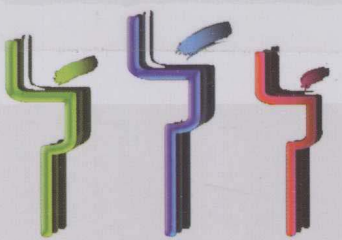
AnQuan

普通高校信息安全系列教材

林果园　张爱娟
张永平　曹天杰　编著

操作系统安全

CAOZUO
XITONG ANQUAN



北京邮电大学出版社
www.buptpress.com

普通高校信息安全系列教材

操作系统安全

林果园　张爱娟　张永平　曹天杰　编　著

北京邮电大学出版社
·北京·

内 容 简 介

本书是普通高校信息安全系列教材之一的操作系统安全教材。全书共分为8章，主要包括：操作系统安全的基本概念、安全机制、安全模型、安全体系结构、安全设计与验证、安全评测和主流操作系统Windows和UNIX/Linux的安全机制与技术。

本书深入浅出，注重操作系统安全的基本理论和基本概念与实际操作系统安全技术相结合，注意吸收最新的操作系统安全研究成果。

本书可以作为信息安全、计算机科学与技术、网络工程、通信工程等专业的本科生教材，也可以作为相关专业的本科生、研究生和与信息安全相关的教学、科研人员的参考书。

图书在版编目(CIP)数据

操作系统安全/林果园等编著. --北京：北京邮电大学出版社，2010.7

ISBN 978-7-5635-2305-4

Ⅰ.①操… Ⅱ.①林… Ⅲ.①操作系统—安全技术—高等学校—教材 Ⅳ.①TP316

中国版本图书馆CIP数据核字(2010)第132829号

书　　名：操作系统安全

作　　者：林果园　张爱娟　张永平　曹天杰

责任编辑：刘　颖

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路10号(邮编：100876)

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京源海印刷有限责任公司

开　　本：787 mm×960 mm　1/16

印　　张：12.25

字　　数：266千字

印　　数：1—3 000册

版　　次：2010年7月第1版　2010年7月第1次印刷

ISBN 978-7-5635-2305-4　　定　价：22.00

前言

随着互联网和计算机技术的迅猛发展，人们的工作和生活方式都在发生着深刻的变化，对计算机和网络技术的依赖程度不断增加。信息技术的发展给人们的生产生活带来方便的同时，也带来了日益严峻的信息安全问题。

信息安全问题的核心是信息系统的完整性、可用性和保密性，而在整个信息系统中操作系统是最核心的基础软件，它是计算机资源的直接管理者，是其他软件和硬件的桥梁，同时也是用户和网络通信的接口。在计算机网络环境中，大多数的安全问题都会在计算机主机中体现，因此操作系统的安全问题是整个计算机网络安全的基础。

本书共分 8 章，比较全面地介绍了操作系统安全的基本概念、基本理论和相应技术。第 1 章介绍了操作系统安全的发展概况、操作系统的安全威胁、操作系统功能与安全的关系、安全操作系统与可信计算基的关系以及相关的基本概念。第 2 章介绍了操作系统的安全机制，包括访问控制、主体标识与鉴别机制、安全审计、内存存取保护、文件系统保护、信息通路保护机制、最小特权管理、安全配置机制。第 3 章介绍了常用的安全模型，包括 BLP 模型、Biba 模型、Clark-Wilson 完整性模型、中国墙模型、DTE 模型和无干扰模型。第 4 章主要介绍了权能体系结构和 Flask 体系结构。第 5 章主要介绍了与操作系统安全有关的形式化技术的基本原理及其应用，包括形式化的基本方法和原理、操作系统安全的形式化设计技术、形式化验证技术和形式化设计与验证的实例。第 6 章介绍操作系统安全评测，包括常见的评价标准 TCSEC、ITSEC、CTCPEC、CC 和 GB/T 18336—2001，对它们之间的差异进行了比较，并简单介绍了安全评测的技术和方法。第 7 章介绍 Windows 操作系统的安全技术，包括身份验证、访问的安全控制、注册表安全、域管理机制、文件系统安全、日志与安全设置以及 Windows 7 的几个安全技术。第 8 章主要从账户安全管理、口令安全与访问控制、文件系统安全、日志查看与分析、网络服务安全、备份与恢复六个方面讲述了 UNIX/Linux 操作系统安全技术。

