信息安全系列教材

操作系统安全

主编 贾春福 郑 鹏

WUHAN UNIVERSITY PRESS
武汉大学出版社

信息安全系列教材

操作系统安全

主编 贾春福 郑 鹏
参编 杨 峰 钟安鸣 段雪涛

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

操作系统安全/贾春福,郑鹏主编.—武汉:武汉大学出版社,2006.12
信息安全系列教材
ISBN 7-307-05302-0

Ⅰ.操… Ⅱ.①贾… ②郑… Ⅲ.操作系统—安全技术—高等学校—教材 Ⅳ.TP316

中国版本图书馆 CIP 数据核字(2006)第 132974 号

责任编辑:林 莉 责任校对:程小宜 版式设计:支 笛

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)
(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.com.cn)
印刷:湖北新华印务有限责任公司
开本:787×1092 1/16 印张:12.5 字数:307 千字
版次:2006 年 12 月第 1 版 2006 年 12 月第 1 次印刷
ISBN 7-307-05302-0/TP·223 定价:19.00 元

信息安全系列教材

编 委 会

内容简介

本书是关于操作系统安全的教材，共分为七章，较为全面地介绍了操作系统安全的理论和关键技术。主要内容包括：操作系统安全的相关概念（基本名词和基本概念）、操作系统的安全机制、操作系统安全模型、操作系统的安全结构、主流操作系统（UNIX/Linux 和 Windows）的安全机制与技术、操作系统的安全评测，以及操作系统的安全设计等方面的内容。

本书内容丰富，深入浅出，特点鲜明，注重理论与实际应用的结合，利于学生较好地掌握所学到的知识和相关的技能。

本书可作为信息安全、计算机科学技术、通信工程等专业的高年级本科生的教材；也可作为相关专业本科生和研究生，以及从事相关领域科研和工程的技术人员的参考书。

序　言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006 年 9 月 19 日

前 言

计算机和网络技术的飞速发展和广泛应用，极大地改变了人们的工作和生活方式，推动了整个社会的快速发展。随着人们对计算机和网络技术依赖程度的不断增加，信息安全问题更多地受到人们的关注。计算机主机系统和网络安全是信息安全的关键。

操作系统是计算机系统的系统软件，是计算机资源的直接管理者，它可以直接与硬件打交道，并为用户提供接口，是计算机软件的基础和核心。在计算机网络环境中，整个网络的安全依赖于其中各主机系统的安全可信性。如果没有操作系统安全的基础，就谈不上主机系统和网络系统的安全，也就不能真正解决数据库和其他应用软件的安全问题。因此，操作系统的安全是整个计算机系统安全的基础。

此外，一个有效可靠的操作系统自身也应该具有很强的安全性，它必须具有相应的保护措施，能够杜绝或限制后门、隐蔽通道、特洛伊木马等系统安全隐患；对系统中的信息提供足够的保护，防止未授权用户的滥用和蓄意破坏。硬件是计算机系统的支撑，但仅有硬件还不能提供足够的安全保护手段，操作系统的安全机制与相关硬件相结合才能提供强有力的保护。因此，操作系统安全是计算机信息系统安全的一个不可缺少的支柱，对安全操作系统进行研究具有重要的意义。

本书共分为七章，较为全面地介绍了操作系统安全的理论和关键技术。第一章介绍了操作系统安全的相关概念，包括基本名词和基本概念等；第二章介绍了操作系统的安全机制，包括标识与鉴别机制、访问控制、最小特权管理、安全审计机制、可信通路和存储与运行保护等内容；第三章介绍了操作系统安全模型的相关概念及几种重要的操作系统安全模型；第四章介绍了操作系统的安全结构的内容；第五章介绍了主流操作系统（UNIX/Linux 和 Windows）的安全机制和技术；第六章介绍了操作系统的安全评测问题，包括国内外安全操作系统的评估标准和方法；第七章介绍了操作系统的安全设计等方面的内容。本书第一章至第五章由南开大学贾春福、杨峰、钟安鸣和段雪涛编写，第六章和第七章由武汉大学郑鹏编写。

