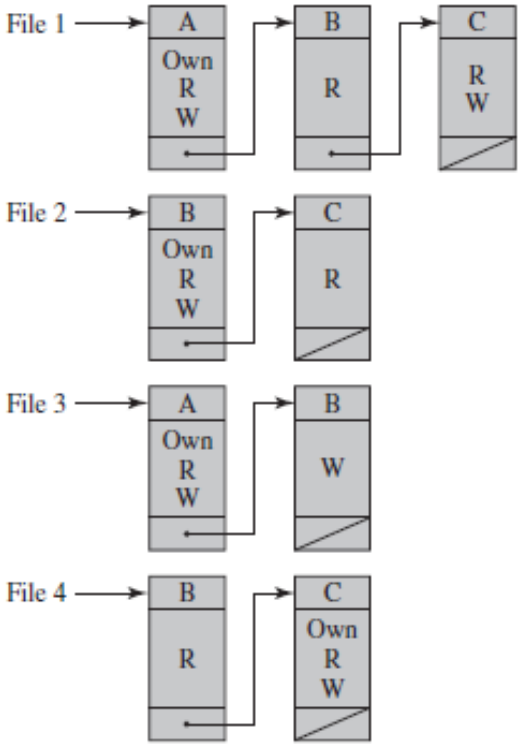
- 使用访问矩阵
  - 一维由试图访问资源的被标识的主体组成
  - 另一维列出可以被访问的客体

- 矩阵中的每项表示一个特定主体对一个特定客体的访问权

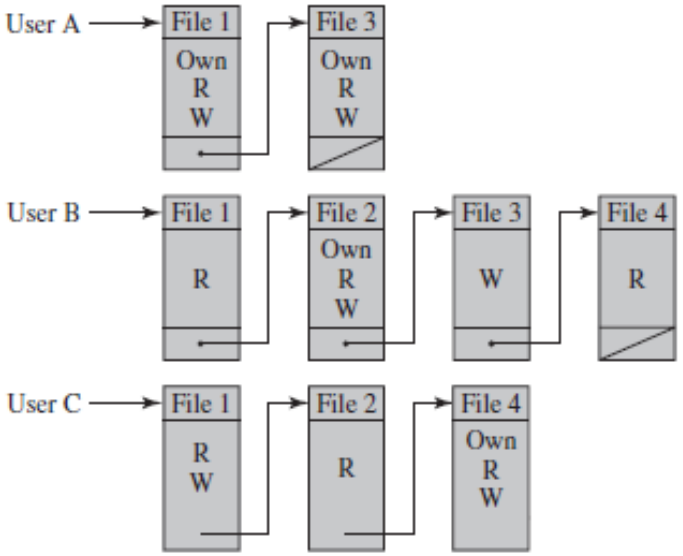
访问矩阵

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

访问控制表



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)

授权表

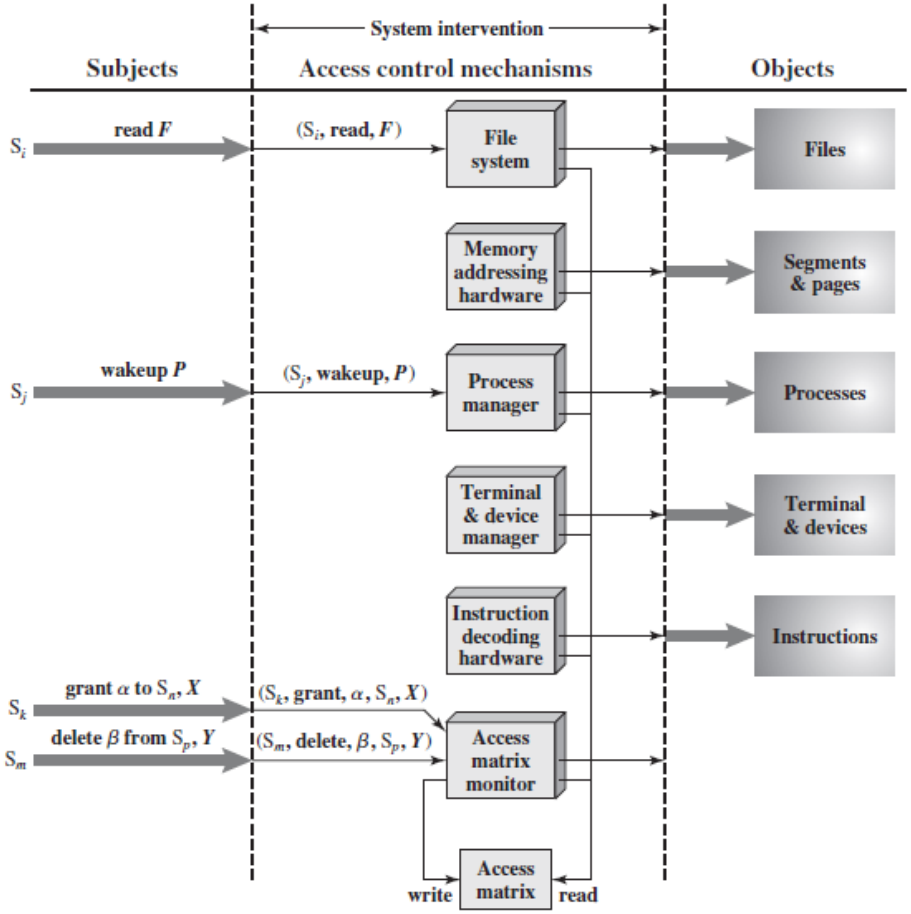
Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

扩展的访问控制矩阵

		OBJECTS								
		Subjects			Files		Processes		Disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read*	read owner	wakeup	wakeup	seek	owner
	S_2		control		write*	execute			owner	seek*
	S_3			control		write	stop			

* = copy flag set

访问控制功能


System intervention
Subjects
Access control mechanisms
Objects
S_i
read F
(S_i, read, F)
File system
Files
Memory addressing hardware
Segments & pages
S_j
wakeup P
(S_j, wakeup, P)
Process manager
Processes
Terminal & device manager
Terminal & devices
Instruction decoding hardware
Instructions
S_k
grant α to S_n, X
$(S_k, \text{grant}, \alpha, S_n, X)$
S_m
delete β from S_p, Y
$(S_m, \text{delete}, \beta, S_p, Y)$
Access matrix monitor
Access matrix
write
read

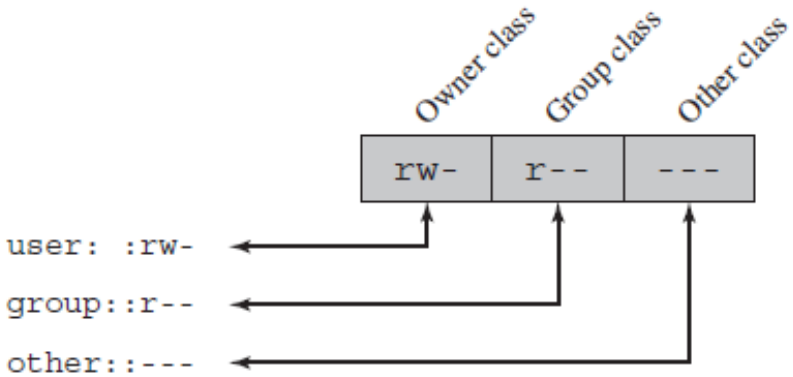
UNIX文件访问控制

- **所有类型的UNIX文件都由操作系统通过inode管理 (index nodes)**
  - 包含操作系统对一个文件所需的关键信息的控制结
  - 几个文件名可以与一个inode关联
  - 一个活动inode仅与一个文件关联
  - 文件的属性及访问许可和其他控制信息都存储在inode中
  - 在磁盘上有个inode表，其中包含了文件系统中所欲文件的inode
  - 打开一个文件时，它的inode被读进主存，存储在驻留内存的inode表中

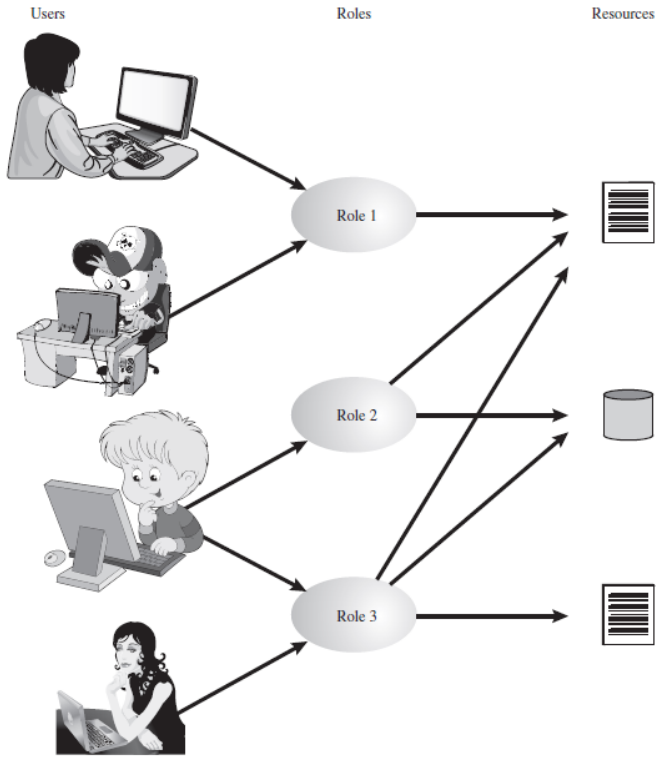
- **目录呈分层树状结构**
  - 每个目录包含文件或其他目录
  - 包含文件名和指向关联indeo的指针列表

