

“信息化与信息社会”系列丛书之  
高等学校信息安全专业系列教材

# 信息系统安全概论

(第2版)

石文昌 编著



电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>

“信息化与信息社会”系列丛书之  
高等学校信息安全专业系列教材

# 信息系统安全概论

(第2版)

石文昌 编著

電子工業出版社

Publishing House of Electronics Industry  
北京·BEIJING

## 内 容 简 介

本书以独特的方式介绍以主机为切入点的系统安全的基本思想、技术和方法。本书的宗旨是帮助读者认识每个人手上、家里、工作单位中，甚至庞大的数据处理中心深处的计算机系统的安全问题及其解决途径。

本书由10章构成，内容包括信息系统安全绪论、信息安全经典模型、系统安全硬件基础、用户身份认证机制、操作系统基础安全机制、操作系统强制安全机制、数据库基础安全机制、数据库强制安全机制、系统可信检查机制和云计算环境安全机制等。

本书的风格是透过实际案例的剖析，洞察内部技术机理。注重基本概念和基本思想，通过对安全机制的考察把握系统安全的关键技术和方法。考察身份认证机制、基础安全机制、强制安全机制和可信性检查机制等安全机制，涉及操作系统和数据库系统等关键基础软件。从单台主机开始，延伸至云计算环境，纵览系统安全的知识体系。

本书的编著过程参照了教育部信息安全专业教学指导委员会制定的信息安全专业指导性专业规范的相关要求，可作为高等学校信息安全、计算机、电子与通信及相关专业的本科生和研究生教材或参考书，也可供从事相关专业教学、科研和工程技术的人员参考。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有，侵权必究。

### 图书在版编目（CIP）数据

信息系统安全概论 / 石文昌编著. —2 版. —北京：电子工业出版社，2014.1

（“信息化与信息社会”系列丛书）

高等学校信息安全专业系列教材

ISBN 978-7-121-22143-9

I. ①信… II. ①石… III. ①信息系统—安全技术—高等学校—教材 IV. ①TP309

中国版本图书馆 CIP 数据核字（2013）第 299574 号

策划编辑：刘宪兰

责任编辑：张 京

印 刷：北京京师印务有限公司

装 订：北京京师印务有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本：787×1092 1/16 印张：21.25 字数：476 千字

印 次：2014 年 1 月第 1 次印刷

印 数：3000 册 定价：43.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

## 第2版“信息化与信息社会”系列丛书编委会名单

编委会主任 曲维枝

编委会副主任 周宏仁 张尧学 徐 愈

编委会委员 何德全 邬贺铨 高新民 高世辑 张复良 刘希俭  
刘小英 李国杰 秦 海 赵泽良 杜 链 朱森第  
方欣欣 陈国青 李一军 李 琪 冯登国

编委会秘书处 廖 瑾 刘宪兰 刘博等

## 第2版高等学校信息安全专业系列教材编委会名单

专业编委会顾问 (以汉字拼音为序)

蔡吉人 方滨兴 何德全 刘小英 宁家骏 曲成义  
沈昌祥 邬贺铨 熊澄宇 赵泽良

专业编委会主任 冯登国

专业编委会委员 (以汉字拼音为序)

陈克非 封化民 韩 臻 胡爱群 黄继武 黄刘生  
李 超 李建华 刘建伟 陆哲明 马建峰 秦玉海  
秦志光 石文昌 王怀民 王清贤 王小云 向 宏  
谢冬青 杨义先 俞能海 曾庆凯 张宏莉 张焕国  
郑 东



## 作者简介

### 石文昌

博士，教授，博士生导师，电子证据司法鉴定人，教育部信息安全专业教学指导委员会委员；北京大学计算机科学与技术理学学士，中国科学院计算机软件工学硕士和计算机软件与理论工学博士；中国科学院院长奖获得者。主要研究方向为系统安全、可信计算、操作系统与计算机取证。现任中国人民大学信息学院教授、计算机系主任；中国人民大学信息安全专业和学科的创建者与学术带头人；中国计算机学会信息保密、系统软件、开放系统等专业委员会委员；曾任中国科学院软件所研究员、中国科学院研究生院教授。长期从事相关方向的研究、开发与人才培养工作。拥有多年的系统开发实践经验，攻读硕士学位期间，成功实现了 **UNIX** 操作系统的移植；攻读博士学位期间，成功完成了基于 **Linux** 的安全操作系统的研制。负责和承担了包括国家 863 高技术研究发展计划项目和国家自然科学基金项目在内的一系列重要科研项目，在安全操作系统和可信操作系统等方面取得了多项重要的理论研究成果和技术开发成果。



