操作系统安全

第二部分 操作系统安全理论

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

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
自有住房/还贷中
喜欢海淘 常手机支付
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

操作系统安全理论

- 1.操作系统安全理论概述
  - 操作系统安全理论基本概念
  - 操作系统安全设计
- 2.操作系统安全模型
  - 安全模型的概念
  - 安全模型的分类
- 3.操作系统安全机制
  - 标识与鉴别
  - 访问控制
  - 安全审计
  - 可信路径
- 4.操作系统安全体系结构
  - 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
- 5.操作系统安全测评
  - 操作系统安全测评概念及技术
  - 安全测评的标准
    - TCSEC
    - CC
    - 等保

操作系统安全

2-1 操作系统安全理论概述

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

目录

操作系统安全的基本概念

- **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

操作系统安全的基本概念

- 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

操作系统安全的基本概念

- 可信软件和不可信软件
  - 软件的三大可信类别：**可信的**、**良性的**、**恶意的**
  - 可信软件是可信计算基的软件部分

- 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。

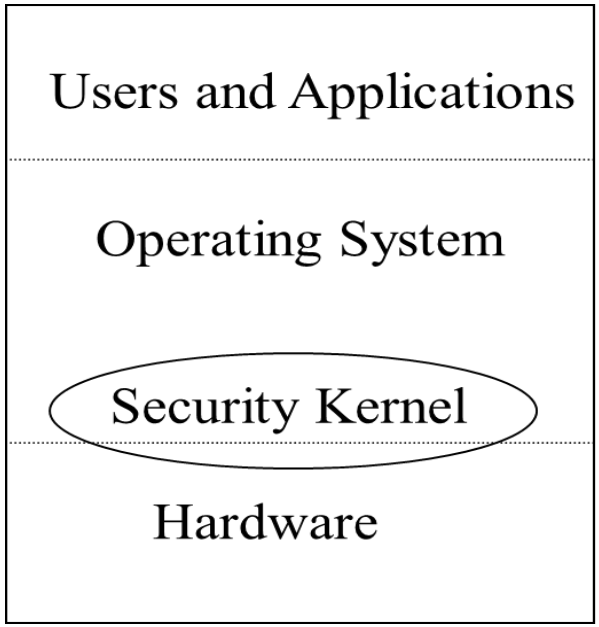
- **可信≈安全+可靠**
- 可信计算机系统是能够提供可信计算服务的计算机软硬件实体，它能够提供系统的可靠性、可用性、主体行为与信息的安全性。

操作系统安全的基本概念

- 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

操作系统安全基本概念

- 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

目录

操作系统安全

- 概述：
  - 什么是操作系统安全？
    - 操作系统安全是指该系统能够控制外部对系统信息的访问，即只有经过授权的用户（或进程）才能对信息资源进行相应的读写删除等操作，以保护合法用户对授权资源的使用，防止非法入侵者对系统资源的侵占与破坏。

操作系统安全一般包括两层意思：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。

操作系统安全的目标

- 概述
  - 操作系统安全的主要目标：
    - 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。

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

构建安全的基本要素

策略: 描述安全
做什么?

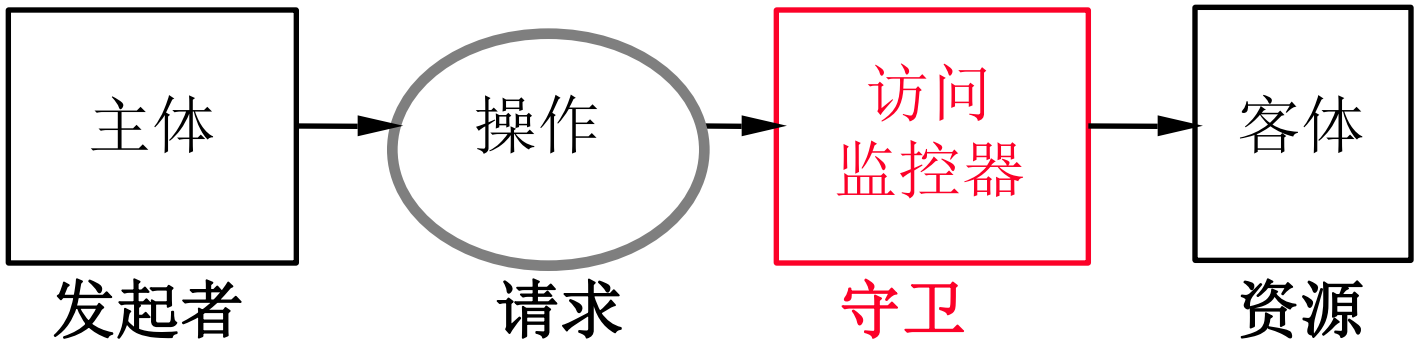
机制: 实现安全
怎样去做?

保证: 安全的正确性
是否有效?

Military
Commercial
Clark-Wilson
Separation of Duty
Chinese Wall

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
    - . . .

谢谢！

保证: 多层防御体系

- 网络, 使用防火墙
- 操作系统, 使用沙盒
  - 基本OS (如 UNIX/NT)
  - 上层OS (如 Java)
- 应用程序，直接检查授权

- 都需要鉴别/认证

- “海网云协同”的防御体系