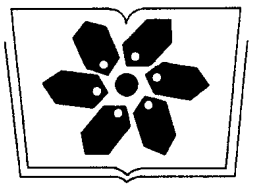
Introduction to Operating System Security

操作系统安全导论

卿斯汉 刘文清 刘海峰 著

科学出版社
www.sciencep.com



中国科学院科学出版基金资助出版

操作系统安全导论

卿斯汉　刘文清　刘海峰　著

国家重点基础研究发展规划资助项目（项目编号：G1999035810）
国家自然科学基金项目资助项目（项目编号：60083007）

科学出版社
北京

内 容 简 介

本书是关于操作系统安全的研究专著，全书由操作系统安全、操作系统安全机制、安全操作系统设计、安全操作系统评测、安全操作系统应用以及国外安全操作系统的新进展等8章组成. 书中首先介绍操作系统安全的有关概念及相关问题，并介绍UNIX，Windows等流行操作系统存在的安全问题. 然后讲述高安全级别操作系统的有关安全机制，重点介绍了如何进行设计开发高安全级别的操作系统. 最后，阐述操作系统安全评测、安全操作系统的应用和国外在安全操作系统领域的一些新进展.

本书既总结归纳了当前这一领域的最新研究成果，又是作者在这一领域潜心研究多年的结晶. 本书的特点是，内容翔实，理论和实践相结合，针对性强，是我国第一部有关操作系统安全的专著.

本书可以作为计算机专业、通信专业、信息安全专业本科高年级学生、硕士生和博士生的教材，也可供相关专业的广大工程技术人员参考.

图书在版编目(CIP)数据

操作系统安全导论/卿斯汉，刘文清，刘海峰著. —北京：科学出版社，2003.1

ISBN 7-03-011017-X

Ⅰ.操… Ⅱ.①卿… ②刘…③刘… Ⅲ.操作系统-安全技术 Ⅳ.TP316

中国版本图书馆CIP数据核字(2002)第098343号

责任编辑：鞠丽娜 刘永道 /责任校对：包志虹
责任印制：吕春珉 /封面设计：郝希平

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
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2003年1月第 一 版 开本：787×1092 1/16
2003年1月第一次印刷 印张：16 1/4
印数：1—4 000 字数：38 000

定价：28.00元

(如有印装质量问题，我社负责调换〈环伟〉)

序

CPU 和操作系统是信息产业的两大支柱. 多年来,国外操作系统,例如 Windows 系列操作系统等成为主流平台,主宰着操作系统市场. 随着计算机的普及和因特网的发展,我国信息化基础建设在技术与装备上对外国的依赖性,使信息安全的问题日益突出. 尽管出于种种原因,我国多年来自主研制的若干操作系统项目,没有形成产品,没有真正得到推广应用,但是,我国广大工程技术人员,在操作系统这一领域曾经做过许多工作,积累了许多宝贵的经验和教训. 特别是,近年来 Linux 操作系统这一新星的出现,更为我们提供了机遇和挑战. 在新的世纪,我国必须加强信息领域核心技术的研究,必须尽快研制具有我国自主版权的操作系统. 其中,安全操作系统的研究是关键的一环,对加强我国信息化安全基础设施建设,具有十分重要的意义.

《操作系统安全导论》一书,是我国著名信息安全专家卿斯汉和他的学生们的一部力作. 本书详尽地分析了现行主流操作系统的安全缺陷,在此背景的基础上,全面地论述了操作系统的安全机制、安全设计、操作系统评测和安全应用. 本书包含了现代安全操作系统的主要内容,反映了 20 世纪后期安全操作系统的发展主流,使读者对操作系统安全有一个清晰和完整的认识.

卿斯汉研究员领导的课题组,在安全操作系统的研究方面具有扎实的理论基础和丰富的实践经验. 他们研制的安胜安全操作系统,是基于 Linux 核心资源、自主开发的安全操作系统,达到了我国国家标准 GB17859-1999《计算机信息系统安全保护等级划分准则》第三级《安全标识保护级》功能要求. 该系统已通过公安部计算机信息系统安全产品质量监督检验中心和国家信息安全测评认证中心的测评和认证.

本书内容丰富,理论和实践相结合,填补了我国操作系统安全专著的空白,是一本难得的佳作. 本书的出版,既反映了操作系统安全的发展潮流,也包含了作者的最新科研成果. 我相信本书的出版,将对我国信息安全领域产生积极的影响并将有力地促进操作系统的研究工作.