在本书写作过程中，参考了很多著名学者的学术著作和同行的科研成果，有的已经在参考文献中列出，但由于篇幅所限，恕不能一一列出，在此一并表示感谢。参加本书文字编写工作的还有孙统风、贺珊、王国辉、陈珍珍。

由于作者水平有限，书中难免有错误与疏漏之处，敬请读者批评指正。

作　者

目 录

第1章 导 论

信息安全本身包括的范围很大，大到国家军事政治等机密安全，小到如何防范商业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（例如访问控制、数字签名、信息认证、数据加密等），直至系统安全，其中任何一个安全漏洞都可以威胁全局安全。

众所周知，操作系统是计算机的系统软件，是计算机资源的直接管理者，它直接与硬件打交道，并为用户提供接口，是计算机软件的基础与核心。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作为基础，就谈不上主机系统和网络系统的安全。因此，操作系统的安全是整个信息安全体系的基石。

本章主要介绍操作系统安全的发展概况、操作系统安全与基本功能的关系以及跟操作系统相关的基本概念。

1.1 操作系统安全的发展历程

有关操作系统安全的研究发展历程虽然有不同的说法，但大多以时间为线索，而且是根据安全操作系统研究与开发工作的特点，进行阶段划分。本书将从技术发展过程和标准化过程两个角度介绍操作系统安全的研究发展。

1. 技术发展过程

(1) 萌芽时期

早在20世纪60年代，许多研究机构就展开了对安全操作系统的研究，此阶段又称为安全操作系统研究的起步阶段。在这个阶段里，以美国国防科学部旗下的计算机安全特别部队的组建为标志，拉开了操作系统安全研究的序幕。此阶段最受关注的是Multics的操作系统的研发。

1965年，美国贝尔实验室(Bell Lab)、麻省理工学院(MIT)和通用电器公司计划开发

一个称为 Multics 的操作系统。Multics 是一种多路转换信息和计算服务的系统，旨在为大量的用户通信提供各种各样的服务。该系统虽然没有把安全性列入设计目标，但保护功能的设计是一个创新。由于这个计划的研制难度超出了所有人的预料，最后这个系统以失败告终。

虽然 Multics 未能成功，但 Multics 的设计思想却为后来的安全操作系统提供了很多提示，它使安全操作系统的研究迈出了重要的一步。60 年代末，一位在贝尔实验室曾参加过 Multics 研制工作的计算机科学家 Ken Thompson，在一台无人使用的 PDP-7 机器上开发出了一套简化的、单用户版的 Multics，后来此 Multics 促成了 UNIX 操作系统的诞生。

(2) 发展时期

在这个时期，安全操作系统经历了从无到有的过程，众多的安全理论相继推出，标志着安全操作系统的设计思想、技术和方法逐步形成。

1969 年，C. Weissman 提出了一个分时安全操作系统，称为 Adept-50，它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——高水印模型(High-Watermark 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；
- 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。

1970 年，W. H. Ware 对多渠道访问的资源共享的计算机系统所引起的安全问题进行了研究。研究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。

1972 年，J. P. Anderson 提出了参照监视器、访问控制验证、安全内核和安全建模的重要思想。

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、系统资源、共享的类型和受控共享思想等。这些因素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。

1973 年，D. E. Bell 和 L. J. LaPadula 提出了第一个安全系统的数学模型——BLP 模型。BLP 模型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 模型是一个状态机模型，它定义的系统包含一个初始状态和由一些三元组(请求、判定、状态)组成的序列，三元组序列中相邻状态之间满足某种关系。如果一个系统的初始状态是安全的，并且三元组序列中的所有状态都是安全的，那么这样的系统就是一个安全系统。

