普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

操作系统安全
（第2版）

卿斯汉 沈晴霓 刘文清 等编著
肖国镇 审

http://www.tup.com.cn

根据教育部高等学校信息安全类专业教学指导委员会制订的
《信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

操作系统安全
（第2版）

卿斯汉 沈晴霓 刘文清 刘海峰 温红子 编著
肖国镇 审

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全类专业教学指导委员会制订的
《信息安全专业指导性专业规范》组织编写

清华大学出版社
北京

内 容 简 介

本书是一部关于操作系统安全的教材，第2版在原书的基础上进行了修订与补充，增加了第11章“可信计算与可信操作系统”与第12章“新型操作系统发展与展望”。全书共分12章，全面介绍操作系统安全的基本理论、关键技术和发展趋势。主要内容包括操作系统安全的基本概念和理论（由基本概念、安全机制、安全模型、安全体系结构等章节构成），操作系统安全的关键技术与方法（如形式化规范与验证、隐蔽通道分析与处理、安全操作系统设计、操作系统安全评测和安全操作系统的网络扩展），可信计算与可信操作系统技术以及面向网络和云计算的新型操作系统发展趋势与安全性分析。

本书内容丰富，题材新颖，深入浅出，特点鲜明，理论结合实际，包括操作系统安全研究的最新成果，也包括作者在此研究领域长期潜心研究的科研成果。

本书可以作为计算机、软件工程、通信、信息安全等专业的高年级本科生、硕士生和博士生的教材，也可以作为广大从事相关专业的教学、科研和工程技术人员的参考书。

图书在版编目（CIP）数据

操作系统安全 / 卿斯汉等编著. —2版. —北京：清华大学出版社，2011.6
（高等院校信息安全专业系列教材）
ISBN 978-7-302-25911-4

Ⅰ. ①操… Ⅱ. ①卿… 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(2011)第115743号

责任编辑：张　民　徐跃进
责任校对：梁　毅
责任印制：何　芊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　　**印　张**：23　　**字　数**：543千字
版　　次：2011年6月第2版　　**印　次**：2011年6月第1次印刷
印　　数：1～4000
定　　价：33.00元

产品编号：041380-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中,以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍,同时也欢迎广大读者对本系列教材提出宝贵意见,以便我们对本系列教材的组织、编写与出版工作不断改进,为我国信息安全专业的教材建设与人才培养做出更大的贡献。

"高等院校信息安全专业系列教材"已于2006年年初正式列入普通高等教育"十一五"国家级教材规划(见教高[2006]9号文件《教育部关于印发普通高等教育"十一五"国家级教材规划选题的通知》)。我们会严把出版环节,保证规划教材的编校和印刷质量,按时完成出版任务。

2007年6月,教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办,清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。"高等院校信息安全专业系列教材"将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下,进一步体现科学性、系统性和新颖性,及时反映教学改革和课程建设的新成果,并随着我国信息安全学科的发展不断修订和完善。

我们的E-mail地址:zhangm@tup.tsinghua.edu.cn;联系人:张民。

清华大学出版社

前言

近几年来，因特网的应用迅速普及与发展，特别是我国电子政务与电子商务的应用日新月异。信息技术的发展加大了信息共享的程度，但信息共享与信息安全是一对矛盾；因而信息共享的发展呼唤信息安全。目前，我国正在大力发展信息技术与信息基础平台的建设。与此同步，我们必须大力加强信息安全基础设施建设，首先应当从加强我国自主版权的高等级安全操作系统的研制与开发抓起。

信息安全基础设施的关键是安全操作系统，建设以我国自主知识产权为基础的安全操作系统，形成一系列基于安全操作系统的信息安全产品，是加强我国信息安全基础设施的根本保证。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系统的安全问题。西方国家，无论在高安全等级操作系统的关键技术，还是产品出口方面，都对我们进行保密与限制。在一定程度上，一个国家安全操作系统的研制水平，代表一个国家信息安全领域的整体水平。

近年来，我国加强了安全操作系统的研究，包括操作系统安全基础理论的研究与高安全等级操作系统的研制。但遗憾的是，长期以来，我国关于操作系统安全的著作几乎为空白，不利于我国安全操作系统领域的整体发展。有鉴于此，基于我们在此领域的长期技术积累与工程实践，在中国科学院科学出版基金的支持下，于 2003 年初由科学出版社出版了《操作系统安全导论》——我国关于操作系统安全的第一部专著。该书不但全面介绍了操作系统的安全特性，总结了国际最新研究成果，也包括作者的最新成果。其中，既包含作者在安全操作系统理论研究方面的成果，也包含作者在工程实践方面的成果，即安胜安全操作系统的设计、体系结构与实现等方面的特点。

上述专著出版后，反响很好。不少专家与领导建议，尽快出版一部关于操作系统安全的教材，满足我国高等学校和研究机构培养高素质信息安全人才的迫切需求。在清华大学出版社与本丛书编委会的大力推动与支持下，本书第 1 版于 2004 年第一次与广大读者见面。本书发行以来受到社会广泛好评，许多高校都将本书选为本科生高年级或硕士研究生甚至博士研究生教材。在清华大学出版社的大力支持下，本书第 2 版已被列入十二五规划教材，修订出版。为了适应学生学习与教师教学的需求，本书进行了精心的选材和编排。本书强调少而精，亦即非基本的内容不选，对精选的内容尽量清楚、明确地阐述。其次，本书还有以下特色：书中包括作者多年来的科研成

果,包含了国内外文献中很少涉及的技术细节,有助于读者加深对操作系统安全内涵的理解。此外,本书每一章后面都附有习题,便于读者对本章内容进行进一步的思考。最后,本书对操作系统安全领域关键理论与技术的热点问题,以及面向网络和云计算的新型操作系统发展方向进行了探讨。