中国工程院院士
沈昌祥
2001 年 8 月

前　言

操作系统是计算机资源的直接管理者，它直接和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. 数据库管理系统 DBMS 是建立在操作系统之上的，如果没有操作系统安全机制的支持，就不可能保障其存取控制的安全可信性. 在网络环境中，网络安全依赖于各主机系统的安全可信性，没有操作系统的安全，就谈不上主机系统和网络系统的安全性. 因此，操作系统的安全是整个计算机系统安全的基础，没有操作系统安全，就不可能真正解决数据库安全、网络安全和其他应用软件的安全问题.

另外，一个有效可靠的操作系统也应具有很强的安全性，必须具有相应的保护措施，杜绝或限制天窗、隐蔽通道、特洛伊木马等对系统构成的安全隐患；对系统中的信息提供足够的保护，防止未授权用户的滥用或毁坏. 只靠硬件不能提供充分的保护手段，必须由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.

长期以来，我国关于信息安全方面的书籍出版甚少，有关操作系统安全的专著几乎没有. 本书出版的目的之一是想填补这一空白，满足广大读者的需求.

本书专门讨论操作系统的安全性，对相关内容进行了精心安排，并加入了作者科研工作的成果，读者阅读本书之后，将对操作系统的安全特性和安全操作系统有一个全面的了解.

全书分为 8 章. 第 1 章介绍操作系统安全的基本概念及预备知识；第 2 章和第 3 章分别介绍 UNIX/Linux 和 Windows NT/XP 等主流操作系统的安全问题；第 4 章介绍高安全级别操作系统的相关概念及其重要组成部分，包括安全机制、自主存取控制、强制存取控制、最小特权管理、系统审计、可信通路等；第 5 章介绍如何设计开发高安全级别的操作系统，如安全模型设计、安全内核设计等. 第 6 章介绍操作系统的安全评测问题，包括国内外的安全操作系统评测标准和评测方法；第 7 章介绍安全操作系统的应用；第 8 章介绍国外安全操作系统研究的新进展.

作者长期从事信息安全和操作系统安全的研究和产品开发，本书是作者在操作系统安全领域工作的总结. 作者感谢中国科学院信息安全技术工程研究中心广大同仁和研究生在本书出版过程中和安全操作系统研制开发中的支持和帮助. 本书实际上是中心全体成员集体智慧的结晶. 在此，我们特别感谢中心副主任倪惜珍和贺也平两位研究员的支持. 刘克龙博士、蒙杨博士、朱继锋博士、李丽萍博士和唐烨硕士、石怡硕士、王涛硕士参与了本书的部分写作与出版工作，作者表示深深的谢意.

本书在写作和出版过程中，以及作者在长期操作系统安全的研究中，得到了许多部门和专家的支持和鼓励. 他们是：中国科学院、中国科学院科学出版基金委员会、中国科学院软件研究所、国家自然科学基金委员会、科学出版社、张效祥、何德全、沈昌祥、蔡吉人、周仲义、魏正耀、胡启恒等院士，中国科学院高技术研究与发展局局长桂文庄研究员.