## 第 2 版总序

信息化是世界经济和社会发展的必然趋势。近年来，在党中央、国务院的高度重视和正确领导下，我国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。

作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会按照党中央、国务院领导同志的要求，就我国信息化发展中的前瞻性、全局性和战略性的问题进行调查研究，提出政策建议和咨询意见。信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力。大量培养符合中国信息化发展需要的人才，是国家信息化发展的一个紧迫需求，也是我国推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。2006年5月，我国公布《2006—2010年国家信息化发展战略》，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。

为了促进上述目标的实现，国家信息化专家咨询委员会致力于通过讲座、论坛、出版等各种方式推动信息化知识的宣传、教育和培训。2007年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了“信息化与信息社会”系列丛书编委会，共同推动“信息化与信息社会”系列丛书的组织编写工作。编写该系列丛书的目的是，力图结合我国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效梳理信息化的基本概念和知识体系，通过高校教师、信息化专家、学者与政府官员之间的相互交流和借鉴，充实我国信息化实践中的成功案例，进一步完善我国信息化教学的框架体系，提高我国信息化图书的理论和实践水平。毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一个重要举措，对于推动国家的信息化人才教育和培养工作，加强我国信息化人才队伍的建设具有重要意义。

考虑到当时国家信息化人才培养的需求，各个专业和不同教育层次（博士生、硕士生、本科生）的需要，以及教材开发的难度和编写进度时间等问题，“信息化与信息社会”系列丛书编委会采取了集中全国优秀学者和教师，分期分批出版高质量的信息化教育丛书的方式，结合高校专业课程设置情况，在“十一五”期间，先后组织出版了“信息管理与信息系统”、“电子商务”、“信息安全”三套本科专业高等学校系列教材，受到高校相关专业学科以及相关专业师生的热烈欢迎，并得到业内专家和教师的一致好评和高度评价。

但是，随着时间的推移和信息技术的快速发展，上述专业的教育面临着持续更新、不断完善的迫切要求，日新月异的技术发展及应用变迁也不断对新时期的建设和人才培养提出新要求。为此，“信息管理与信息系统”、“电子商务”、“信息安全”三个专业教育需以综合的视角和发展的眼光不断对自身进行调整和丰富，已出版的教材内容也需及时进行更新和调整，以满足需求。

这次，高等学校“信息管理与信息系统”、“电子商务”、“信息安全”三套系列教材的修订是在涵盖第1版主题内容的基础上进行的更新和调整。我们希望在内容构成上，既保持原第1版教材基础的经典内容，又要介绍主流的知识、方法和工具，以及最新的发展趋势，同时增加部分案例或实例，使每一本教材都有明确的定位，分别体现“信息管理与信息系统”、“电子商务”、“信息安全”三个专业领域的特征，并在结合我国信息化发展实际特点的同时，选择性地吸收国际上相关教材的成熟内容。

对于这次三套系列教材（以下简称系列教材）的修订，我们仍提出了基本要求，包括信息化的基本概念一定要准确、清晰，既要符合中国国情，又要与国际接轨；教材内容既要符合本科生课程设置的要求，又要紧跟技术发展的前沿，及时地把新技术、新趋势、新成果反映在教材中；教材还必须体现理论与实践的结合，要注意选取具有中国特色的成功案例和信息技术产品的应用实例，突出案例教学，力求生动活泼，达到帮助学生学以致用的目的，等等。

为力争修订教材达到我们一贯秉承的精品要求，“信息化与信息社会”系列丛书编委会采用了多种手段和措施保证系列教材的质量。首先，在确定每本教材的第一作者的过程中引入了竞争机制，通过广泛征集、自我推荐和网上公示等形式，吸收优秀教师、企业人才和知名专家参与写作；其次，将国家信息化专家咨询委员会有关专家纳入到各个专业编委会中，通过召开研讨会和广泛征求意见等多种方式，吸纳国家信息化一线专家、工作者的意见和建议；再次，要求各专业编委会对教材大纲、内容等进行严格的审核，并对每本教材配有一至两位审稿专家。