UNIX文件访问控制

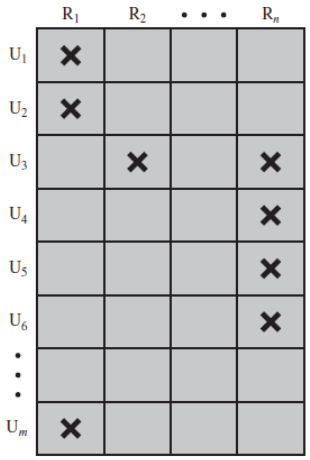
- 每个UNIX文件被分配一个唯一的用户标识号(user ID)
- 用户是主组的成员，使用组ID标识
- 属于一个特定的组
- 12个保护位
  - 指定文件属主、同组用户和其他用户的读、写和执行许可
- 属主ID、属组ID和保护位都是inode的一部分



基于角色的访问控制



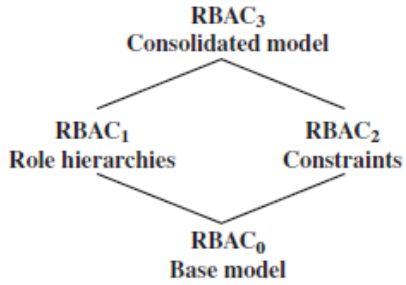
基于角色的访问控制



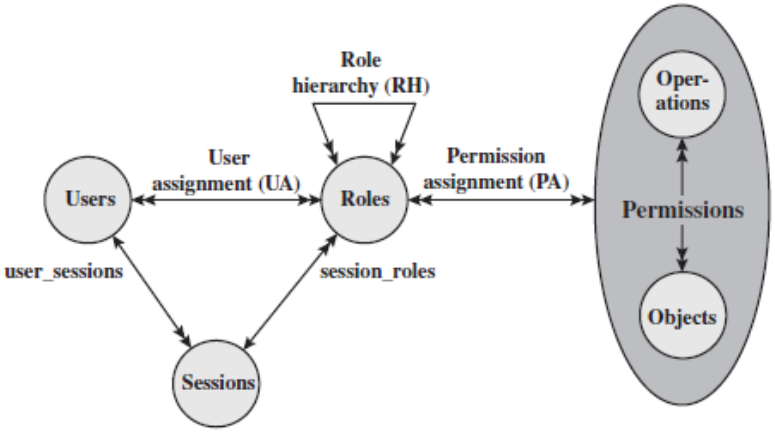
OBJECTS

ROLES	R1	R2	Rn	F1	F2	P1	P2	D1	D2
R1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R2		control		write *	execute			owner	seek *
•									
•									
•									
Rn			control		write	stop			

RBAC 参考模型

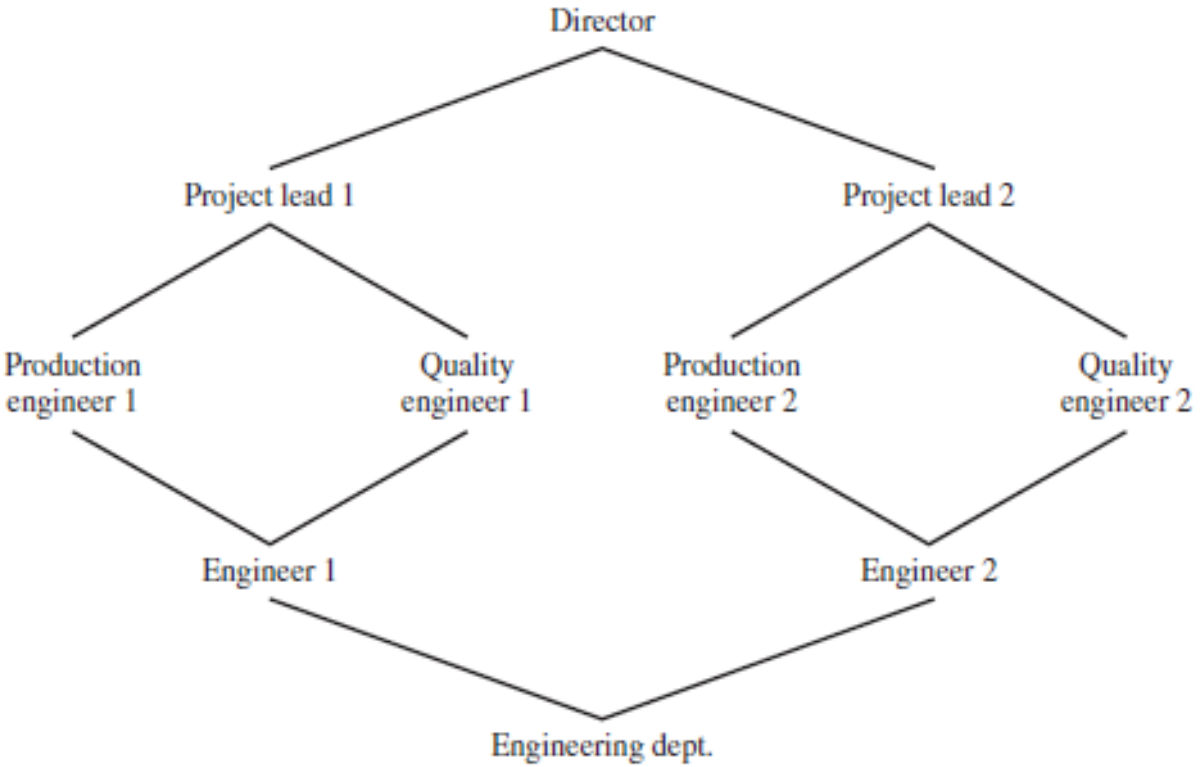


(a) Relationship among RBAC models



(b) RBAC models

角色层次


Director
Project lead 1
Project lead 2
Production engineer 1
Quality engineer 1
Production engineer 2
Quality engineer 2
Engineer 1
Engineer 2
Engineering dept.

约束 - RBAC

- 提供了一种令RBAC适应组织中的管理和安全策略细节的手段
- 约束是在角色之间定义的关系或与角色相关的条件
- 类型:
  - **互斥角色**
    - 一个用户只能被分配给集中集合中的一个角色 (静态或者动态)
    - 任何许可 (访问权)只能被授予给集合中的一个角色
  - **基数**
    - 设置关于角色的最大数值
  - **先决条件**
    - 规定用户被分配一个指定角色时，只能先被分配一个特定角色

基于属性的访问控制

- 能够定义表达资源和主体二者属性条件的授权
- 优势在于灵活性以及表达能力
- 主要障碍是需要考虑每次访问对资源和用户属性的评价所造成的性能影响
- Web服务是实现ABAC模型的开创性技术，尤其是引入可扩展的访问控制标记语言(XAMCL)
- 将ABAC应用到云服务