目　录

序

前言

第 1 章　绪论 …… 1

1.1　信息系统的脆弱性 …… 1

1.2　安全操作系统的重要性 …… 3

1.3　安全操作系统的发展状况 …… 4

1.4　基本概念 …… 6

1.5　本书的组织和编排 …… 8

第 2 章　UNIX/Linux 操作系统安全 …… 9

2.1　UNIX/Linux 的历史发展和现状 …… 9

2.2　UNIX/Linux 系统分析 …… 10

2.2.1　文件子系统 …… 11

2.2.2　进程子系统 …… 14

2.2.3　系统调用 …… 16

2.3　UNIX/Linux 的安全性 …… 18

2.3.1　标识 …… 18

2.3.2　鉴别 …… 19

2.3.3　存取控制 …… 19

2.3.4　审计 …… 21

2.3.5　密码 …… 22

2.3.6　网络 …… 23

2.3.7　网络监视和入侵检测 …… 25

2.3.8　备份/恢复 …… 25

2.4　UNIX 常见安全漏洞及解决方法 …… 25

2.5　Linux 常见安全漏洞及解决方法 …… 31

第 3 章　Windows NT/XP 操作系统安全 …… 39

3.1　Windows NT/XP 操作系统简介 …… 39

3.2　Windows NT/XP 安全模型 …… 41

3.2.1　用户和工作组 …… 42

3.2.2　域和委托 …… 43

3.2.3　活动目录 …… 44

3.2.4　登录 …… 48

3.2.5　资源访问控制 …… 50

3.2.6 Windows NT/XP 的审计子系统 …… 51
3.3 注册表 …… 53
3.4 文件系统 …… 54
3.4.1 FAT …… 54
3.4.2 HPFS …… 55
3.4.3 NTFS …… 55
3.4.4 NPFS …… 58
3.4.5 MSFS …… 58
3.5 Windows XP 系统的激活机制及授权新机制 …… 58
3.5.1 Windows XP 产品的激活原理 …… 58
3.5.2 激活机制与授权机制对国家信息安全的影响 …… 59
3.6 Windows NT/XP 安全漏洞及对策 …… 60
3.6.1 Windows NT 安全漏洞及对策 …… 60
3.6.2 Windows NT 常用软件的安全漏洞及对策 …… 67
3.6.3 目前已知的 Windows XP 安全性漏洞 …… 70
第 4 章 操作系统的安全机制 …… 73
4.1 硬件安全机制 …… 73
4.1.1 存储保护 …… 73
4.1.2 运行保护 …… 75
4.1.3 I/O 保护 …… 77
4.2 软件安全机制 …… 77
4.2.1 标识与鉴别 …… 77
4.2.2 存取控制 …… 82
4.2.3 最小特权管理 …… 91
4.2.4 可信通路 …… 96
4.2.5 隐蔽通道 …… 100
4.2.6 安全审计 …… 105
4.2.7 病毒防护 …… 108
第 5 章 安全操作系统设计 …… 114
5.1 安全操作系统的设计原则与一般结构 …… 114
5.2 可信计算基(TCB) …… 115
5.3 访问监督器和安全内核 …… 115
5.4 安全模型 …… 118
5.4.1 安全模型的作用和特点 …… 118
5.4.2 安全模型介绍 …… 119
5.4.3 状态机模型 …… 120
5.4.4 Bell-LaPadula 模型 …… 121
5.4.5 基于角色的存取控制(RBAC)模型 …… 131

5.4.6 伯巴模型 …… 135
5.4.7 信息流模型 …… 138
5.4.8 其他几个安全模型 …… 143
5.5 安全操作系统的开发方法 …… 145
5.6 安全操作系统的开发过程 …… 148
5.7 开发过程中不容忽视的几个问题 …… 149
5.7.1 配置管理和文档管理 …… 149
5.7.2 安全性能友好 …… 150
5.7.3 兼容性和效率 …… 150
5.8 安全操作系统设计举例 …… 150
5.8.1 安胜安全操作系统 v3.0 …… 150
5.8.2 安胜安全操作系统 v4.0 …… 165
第 6 章 操作系统安全评测 …… 170
6.1 操作系统安全漏洞扫描 …… 170
6.2 操作系统安全评测 …… 171
6.2.1 操作系统安全评测的基础 …… 171
6.2.2 操作系统安全评测方法 …… 171
6.2.3 国内外计算机系统安全评测准则概况 …… 172
6.2.4 美国国防部可信计算机系统评测准则 …… 174
6.2.5 中国计算机信息系统安全保护等级划分准则 …… 180
6.2.6 通用安全评价准则 CC …… 183
6.2.7 中国推荐标准 GB/T18336-2001 …… 217
第 7 章 安全操作系统应用 …… 218
7.1 操作系统安全与 WWW 安全 …… 218
7.1.1 WWW 系统描述 …… 218
7.1.2 安全 WebServer 概念的提出及相应的解决方案 …… 220
7.1.3 基于 BLP 模型的 SecWeb 系统描述 …… 221
7.2 操作系统安全与防火墙安全 …… 230
7.2.1 防火墙介绍 …… 230
7.2.2 防火墙涉及的安全技术 …… 232
7.2.3 防火墙利用安全操作系统的保护机制 …… 232
第 8 章 国外安全操作系统研究的新进展 …… 236
8.1 SELinux …… 236
8.1.1 从 DTMach 到 SELinux …… 236
8.1.2 SELinux 的安全体系结构 …… 236
8.1.3 SELinux 的安全策略配置 …… 238
8.2 EROS …… 239
8.2.1 EROS 的历史 …… 239

8.2.2 权能与访问控制列表 …… 240
8.2.3 EROS 的体系结构 …… 241
8.3 多安全策略支持框架 …… 243
8.3.1 存取控制广义框架 …… 243
8.3.2 FAM 框架 …… 244
8.3.3 配置 RBAC 模型支持多策略 …… 245
8.3.4 FLASK 框架 …… 245
8.3.5 多安全策略支持框架的比较 …… 245
主要参考文献 …… 247

第1章 绪 论

1.1 信息系统的脆弱性

一个安全的信息系统应该满足用户系统的保密性(Confidentiality)、完整性(Integrity)及可用性(Availability)的要求,亦即所谓CIA的要求.随着网络技术的飞速发展,信息资源的共享程度进一步加强.特别是,因特网的大规模应用以及金融等重要网络的接入,越来越多的系统遭到入侵攻击的威胁.这些威胁大多是通过挖掘操作系统和应用服务程序的弱点或缺陷实现的,1988年的蠕虫事件就是一个很好的例子.