我们衷心期望，系列教材的修订能对我国信息化相应专业领域的教育发展和教学水平的提高有所裨益，对推动我国信息化的人才培养有所贡献。同时，我们也借系列教材修订出版的机会，向所有为系列教材的组织、构思、写作、审核、编辑、出版等做出贡献的专家学者、教师和工作人员表达我们最真诚的谢意！

应该看到，组织高校教师、专家学者、政府官员以及出版部门共同合作，编写尚处于发展动态之中的新兴学科的高等学校教材，有待继续尝试和不断总结经验，也难免会出现这样那样的缺点和问题。我们衷心希望使用该系列教材的教师和学生能够不吝赐教，帮助我们不断地提高系列教材的质量。

**曲作波**

2013年11月1日

## 第 1 版总序

信息化是世界经济和社会发展的必然趋势。近年来，在党中央、国务院的高度重视和正确领导下，我国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。

作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会一直在按照党中央、国务院领导同志的要求就信息化前瞻性、全局性和战略性的问题进行调查研究，提出政策建议和咨询意见。在做这些工作的过程中，我们愈发认识到，信息技术和信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力，大量培养符合中国信息化发展需要的人才已成为国家信息化发展的一个紧迫需求，成为我国应对当前严峻经济形势，推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。2006年5月，我国《2006—2010年国家信息化发展战略》公布，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。

为了促进上述目标的实现，国家信息化专家咨询委员会一直致力于通过讲座、论坛、出版物等各种方式推动信息化知识的宣传、教育和培训工作。2007年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了“信息化与信息社会”系列丛书编委会，共同推动“信息化与信息社会”系列丛书的组织编写工作。编写该系列丛书的目的是，力图结合我国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效梳理信息化的基本概念和知识体系，通过高校教师、信息化专家、学者与政府官员之间的相互交流和借鉴，充实我国信息化实践中的成功案例，进一步完善我国信息化教学的框架体系，提高我国信息化图书的理论和实践水平。毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一个重要举措，对于推动国家的信息化人才教育和培养工作，加强我国信息化人才队伍的建设具有重要意义。

考虑当前国家信息化人才培养的需求、各个专业和不同教育层次（博士生、研究生、本科生）的需要，以及教材开发的难度和编写进度时间等问题，“信息化与信息社会”系列丛书编委会采取了集中全国优秀学者和教师、分期分批出版高质量的信息化教育丛书的方式，根据当前高校专业课程设置情况，先开发“信息管理与信息系统”、“电子商务”、“信息安全”三个本科专业高等学校系列教材，然后再根据我国信息化和高等学校相关专业发



展的情况陆续开发其他专业和类别的图书。

对于新编的三套系列教材（以下简称系列教材），我们寄予了很大希望，也提出了基本要求，包括信息化的基本概念一定要准确、清晰，既要符合中国国情，又要与国际接轨；教材内容既要符合本科生课程设置的要求，又要紧跟技术发展的前沿，及时地把新技术、新趋势、新成果反映在教材中；教材还必须体现理论与实践的结合，要注意选取具有中国特色的成功案例和信息技术产品的应用实例，突出案例教学，力求生动活泼，达到帮助学生学以致用为目的，等等。

为力争出版一批精品教材，“信息化与信息社会”系列丛书编委会采用了多种手段和措施保证系列教材的质量。首先，在确定每本教材的第一作者的过程中引入了竞争机制，通过广泛征集、自我推荐和网上公示等形式，吸收优秀教师、企业人才和知名专家参与写作；其次，将国家信息化专家咨询委员会有关专家纳入到各个专业编委会中，通过召开研讨会和广泛征求意见等多种方式，吸纳国家信息化一线专家、工作者的意见和建议；再次，要求各专业编委会对教材大纲、内容等进行严格的审核，并对每一本教材配有一至两位审稿专家。

如今，我们很高兴地看到，在教育部和原国务院信息化工作办公室的支持下，通过许多高校教师、专家学者及电子工业出版社的辛勤努力和付出，“信息化与信息社会”系列丛书中的三套系列教材即将陆续和读者见面。

我们衷心期望，系列教材的出版和使用能对我国信息化相应专业领域的教育发展和教学水平的提高有所裨益，对推动我国信息化的人才培养有所贡献。同时，我们也借系列教材开始陆续出版的机会，向所有为系列教材的组织、构思、写作、审核、编辑、出版等做出贡献的专家学者、老师和工作人员表达我们最真诚的谢意！

