网络与计算机安全丛书

# 操作系统访问控制研究

单智勇　石文昌　著

科学出版社
www.sciencep.com

网络与计算机安全丛书

# 操作系统访问控制研究

单智勇　石文昌　著

国家自然科学基金(60703103)
国家863计划项目(2007AA01Z414)　资助出版

科学出版社
北京

## 内 容 简 介

操作系统安全性是计算机安全的重要基础，要妥善解决日益泛滥的计算机安全问题，必须有稳固的安全操作系统作后盾。本书专门介绍作者近年在操作系统访问控制领域的研究成果，包括强制访问控制和角色访问控制，支持多安全政策的访问控制框架和访问控制管理，以及新型访问控制——可用性访问控制和可生存性访问控制等。书中所述大部分内容已经应用到商品化安全操作系统中，并获得北京市科技进步奖。

本书可供操作系统和信息安全研究者及相关专业高校师生阅读参考。

**图书在版编目(CIP)数据**

操作系统访问控制研究/单智勇，石文昌著. —北京：科学出版社，2009
(网络与计算机安全丛书)
ISBN 978-7-03-024300-3

Ⅰ.操… Ⅱ.①单…②石… Ⅲ.计算机网络-操作系统(软件)-系统管理-研究 Ⅳ.TP316.8

中国版本图书馆 CIP 数据核字(2009)第 042137 号

责任编辑：任 静 王志欣 / 责任校对：陈玉凤
责任印制：赵 博 / 封面设计：耕者设计工作室

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

丽源印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2009 年 3 月第 一 版 开本：B5(720×1000)
2009 年 3 月第一次印刷 印张：12 1/2
印数：1—3 000 字数：249 000

**定价：38.00 元**

**(如有印装质量问题，我社负责调换〈路通〉)**

# 前　言

操作系统安全是计算机安全的重要基础，要妥善解决日益泛滥的计算机安全问题，必须有稳固的安全操作系统作后盾。早在20世纪60年代，操作系统安全性就引起了研究机构(尤其是美国军方)的重视。至今，人们已在这个领域付出了40余年的努力，开展了大量的工作，取得了丰富的成果。

但是，随着网络的应用越来越普及和深入，操作系统所面临的来自网络的威胁越来越严峻。缓冲区溢出、病毒、蠕虫、木马、拒绝服务等各种攻击层出不穷，严重影响了人们使用因特网，给公司、政府带来了巨大的损失，甚至影响到国家的国防安全。深入研究其原因，重要一点是作为软件系统基座的操作系统本身不够安全，无法有效防御各类攻击。而居于操作系统安全机制核心地位的访问控制，理应受到置疑。因此，操作系统访问控制迫切需要改进，这是一个非常值得重视的研究领域。

应该说，人们已经发展了多种多样的可以严格证明其安全性的访问控制模型、策略和实施框架。然而，将它们应用到主流商用操作系统时，却无法避免它们妨碍了种类繁多的应用软件的运行。同时，要正确而不留安全漏洞地配置它们，对普通用户来说可望而不可及。而且，很多的访问控制模型是主机时代开发的，缺乏对网络因素的深入考虑。

本书探讨了如何构建能够适应新环境的操作系统访问控制理论、模型、框架和原型系统。首先，介绍了操作系统访问控制研究的相关工作，包括访问控制的基础理论、模型、框架和安全操作系统等。然后，介绍了对访问控制模型方面的研究，包括对强制访问控制模型的一种可适应性实施方法，以增强对应用程序的兼容性；对经典角色访问控制模型的面向操作系统的扩展和实施；提出一种基于感染传播的可用性访问控制模型，以在保护安全的同时提供良好兼容性和易用性；提出另一种可以在系统被攻破的情况下仍然可以保护关键服务和数据的可生存性访问控制模型。之后，介绍了对访问控制框架方面的研究，包括扩展通用访问控制框架以解决其效率低下的问题，提出一种环境适应的访问控制框架。最后，介绍了对安全管理方面的研究，包括基于CC国际标准的安全管理机制和对疑难