建立一个安全的信息系统较之建立一个正确无误的信息系统要简单得多.但是,目前市场上尚无任何一个大型操作系统可以做到完全正确.所有大型操作系统的生产厂商都定期推出新的操作系统版本,其中包括数以千计修改了的语句和代码,而这些改动绝大多数是为了纠正系统中的错误或弥补其缺陷而进行的.实际上,从来没有一个操作系统的运行是完美无缺的,也没有一个厂商敢保证他们的操作系统不会出错.工业界已经承认这样一个事实:任何操作系统都是有缺陷的.但是,另一方面,我们可以说绝大多数操作系统是可靠的,可以基本完成其设计功能.

就计算机安全而言,一个操作系统仅仅完成其大部分的设计功能是远远不够的.当我们发现计算机操作系统的某个功能模块上只有一个故障时,我们可以忽略它,这对整个操作系统的功能影响甚微;若干种故障的某种组合才会对操作系统造成致命的影响.但是,信息系统安全的每一个漏洞都会使整个系统的安全控制机制变得毫无价值.这个漏洞如果被蓄意入侵者发现,后果将是十分严重的.这如同一个墙上有洞的房间,虽然可以居住,却无法将盗贼拒之门外.

另外,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.例如,文件系统常被配置得没有安全性,所以应对其进行仔细的检查.当配置文件所有权和权限时,常常由于文件的账户所有权不正确或文件权限设置的不正确而导入潜在漏洞.

对操作系统安全构成的威胁主要有以下几种:

(1)计算机病毒

指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码.计算机病毒具有以下基本特点:

1)隐蔽性.病毒程序代码驻存在磁盘等介质上,无法以操作系统提供的文件管理方法观察到.有的病毒程序设计得非常巧妙,甚至用一般的系统分析软件工具都无法发现它的存在.

2)传染性.当用户利用磁盘片、网络等载体交换信息时,病毒程序趁机以用户不能察

觉的方式随之传播.即使在同一部计算机上,病毒程序也能在磁盘上的不同区域间传播,附着到多个文件上.

3)潜伏性.病毒程序感染正常的计算机之后,一般不会立即发作,而是潜伏下来,等到激发条件(如日期、时间、特定的字符串等)满足时才产生破坏作用.

4)破坏性.当病毒发作时,通常会在屏幕上输出一些不正常的信息,同时破坏磁盘上的数据文件和程序.如果是开机型病毒,可能会使计算机无法启动.有些"良性"病毒不破坏系统内现存的信息,只是大量地侵占磁盘存储空间,或使计算机运行速度变慢,或造成网络堵塞.

(2)特洛伊木马

特洛伊木马是一段计算机程序,表面上在执行合法功能,实际上却完成了用户不曾料到的非法功能.受骗者是程序的用户,入侵者是这段程序的开发者.特洛伊木马必须具有以下几项功能才能成功地入侵计算机系统:

1)入侵者要写一段程序进行非法操作,程序的行为方式不会引起用户的怀疑.

2)必须设计出某种策略诱使受骗者接受这段程序.

3)必须使受骗者运行该程序.

4)入侵者必须有某种手段回收由特洛伊木马发作为他带来的实际利益.特洛伊木马程序与病毒程序不同,是一个独立的应用程序,不具备自我复制能力,但它同病毒程序一样,具有潜伏性,且常常具有更大的欺骗性和危害性.特洛伊木马也可能包含蠕虫或病毒程序.