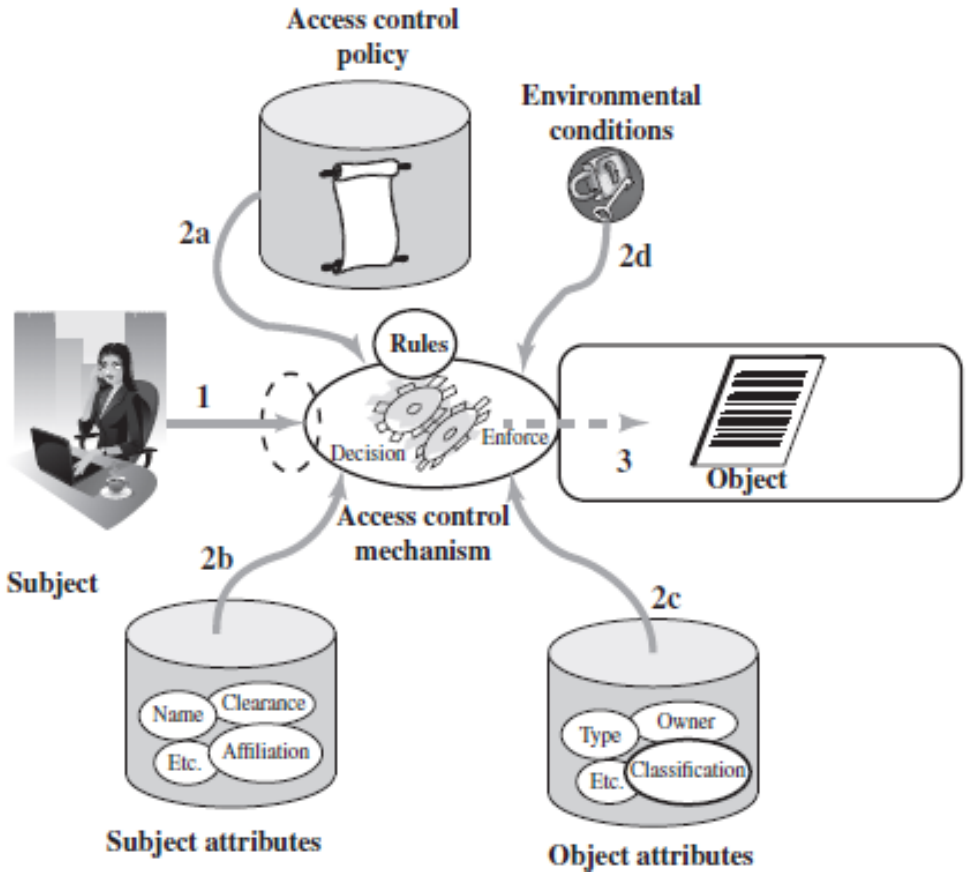
基于属性的访问控制

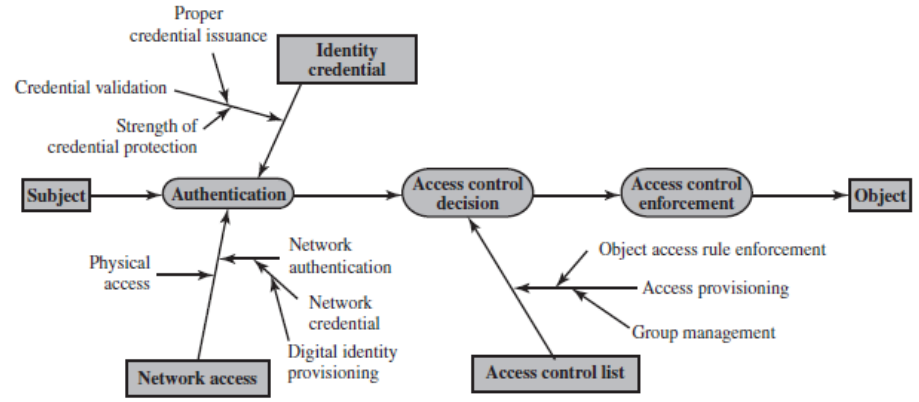
- **主体属性**
  - 主体是一个主动的实体，能引起客体间的信息流动或者系统状态的改变
  - 每个主体都有能够定义其身份和特征的关联属性
- **客体属性**
  - 客体（资源）是一个被动的包含或接收信息的与信息系统相关的实体
  - 客体具有可以用来制定访问控制决策的属性
- **环境属性**
  - 描述信息访问发生时所处的运行的、技术的甚至态势的环境或情境

基于属性的访问控制

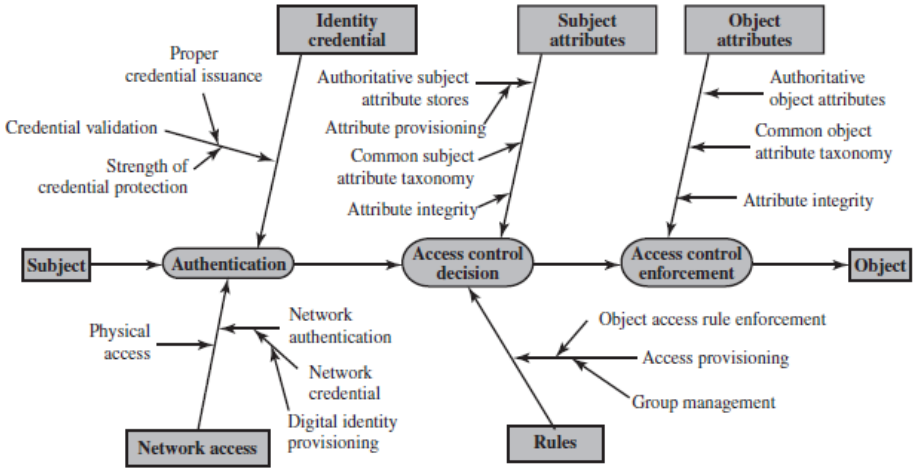
- 通过对实体（主体和客体）属性、操作及与请求相关的环境的评价规则来控制对客体的访问
- 依赖于对给定环境中的主体属性、客体属性以及定义主客体属性组合所允许操作的形式化联系或访问控制规则的评价
- 能够实现DAC, RBAC, 和 MAC 的思想
- 允许更大规模的离散式输入进入访问控制决策

ABAC 情景


Access control policy
Environmental conditions
2a
2d
Rules
1
Decision
Enforce
3
Object
Subject
Access control mechanism
2b
2c
Name
Clearance
Etc.
Affiliation
Type
Owner
Etc.
Classification
Subject attributes
Object attributes



(a) ACL Trust Chain

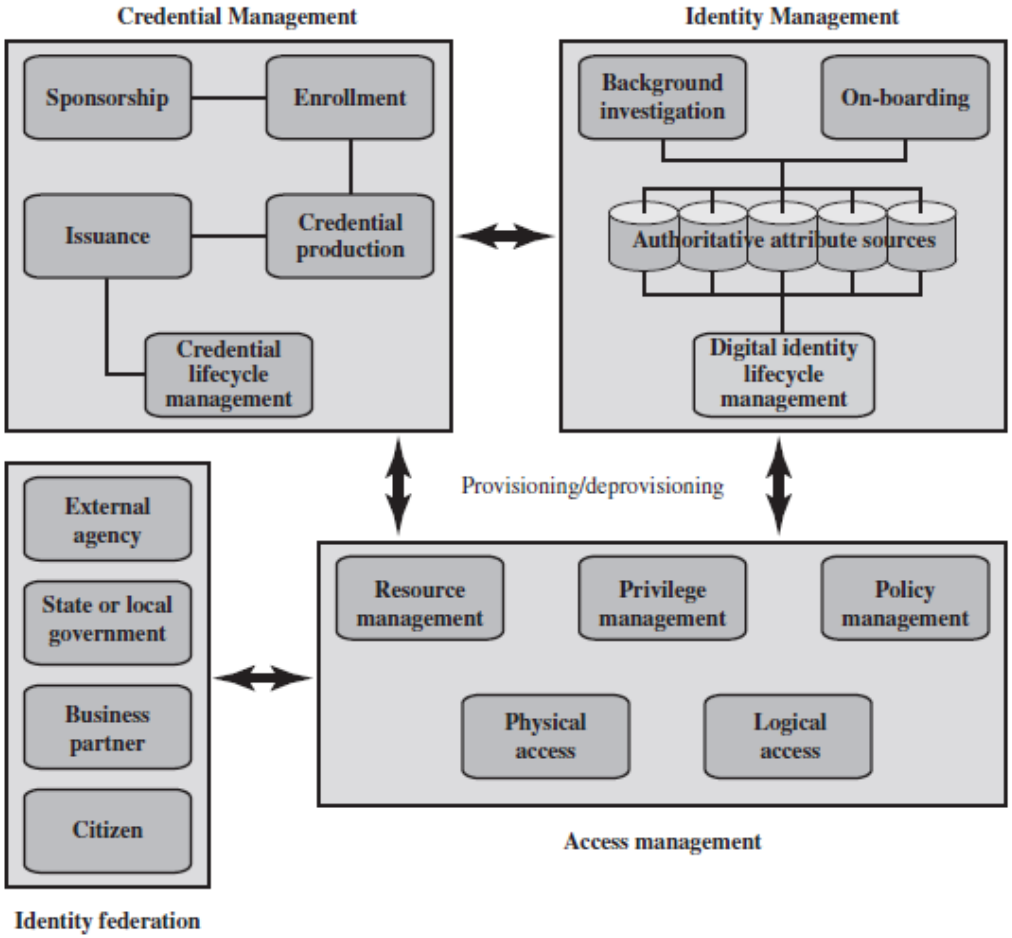


(b) ABAC Trust Chain

身份、凭证和访问管理（ICAM）

- 管理和实现数字身份（及相关属性）、凭证和访问控制的总和性方法
- 由美国政府开发
- 旨在:
  - 创建个体以及“非人实体（NPE）”的可信数字身份表示
  - 将这些身份绑定到可能成为个体或NPE提供访问交易代理的凭证
    - 凭证是一个对象或数据结构，将身份及可选的附加属性权威的绑定到用户所拥有的并控制的权标
  - 使用凭证对机构资源提供授权访问

ICAM


Credential Management
Identity Management
Sponsorship
Enrollment
Issuance
Credential production
Credential lifecycle management
Background investigation
On-boarding
Authoritative attribute sources
Digital identity lifecycle management
Provisioning/deprovisioning
External agency
State or local government
Business partner
Citizen
Identity federation
Resource management
Privilege management
Policy management
Physical access
Logical access
Access management

身份管理

- 关注的是将属性分配到数字身份上去，并且将数字身份与个体或者NPE连接起来
- 目标是建立一个独立于特定应用或情境的可信的数字身份
- 传统的且仍在广泛使用的应用和程序访问控制方法是为使用这些资源创建一个数字化表示的身份
- 结果，维护和保护身份自身被视为仅次于与应用相关的任务
- 最后一个要素，生命周期管理包含:
  - 保护个人身份信息的机制、策略和规程
  - 控制对身份数据的访问
  - 用于将权威身份数据分享给相关应用的技术
  - 撤销企业身份