问题“安全属性即时撤销”的解决。其中大部分的研究成果已经纳入到开发的红旗安全操作系统中，该操作系统2002年通过中国科学院组织的专家鉴定，2003年国家权威部门检验认定达到国家标准GB17859第三级，获得安全产品销售许可证，并在实际的产业应用中产生了积极影响。2005年，获得北京市科技进步二等奖。

由于作者水平有限，书中不足之处在所难免，恳请读者批评指正。

作　者

2009年3月

# 目　　录

# 第1章 绪 论

## 1.1 现代操作系统面临的挑战

进入21世纪，互联网应用已经全面渗透到日常生活、金融、电信、电子商务、电子政务和军事等社会的各个领域。但是，互联网本身具有的开放性和动态性正在越来越多地引发各种安全问题，而且速度越来越快，范围越来越大。全世界由于计算机系统的安全脆弱性而导致的经济损失正在逐年上升，平均每20秒就发生一次入侵计算机互联网的事件。互联网的防火墙，超过三分之一被攻破。因此，包括Microsoft，Sun和IBM在内的众多系统软件厂商开始重视并逐步建立起安全和可信的操作系统。然而，这种具有较高安全性和可信性的操作系统离用户可接受程度还有一定距离。安全的操作系统已成为学术界和工业界积极研究的课题。

微软Redmond研究院撰文认为：可信、安全、系统可配置性、系统可扩展性以及多核编程是当前操作系统研究的五个挑战。Vista是微软第一款根据“安全开发生命周期(security development lifecycle，SDL)”机制进行开发的操作系统。它首次实现了从用户易用优先向系统安全优先的转变，其中所有选项的默认设置也都是以安全性为第一要素考虑的，这和以往的Windows客户端操作系统把易用性放在第一位大不相同。

作为国民经济和社会信息化的关键的基础设施，操作系统是唯一紧靠硬件的基础软件，其安全职能是其他软件安全职能的根基，缺乏这个安全的根基，构筑在其上的应用系统以及安全系统，如商务网站、文件服务器、防火墙、入侵检测、PKI、加密解密技术的安全性是得不到根本保障的。

当今的数字世界，各种违背安全原则的情况随处可见，泄密、破坏、犯罪事件对信息安全、经济安全甚至国家安全产生越来越严重的影响。对各式各样的数字威胁和攻击，我们必须采取有力的安全机制进行保护和防御，但目前信息安全工作集中在应用层或者传输通信层，可以说，IT业界尚未重视操作系统对安全的重要作用。没有操作系统的安全，信息安全是“沙地上的城堡”。

操作系统是一切软件运行的基础，而安全在操作系统的含义则是在操作系统的管辖范围内，提供尽可能强的访问控制，允许符合安全策略的访问，禁止非法的访问，并通过身份认证与鉴别机制确保用户身份的真实合法，通过审计机制记录

用户访问操作以便事后追踪。这样，在整个软件信息系统的最底层实现对整个信息系统的保护。

按照有关信息系统安全标准的定义，安全的操作系统应该具有这样的特征：最小特权原则，即每个特权用户只拥有能进行他工作的权力；有 ACL 的自主访问控制；强制访问控制，包括保密性访问控制和完整性访问控制；安全审计和审计管理；安全域隔离和可信通路。只有有了这些最底层的安全功能，各种运行在操作系统之上的病毒、木马程序、蠕虫、网络入侵和用户非法操作才能被真正抵制，因为他们违背了操作系统的安全策略，被安全机制所阻挡。

很多互联网网站被黑客和恶意软件攻击而被窜改得面目全非，这些被攻击的网站往往是国家政要部门或有重大影响和为广泛用户提供服务的网站，例如搜索引擎、政府网站、数据库查询网站等。这些网站一旦被攻击，不但有损形象，而且给网络的重要功能组织带来破坏，经济损失显著。究其原因，很大程度上是因为黑客利用了网站服务器操作系统存在的安全隐患，操作系统缺乏访问控制机制，存在超级用户等问题造成的。这些问题，无论使用哪种反扫描工具、防火墙、反病毒软件都不能得到根本解决。而对于使用安全操作系统的网站服务器，利用自主访问控制和强制访问控制都可以轻而易举地达到对网页内容和应用的保护。