(3)隐蔽通道

隐蔽通道可定义为系统中不受安全策略控制的、违反安全策略的信息泄漏路径.按信息传递的方式和方法区分,隐蔽通道分为存储隐蔽通道和时间隐蔽通道.存储隐蔽通道在系统中通过两个进程利用不受安全策略控制的存储单元传递信息.前一个进程通过改变存储单元的内容发送信息,后一个进程通过观察存储单元的变化接收信息.时间隐蔽通道在系统中通过两个进程利用一个不受安全策略控制的广义存储单元传递信息.前一个进程通过改变广义存储单元的内容发送信息,后一个进程通过观察广义存储单元的变化接收信息,并用如实时时钟这样的坐标进行测量.广义存储单元只能在短时间内保留前一个进程发送的信息,后一个进程必须迅速地接收广义存储单元的信息,否则信息将消失.判别一个隐蔽通道是否是时间隐蔽通道,关键是看它有没有一个实时时钟、间隔定时器或其他计时装置,不需要时钟或定时器的隐蔽通道是存储隐蔽通道.

(4)天窗

天窗是嵌在操作系统里的一段非法代码,渗透者利用该代码提供的方法侵入操作系统而不受检查.天窗由专门的命令激活,一般不容易发现.而且,天窗所嵌入的软件拥有渗透者所没有的特权.通常,天窗设置在操作系统内部,而不在应用程序中,天窗很像是操作系统里可供渗透的一个缺陷.的确,安装天窗就是为了渗透.天窗可能是由操作系统生产厂家的一个不道德的雇员装入的,安装天窗的技术很像特洛伊木马的安装技术,但在操作系统中实现就更为困难.与特洛伊木马和隐蔽通道不同,天窗只能利用操作系统的缺陷或者混入系统的开发队伍中进行安装,因此,开发安全操作系统的常规技术就可以避免天

窗，而不需要专门的技术解决这个问题.

总之，保护信息系统的安全一直是一场智力的斗争. 入侵者总是在极力寻找信息系统的漏洞，设计者总是在想方设法把这些漏洞堵住. 信息系统的设计者们永远无法充满自信地宣布已经找出了系统中的所有漏洞，而入侵者们也不会公布他们的发现. 当你将重要的敏感信息委托给一个大型操作系统或网络中的一个计算机的时候，你没有理由不为你的信息的保密性而担忧，尤其是当这些信息对入侵者有足够的价值的时候，你更没有理由认为黑客的入侵行动会失败.

不管如何，防止入侵还是有希望的，使用适当的技术手段，可使系统的安全控制有较好的效果. 尽管整个计算机系统仍有许多漏洞，我们还是可以使该系统的安全系数大大提高. 在这里，重要的因素不是系统出错的可能性(一般都较高)，而是入侵者发现错误而导致损失的可能性(我们希望这种可能性变得最小). 虽然我们永远也不能确信计算机系统是否百分之百的安全，但我们可以使之达到相当高的安全水平，使黑客的入侵行动变得极端困难、危险和耗资巨大，以至于最后窃取到的信息的价值低于入侵成功而付出的代价.

系统而合理地使用安全技术，是使计算机系统的安全达到令人满意的水平的关键. 使用不切实际的技术手段，其后果是相当严重的：轻者，会导致使用过多的投资建立起毫无实际意义的超高水平的保护体系，浪费财力，应用不便；重者，它会发出错误的报警信号，干扰正常的工作，而对真正的入侵行为却不能及时发现.

1.2 安全操作系统的重要性

根据计算机软件系统的组成，软件安全可划分为：应用软件安全、数据库安全、操作系统安全和网络软件安全. 操作系统用于管理计算机资源，控制整个系统的运行，它直接和硬件打交道，并为用户提供接口，是计算机软件的基础. 数据库通常是建立在操作系统之上的，若没有操作系统安全机制的支持，数据库就不可能具有存取控制的安全可信性. 在网络环境中，网络的安全可信性依赖于各主机系统的安全可信性，而主机系统的安全性又依赖于其操作系统的安全性. 因此，若没有操作系统的安全性，就没有主机系统的安全性，从而就不可能有网络系统的安全性. 计算机应用软件都建立在操作系统之上，它们都是通过操作系统完成对系统中信息的存取和处理. 因此，可以说操作系统的安全是整个计算机系统安全的基础，没有操作系统安全，就不可能真正解决数据库安全、网络安全和其他应用软件的安全问题.

AT&T 实验室的 S. Bellovin 博士曾经对美国 CERT (Computer Emergency Response Term)提供的安全报告进行过分析，结果表明，很多安全问题都源于操作系统的安全脆弱性.

我们并不否认数据加密在信息处理中的作用，它是保密通信中必不可少的手段，也是保护存储文件的有效方法. 但数据加密、解密所涉及到的密钥分配、转储等过程必须用计算机实现. 如果不相信操作系统可以保护数据文件，那就不应相信它总能适时地加密文件并能妥善地保护密钥. 这就使得：若无安全的计算机操作系统做保护，数据加密就可以比喻为“纸环上套了个铁环”. 数据加密并不能提高操作系统的可信度，要解决计算机内信息

的安全性，必须解决操作系统的安全性. 因此，我们说操作系统安全是计算机安全的必要条件.

