高等院校信息安全专业系列教材
中国计算机学会教育专业委员会与清华大学出版社联合组织编写

名誉主编：何德全　编委会主任：肖国镇

操作系统安全

卿斯汉　刘文清　温红子　刘海峰　编著

国家自然科学基金资助项目（项目编号：
国家重点基础研究发展规划（973）资助项目（项目编号：

清 华 大 学 出 版 社
北　京

内 容 简 介

本书共分 5章，全面介绍操作系统安全的基本理论与关键技术。主要包括：操作系统安全的基本概念和理论，介绍基本概念、安全机制、安全模型、安全体系结构等内容；操作系统安全的关键技术与方法，如形式化规范与验证、隐蔽通道的分析与处理、安全操作系统设计等；操作系统安全评测；安全操作系统的网络扩展。

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，也包括作者在此领域长期潜心研究的科研成果。

本书可以作为计算机、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，也可以作为广大教学、科研和工程技术人员的参考书。

图书在版编目（悦陨孕）数据

操作系统安全 辕卿斯汉等编著援—北京：清华大学出版社，圆园园源援愿

（高等院校信息安全专业系列教材）

陨杂月 苑鄄猿园圆鄄园愿怨源怨鄄圆

Ⅰ援操… 摇Ⅱ援卿… 摇Ⅲ援操作系统 原安全技术 原高等学校 原教材摇Ⅳ援栽孕猿员远

中国版本图书馆 悦陨孕数据核字（圆园园源）第 园苑园怨远园号

出 版 者：清华大学出版社摇摇摇摇摇摇摇摇摇摇摇摇摇地　　址：北京清华大学学研大厦

澡贼贼责:辕辕憎憎憎援贼怎责援糟燥皂援糟灶　　　　邮　　编：员园园园愿源

社 总 机：园员园鄄远圆苑苑园员苑缘　　　　客户服务：园员园鄄远圆苑苑远愿远怨

策划编辑：张摇民

文稿编辑：徐跃进

印 刷 者：北京牛山世兴印刷厂

装 订 者：北京市密云县京文制本装订厂

发 行 者：新华书店总店北京发行所

开　　本：员愿缘伊圆远园摇印张：圆源援缘摇字数：缘远园千字

版　　次：圆园园源年 愿月第 员版摇圆园园源年 愿月第员次印刷

书　　号：陨杂月 苑鄄猿园圆鄄园愿怨源怨鄄圆辕栽孕·远圆缘园

印　　数：员~猿园园园

定　　价：圆怨援园园元

高等院校信息安全专业系列教材

编审委员会

丛书序

摇摇在社会信息化的进程中，信息已成为社会发展的重要资源，信息安全也成为 圆员世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益，各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性和全球性的研究课题。

我国的信息安全事业正在蓬勃发展，国家领导高度重视，各部门通力合作、统筹规划，大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展，社会对信息安全人才的需求在不断增加，在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前，许多大学和科研院所已开创性地进行了信息安全领域的研究或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度，认真组织全国各高校和科研院所的专家、学者，共同研讨信息安全专业的教育方法和课程体系，并在进行大量前瞻性研究工作的基础上，启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材，相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去，也希望这套教材能够取得成功并不断完善，以促进各高等院校培养出更多、更好的信息安全专门人才，为我国的信息安全事业作出更大的贡献。

何德全

中国工程院院士

高等院校信息安全专业系列教材编审委员会名誉主编

圆园园缘年 苑月于北京

出版说明

摇摇圆员世纪是信息时代，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，国家对信息安全人才的需求量不断增加，但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，以满足社会的需求。为此，教育部继 圆园园员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、通信工程、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何德全院士担任名誉主编，著名学者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，确定了编写教材的作者，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，还经专家推荐和审定，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作出更大的贡献。

我们的 [illegible] 地址是 [illegible]，联系人张民。

中国计算机学会教育专业委员会

清华大学出版社

[illegible] 年 [illegible] 月

前 言

摇摇近几年来，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。信息技术的发展提高了信息共享的程度，但信息共享与信息安全是一对矛盾，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的建设，这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，还是在产品出口方面，都对我们实行保密与限制。因此，可以说，在一定程度上，一个国家的安全操作系统研制水平，代表一个国家在信息安全领域的整体水平。

最近，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 [illegible] 年初由科学出版社出版了我们的专著——《操作系统安全导论》。这是我国关于操作系统安全的第一部专著，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，也包括作者的最新科研成果。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，即安全操作系统的设计、实现与体系结构等方面的具体成果。

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

书作为这方面的教材，即将与广大读者见面。该书与专著《操作系统安全导论》有了很大的不同。专著强调理论的先进性与最新科研成果；本书强调技术的成熟性与基本理论和技术。二者互为补充。为了适应学生学习与教师教学的需求，本书首先进行了精心的选材和编排，不强调多而全，而强调少而精，即非基本的内容不选，对精选的内容尽量给予清楚、明确的阐述。其次，本书还有以下特色：书中包括作者自身的科研成果，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及发展方向进行了充分的探讨。