凭证管理

- 对凭证生命周期的管理
  - 凭证的实例包括智能卡、私有/公开密钥和数字证书
- 凭证管理包括5个逻辑组件:
  - 授权的个体发起需要凭证的个体或实体建立对凭证的需求，例如部门主管发起部门员工
  - 受发起的个体注册凭证
    - 过程包括证明身份、采集个人经历有生物特征数据
    - 还可能涉及合并由身份管理组件维护的权威属性数据
  - 凭证生成
    - 根据凭证类型，生成过程可能涉及加密、使用数字签名、生成智能卡及其他功能
  - 凭证颁发给个体或NPE
  - 凭证必须在其生命周期内得到维护
    - 可能涉及撤销、补发/替换、重新注册、到期、个人标识码（PIN）重置、挂起或者恢复等

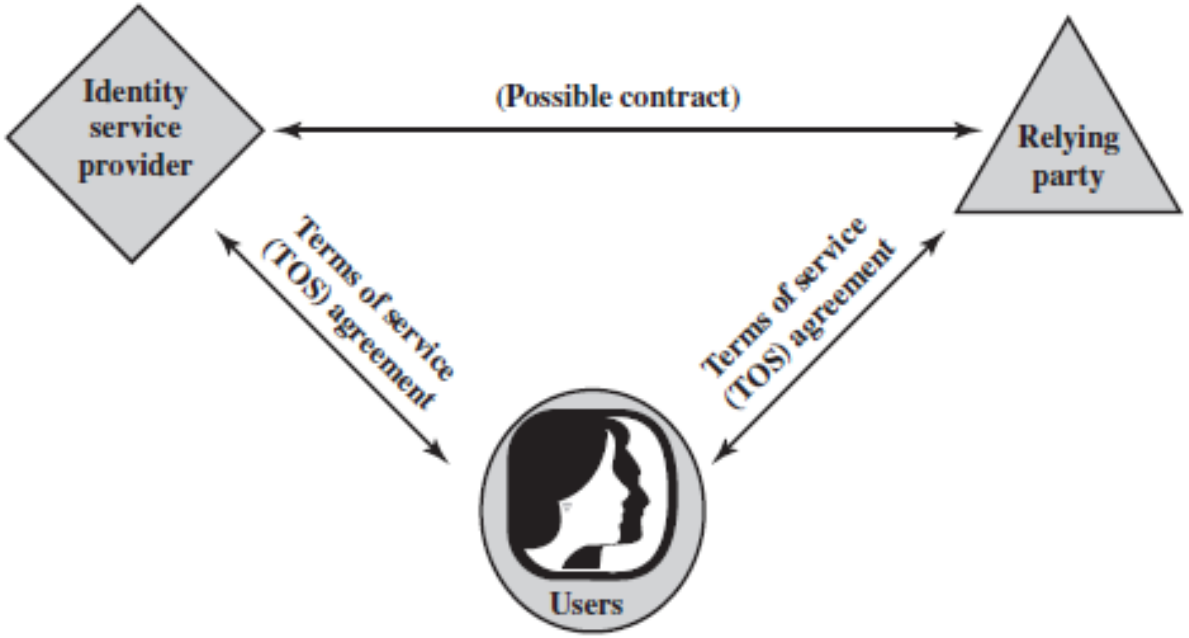
访问管理

- 对实体被授权访问资源的方法进行管理和控制
- 包括逻辑上和物理上的访问
- 可以在系统内部，也可以在外部单元
- 目的是确保当个体试图访问安全敏感的建筑物、计算机系统或数据时，进行适当的身份验证
- 企业级的访问控制设施需要以下三个支持要素:
  - 资源管理
  - 特权管理
  - 策略管理

身份联合问题

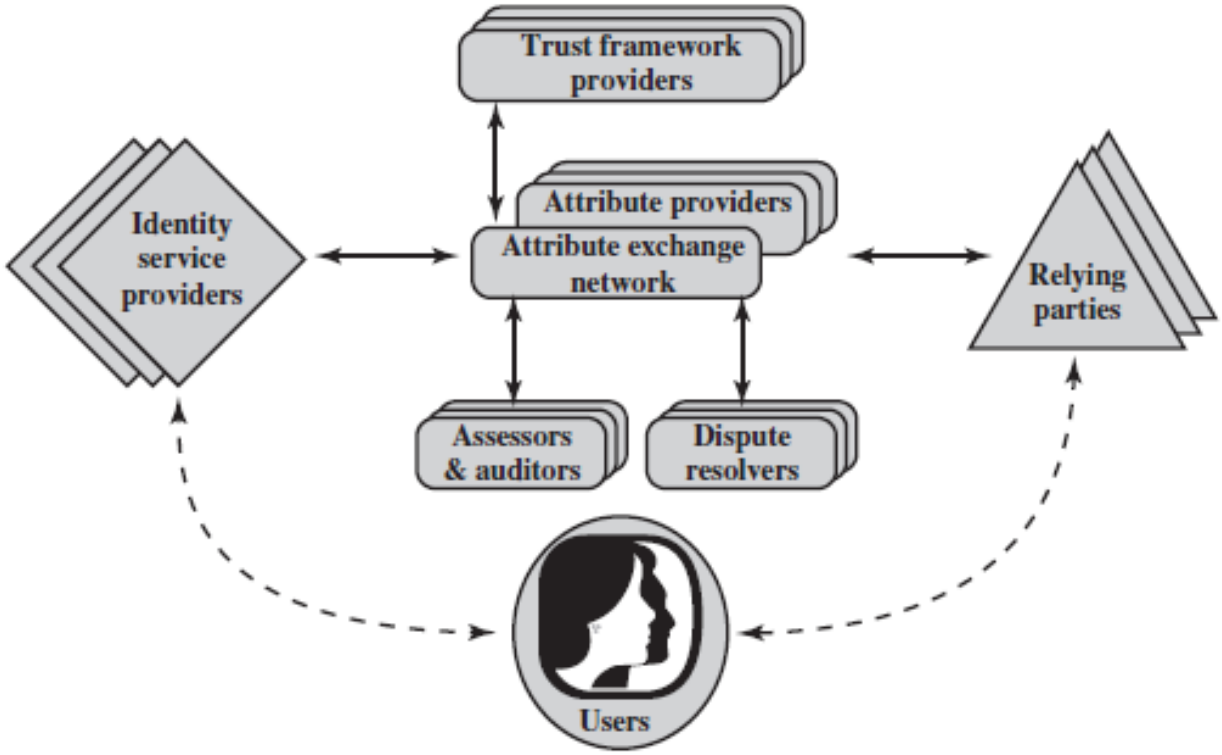
- 身份联合用来描述允许一个组织信任由另一个组织创建和发布的数字身份、身份属性与凭证的技术、标准、策略和过程
- 解决两个问题:
  - 如何信任需要访问自己系统且来自外部组织的个体的身份?
  - 当组织中的个体需要与外部组织合作时，你如何保证他们的身份?

身份信息交换



(a) Traditional triangle of parties involved in an exchange of identity information

身份信息交换



(b) Identity attribute exchange elements

银行业实例的职责和角色

(a) Functions and Official Positions

Role	Function	Official Position
A	financial analyst	Clerk
B	financial analyst	Group Manager
C	financial analyst	Head of Division
D	financial analyst	Junior
E	financial analyst	Senior
F	financial analyst	Specialist
G	financial analyst	Assistant
•••	•••	•••
X	share technician	Clerk
Y	support e-commerce	Junior
Z	office banking	Head of Division