当前，保障网络及信息安全的问题已引起人们的广泛关注，但随着防火墙、网络保密机、网络安全服务器、安全管理中心等网络安全产品的研制和使用，人们不得不思考这样的问题：这些安全产品的“底座”(操作系统)可靠坚固吗？

现在应用最广泛的 Windows 系列操作系统在安全性方面漏洞很多，有人批评 Windows 的体系结构有弱点，这可能是它容易遭受病毒袭击的原因之一. 另外，已发现在 Windows95 和 Windows98 中都存在着“后门”，也发现在 Word97 中有追踪用户 ID 的手段，尽管微软已发布了可以禁止这些“后门”的补丁，但仍难以消除人们的顾虑. 由于 Windows 操作系统不提供源码，像一个“黑盒子”，对它的安全性难以估量和增强.

另外，一个有效可靠的操作系统也应具有很强的安全性，必须具有相应的保护措施，消除或限制如天窗、隐蔽通道、特洛伊木马等对系统构成的安全隐患.

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方面，研究和开发安全操作系统具有重要意义.

1.3　安全操作系统的发展状况

Multics 是开发安全操作系统最早期的尝试. 1965 年，美国贝尔实验室和麻省理工学院的 MAC 课题组等一起联合开发一个称为 Multics 的新操作系统，其目标是要向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. 贝尔实验室中后来参加 UNIX 早期研究的许多人当时都参加了 Multics 的开发工作. 由于 Multics 预期的复杂性和理想性，结果未能达到预期的目标，而且连他们自己也不清楚什么时候才算达到设计的目标. 虽然 Multics 未能成功，但它在安全操作系统的研究方面迈出了重要的第一步，Mitre 公司的 Bell 和 LaPadula 合作设计的安全模型 Bell-La Padula 首次成功地用于 Multics. Multics 为后来的安全操作系统研究积累了大量的经验.

KSOS(Kernelized Secure Operating System)是美国国防部研究计划局 1977 年发起的一个安全操作系统研制项目，由 Ford 太空通讯公司承担. KSOS 采用了形式化说明与验证的方法，目标是高安全可信性.

UCLA Secure Unix 也是美国国防部研究计划局发起的一个安全操作系统研制项目，由加利福尼亚大学承担. UCLA Secure Unix 的系统设计方法及目标几乎与 KSOS 相同.

美国国防部于 1985 年出版了《可信计算机系统评价准则(TCSEC)》，为计算机系统的可信程度划分和评价提供了准则，因其封面为橘黄色而又被称为橘皮书. 虽然橘皮书并不是一本设计说明书，但现在的设计者已把橘皮书中的思想溶于安全操作系统的设计中了.

LINVS Ⅳ是 1984 年开发的基于 UNIX 的一个实验安全操作系统，系统的安全性可达到美国国防部橘皮书的 B2 级.

Secure Xenix 是 IBM 公司于 1986 年在 SCO Xenix 的基础上开发的一个安全操作系统，它最初是在 IBM PC/AT 平台上实现的. Secure Xenix 对 Xenix 进行了大量的改造开发，并采用了一些形式化说明与验证技术. 它的目标是 TCSEC 的 B2 到 A1 级.

1987 年，美国 Trusted Information Systems 公司以 Mach 操作系统为基础开发了 B3 级的 TMach(Trusted Mach)操作系统. 除了进行用户标识和鉴别及命名客体的存取控制外，它将 BLP 模型加以改进，运用到对 Mach 核心的端口、存储对象等的管理当中，通过对端口间的消息传送，对端口、存储对象、任务等的安全标识加强微核心的安全机制.

1989 年，加拿大多伦多大学开发了与 UNIX 兼容的 TUNIS 操作系统，其目标是 B3 级. 它用 Turing Plus 语言(而不是 C)重新实现了 UNIX 内核，这是一种强类型高级语言，其大部分语句都具有用于正确性证明的形式语义. TUNIS 的模块性相当好. 它在实现中改进了 BLP 模型.

OSF/1 是开放软件基金会于 1990 年推出的一个安全操作系统，被美国国家计算机安全中心(NCSC)认可为符合 TCSEC 的 B1 级，其主要安全性表现为

- 系统标识；
- 口令管理；
- 强制存取控制和自主存取控制；
- 审计.