一言蔽之，如何强化操作系统的安全性是现代操作系统的巨大挑战，随着信息安全事故的不断涌现而越来越具有现实紧迫性。解决这个问题的核心是寻找高安全性和良好兼容性的访问控制模型和机制。

## 1.2 操作系统访问控制

一分防护胜过十分检测，访问控制是常用的重要安全防护技术，是信息安全保障机制的核心内容。它是实现数据保密性和完整性机制的主要手段。信息系统中的访问包括打开文件、读取数据、更改数据、运行程序、发起连接等。访问控制是为了限制访问主体（或称为发起者，是一个主动的实体，如用户、进程、服务等），对访问客体（需要保护的资源，如文件、设备、端口等）的访问权限，从而使计算机系统在合法范围内使用。访问控制机制决定用户及代表用户在系统中活动的程序能做什么，及做到什么程度。

很多重要的计算机安全产品都是以访问控制为核心，如防火墙、虚拟专用网和安全数据库。毫无疑问，在操作系统安全性机制中访问控制也是核心。访问控制与身份认证和审计结合起来构成操作系统安全机制的最基础部分。图 1-1 抽象描述了操作系统安全机制的基本原理。

用户通过系统认证后登录到系统中，访问系统资源之前发送请求给访问控制的引用监控器，引用监控器在参考授权数据库之后决定是否允许访问。授权数据

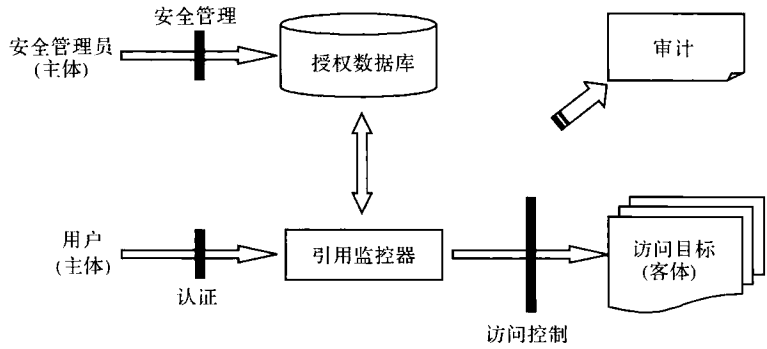


图 1-1　操作系统安全机制

库由安全管理员通过安全管理工具进行管理。所有的用户操作都被审计记录下来，以便事后追踪。认证的目的是确保用户身份的合法性和真实性，为访问控制做好铺垫；审计以访问控制活动作为主要对象，为访问控制进行事后追责；安全管理为访问控制修改主体访问客体的授权情况，为访问控制服务；访问控制居于操作系统安全机制的核心，直接阻挡非法和越权访问。

引用监控器是访问控制的核心，源自引用监控机理论。授权数据库是访问控制决策的依据，是访问矩阵的实现。引用监控机和访问矩阵是访问控制的两大基础理论。从实现上说，访问矩阵有访问控制列表、能力表和授权表等三种实现方法。从访问控制策略上说，访问控制包括自主访问控制、强制访问控制和角色访问控制。

# 第 2 章　操作系统访问控制研究概述

## 2.1　基础理论的形成

世界上第一个操作系统——批处理系统诞生于 20 世纪 50 年代中期，第一个分时操作系统 CTSS 诞生于 60 年代初期。从 CTSS 到第一个安全操作系统安全 Adept-50，相距约 5 年，可以说，安全操作系统的研究在分时系统诞生后不久就开始了。1967 年，计算机资源共享系统的安全控制问题引起了美国国防部的高度重视，国防科学部(Defense Science Board)旗下的计算机安全特别部队(Task Force on Computer Security)的组建拉开了操作系统安全研究的序幕。