应该看到，组织高校教师、专家学者、政府官员以及出版部门共同合作，编写尚处于发展动态之中的新兴学科的高等学校教材，还是一个初步的尝试。其中，固然有许多的经验可以总结，也难免会出现这样那样的缺点和问题。我们衷心地希望使用系列教材的教师和学生能够不吝赐教，帮助我们不断地提高系列教材的质量。

**曲作技**

2008年12月15日



## 第 2 版序言

“十一五”期间，由国家信息化专家咨询委员会牵头，教育部信息安全专业类教学指导委员会有关领导、学者组织，众多信息安全专业著名专家和教师参与开发，并由电子工业出版社出版的“高等学校信息安全专业系列教材”，由于在体系设计上较全面地覆盖了新时期信息安全专业教育的各个知识层面，包括宏观视角上对信息化大环境下信息安全相关知识的综合介绍，对信息安全应用发展前沿的深入剖析，以及对信息安全系统建设各项核心任务的系统讲解和对一些重要信息安全应用形式的讨论，在“高等学校信息安全专业系列教材”面市后，受到高校该专业学科及相关专业师生的热烈欢迎，得到业内专家和教师的好评和高度评价，被誉为该学科专业教材中的精品系列教材。


但是，随着信息技术的快速发展，信息安全专业教育面临着持续更新、不断完善的迫切要求，其日新月异的技术发展及应用变迁也不断对新时期信息安全建设和人才培养提出新的要求。为此，信息安全专业教育需以综合的视角和发展的眼光不断对教学内容进行调整和丰富，已出版的教材内容也需及时进行更新和修改，以满足需求。

这次修订，除对“高等学校信息安全专业系列教材”第 1 版各册教材的主题内容进行了相应更新和调整外，同时对系列教材的总体架构进行了调整并增加了 3 个分册，即《信息安全数学基础》、《信息安全实验教程》和《信息隐藏概论》。

调整后的教材在体系架构和内容构成上既保持了经典的经典内容，又介绍了主流的知识、方法和工具，以及最新发展趋势，同时增加了部分案例或实例。使得系列中的每一本教材都有明确的定位，充分体现了国家“信息安全”的领域特征，在结合我国信息安全实际特点的同时，还注重借鉴国际上相关教材中适于作为信息安全本科教育知识的成熟内容。

我们希望这套修订教材能够成为新形势下高等学校信息安全专业的精品教材，成为高等学校信息安全专业学生循序渐进了解和掌握专业知识不可或缺的教科书和知识读本，成为国家信息安全新环境下从业人员及管理者学习信息安全知识的有益参考书。

高等学校信息安全专业系列教材编委会  
2013 年 10 月于北京



## 第 1 版序言

人类走过了农业社会、工业社会，如今正处于信息社会的伟大时代，“信息社会”这个词语无疑已经家喻户晓，信息化大潮正席卷着世界的每一个角落。地球两端，万里之隔，人们能通过互联网与亲朋畅快交流，音容笑貌犹如就在眼前，真正是天涯变咫尺；分支机构遍布全球的庞大企业运转有条不紊，各机构协作顺畅，其功能强大的信息系统功勋卓著；分析复杂神秘的生物基因，预测瞬息万变的天气趋势，有了容量惊人的数据库系统和“聪明绝顶”的高性能计算系统，科学家们如虎添翼。总之，人类处处受益于信息化成果并正在信息化这条大道上加速前进，决不会放慢脚步。

然而，阳光之下总会有阴影，人类越依赖于信息系统，信息安全问题就越发凸显。关于信息安全的形形色色的新闻日益频繁地见诸于媒体：某银行数据库数据被窃取导致客户信息泄露，使客户惶惶不安，银行面临信任危机；某计算机病毒大肆泛滥，无数用户系统瘫痪，让相关企业损失惨重；某国军方网络被黑客侵入，军事机密竟被人如探囊取物般轻易窃取……这样的事件一再提示我们，信息安全问题是社会信息化发展进程中无法回避的客观产物，只有主动积极地面对和解决这一问题才能保障信息化的顺利推进，确保经济、社会的稳定乃至国家的安全。

目前，世界各国政府在信息安全领域的重视程度正在不断加大，并纷纷推出了本国的相关标准、规范或法律，大力扶持高校和其他科研机构对信息安全问题的研究，同时采取各种措施促进信息安全领域的人才培养以满足本国信息化建设的需要，为本国的信息产业发展提供中坚力量。特别是一些信息化进程起步较早，水平较高的发达国家，其信息安全领域的研究水平和产业化程度已相当令人瞩目。