UNIX SVR4.1ES 是 UI(UNIX 国际组织)于 1991 年推出的一个安全操作系统，被美国国家计算机安全中心(NCSC)认可为符合 TCSEC 的 B2 级，除 OSF/1 外的安全性主要表现在：

- 更全面的存取控制；
- 最小特权管理；
- 可信通路；
- 隐蔽通道分析和处理.

1991 年，在欧洲共同体的赞助下，英、德、法、荷四国制定了拟为欧共体成员国使用的共同标准——信息技术安全评定标准(ITSEC). 随着各种标准的推出和安全技术产品的发展，美国伙同加拿大及欧共体国家一起制定通用安全评价准则(Common Criteria for IT Security Evaluation，CC)，1996 年 1 月发布了 CC 标准的 1.0 版. CC 标准的 2.0 版已于 1997 年 8 月颁布，并于 1999 年 7 月通过国际标准组织认可，确立为国际标准，即 ISO/IEC 15408.

CC 标准本身由两个部分组成，一部分是一组信息技术产品的安全功能需要定义，另一部分是对安全保证需求的定义. CC 标准吸收了各国有关信息系统安全的经验与知识，将会对未来信息安全的研究与应用带来重大影响.

1997 年美国安全计算公司(SCC)和国家安全局(NSA)完成了 DTOS(Distributed Trusted Operating System)安全操作系统. 与传统的基于 TCSEC 标准的开发方法不同，DTOS 采用了基于安全威胁的开发方法. 设计目标为

- 策略灵活性：DTOS 内核应该能够支持一系列的安全策略，包括诸如国防部的强制存取控制多级安全策略；

· 与 Mach 兼容，现有的 Mach 应用应能在不做任何改变的情况下运行；

· 性能应与 Mach 接近.

2001 年，美国国家安全局(NSA)等单位以 Flask 安全体系结构为指导，在 Linux 基础上开发了 SELinux. SELinux 定义了一个类型实施(TE)策略，基于角色的访问控制(RBAC)策略和多级安全(MLS)策略组合的安全策略.

还有一些其他安全操作系统开发项目，如 Honeywell 的 STOP，Gemini 的 GEMSOS，DEC 的 VMM(Virtual Machine Monitor)，ASOS(Army Secure Operating System)等，以及 HP 和 Data General 等公司开发的安全操作系统.

在我国，也进行了一些有关安全操作系统的开发研制工作. 例如海军计算技术研究所、中国软件与技术服务总公司等的成果.

我国国家技术监督局于 1999 年 10 月 19 日发布了国家标准 GB17859-1999《计算机信息系统安全保护等级划分准则》，为计算机信息系统安全保护能力划分了等级. 该标准已于 2001 年起强制执行.

2000 年 11 月 18 日，公安部计算机信息系统安全产品质量监督检验中心，在网站 http://www.mctc.gov.cn 上发布公告："国内首家安全操作系统通过检测". 公告说：由中科安胜信息技术有限公司研制的安胜安全操作系统 v1.0，经过本检验中心的严格测试检验，已于 2000 年 11 月 17 日，成为第一个通过按国家标准《计算机信息系统安全保护等级划分准则》(GB17859-1999)检验的安全操作系统. 它实现了《计算机信息系统安全保护等级划分准则》第 3 级的全部安全功能要求，并具有第 4 级的部分安全功能. 同时还扩展了最小特权管理、加密服务和网络安全管理功能.

安胜安全操作系统 v1.0 于 2001 年 2 月 20 日首家通过了中国国家信息安全测评认证中心的评测认证，获准国家信息安全产品型号认证.

1.4 基本概念

以下列举一些重要的、有关安全操作系统的基本概念和术语.

· 计算机信息系统 (Computer Information System)：由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统.

· 可信计算基 (Trusted Computing Base)：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. 它建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务.

· 主体(Subject)：系统中能够发起行为的实体，如进程.

· 客体(Object)：系统中被动的主体行为承担者. 对一个客体的访问隐含着对其包含信息的访问. 客体的实体有：记录、程序块、页面、段、文件、目录、目录树和程序，还有位、字节、字、字段、处理器、视频显示器、键盘、时钟、打印机和网络节点等.

· 参考监督器 (Reference Monitor)：监督主体和客体之间授权访问关系的部件.

· 安全策略 (Security Policy)：有关管理、保护和发布敏感信息的法律、规定和实施

细则. 简单地说,就是用户对安全的要求的描述.