银行业实例的职责和角色

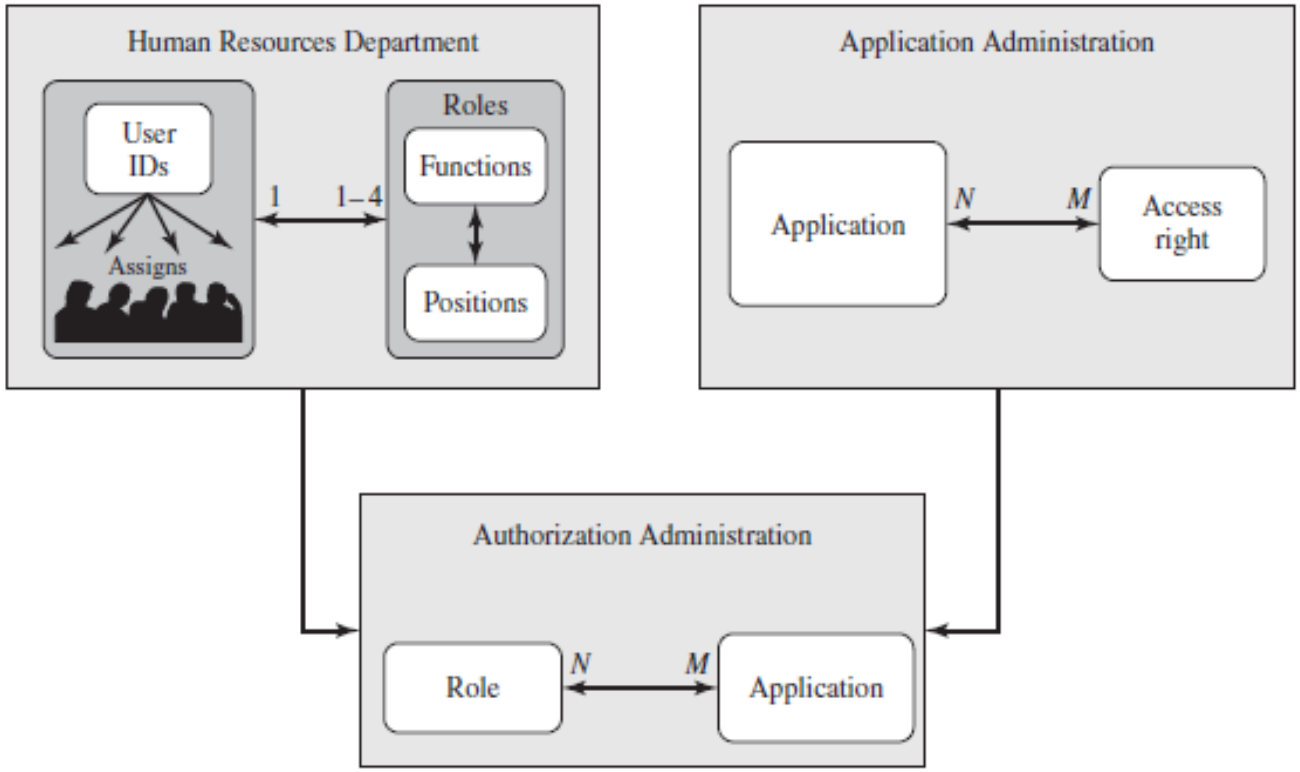
(b) Permission Assignments

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	1, 2, 3, 4, 7
	derivatives trading	1, 2, 3, 7, 10, 12, 14
	interest instruments	1, 4, 8, 12, 14, 16
	private consumer instruments	1, 2, 4, 7
• • •	• • •	• • •

(c) PA with Inheritance

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	7
	derivatives trading	14
	private consumer instruments	1, 2, 4, 7
• • •	• • •	• • •

访问控制管理


Human Resources Department
User IDs
Assigns
1
1–4
Roles
Functions
Positions
Application Administration
Application
N
M
Access right
Authorization Administration
Role
N
M
Application

03

多级安全

多级安全（MLS）

- RFC 2828 定义了多级安全：

一种系统运行模式，其中，当访问系统的某些用户对系统处理的某些数据既没有安全许可也不符合“须知”原则的时候，允许其在同一个系统里并发处理两个或多个安全级别的信息，分别以许可和密级为基础实现的用户与涉密材料的分离，依赖于系统的控制

BLP模型

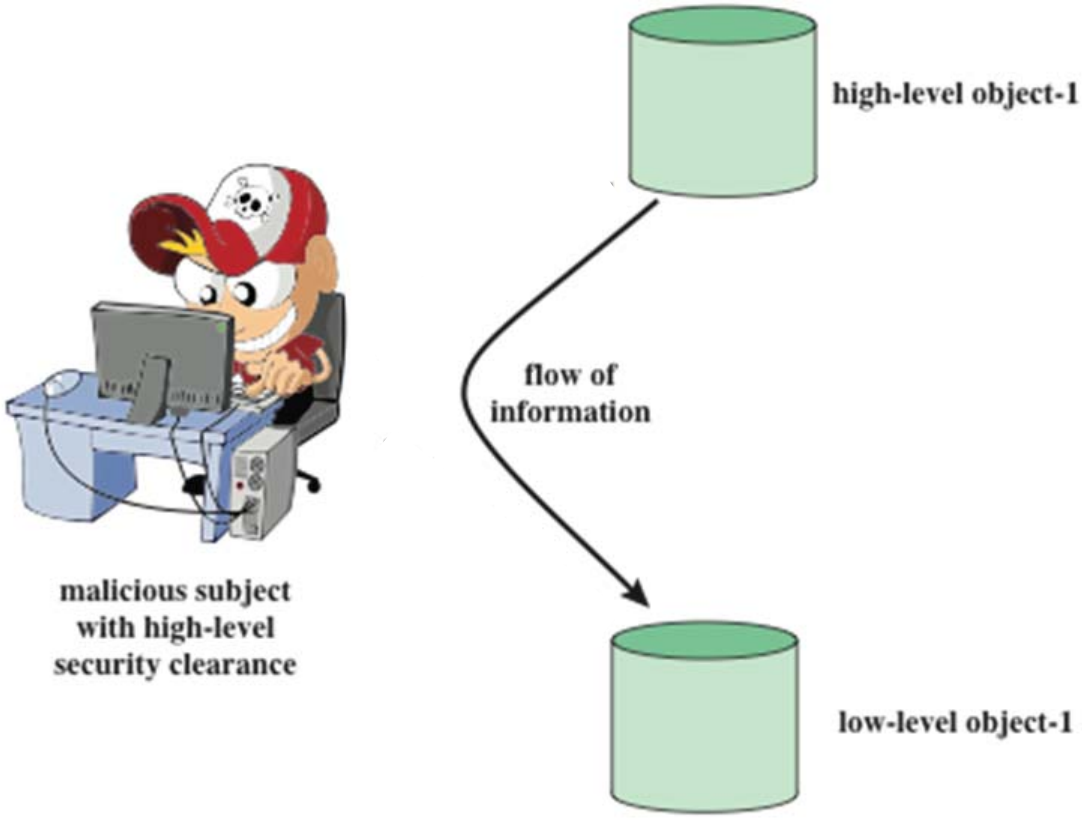
- 访问控制的形式化模型
  - 20世纪70年代开发出来的
- *主体和客体被分配一个安全等级*
  - 主体具有指定级别的安全许可
  - 客体具有指定级别的安全等级
  - 安全类形成严格的层次结构，成为安全级别
    - 绝密级 > 机密级 > 秘密级 > 内部级 > 公开级
  - 安全类控制主体访问客体的方式

BLP的访问模式

- 读
  - 主体仅被允许对客体读访问
- 追加
  - 主体仅被允许对客体写访问
- 写
  - 主体仅被允许对客体读、写访问
- 执行
  - 主体不被允许对客体读或写访问，但可以调用客体执行

多级安全策略

- 不上读
  - 主体只能读取相同或者更低安全级别的客体
  - 称为简单安全性
    - ss-property
- 不下写
  - 主体只能写入相同或者更高安全级别的客体
  - 称为 *-property


high-level object-1
flow of
information
malicious subject
with high-level
security clearance
low-level object-1

多级安全策略

- **ds-property：**一个个体（或角色）可以基于文件属主的判断、在MAC规则的约束下授予另一个个体（或角色）对一个文件的访问权
- **位置策略覆盖所有的自主访问控制**