BLP模型支持的是信息的保密性。基于信息完整性的考虑，K. J. Biba提出了与BLP模型异曲同工的Biba模型。

随后，越来越多的安全操作系统研究项目被启动，一系列的安全操作系统被设计和开发出来，典型的有Mitre安全核、UCLA数据安全UNIX、KSOS和PSOS等。

相对来说，中国的安全操作系统研究起步比较晚，但也开展了一系列的工作。

1993年，国防科技大学对安全操作系统SUNIX的研究与开发进行了探讨。在SUNIX的开发过程中，研究人员提出了一个面向最小特权原则的改进的BLP模型，该模型主要对BLP模型的系统状态和公理系统进行了扩充和改造；同时，提出了一个病毒防御模型，并把它应用到了SUNIX病毒防御子系统的设计与实现之中。

以Linux为代表的自由软件在中国的广泛流行对中国安全操作系统的研究与开发具有积极的推动作用。

1999年，中国科学院软件研究所推出了红旗Linux中文操作系统发行版本，同时，开展了基于Linux的安全操作系统的研究与开发工作。

到2000年，中国的安全操作系统研究人员相继推出了一批基于Linux的安全操作系统开发成果。

中国科学院计算技术研究所研究开发了基于Linux的安全操作系统LIDS。LIDS系统开发的基本出发点是保护文件系统、保护进程系统和对核心进行封装，该系统通过权能机制实现对整个系统的控制，提供访问控制表支持，具有入侵检测和响应功能。

南京大学开发了基于Linux的安全操作系统SoftOS，该系统提供了强制访问控制、审计、禁止客体重用、入侵检测和扩展的系统资源访问控制等功能模块。

中国科学院信息安全技术工程研究中心开发了基于Linux的安全操作系统SecLinux，该系统以TCSEC标准的B1安全等级和中国等级准则第三级的要求为设计目标，提供身份标识与鉴别、自主访问控制、强制访问控制、最小特权管理、安全审计、可信通路、密码服务和网络安全服务等方面的支持。

中国计算机软件与技术服务总公司以TCSEC标准的B1安全等级为目标对Linux进行了改造，开发了COSIX Linux V2.0的安全增强版本。

此外，原信息产业部电子第30研究所、国防科技大学等单位也以Linux为基础开展了安全操作系统的研究与开发工作。

2. 标准化过程

在开发安全操作系统的同时，人们也在研究着如何建立评价标准去衡量计算机系统的安全性。第一个计算机系统安全评价标准的诞生，把安全操作系统研究带入了一个新的阶段。

1983年美国国防部出版了历史上第一个计算机安全评价标准——《可信计算机系统评价准则(TCSEC)》，TCSEC最初只是军用标准，后来延伸至民用领域。

TCSEC 标准是在基于安全核技术的安全操作系统研究的基础上制定出来的，标准中使用的可信计算基(Trusted Computing Base，TCB)就是安全核研究结果的表现。

随着 20 世纪 90 年代初 Internet 影响的迅速扩大、分布式应用的迅速普及，单一安全标准的范型与安全标准多种多样的现实世界之间拉开了很大的差距。1992 年，美国推出联邦标准草案，欲取代 TCSEC，消除 TCSEC 的局限性。1993 年，美国国防部在 TAFIM (Technical Architecture for Information Management)计划中推出新的安全体系结构 DGSA(DoD Goal Security Architecture)。DGSA 的显著特点之一是对多种安全标准支持的要求，这为安全操作系统的研究提出了新的挑战，促使安全操作系统研究进入了一个新的时期。

在我国，也进行了许多有关操作系统的安全标准研发工作，1996 年，我国国防科学技术工业委员会发布了军用计算机安全评估标准 GJB 2646—96。

1999 年 10 月 19 日，我国国家技术监督局发布了国家标准 GB/T 17859—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。