### 2.1.1　访问控制抽象

1969 年，Weissman 发表了有关 Adept-50 的安全控制的研究成果。安全 Adept-50是历史上的第一个安全操作系统，可以实际投入使用，运行于 IBM/360 硬件平台，它以一个形式化的安全模型——高水标模型(high water mark model)为基础，实现了美国的一个军事安全系统模型，为给定的安全问题提供了一个比较形式化的解决方案。在该系统中，可以为客体标上敏感级别(sensitivity level)属性。系统支持的基本安全条件是，对于读操作，不允许信息的敏感级别高于用户的安全级别(clearance)；对于写操作，在授权情况下，允许使信息从高敏感级别移向低敏感级别。

同年，Lampson 通过形式化表示方法运用主体(subject)、客体(object)和访问矩阵(access matrix)的思想第一次对访问控制问题进行了抽象。主体是访问操作中的主动实体，客体是访问操作中被动实体，即主体对客体进行访问。访问矩阵是以主体为行索引、客体为列索引的矩阵，矩阵中的每一个元素表示一组访问方式，是若干访问方式的集合。矩阵中第 $i$ 行第 $j$ 列的元素 $M_{ij}$ 记录着第 $i$ 个主体 $S_i$ 可以执行的对第 $j$ 个客体 $O_j$ 的访问方式，比如 $M_{ij}$ 等于{read, write}表示 $S_i$ 可以对 $O_j$ 进行读和写访问。

1970 年，Ware 推出的研究报告对多渠道访问的资源共享的计算机系统引起的安全问题进行了研究。报告结合实际的国防信息安全等级划分体制，分析了资源共享系统中敏感信息可能受到的安全威胁，提出了解决计算机安全问题的建议途径。

报告研究的主要目标是多级安全系统(multi-level security system)在计算机中的实现。报告指出,安全级别和该知(need-to-know)权限是多级安全问题中的重要成分,基本的多级安全问题就是要确定具有特定安全级别和该知权限的个体是否能够访问给定物理环境中的某个范围的敏感信息。报告对计算机安全系统的设计提出了两个限制条件:

(1) 计算机安全系统必须与现实的安全等级划分结构一致。

(2) 计算机安全系统必须与现实的手工安全控制规程相符。

报告建议的计算机安全系统涉及系统灵活性(在应用中可调整个体和信息的安全等级)、可靠性(贯彻"失败-保险"思想,当不能确定是否授权时,采取不授权的措施)、可审计性(记录安全相关行为)、可管理性(安全控制、审计控制等管理)、可依赖性(避免拒绝对用户的服务)、配置完整性(确保系统自身的完整)等特点。报告讨论了在存储资源管理方面避免遗留信息泄漏问题。报告认为,计算机系统的安全控制是一个系统设计问题,必须从硬件、软件、通信、物理、人员和行政管理规程等各个方面综合考虑。报告还给出了访问控制问题的形式化描述。

### 2.1.2　引用监控机

1972 年,作为承担美国空军的一项计算机安全规划研究任务的研究成果,Anderson 在一份研究报告中提出了引用监控机(reference monitor)、引用验证机制(reference validation mechanism)、安全核(security kernel)和安全建模(security modeling)等重要思想。这些思想是在研究系统资源受控共享(controlled sharing)问题的背景下产生的。

把授权机制与能够对程序的运行加以控制的系统环境结合在一起,可以对受控共享提供支持,授权机制负责确定用户(程序)对系统资源(数据、程序、设备等)的引用①许可权,程序运行控制负责把用户程序对资源的引用控制在授权的范围之内。这一思想可以形象地表示为图 2-1 的形式。

引用监控机思想是为了解决用户程序的运行控制问题而引入的,其目的是在用户(程序)与系统资源之间实施一种授权的访问关系。Anderson 把引用监控机的职能定义为:以主体(用户等)所获得的引用权限为基准,验证运行中的程序(对程序、数据、设备等)的所有引用。对应到图 2-1,引用监控机是在"程序运行控制"的位置上发挥作用的。