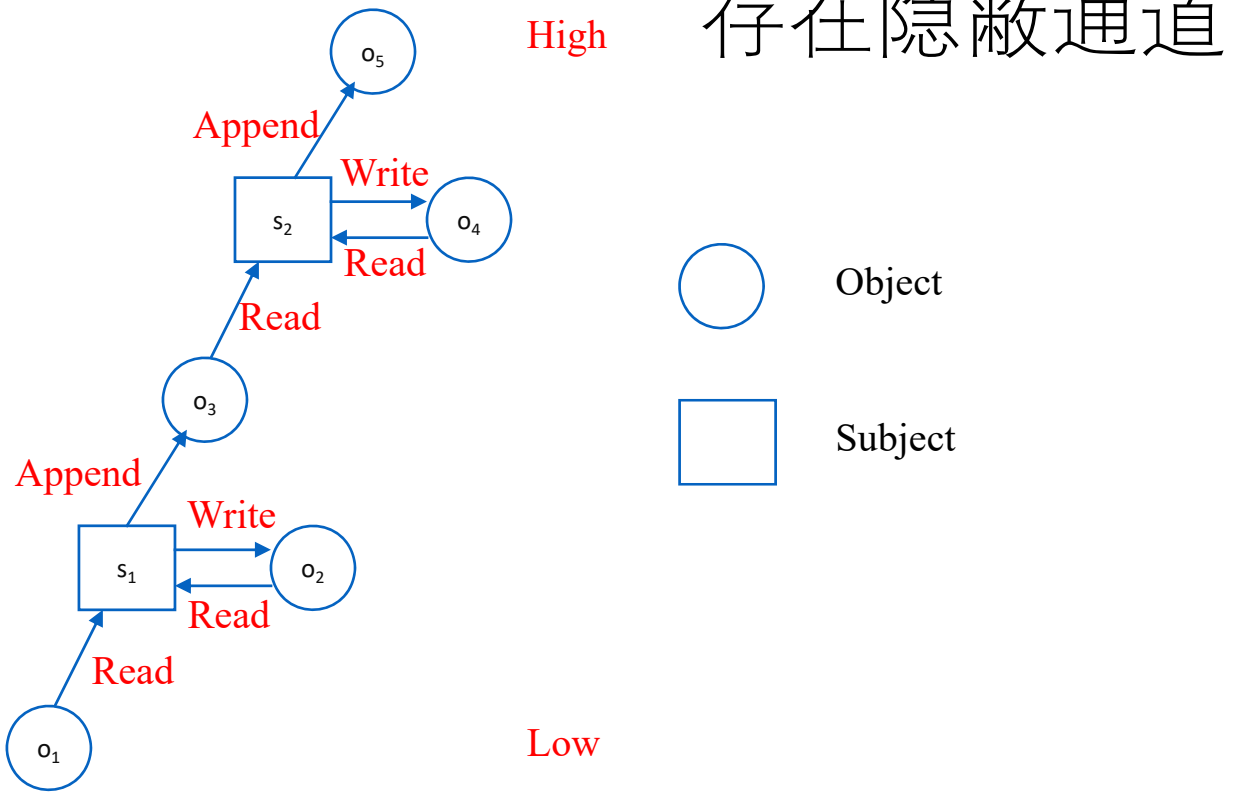
BLP的形式化描述

- 基于“系统当前状态”这一概念，状态用四元组(b, M, f, H)描述:
  - 当前访问集**b**: 形如（主体，客体，访问方式）的三元组的集合 (s, o, a)
    - 主体*s*以访问方式*a*对客体*o*进行访问
  - 访问矩阵**M**: 矩阵元素M_{ij}
    - 记录主体S_i 被允许对客体O_j的访问方式
  - 级别函数**f**: 给给每个主体和客体分配一个安全级别
    - $f_o(O_j)$客体O_j的密级
    - $f_s(S_i)$ 主体S_i的安全许可
    - $f_c(S_i)$ 主体S_i的当前安全级别
  - 层次**H**: 一颗有向有根树，其结点对应于系统中的客体

BLP的形式化描述

- BLP的三个特性:
  - **ss-特性**: $\forall (S_i, O_j, \text{read})$ has $f_c(S_i) \geq f_o(O_j)$
  - ***-特性**: $\forall (S_i, O_j, \text{append})$ has $f_c(S_i) \leq f_o(O_j)$
    and $\forall (S_i, O_j, \text{write})$ has $f_c(S_i) = f_o(O_j)$
  - **ds-特性**: current (S_i, O_j, A_x) implies $A_x \in M[S_i\ O_j]$
- BLP给出了形式化的命题
  - 理论上可以证明一个系统是安全的
  - 实践上很难

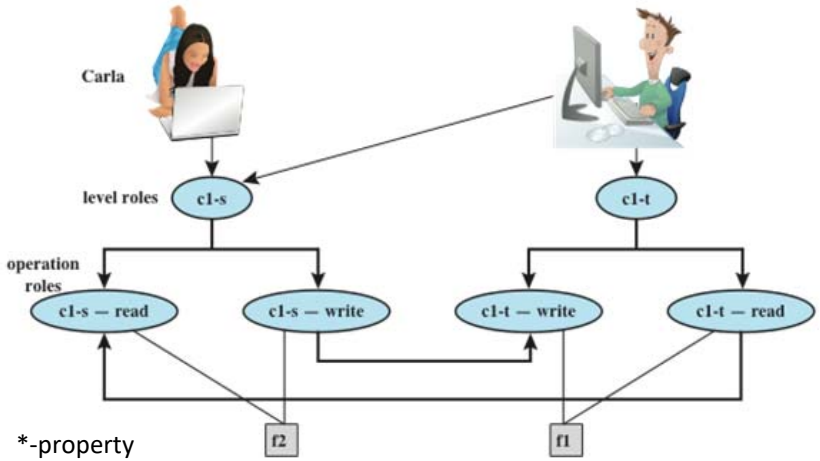
存在隐蔽通道


High
Low
o_5
Append
Write
s_2
o_4
Read
Read
o_3
Append
Write
s_1
o_2
Read
Read
o_1
Object
Subject

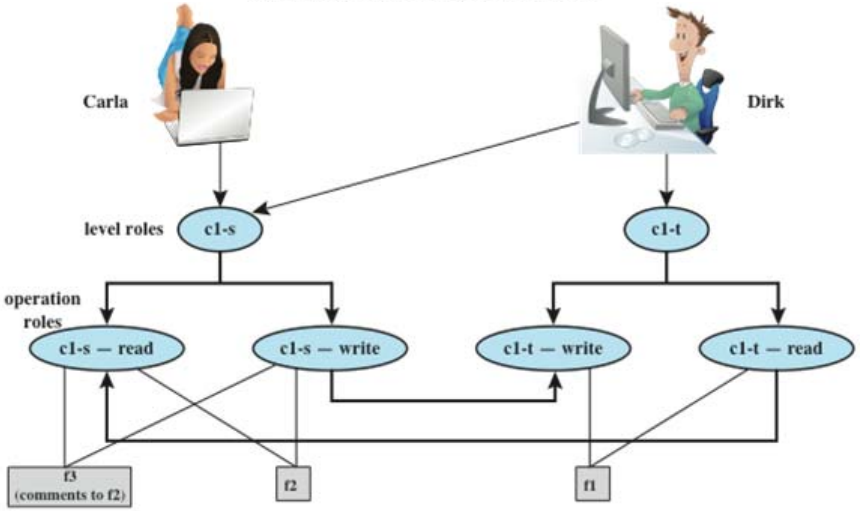
BLP的规则

1. 获得访问
2. 释放访问
3. 改变客体级别
4. 改变当前级别
5. 给予访问许可
6. 废除访问许可
7. 创建客体
8. 删除客体组

BLP实例

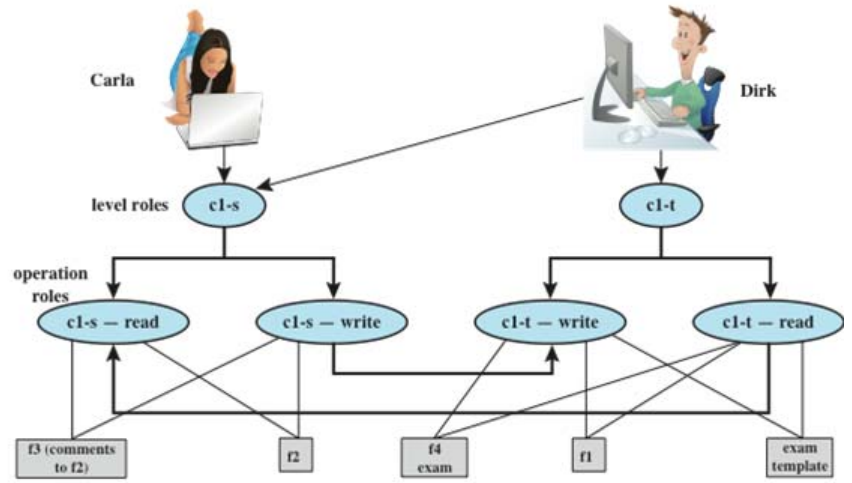


(a) Two new files are created: f1: c1-t; f2: c1-s



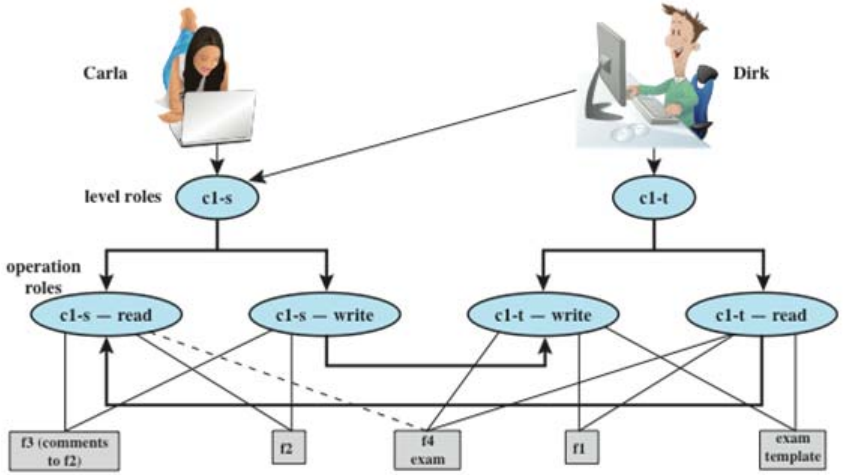
(b) A third file is added: f3: c1-s

BLP 实例



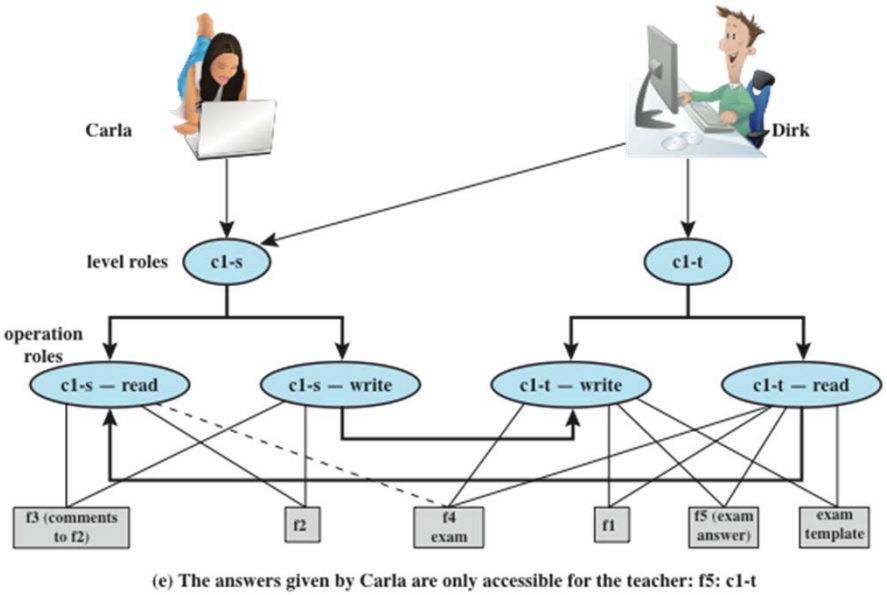
(c) An exam is created based on an existing template: f4: c1-t