由于作者水平有限，加之时间仓促，书中难免有错漏之处，敬请广大读者批评指正。

本书得到了天津市科技发展计划项目（05YFGZGX24200）的支持，在此表示感谢。

作者

2006 年 9 月

目 录

第1章 绪 论

随着计算机和网络技术在全球的普及和发展，计算机通信网络在社会、政治、经济、文化、军事等方面的作用日益增大，电子商务、网络办公、金融电子化等新兴事物的出现，极大地改变了人们学习和生活的方式，计算机技术的普及使得越来越多的人对电脑的依赖程度增加。然而，计算机网络的开放性，尤其是 Internet 的跨国界性，使计算机网络面临着巨大的安全威胁。随着社会网络化程度的增加，计算机网络体系的安全性隐患日益明显地暴露出来。

计算机网络体系的安全威胁，其来源主要有以下几个方面：一个是计算机结构上的安全缺陷；一个是操作系统的不安全性；还有一个就是网络协议的不安全性。目前国际上流行的可信计算技术就是为了弥补计算机结构上的安全缺陷而提出的，可信计算机的核心和基础就是安全的操作系统。而逐渐获得应用的 IPv6 网络协议已经更多地考虑了安全性方面的要求，安全的网络协议只有在安全的操作系统之上运行才能体现它的安全价值。由此可见，操作系统安全在整个信息安全领域的重要性。

安全操作系统是信息安全基础设施的关键技术，研究操作系统安全对我国信息化的建设具有重要意义。

1.1 操作系统面临的安全威胁

信息安全的很多问题都源于操作系统存在的安全弱点，要解决操作系统的安全问题，就要研究系统所遭到的各种各样的成功的和未成功的入侵攻击的威胁，这样才能有的放矢，提高操作系统的安全性。

计算机安全是建立在保密性、完整性和可用性之上的，破坏了信息的保密性、完整性或可用性，也就破坏了信息的安全性。从这个角度上看，操作系统所受到的安全威胁可以分为保密性威胁、完整性威胁和可用性威胁。

1.1.1 保密性威胁

信息的保密性是指信息的隐藏，目的是对非授权的用户不可见。信息保密的需求来源于计算机在敏感领域的使用，比如军事应用、企业应用等。军事部门经常需要控制某些信息只能被特定的人群访问。企业也有很多数据，例如公司的专利、采购价格等，是不能对所有人公开的。

保密性也指保护数据的存在性，存在性有时候比数据本身更能暴露信息。精确地知道某个地区参与游行的人数，可能并不会比知道该地区发生了游行事件这一信息更重要，因此保护数据的存在性也是非常重要的。

操作系统受到的保密性威胁很多，例如嗅探。嗅探就是对信息的非法拦截，它是某种形式

的信息泄露。通过嗅探可以获得很多敏感信息,甚至可以获得用户使用某种服务的密码以及重要的交易记录等。

保密性威胁中,木马和后门事件的危害是最为严重的,因为此类事件隐蔽性非常强,是造成失泄密危害的重要原因。2005 年,国家计算机网络应急技术处理协调中心对常见的 28 种木马程序的活动状况进行了抽样监测,发现我国大陆地区 22 500 多个 IP 地址的主机被植入木马,同时发现大陆地区以外 22 800 多个主机地址和这些木马进行通信。这些数据只是对我国互联网上木马活动情况的初步统计,实际情况会更加严重和复杂。随着我国互联网应用的普及,日益增加的木马程序将造成计算机数据的失窃和被控,感染木马的计算机不仅面临严重的泄密威胁,更容易被黑客利用,从而发起有组织的大规模攻击,而且木马类程序不断出现,用户很难发觉,因此造成的影响往往比较长久。

还有一类威胁信息保密性的程序叫做间谍软件(Spyware)。间谍软件通常是一个独立的程序,它监视用户和系统活动、窃取用户敏感信息,包括用户名、密码、银行卡和信用卡信息等,然后将窃取到的信息以加密的方式发送给攻击者。近几年来,间谍软件的数量、种类和危害不断增加,引起了广泛重视。现在大部分蠕虫、木马等恶意代码也都加入了间谍软件功能,敏感信息失窃成为用户面临的主要威胁。2005 年,我国大陆至少有 70 万台主机被植入了某种类型的间谍软件。这些间谍软件向服务器汇报搜集到的信息,从服务器读取关键字、下载更新版本,极大地破坏了用户信息的保密性。