引用监控机是一个抽象的概念,它表现的是一种思想。Anderson 把引用监控机的具体实现称为引用验证机制,它是实现引用监控机思想的硬件和软件的组合。引用验证机制需要同时满足以下 3 个原则:

---

① 这里"引用"的含义实际上就是"访问"。

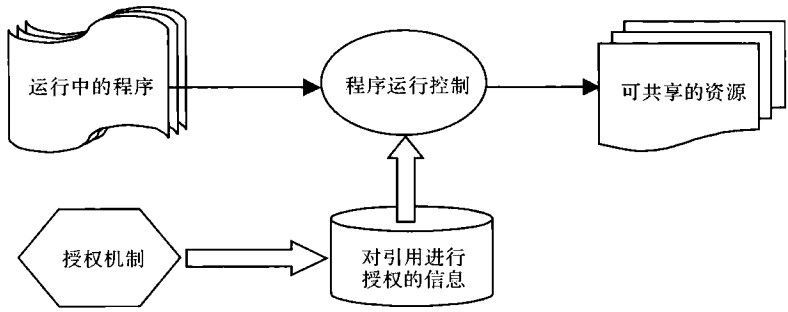


图 2-1 系统资源的受控共享

(1) 必须具有自我保护能力。

(2) 必须总是处于活跃状态。

(3) 必须设计得足够小,以利于分析和测试,从而能够证明它的实现是正确的。

第一个原则保证引用验证机制即使受到攻击也能保持自身的完整性。第二个原则保证程序对资源的所有引用都得到引用验证机制的仲裁。第三个原则保证引用验证机制的实现是正确的和符合要求的。

在受控共享和引用监控机思想的基础上,Anderson 定义了安全核的概念。安全核是系统中与安全性的实现有关的部分,包括引用验证机制、访问控制机制、授权机制和授权的管理机制等成分。

Anderson 指出,要开发安全系统,首先必须建立系统的安全模型。安全模型给出安全系统的形式化定义,正确地综合系统的各类因素。这些因素包括,系统的使用方式、使用环境类型、授权的定义、共享的客体(系统资源)、共享的类型和受控共享思想等。这些因素应构成安全系统的形式化抽象描述,使得系统可以被证明是完整的、反映真实环境的、逻辑上能够实现程序的受控执行的。完成安全系统的建模之后,再进行安全核的设计与实现。

### 2.1.3 BLP 模型

1973 年,Lampson 通过对程序的禁闭(confinement)问题的研究提出了隐通道(covert channel)的概念。研究的背景是程序的调用与信息的传送,设程序 B 是由程序 A 调用运行的,所谓对程序 B 的禁闭就是指,制止程序 B 在运行期间向其他程序(程序 A 除外)传送信息。程序 B 向它的拥有者(owner)传送有关程序 A 的信息属于信息泄漏。Lampson 在归纳这种情形的信息泄漏的各种渠道时,把隐通道定义为,按常规不会用于传送信息但却被利用于泄漏信息的信息传送渠道。比如,一个程序对系统负载的影响,似乎与信息传送渠道无关,但该程序可以通过

改变其对系统负载的影响，利用对系统负载的影响的变化情况来向另一个程序暗示某种信息，这种信息泄漏的渠道就属于隐通道。

同年，Bell 和 LaPadula 提出了第一个可证明的安全系统的数学模型，这就是 Bell&LaPadula 模型，简称 BLP 模型。在随后的几年，该模型得到了进一步的充实和完善。Bell 和 LaPadula 在 1976 年完成的研究报告给出了 BLP 模型的最完整表述，其中包含模型的形式化描述和非形式化说明，以及模型在 Multics 系统中实现的解释。

BLP 模型是根据军方的安全策略设计的，它要解决的本质问题是对具有密级划分的信息的访问进行控制。BLP 模型支持的是信息的保密性。继 BLP 模型之后，Biba 提出了与 BLP 模型异曲同工的 Biba 模型，Biba 模型支持的是信息的完整性。

### 2.1.4　权能与访问控制表

1975 年，Saltzer 和 Schroeder 以保护机制的体系结构为中心，探讨了计算机系统的信息保护问题，重点考察了权能(capability)实现结构和访问控制表(access control list，ACL)实现结构，给出了信息保护机制的八条设计原则。