· 安全模型 (Security Model):用形式化的方法来描述如何实现系统的安全要求:机密性、完整性和可用性.

· 安全内核(Security Kernel):控制对系统资源的访问而实现基本安全规程的计算机系统的中心部分.

· 安全周边(Security Perimeter):用半径来表示的空间. 该空间包围着用于处理敏感信息的设备,并在有效的物理和技术的控制之下,防止未授权的进入或敏感信息的泄漏.

· 客体重用(Object Reuse):对曾经包含一个或几个客体的存储介质(如内存、盘扇面、磁带)重新分配和重用. 为了安全地重分配、重用,介质不得包含重分配前的残留数据.

· 标识与鉴别(Identification & Authentication):用于保证只有合法用户才能进入系统,进而访问系统中的资源.

· 访问控制(Access Control):限制已授权的用户、程序、进程或计算机网络中其他系统访问本系统资源的过程.

· 访问控制列表(Access Control List):与系统中客体相联系的,用来指定系统中哪些用户和组可以以何种模式访问该客体的控制列表.

· 自主访问控制(Discretionary Access Control):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,该客体的拥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.

· 强制访问控制(Mandatory Access Control):用于将系统中的信息分密级和分类进行管理,保证每个用户只能够访问那些被标明能够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.

· 最小特权原理(Least Privilege Principle):系统中每一个主体只拥有和其操作相符的所要求的必需的最小的特权集.

· 隐蔽通道(Covert Channel):允许进程以危害系统安全策略的方式传输信息的通信信道.

· 审计(Audit):一个系统的审计就是对系统中有关安全的活动进行记录、检查及审核.

· 审计跟踪(Audit Trail):系统活动的流水记录. 该记录按事件从始至终的途径、顺序,审查和检验每个事件的环境及活动.

· 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):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权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.

· 鉴别(Authentication):验证用户、设备和其他实体的身份;验证数据的完整性.

· 授权(Authorization):授予用户、程序或进程访问权.

· 保密性(Confidentiality):为秘密数据提供保护方法及保护等级的一种特性.

· 数据完整性(Data Integrity):信息系统中的数据与原始数据没有发生变化,未遭受偶然或恶意的修改或破坏时所具有的性质.

· 漏洞(Loophole):由于软硬件的设计疏忽导致的,是能避开系统的安全措施的一种错误.

· 安全配置管理(Secure Configuration Management):控制系统硬件与软件结构更改的一组规程,其目的是保证这种更改不违反系统的安全策略.

· 操作系统安全(Operating System Security):操作系统无错误配置、无漏洞、无后门、无特洛伊木马等,能防止非法用户对计算机资源的非法存取,一般用来表达对操作系统的安全需求.

· 操作系统的安全性(Security of Operating System):操作系统具有或应具有的安全功能,比如存储保护、运行保护、标识与鉴别、安全审计等.

· 安全操作系统(Secure Operating System):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.通常,一种安全操作系统是从开始设计时,就充分考虑到系统的安全性.另一种是基于一个通用的操作系统,专门进行安全性改进或增强,并通过相应的安全性评测.

· 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,比如符合美国橘皮书(TCSEC)B1 级及以上的安全操作系统.

1.5　本书的组织和编排

本书共分 8 章.第 1 章是绪论,介绍了信息系统的脆弱性,安全操作系统的重要性,安全操作系统的发展状况,以及与操作系统安全有关的若干重要概念和术语.第 2 和第 3 章分别分析了 UNIX/Linux 和 Windows 等流行操作系统存在的安全问题,并对其安全模型、审计系统、存取控制方式、安全漏洞及其对策等进行了详尽的讨论.第 4 章讨论了高级别安全操作系统的有关安全机制,包括自主存取控制、强制存取控制、最小特权管理、系统审计、可信通路、隐蔽通道、病毒防护、标识与鉴别、存储保护、运行保护和输入/输出保护等.第 5 章介绍了如何设计和开发高级别的安全操作系统,详尽讨论了安全操作系统设计的原则、可信计算基、访问监督器、安全内核、安全模型等.本章还以我们亲身设计的安胜安全操作系统为例,讲述了安全操作系统的开发方法和开发过程.第 6 章的内容涉及操作系统的安全评测,包括操作系统安全评测的基础、操作系统安全评测的方法、操作系统安全评测的准则以及国内外著名的安全操作系统评测标准等.第 7 章阐述了安全操作系统的应用,着重讨论了操作系统安全与 Web 服务器安全、操作系统安全与防火墙安全.第 8 章则介绍国外安全操作系统研究的一些新进展.