2001 年 3 月 8 日，我国国家技术监督局发布了国家标准 GB/T 18336—2001《信息技术 安全技术 信息技术安全性评估准则》，它基本上等同于国际通用安全评价准则(CC)。

1.2 操作系统的安全威胁

1988 年 11 月 20 日，康奈尔大学的一个学生向 Internet 发布了世界上第一个蠕虫(Worm)程序，这个蠕虫程序在一小时之内就侵入到美国各地，致使计算机网络中的6 000 多台计算机系统受到感染，许多联网计算机被迫停机，直接经济损失达 9 600 万美元。此后，系统安全问题越来越受到重视。

操作系统是对软件、硬件资源进行调度控制和信息产生、传递、处理的平台，它的安全性属于系统级安全的范畴，它为文件、目录、网络和邮件系统等提供底层的安全保障平台，所以操作系统的安全缺陷和安全漏洞，往往会造成严重的后果。许多网络遭到的攻击，都是针对其服务器所使用的操作系统的漏洞而进行的，因此安全机制是操作系统的重要组成部分。它的安全级别是对其性能进行评估的一个重要指标。

操作系统受到的安全威胁主要有以下几种：

(1) 计算机病毒(Computer Virus)

在《中华人民共和国计算机信息系统安全保护条例》中明确定义，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数据，影响计算机使用并且能够自我复制的一组计算机指令或程序代码。

其具有以下特点：

① 寄生性：计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

② 传染性：计算机病毒不但本身具有破坏性，更有害的是其具有传染性，一旦病毒被复制或产生变种，其速度之快令人难以预防。传染性是病毒的基本特征。

③ 潜伏性：有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。比如，黑色星期五病毒，不到预定时间一点都觉察不出来，等到条件具备的时候一下子就爆发开来，对系统进行破坏。

④ 隐蔽性：计算机病毒具有很强的隐蔽性，有的可以通过杀毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

⑤ 破坏性：计算机系统中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或受到不同程度的损坏。通常表现为增加、删除、篡改、移动。

⑥ 计算机病毒的可触发性：因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。

(2) 系统漏洞

系统漏洞是指操作系统在逻辑设计上的缺陷或在编写时产生的错误，也可能是由操作系统生产厂家的一个不道德的雇员装入的，这个漏洞可以被不法者或者计算机黑客利用，通过植入木马、病毒等方式来攻击或控制整个计算机，从而窃取计算机中的重要资料和信息，甚至破坏整个操作系统。漏洞会影响到很大的范围，包括系统本身及其支撑软件，网络客户和服务器软件，网络路由器和安全防火墙等。换而言之，在这些不同的软、硬件设备中都可能存在不同的安全漏洞问题。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

(3) 特洛伊木马(Trojan Horse)

特洛伊木马是一种恶意程序，它悄悄地在宿主机器上运行，能在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。一般而言，大多数特洛伊木马都模仿一些正规的远程控制软件的功能，如 Symantec 的 pcAnywhere。但特洛伊木马也有一些自身的特点，例如它的安装和操作都是在隐蔽之中完成。攻击者经常把特洛伊木马隐藏在一些游戏或小软件之中，诱使粗心的用户在自己的计算机上运行。最常见的情况是，上当的用户要么从不正规的网站下载和运行了带恶意代码的软件，要么不小心点击了带恶意代码的邮件附件。

大多数特洛伊木马包括客户端和服务器端两个部分。攻击者利用一种称为绑定程序的工具将服务器部分绑定到某个合法软件上，诱使用户运行合法软件。只要用户一运行软件，特洛伊木马的服务器部分就在用户毫无知觉的情况下完成了安装过程。通常，特洛伊木马的服务器部分都是可以定制的，攻击者可以定制的项目一般包括服务器运行的 IP 端口号、程序启动时机、如何发出调用、如何隐身、是否加密。另外，攻击者还可以设置登录服务器的密码、确定通信方式等。