本书共分 [illegible] 章。第 [illegible] 章是引言（卿斯汉、刘文清编写），介绍操作系统面临的安全威胁、安全操作系统研究的发展历程、有关的定义和术语以及本书的组织与编排。第 [illegible] 章是基本概念（卿斯汉、刘文清编写），介绍操作系统安全的基本概念及预备知识。第 [illegible] 章是安全机制（刘文清编写），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，并具体介绍了 [illegible] 操作系统的安全机制。第 [illegible] 章是安全模型（卿斯汉、刘海峰编写），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，如 [illegible] 信息流和无干扰模型。第 [illegible] 章是安全体系结构（季庆光编写），通过详细讲解 [illegible] 体系和权能体系两个典型实例，说明安全体系结构的含义、类型及设计原则。第 [illegible] 章是形式化规范与验证（温红子编写），内容包括形式化安全验证的原理、系统结构和典型实例——[illegible]。第 [illegible] 章是隐蔽通道的分析与处理（朱继锋编写），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 [illegible] 章是安全操作系统设计（刘文清编写），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 [illegible] 章是操作系统安全评测（刘海峰、刘文清编写），介绍了评测方法以及国内外相关评测标准。第 [illegible] 章是安全操作系统的网络扩展（温红子、赵志科编写），介绍了安全操作系统的概念、策略、机制等在网络上的扩展和应用。本书成文后，温红子、刘文清做了进一步处理与修改。全书由卿斯汉统一策划与设计，并做了最后的校对、完善与统稿。

在本书的写作过程中，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。本书涉及的许多科研成果，是由他们共同努力完成的。在此，我们特别感谢：倪惜珍研究员、贺也平副研究员、朱继锋博士生、季庆光博士生、李丽萍博士生、唐柳英博士生、沈晴霓博士生、何建波博士生、赵志科硕士。

在本书写作与出版方面，以及在作者对操作系统安全的研究中，得到了主管单位与许多部门，以及著名专家的支持和鼓励。其中包括中国科学院、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、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、桂文庄。

本书的出版得到国家自然科学基金（[illegible]）和国家重点基础研究发展规划（[illegible]）项目（[illegible]）的支持，在此表示感谢。作者还要特别提到本丛书的编委会主任肖国镇教授，对他的一贯支持与指导，以及为本书作序表示谢意。作者同时感谢本书的责任编委胡道元教授，他对本书的架构与组织提出了宝贵建议。最后，作者衷心感谢清华大学出版社的支持和努力。

本书主要的读者对象是信息安全、计算机等专业的高年级本科生、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。

作者谨识于

中国科学院信息安全技术工程研究中心

[illegible]年 [illegible]月

目 录

第 员章 引　　言

摇 员援员 摇操作系统面临的安全威胁摇

摇摇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以近乎“疯狂”速度发展的原动力，也造就了 圆园世纪后 圆园年的 陨灶贼藻则灶藻贼业繁荣。但是进入 圆员世纪后，陨灶贼藻则灶藻贼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——“陨灶贼藻则灶藻贼业怎么了？”。其实以计算机技术为核心的 陨灶贼藻则灶藻贼业的发展所遇到的问题，除了过度投资等原因之外，另一个根本的原因就在于，还没有完全具备解决信息处理中的安全问题的能力，特别是不具备能够有效满足在因特网这样辉煌背景下的经济、政治、金融、军事等领域对信息安全保障近似苛刻的要求的能力。可以说，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于 员怨愿愿年的蠕虫事件。[illegible] 博士曾对美国计算机网络紧急响应队 (悦藻灶贼藻则 [illegible]) 提供的安全报告进行过分析，结果表明很多安全问题都是源于操作系统的安全脆弱性。所以，必须研究操作系统的安全性问题。下面首先介绍针对操作系统安全的主要威胁。

1.1.1 摇病毒和蠕虫

病毒是能够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：

- 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们的存在。
- 传染性。当用户利用磁盘、光盘、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。即使在同一台计算机上，病毒程序也能在磁盘的不同区域间传播，附着到多个文件上。

- 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）满足时才触发执行病毒程序的恶意代码部分，从而产生破坏作用。
- 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。如果是引导型病毒，可能会使计算机无法启动。另外有些病毒并不直接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，从而造成网络堵塞。

蠕虫类似于病毒，它可以侵入合法的数据处理程序，更改或破坏这些数据。尽管蠕虫不像病毒一样复制自身，但蠕虫攻击带来的破坏可能与病毒一样严重，尤其是在没有及时发觉的情况下。不过一旦蠕虫入侵被发现，系统恢复会容易一些，因为它没有病毒的复制能力，只有一个需要被清除的蠕虫程序。最具代表性的[illegible]蠕虫是一个[illegible]电子邮件和新闻组蠕虫，它被伪装为“[illegible]”的电子邮件附件，首次运行时会显示焰火，运行之后，每个从本机发送的电子邮件和新闻组布告都会导致再次发送消息。由于人们收到的“[illegible]”来自于他们所认识的人，通常会信任这个附件并且运行它。

1.1.2 逻辑炸弹

逻辑炸弹是加在现有应用程序上的程序。一般逻辑炸弹都被添加在被感染应用程序的起始处，每当该应用程序运行时就会运行逻辑炸弹。它通常要检查各种条件，看是否满足运行炸弹的条件。如果逻辑炸弹没有取得控制权就将控制权归还给主应用程序，逻辑炸弹仍然安静地等待。当设定的爆炸条件被满足后，逻辑炸弹的其余代码就会执行。此时它通常造成程序中断、发生刺耳噪音、更改视频显示、破坏磁盘上的数据、利用硬件缺点引发硬件失效、磁盘异常、操作系统运行速度减慢或系统崩溃等危害。它也可以通过写入非法值控制视频卡的端口使监视功能失败、使键盘失效、破坏磁盘以及释放出更多的逻辑炸弹以及病毒（间接攻击）。逻辑炸弹不能复制自身，不能感染其他程序，但这些攻击已经使它成为了一种极具破坏性的恶意代码类型。

逻辑炸弹具有多种触发方式，例如计数器触发方式、时间触发方式、复制触发方式（当病毒副本数量达到某个设定值时激活）、磁盘空间触发方式、视频模式触发方式（当视频处于某个设定模式或设定模式改变时激活）、基本输入输出系统（[illegible]）触发方式、只读内存（[illegible]）触发方式、键盘触发方式以及反病毒触发方式等。