隐蔽通道也是一类不易被发现的数据泄密途径。隐蔽通道是一种允许违背合法的安全策略的方式进行操作系统进程间通信(IPC)的通道。隐蔽通道又分为隐蔽存储通道与隐蔽时间通道。隐蔽存储通道通过两个进程利用同一块不受安全策略限制的存储空间来传递信息。前一个进程向该存储单元中写入要传递的信息,后一个进程检测到该单元内容发生改变后就读取该信息。隐蔽时间通道原理上与隐蔽存储通道相同,不同的是隐蔽时间通道具有一个实时时钟或定时器等计时装置。前一个进程写入信息后,后一个进程必须迅速接收该信息,否则信息有可能会被覆盖。接收进程利用计时装置进行测量,判断接收信息的时间。

1.1.2 完整性威胁

信息的完整性指的是信息的可信程度。保证完整性的信息应该没有经过非法的或者是未经授权的数据改变。完整性包括信息内容的完整性和信息来源的完整性。如果信息被非法改变了,就破坏了信息的内容完整性,使其内容的可信程度受到质疑。同样,信息的来源可能会涉及来源的准确性和可信性,也涉及了人们对此信息所赋予的信任性。例如,有些网站上可能会发布一些从政府泄露出来的信息,却声称该信息来自于其他的信息源。虽然信息按原样刊登,保证了信息内容的完整性,但是信息的来源是错误的,即破坏了信息的来源完整性。因此,该信息同样是不可信的。完整性要同时包括数据的正确性和可信性、信息的来源(即如何获取信息和从何处获取信息)、信息在到达当前机器前所受到的保护程度,以及信息在当前机器中所受到的保护程度都会影响信息的完整性。

根据信息完整性的特点,信息的完整性威胁主要可以分为两类:破坏和欺骗。破坏指中断或妨碍正常操作。数据遭到破坏后,其内容就可能会发生非正常改变,破坏了信息的内容完整性。欺骗指接受虚假数据。欺骗过程中,一些实体要根据修改后的数据来决定采取什么样的

动作，或者不正确的信息会被当做正确的信息被接受和发布。例如，网上先后出现了假冒中国银行、农业银行、工商银行的网站，这些冒牌网站的共同特点是网址及页面均与真网站相似。如假冒中国银行网站的域名是 www. bank-off-china. com，比中国银行网站的域名 www. bank-of-china. com 多一个英文字母 f；假冒中国工商银行网站的域名是 www. 1cbc. com. cn，与中国工商银行网站的域名 www. icbc. com. cn 也只是“1”和“i”一字之差；而假冒中国农业银行网站的域名是 www. 965555. com，与中国农业银行网站 www. 95599. com 也较为相近。不法分子通过设立假冒银行网站，试图骗取该行用户的账号和密码，用户一旦输入了账号及密码，用户的资料就会落入欺骗者的手中，后果将不堪设想。欺骗会破坏信息来源的完整性。

计算机病毒是操作系统所受到的安全威胁中人们最为熟悉的一种。绝大部分的病毒都会对信息的内容完整性产生危害。计算机病毒是一个程序，一段可执行代码，具有寄生性、潜伏性、隐蔽性、传染性等特点。就像生物病毒一样，计算机病毒有自我复制的能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。计算机病毒可以通过磁盘、磁带和网络等媒介传播扩散，能够感染其他的程序。与生物病毒不同的是几乎所有的计算机病毒都是人为地故意制造出来的，有时一旦扩散出来后连编写者自己也无法控制。它已经不是一个简单的纯计算机学术问题，而是一个严重的社会问题了。几年前，大多数类型的病毒主要是通过软盘传播，但是，因特网引入了新的病毒传播机制。由于电子邮件被用做重要的企业通信工具，病毒比以往任何时候扩展得都要快。附着在电子邮件信息中的病毒，仅仅在几分钟内就可以感染整个企业，让公司每年在生产损失和清除病毒开销上花费数百万美元。按美国国家计算机安全协会发布的统计资料，已有超过 10 000 种病毒被辨认出来，而且每个月都在产生 200 种新型病毒。1999 年 4 月 26 日，全世界至少有六千万台计算机遭受了 CIH 病毒的侵害，计算机系统瘫痪或硬盘分区表被改写，甚至许多机器的数据永久地丢失了。直到现在，每到 4 月 26 日，还会有很多安全意识不强的用户受到 CIH 病毒的侵害。没有一个使用多台计算机的机构，可以是对病毒免疫的。因此，如何有效地减少计算机病毒对操作系统的安全威胁，是安全操作系统设计过程中所要考虑的一个很重要的问题。