(4) 隐藏通道

隐藏通道可定义为系统中不受安全策略控制的或者违反安全策略的信息泄露途径，是一种简易而有效的方法，可使得建立在未授权或未预料的方法之上的通信机制成为可能，它们能跨越多种访问控制/监视报告系统。隐藏通道技术常常基于隧道技术。这种机制允许将任何协议封装在已被授权的可行协议内，因此通过在被授权的协议数据流内夹带任何其他协议数据，便可实现此类通信。

一个有效可靠的操作系统应具有很强的安全性，且必须具有相应的保护措施，消除和限制计算机病毒、漏洞、特洛伊木马和隐藏通道等对系统构成的安全威胁。

1.3 操作系统的功能与安全

1.3.1 操作系统的基本功能

操作系统的形态非常多样，不同计算机安装的操作系统可从简单到复杂，可从手机的嵌入式系统到超级计算机的大型操作系统。许多操作系统制造者对操作系统的定义也不大一致，例如有些操作系统集成了图形化用户界面，而有些操作系统仅使用文本接口，而将图形界面视为一种非必要的应用程序。操作系统理论在计算机科学中是历史悠久而又活跃的分支，而操作系统的设计与实现则是软件工业的基础与内核。

作为一个底层的系统软件，操作系统肩负诸如管理与配置内存、决定系统资源供需的优先次序、控制输入与输出设备、操作网络与管理文件系统等基本事务。操作系统是管理计算机系统的全部硬件资源(包括软件资源及数据资源)、控制程序运行、改善人机界面、为其他应用软件提供支持等，使计算机系统所有资源最大限度地发挥作用，为用户提供方便的、有效的、安全的服务界面。操作系统是一个庞大的管理控制程序，大致包括 5 个方面的管理功能：进程与处理机管理、作业管理、存储管理、设备管理、文件管理。目前常见的操作系统有 DOS、OS/2、UNIX、XENIX、Linux、Windows、Netware 等。但所有的操作系统都具有并发性、共享性、虚拟性和不确定性四个基本特征。

1.3.2 操作系统的安全特性

操作系统的安全特性是指操作系统在基本功能基础上增加了安全机制与措施，以保障计算机资源使用的保密性、完整性和可用性。操作系统的安全特性处于硬件和上层应用的中间环节，可以对数据库、应用软件、网络系统提供全方位的保护。

选择安全特性高的操作系统是实施安全加固的基础，是进行其他安全加固措施的先决条件；设置安全的登录过程、选择安全的登录方式以及系统使用中的密码保护用来对系统登录进行加固，减小系统被非法登录的可能性；启用加密文件系统和清除临时文件措施用于防止信息被窃取；系统审核策略则对系统的安全事件以及对象的访问进行记录，使用

户能够及时发现潜在的安全威胁。

目前主流的操作系统有 Windows 和 Linux 操作系统，它们都提供了很好的安全性能，并且还在不断地完善中。在表 1-1 中，对 Windows 和 Linux 两种操作系统从所提供的基本安全、网络安全与协议、应用安全、分发与操作、可信计算以及开放标准等特性进行了对比。