ss-property and *-property



(d) Carla, as student, is permitted acess to the exam: f4: c1-s

BLP 实例



(e) The answers given by Carla are only accessible for the teacher: f5: c1-t

“**降级**” 通过可控制和可监控的方式

“**密级爬升**”: 新文档合并了来自不同来源和级别的信息

完整性如何考虑？

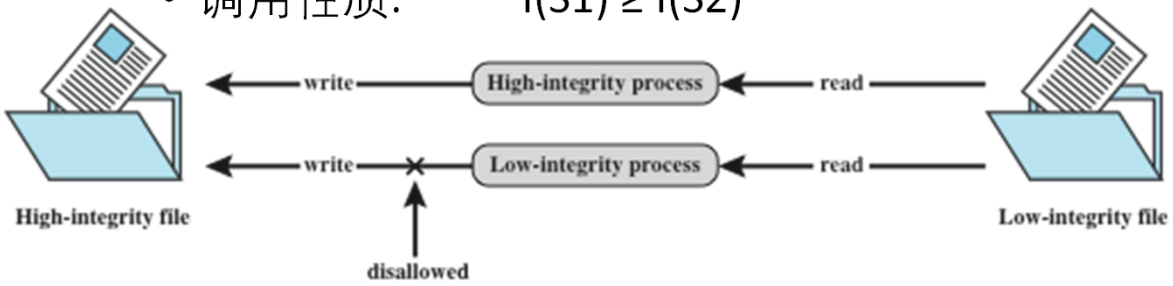
“**隐通道**”: 低级别（不可信）的可执行数据被高级别（可信）主体执行

BLP模型的限制

- 在一个MLS系统中，保密性和完整性不相容
  - MLS要么追求“权力”，要么追求“机密”
  - 这种互斥把一些在BLP风格的MLS环境中有效用的以权力和完整性为中心的有意思的技术排斥在外
- 可用方面的严重限制是在出现隐蔽通道时产生所谓“合谋者”问题
  - 对于共享资源，*-特性变得不可执行
    - 当（不可信的）低密级可执行数据被允许由高许可的（可信的）主体执行时，BLP模型就被有效地破坏了

Biba完整性模型

- 严格的完整性策略:
  - **修改（Modify）**: 在客体中写入或更新信息
  - **观察（Observe）**: 读取客体中的信息
  - **执行（Execute）**: 执行客体
  - **调用（Invoke）**: 从一个主体到另一个主体的通信
  - 简单完整性: $I(S) \geq I(O)$
  - 完整性紧闭: $I(S) \leq I(O)$
  - 调用性质: $I(S1) \geq I(S2)$



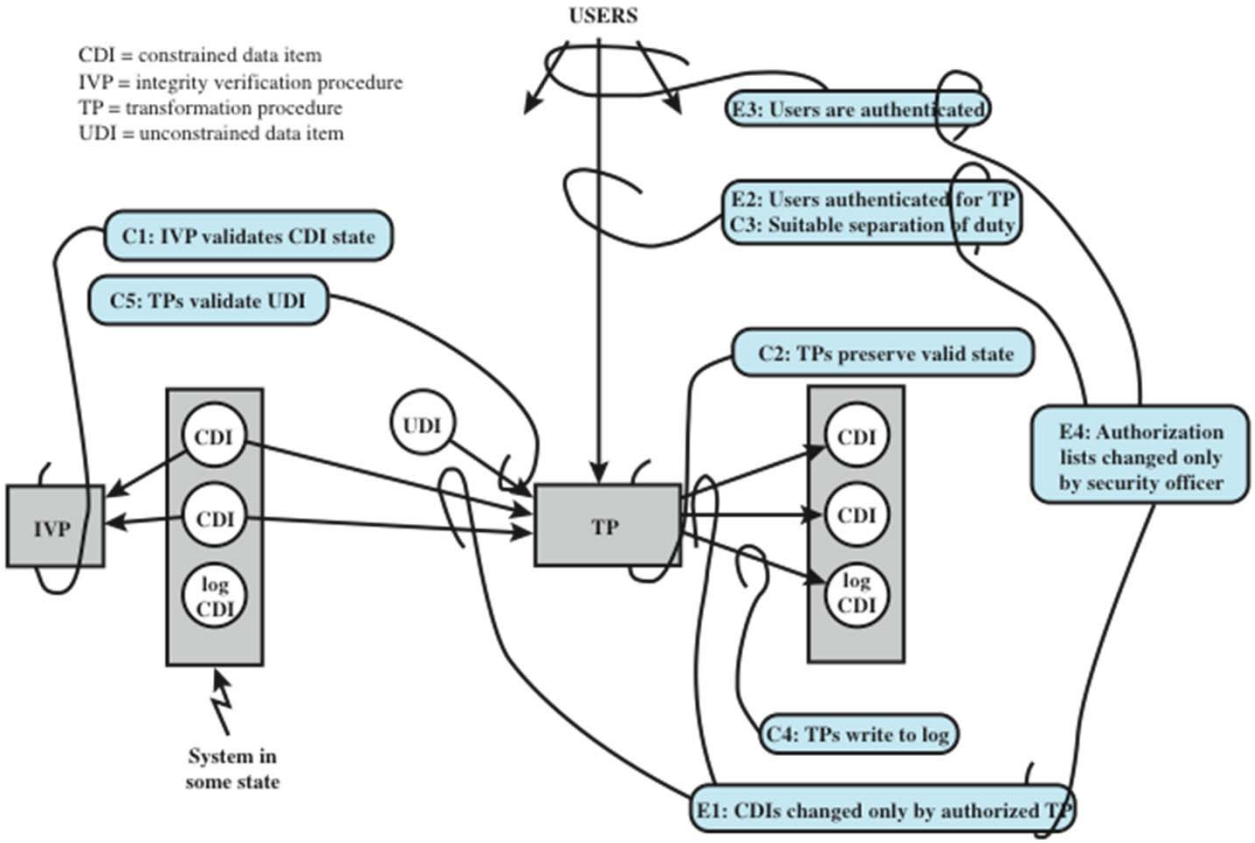
Clark-Wilson完整性模型

- 逼真地模拟了真实的商业运营
  - 良性实物（Well-formed transactions）
    - 用户不能随意操纵数据，只能以受控的方式操作数据，以确保数据完整性
  - 用户职责分离（Separation of duty among users）
    - 任何被允许创建或证明一个良性事物的人不能被允许执行该事务

Clark-Wilson完整性模型

- 模型的主要组件
  - 约束数据项(CDIs)
    - 受到严格完整性控制的主体
  - 无约束数据项(UDIs)
    - 未经检查的数据项，例如纯文本文件
  - 完整性验证过程(IVPs):
    - 旨在确保所有的CDI符合某个应用专用模型的完整性和一致性
  - 转换过程 (TPs):
    - 将CDI从一个一致状态改变到另一个一致状态的系统事务

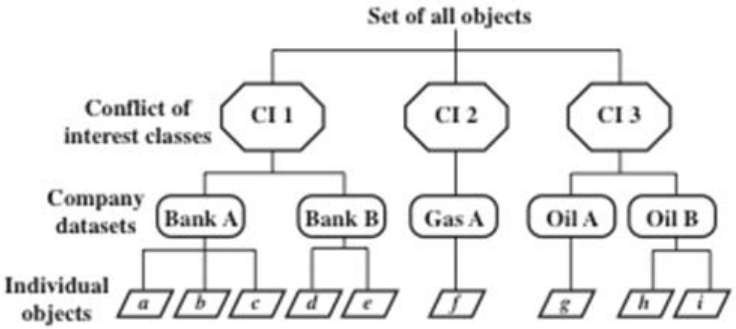
Clark-Wilson完整性模型



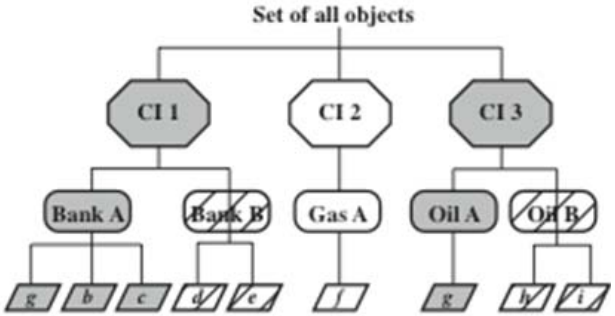
中国墙模型

- 完整性和机密性
- 同时使用了自主和强制访问的概念
  - **主体（Subjects）**：期望访问受保护客体的活动实体，包括用户和进程
  - **信息（Information）**：按三级层次结构组织的公司信息
    - **客体（Objects）**：独立信息项，每一项对应一家公司
    - **数据集（Dataset,** DS **）**：对应同一家公司的所有客体
    - **利益冲突（Conflict of interest** ,CI **）**类: 所有处于竞争地位的公司的数据集
  - **访问规则（Access rules）**：读、写访问规则