1.1.3 可用性威胁

可用性是指对信息或资源的期望使用能力。可用性是系统可靠性与系统设计中的一个重要方面，因为一个不可用的系统起到的作用还不如没有系统。可用性之所以与安全相关，是因为有人可能会蓄意地使数据或服务失效，以此来拒绝对数据或服务的访问。

企图破坏系统的可用性的攻击称为拒绝服务攻击。拒绝服务攻击的目的是使计算机或网络无法提供正常的服务。拒绝有可能发生在服务器的源端（即阻止服务器取得完成任务所需的资源），也可能发生在服务器的目的端（即阻断来自服务器的信息），或者发生在中间路径（即丢弃从客户端或服务器端传来的信息，或者同时丢弃这两端传来的信息）。最常见的拒绝服务攻击有计算机网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。2000 年 2 月，在三天的时间里，黑客组织使全球顶级互联网站——雅虎、亚

马逊、电子港湾、CNN 等陷入瘫痪。黑客使用的就是拒绝服务攻击，即用大量无用信息阻塞网站的服务器，使其不能提供正常服务。据统计，在 2 月 7～9 日三天时间里，这些受害公司的损失就超过了 10 亿美元，其中仅营销和广告收入就高达 1 亿美元。

操作系统可用性威胁的另一个主要来源在于计算机软件设计实现中的疏漏。操作系统功能复杂，规模庞大，而且发展趋势表明，在不远的将来还会变得更加复杂。每千行代码中的 bug 数量随系统的不同而不同，但是不管什么系统，bug 都在 5～50 个之间。即使一个经过了严格质量认证测试的系统每千行仍然会有大约 5 个 bug。一个只经过了特性测试的软件系统，每千行则存在大约 50 个 bug。图 1.1 是 Linux 操作系统从发布到 2.4.17 版的源代码行数。到现在的 Linux 2.6 版本的内核源代码已经超过了三千万行。如此庞大的系统要想保证百分之百的正确是不可能的，其中隐藏的缺陷可能会被缓冲区溢出、符号连接和特洛伊木马等各种各样的攻击手段所利用，这些缺陷一旦被利用，就可能对系统的安全构成致命的威胁。微软 2004 年正式公布了 34 个安全漏洞，2005 年公布了 48 个安全漏洞，这些漏洞大部分是和操作系统相关的。绝对安全的操作系统是不存在的，只有在操作系统设计时就以安全理论作指导，始终贯穿正确的安全原则，才能尽可能地减少操作系统本身的漏洞。

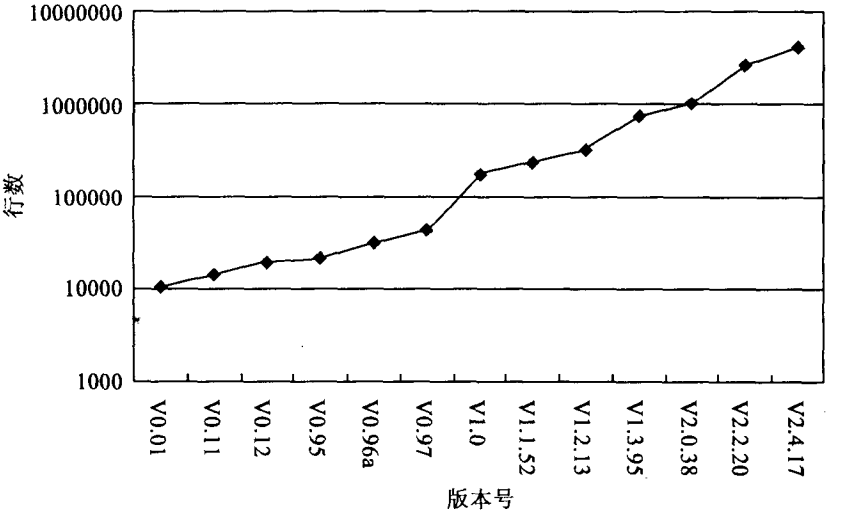

图 1.1　Linux 内核各版本源代码行数

事实上，操作系统面临的威胁已经越来越复杂，各种各样的威胁有时会交织在一起而难以详细区分，这些威胁对操作系统的影响也是多方面的，很多威胁可能会在破坏系统的可用性同时又破坏了数据的完整性。2005 年，国家计算机网络应急技术处理协调中心收到的 9 112 件非扫描类网络安全事件报告按类型统计情况如图 1.2 所示，其中绝大部分事件都与操作系统的安全性相关，并且对系统的影响是多方面的。