为讨论信息保护问题，从概念上，可以为每一个需保护的客体建立一个不可攻破的保护墙，保护墙上留有一个门，门前有一个卫兵，所有对客体的访问都首先在门前接受卫兵的检查。在整个系统中，有很多客体，因而有很多保护墙和卫兵。对客体的访问控制机制的实现结构可分为两种类型：面向门票(ticket-oriented)的实现和面向名单(list-oriented)的实现。在面向门票的实现中，卫兵手中持有一份对一个客体的描述，在访问活动中，主体携带一张门票，门票上有一个客体的标识和可访问的方式，卫兵把主体所持门票中的客体标识与自己手中的客体标识进行对比，以确定是否允许访问；在整个系统中，一个主体可能持有多张门票。在面向名单的实现中，卫兵手中持有一份所有授权主体的名单及相应的访问方式，在访问活动中，主体出示自己的身份标识，卫兵从名单中进行查找，检查主体是否记录在名单上，以确定是否允许访问。

权能结构属于面向门票的结构，一张门票也称作一个权能。访问控制表(ACL)结构属于面向名单的结构。在访问控制矩阵的概念模式下，权能结构对应访问控制矩阵的行结构，行中的每个矩阵元素对应一个权能；ACL 结构对应访问控制矩阵中的列结构，每一列对应一个 ACL。

Saltzer 和 Schroeder 给出的信息保护机制的设计原则有如下几条：

(1) 机制经济性(economy)原则。保护机制应设计得尽可能的简单和短小。有些设计和实现错误可能产生意想不到的访问途径，而这些错误在常规使用中是察觉不出的，难免需要进行诸如软件逐行排查工作，简单而短小的设计是这类工

作成功的关键。

(2) 失败-保险(fail-safe)默认原则。访问判定应建立在显式授权而不是隐式授权的基础上,显式授权指定的是主体该有的权限,隐式授权指定的是主体不该有的权限。在默认情况下,没有明确授权的访问方式,应该视作不允许的访问方式,如果主体欲以该方式进行访问,结果将是失败,这对于系统来说是保险的。

(3) 完全仲裁原则。对每一个客体的每一次访问都必须经过检查,以确认是否已经得到授权。

(4) 开放式设计原则。不应该把保护机制的抗攻击能力建立在设计的保密性的基础之上。应该在设计公开的环境中设法增强保护机制的防御能力。

(5) 特权分离原则。为一项特权划分出多个决定因素,仅当所有决定因素均具备时,才能行使该项特权。正如一个保险箱设有两把钥匙,由两个人掌管,仅当两个人都提供钥匙时,保险箱才能打开。

(6) 最小特权原则。分配给系统中的每一个程序和每一个用户的特权应该是它们完成工作所必须享有的特权的最小集合。

(7) 最少公共机制原则。把由两个以上用户共用和被所有用户依赖的机制的数量减少到最小。每一个共享机制都是一条潜在的用户间的信息通路,要谨慎设计,避免无意中破坏安全性。应证明为所有用户服务的机制能满足每一个用户的要求。

(8) 心理可接受性原则。为使用户习以为常地、自动地正确运用保护机制,把用户界面设计得易于使用是根本。

Saltzer 和 Schroeder 也指出,如何证明硬件和软件保护机制的设计与实现的正确性,是一项已吸引很多注意力的研究课题。

### 2.1.5 操作系统保护理论

1976 年,Harrison、Ruzzo 和 Ullman 提出了操作系统保护(protection)的第一个基本理论。HRU 理论形式化地给出保护系统模型的定义,并通过三个定理给出有关保护系统的一些结果。Harrison 等还用该模型对 Unix 系统的保护系统进行了刻画。

## 2.2 访问控制模型

### 2.2.1 概念辨析

安全模型与安全策略是计算机安全理论中最容易相互混淆的两个概念。依据文献,可以定义安全策略为:一个组织制订的用以安全地管理、保护和发布信息