我国正处于信息化建设的关键阶段，2006年发布的《2006—2010年国家信息化发展战略》更是从战略的高度指出了推进信息化对我国经济建设和国家发展的重要作用，规划出了新时期我国信息化发展的宏伟蓝图。由此可见，我国的信息化建设和信息产业正面临前所未有的机遇和挑战。

正是在这样的时代背景下，信息安全问题越来越引起全社会上下的广泛关注。信息安全领域必须不断提高研究水平以满足经济建设和国家安全的需要，为我国信息化建设的大踏步前进保驾护航，为创建和谐社会，实现可持续发展贡献力量。因此，大量高素质的信息安全人才成为了最急需、最宝贵的资源。

康有为曾经说过：“欲任天下之事，开中国之新世界，莫亟于教育。”我们的国家要想不断发展科技，增强国力，开创出我们自己富强文明的“新世界”，必须加大力度进行信息

化建设。而要使我国的信息化水平走在世界前列，全面提高信息安全领域教育水平，特别是促进高等学校信息安全专业对相关人才的培养和教育，就成为了成败的关键。高等学校信息安全系列教材的编撰就是希望能够为我国的信息安全领域专业人才的培养、为我国信息化水平的腾飞助一臂之力。

信息安全专业教育有其自身的特点，要求学习该专业的学生能够将系统知识与专业知识有机结合，在注重提升理论高度的同时还要能够把理论知识与工程实践紧密联系起来。本系列教材针对高等学校信息安全专业教育的这些特点，同时根据其知识体系、教育层次和课程设置，规划了教材的内容，增加了实际案例，力争做到既紧跟前沿技术的发展，又不失扎实的基本理论和生动活泼的形式，使学生能够学以致用。本系列教材从不同角度论述和总结了信息安全领域的科学问题，有着较强的适用性，既可作为高等学校信息安全专业和相关专业本科生的教材，也可以作为非信息安全专业的公共教科书，同时还可以作为从事信息安全工作的科研技术人员和管理人员的培训教材或参考书，使其了解信息安全相关关键技术和发展态势。

信息安全科学在不断发展，我们也将会努力使本系列教材适应和紧跟这种发展的节奏，使我们培养的信息安全人才能够与时俱进，用自己的所学共筑我国信息安全的万里长城。

限于作者的水平，本系列教材难免存在不足之处，敬请读者批评指正。

高等学校信息安全专业系列教材编委会

2008年10月



## 第 2 版前言

本书第 1 版于 2009 年出版，作者一直在一线教学中以其为教材，四年多的教学实践感悟颇多，同时，从学生们、兄弟院校采用本书作教材的老师及其他读者那里得到了不少珍贵的反馈，另外，技术的发展也带来新的启示，综合多方因素，本书有了较大变化。

保持“透过案例看技术”的风格，本书的最大变化主要体现在易读性的提升和篇幅的精简方面。另外，篇章结构和内容设置也进行了一定的调整，这主要是出于课时安排的可行性和教学内容的专业性考虑的。更新后的内容构成如下。

- 第 1 章 信息系统安全绪论；
- 第 2 章 信息安全经典模型；
- 第 3 章 系统安全硬件基础；
- 第 4 章 用户身份认证机制；
- 第 5 章 操作系统基础安全机制；
- 第 6 章 操作系统强制安全机制；
- 第 7 章 数据库基础安全机制；
- 第 8 章 数据库强制安全机制；
- 第 9 章 系统可信检查机制；
- 第 10 章 云计算环境安全机制。

其中，第 1 章保留了第 1 版中的攻击案例，但大部分内容已经重写。第 2 章由第 1 版中分散在若干章中的安全模型凝练而成。第 3 章是重写的内容。第 4、5 章主要由第 1 版中的第 4 章分离而成。第 6~9 章分别对应第 1 版中的第 5~8 章，但进行了精简和更新。第 10 章是全新的内容。第 1 版中的第 2、9 和 10 章已被删掉。