表 1-1 Windows 和 Linux 操作系统的安全特性对比

分类	特性	Linux	Windows
基本安全	验证、访问控制、加密、审核/日志	可插入的认证模块、插件模块、Kerberos、PKI、Winbind、ACL、LSM、SELinux、受控的访问保护实体检测、内核加密	Kerberos、PKI、访问控制列表、受控的访问保护实体检测、微软的应用程序加密程序接口
网络安全与协议	验证、各协议层	OpenSSL、OpenSSH、OpenLDAP、IPSec	SSL、SSH、LDAP、AD、IP-Sec
应用安全	防病毒、防火墙、入侵检测软件、Web 服务器、E-mail、智能卡支持	OpenAV、Clamav、Mcafee 等杀毒软件、内核内建的防火墙、Snort、A-pache、Sendmail、PKCS11、Exec-shield 系统	McAfee、Symantec、Check Point、IIS、Exchange/Out-look、PCKS11
分发与操作	安装、配置、加固、管理、漏洞扫描器	安装与配置工具、Bas-tille、Nessus、Up2Date 和 YaST 更新工具、Webmin 管理工具	Windows 自带的安装和配置工具、没有特定的加固工具、管理 GUI、使用默认安装的配置
可信计算	可信平台的模块、可信计算软件栈、工具、验证	依赖于硬件，可使用基于可信平台模块的开源驱动程序、可信计算组的软件栈	依赖于硬件，可使用安全启动特性
开放标准	IPSec、POSIX、传输层安全、常见标准	Linux 遵循所有的开放标准	Microsoft 也参与了开放标准，但仍有一些私有标准

1.3.3 操作系统功能与安全的关系

操作系统的安全性是其强大功能的有力保证，没有了操作系统的安全性，其功能就好比是没有地基的城堡。同时，再安全的操作系统如果不能达到用户对于功能的需求，这样的系统也不会得到应用。

一个操作系统的首要任务还是为用户提供方便、有效的服务，不能因为其安全性而影

响系统的功能。例如，端口 21 是 FTP 服务器所开放的端口，用于上传、下载。它也是木马 Doly Trojan、Fore、Invisible FTP、WebEx、WinCrash 和 Blade Runner 所开放的端口。关闭端口 21 可以使系统免受来自黑客的攻击，但用户同时也就无法得到此项功能所提供的服务。

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。如果说操作系统的某个功能模块上有个不太重要的缺陷，我们可以忽略它，这对整个操作系统的功能影响甚微，一般而言多个相关缺陷的组合才可能会对操作系统造成致命的影响。但在信息安全领域，情况就恰恰相反。这就好比“木桶理论”，木桶所能承载的水是以最短的木板为准的。也就是说，在信息系统中与安全相关的每一个系统漏洞都会使整个系统的安全控制机制变得毫无价值。这个“短板”如果被入侵者发现，后果将是十分严重的。

因此，对于操作系统来说安全是保持其正常功能的手段，采取安全措施的目的是提供切实可用的功能。研究安全可靠的操作系统，应均衡操作系统功能与安全的关系，不能因注重系统功能而忽视其安全性，也不能因注重系统安全而忽略其功能的重要性。

1.4 安全操作系统与可信计算基

1.4.1 安全操作系统

安全操作系统与操作系统的安全是两个不同的概念，安全操作系统通常与相应的安全等级相对应，例如，根据 TCSEC 标准，通常称 B1 级以上的操作系统为安全操作系统。操作系统的安全是指操作系统在基本功能基础上增加了安全机制与措施，以保障计算机资源使用的保密性、完整性和可用性。

操作系统安全的重要性我们已经谈及，摆在我们面前的问题是如何开发安全的操作系统或者对已实现基本功能的操作系统进行安全性增强。

开发安全的操作系统是一个复杂且艰巨的工程，首先必须要克服以下问题：

(1) 安全理论与模型问题

在整个安全操作系统开发中，建立适合的安全理论和模型是基础与依据。当前安全操作系统开发所依据的模型多数是传统的 BLP 模型，该模型偏重于信息的保密性，同时在具体实施中存在着若干的诸如隐藏通道等安全隐患，难以适应安全操作系统的发展要求，这就需要我们将安全模型的研究、相应的策略制定与加强评估准则与方法的研究进行有机结合，以保证其保密性和完整性。

(2) 安全体系结构的问题

高安全等级不是安全功能的简单叠加，必须要有严密科学的结构加以保证。加强安全操作系统体系结构的研究，能提供符合安全标准的安全核心体系结构，从形式化描述与验证上下工夫，为解决操作系统安全提供一个整体的理论指导和基础构件的支撑，并为工