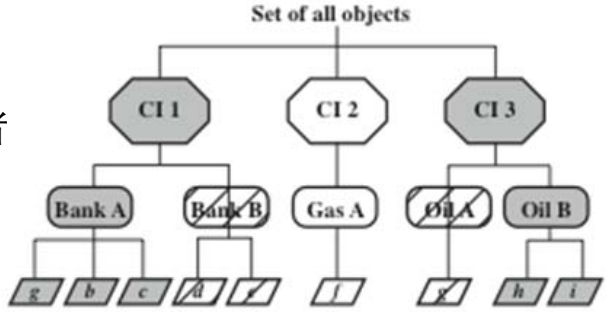
中国墙模型



(a) Example set



(b) John has access to Bank A and Oil A



(c) Jane has access to Bank A and Oil B

简单安全规则: 主体S可以“读”客体O当且仅当

- O与S已访问的一个客体在同一个DS中，或者
- O属于S尚未访问任何信息额一个CI

***-特性规则: 主体S可以“写”客体O当且仅当**

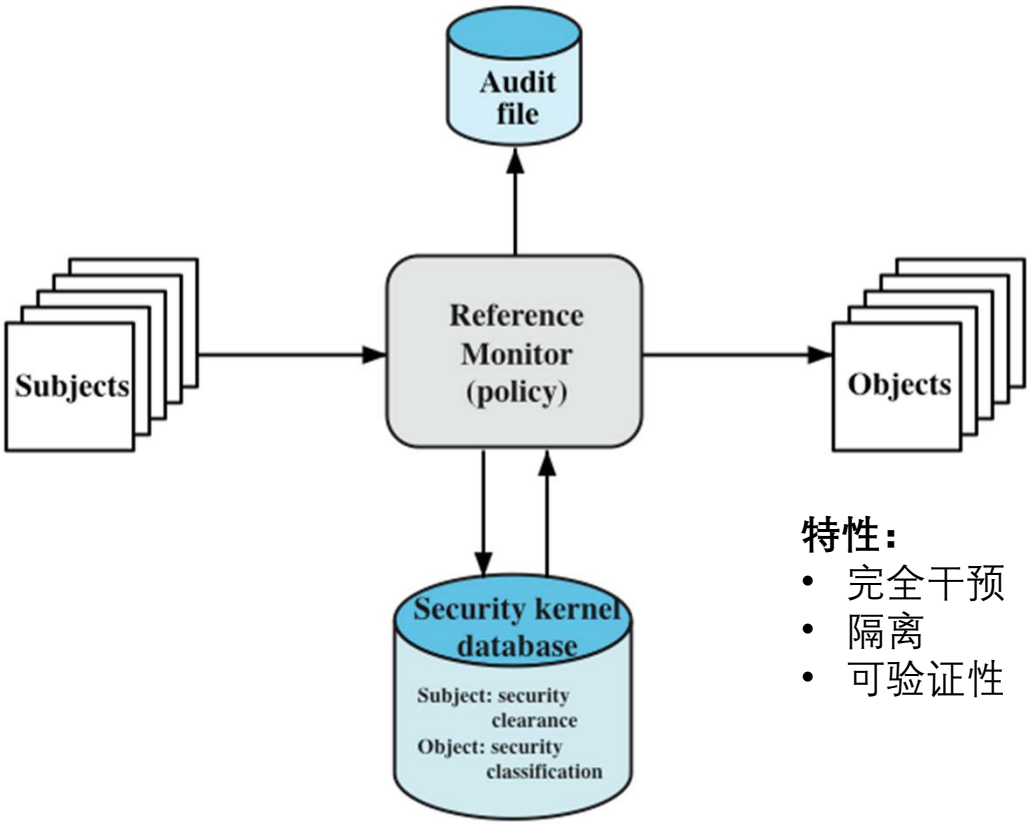
- S可以依据简单安全规则“读”O，以及
- S能访问的所有客体都与O在同一个DS中

sanitized data

可信系统的概念

- **信任（Trust）**：依赖于一个系统的人对该系统满足其要求的相信程度
  - 例如该系统完成其宣称的功能且不执行无用功能
- **可信系统（Trusted system）**：认为执行一组给定属性的设置而达到一定保障程度的系统
- **可信赖性（Trustworthiness）**：使系统值得信任的保障，以便信任可以通过某种令人信服的方式加以保证
  - 例如形式化分析或代码评审
- **可信计算机系统（Trusted computer system）**：部署足够的硬件和软件保障措施以允许对各种敏感或涉密信息同时处理的系统
- **可信计算基（Trusted computing base** (TCB)**）**：系统中用来实施特定策略的一小部分
  - TCB必须抗篡改、抗欺骗
  - TCB应该足够小，以便对其系统进行分析
- **保障（Assurance）**：确保系统按照其安全策略预期而开发和运行的过程
- **评价（Evaluation）**：评估产品是否具有所宣称的安全特性

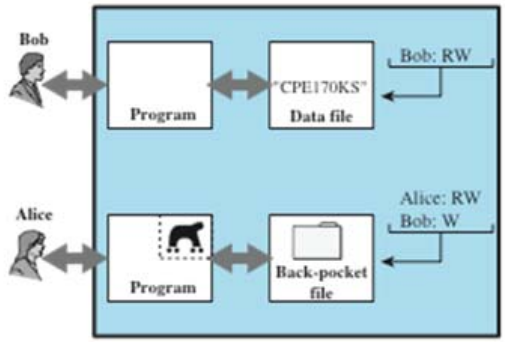
基准监视器

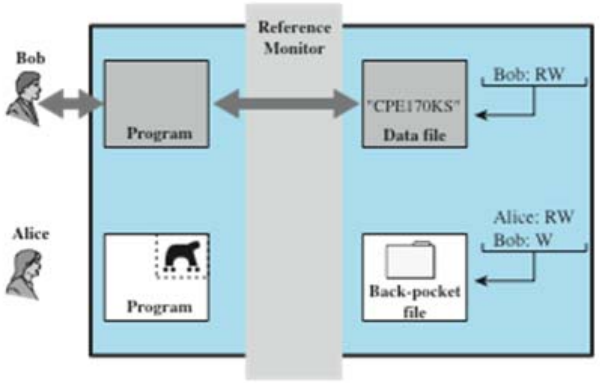


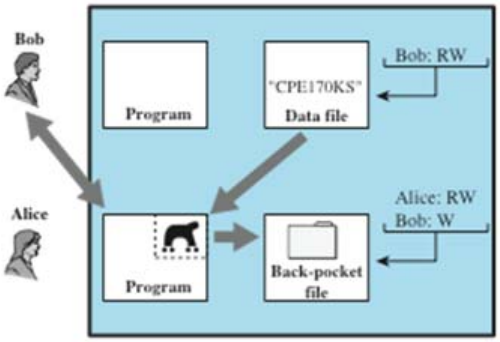
特性：

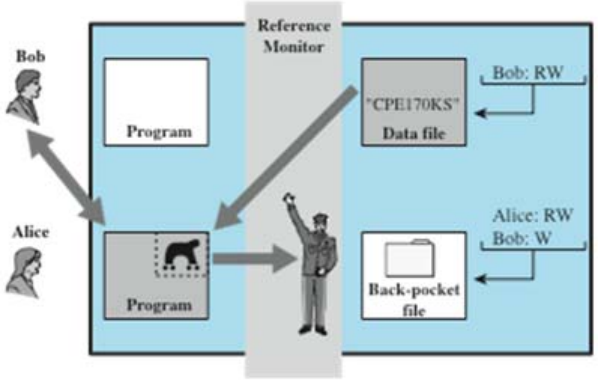
- 完全干预
- 隔离
- 可验证性

特洛伊木马防御


Bob
Program
"CPE170KS"
Data file
Bob: RW
Alice
Program
Back-pocket
file
Alice: RW
Bob: W


Reference
Monitor
Bob
Program
"CPE170KS"
Data file
Bob: RW
Alice
Program
Back-pocket
file
Alice: RW
Bob: W


Bob
Program
"CPE170KS"
Data file
Bob: RW
Alice
Program
Back-pocket
file
Alice: RW
Bob: W


Reference
Monitor
Bob
Program
"CPE170KS"
Data file
Bob: RW
Alice
Program
Back-pocket
file
Alice: RW
Bob: W