本书共分12章:第1章是引言(卿斯汉、刘文清),介绍对操作系统构成的威胁、安全操作系统研究的发展历程、有关术语以及本书的组织与编排;第2章是基本概念(卿斯汉、刘文清),介绍操作系统安全的基本概念及预备知识;第3章是安全机制(刘文清、沈晴霓),内容包括硬件安全机制、标识与鉴别、自主存取控制与强制存取控制、最小特权管理、可信通路、安全审计等内容,并具体介绍UNIX/Linux操作系统的安全机制;第4章是安全模型(卿斯汉、刘海峰、沈晴霓),介绍安全模型在安全操作系统中的重要地位、安全模型的分类以及若干典型的安全模型(Bell-LaPalula、Biba、Clark-Wilson、Chinese Wall、RBAC、DTE、信息流和无干扰模型);第5章是安全体系结构(季庆光、沈晴霓),通过详细讲解两个典型实例(权能体系和Flask体系)以及体现Flask体系的Linux Security Module(LSM)安全框架,说明安全体系结构的含义、类型、设计原则和实现方法;第6章是形式化规范与验证(温红子),内容包括形式化安全验证的原理、系统结构和典型实例——ASOS;第7章隐蔽通道分析与处理(朱继锋),阐述了隐蔽通道的概念、分类、标识技术、带宽计算技术、处理技术等内容;第8章是安全操作系统设计(刘文清、沈晴霓),阐述了安全操作系统设计的原则、方法、过程及应注意的问题,并给出了几个典型的设计实例;第9章是操作系统安全评测(刘海峰、刘文清),介绍评测方法以及国内外相关评测标准;第10章是安全操作系统的网络扩展(温红子、赵志科),介绍安全操作系统的概念、策略、机制等在网络上的扩展和应用;第11章是可信计算与可信操作系统(卿斯汉、沈晴霓),介绍可信计算的概念和技术,以及基于TPM/TCM可信操作系统的核心技术;第12章是新型操作系统发展与展望(卿斯汉、沈晴霓),介绍随着安全问题的日益突出和云计算新技术的出现,当前业界十分关注的新型网络化和云操作系统的发展及其安全技术方面的展望。全书由卿斯汉、沈晴霓统稿。

在本书的修订过程中,得到了中国科学院信息安全技术工程研究中心广大科研人员的鼓励、支持和帮助,并受益于作者在北京大学软件与微电子学院信息安全系的多年教学和科研工作。本书涉及的许多科研成果,是他们共同努力下完成的,在此,我们特别感谢中国科学院软件研究所倪惜珍研究员、贺也平副研究员、朱继锋博士、季庆光博士、李丽萍博士、唐柳英博士、赵志科硕士等以及北京大学软件与微电子学院信息安全系参与本书相关文献检索和整理的研究生们。

本书在写作与出版以及作者对操作系统安全的研究中,得到了中国科学院,北京大学,公安部,国家保密局,中国科学院软件研究所,国家自然科学基金委员会,中国电子学会,中国计算机学会,清华大学出版社,以及张效祥、何德全、沈昌祥、汪成为、蔡吉人、周仲义、魏正耀、胡启恒、李未、倪光南等院士以及中国科学院高技术研究与发展局局长桂文庄研究员等单位和专家的支持与鼓励,在此一并致谢。

本书的出版得到国家自然科学基金(60083007,60573042,60873238,60970135)和国家重点基础研究发展规划项目(G1999035810)的支持,在此表示感谢。作者还特别感谢

本丛书的编委会主任肖国镇教授，对他的一贯支持与指导表示谢意。作者同时感谢本书的审稿专家胡道元教授，他对本书的架构与组织提出了宝贵建议。最后，作者感谢清华大学出版社的广大员工，他们为本书的顺利出版付出了大量心血。

本书作为研究生教材，主要的读者对象是高年级本科生、硕士和博士研究生，也可供计算机、信息和通信等相关专业的教学、科研和工程技术人员参考。受作者水平与时间仓促的限制，如书中出现错误与不足，敬请广大读者不吝赐教。

作　者

2011 年 03 月

目录

第1章 引 言

1.1 操作系统面临安全威胁

作为信息社会的一块最主要的基石,与信息处理相关的计算机技术得到了飞速的发展。社会对信息资源进行共享和有效处理的迫切需求是推动计算机技术近乎以"疯狂"速度发展的原动力,也造就了20世纪后20年的IT业繁荣时代。但是进入21世纪后,IT业的发展遇到了一个比较严酷的调整期,人们都在思考一个问题——"IT业怎么了?",其实除了过度投资等原因之外,另一个根本的原因还在于,以计算机技术为核心的IT业还没有完全具备解决信息处理中安全问题的能力,特别是不具备能够有效满足在因特网这样恢弘背景下的经济、政治、金融、军事等社会基础机构对信息安全保障近似苛刻要求的能力。可以讲信息安全技术的发展将会从根本上影响和制约信息技术的进一步发展。

人们认识信息安全问题通常是从对系统所遭到的各种成功或者未成功的入侵攻击的威胁开始的,这些威胁大多是通过挖掘操作系统和应用程序的弱点或者缺陷来实现的,有记录的第一次这样的大规模攻击当属1988年的蠕虫事件。同时AT&T实验室的S. Bellovin博士曾对美国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还是源于操作系统的安全脆弱性。所以下边首先来介绍对操作系统安全威胁的主要类型。

1.1.1 病毒和蠕虫

1. 病毒

病毒是能自我复制的一组计算机指令或者程序代码。通过编制或者在计算机程序中插入这段代码,以达到破坏计算机功能、毁坏数据从而影响计算机使用的目的。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,通常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。