1.2　安全操作系统研究的发展

为了更好地研究操作系统，使安全操作系统的发展符合现代军事和商业等方面的需要，有

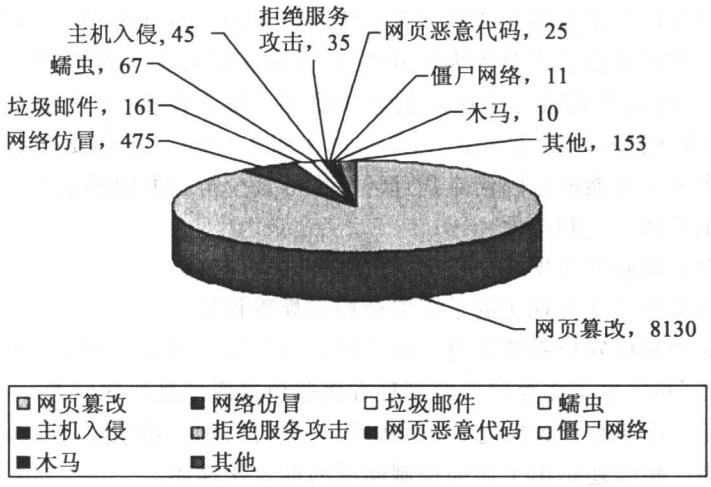

图 1.2 2005 年网络安全事件报告类型分布

必要对安全操作系统的发展规律和发展方向加以了解。下面按时间顺序给出安全操作系统技术发展的历史资料，从中可以看出安全操作系统的基本思想、技术和方法形成及发展的过程。

20 世纪 60 年代是大型计算机快速发展的年代，当时的麻省理工学院因最先实现了兼容分时系统(CTSS, Compatible Time Sharing System)，在电子计算器领域享有相当崇高的地位。1963 年，麻省理工的里克莱德推动了 MAC 计划，MAC 以 IBM 的大型计算机作为主体，连接了将近 160 台终端机，这些终端机就四散在教学区以及教职员的家中，可以让 30 位使用者同时共享计算机资源。这项计划到了 1965 年便不堪负荷，于是麻省理工便决定开发更大型的计算机系统，这项计划便是开发 Multics，其目标是向更大的用户团体提供对计算机的同时访问，支持强大的计算能力和数据存储，并具有很高的安全性。在这一年由麻省理工学院、奇异公司及贝尔实验室这三个成员开始了合作开发。由于 Multics 预期的复杂性和理想性，直到 1969 年在历经四年的奋战后，仍未达到原先规划设计的目标，贝尔实验室决定退出计划。功能未达原始设计目标的 Multics 还是安装在奇异公司的 GE645 大型计算机上供麻省理工使用。虽然 Multics 没有成功，但在安全操作系统的研究方面迈出了重要的一步，是开发安全操作系统最早期的尝试，并为后来的研究开发工作积累了大量有用的经验。

1969 年，出现了历史上的第一个可以实际投入使用的安全操作系统——Adept-50。C. Weissman 发表了有关 Adept-50 的安全控制的研究成果。Adept-50 运行于 IBM360 硬件平台，它以一个形式化的安全模型——高水标模型(High-watermark Model)为基础，实现了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。

同年，在安全操作系统的安全模型研究上也取得了很大进展。B. W. Lampson 第一次对访问控制问题进行了抽象。他通过形式化表示方法运用了主体(Subject)、客体(Object)和访问矩阵(Access Matrix)的思想。主体是访问操作中的主动实体，客体是访问操作中的被动实体，即主体对客体进行访问。访问矩阵是以主体为行索引、以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，W. H. Ware 给出了针对多渠道访问的资源共享的计算机系统引起的安全问题的研究报告。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。报告指出，安全级别和需知（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需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。

该报告建议的计算机安全系统涉及系统灵活性、可靠性、可审计性、可管理性、可依赖性、配置完整性等特点，并讨论了在存储资源管理方面避免遗留信息泄露问题。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。

1972 年，J. P. Anderson 在一份研究报告中提出了引用监控器（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。

引用监控器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。J. P. Anderson 把引用监控器的职能定义为：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。

J. P. Anderson 把引用监控器的具体实现称为引用验证机制，它是实现引用监控器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三个原则：

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。

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）的引用许可权（也可称之为访问许可权），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。在受控共享和引用监控器思想的基础上，J. P. 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（Authorization）机制和授权的管理机制等成分。

J. P. 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。