系统安全的最直观情形是单台主机系统涉及的安全问题，它可以小至移动设备系统，大至云计算系统环境。本书以单台主机系统为切入点，兼顾网络环境，最后延伸到云计算平台。

本书以实际案例为导引，注重基本概念和基本思想，着力通过对安全机制的考察掌握系统安全的关键技术和方法。主要考察的安全机制包括身份认证机制、基础安全机制、强制安全机制和可信性检查机制，涉及的基础软件主要包括操作系统和数据库系统。

第 1~3 章是系统安全的基本概念和理念方面的内容，是理解安全机制的基础。第 4~10 章是系统安全中的代表性安全机制，其中，第 4 章的身份认证机制是其他安全机制发挥作用的基础，而第 10 章的云计算环境安全机制是多种技术的集成应用，尤其第 3 章和第 9

章，是它的直接基础。

本书的编著得到了国家自然科学基金项目（61070192）和北京市自然科学基金项目（4122041）的资助，得到了信息安全专业教材编委会主任冯登国研究员的直接指导，得到了电子工业出版社刘宪兰老师的倾力推动，经历了中国人民大学信息安全专业 2011 级本科生的试用，在此一并致谢。同时，感谢本书第 1 版所有读者的积极反馈。

本书免费提供配套电子课件，我们乐意为本书的教学或阅读提供释疑解惑支持，真诚期盼朋友们批评指正。欢迎通过以下电子邮箱与我们联系。

电子邮箱：[syssecbook@gmail.com](mailto:syssecbook@gmail.com)。

石文昌

2013 年 11 月

于北京中关村中国人民大学理工配楼

## 第 1 版前言

正如人是现实社会生活中的行为单元一样，主机是信息网络空间中的工作单元。为了维护现实社会生活的安定与和谐，公安机关采取了对犯罪分子进行严厉打击的措施，为了确保信息网络空间的安全与可信，有必要对主机系统的安全问题准确地把握。

信息安全事关国家安全，因为信息化已经渗透到人类社会的各个层面。主机系统的安全在信息安全中举足轻重，因为所有的软件最终都必须落实到具体的主机系统上运行。解剖信息网络空间中的安全问题，就能清楚地看到主机系统安全是其中不可或缺的成分，而解剖主机系统的安全问题，就会发现它自身的内容也是丰富多彩的。

本书重点讲授以主机为中心的系统安全的基本思想、技术和方法。值得一提的是：这里所说的主机并非等同于 20 世纪 60~70 年代盛行的大型主机，而是指包含 21 世纪的终端、个人计算机、工作站和服务器等各种计算机设备。正如人不是孤立的人而是社会中的人一样，这里所谈论的主机也绝不是孤立的主机，而是处在开放的网络互联环境中的主机。

本书的内容设计宗旨是帮助读者认识每个人手中、家里、工作单位中，甚至庞大的数据处理中心深处的计算机主机系统的安全问题及其解决途径。信息安全是一个复杂的系统工程，主机系统安全是其中的一个重要环节，而且这个环节与用户息息相关。学习主机系统安全对营造用户身边计算机的安全环境大有裨益。

在信息网络空间的信息安全体系这个层面上，主机系统安全是其中的一个关键点。本书系统地讲授这个点的关键思想，以期帮助读者把握这个点的基本内在机理，并了解这个点在整个面上的地位和作用。本书的编写理念是以点为目标，注意点面结合。学习主机系统安全对于建设整个信息网络空间的安全氛围也一定很有帮助。

本书的特色是透过信息网络空间的宏观安全体系结构去看待主机系统的安全问题；通过主机系统与信息安全知识体系的融合去认识主机系统的安全问题；采取核心硬件、系统软件和应用软件相结合的综合手段去分析主机系统的安全问题；运用安全性与可信性有机统一的整体措施去解决主机系统的安全问题。同时，本书注意体现网络环境对系统安全的影响及系统安全对整体安全的支撑。

本书是在总结编者多年从事系统软件与信息安全的科研实践和人才培养工作的基础上编写而成的。在编写过程中，考虑到了人才培养和人才需求方面的一些实际情况。

鉴此，在内容的选择和编排上，力求知识的系统性，但不求内容的全面性，尤其注重选材的典型性及其应用价值。例如，在安全模型方面，本书并没有列出太多的安全模型，只是有选择地扼要介绍了其中有限的几个，并且有意识地在介绍系统实现时尽量体现所介

绍的安全模型的应用方法，希望以此来帮助读者更好地理解相应的安全模型，并达到举一反三的效果。

本书的内容可以分为三个部分。第一部分为基础篇，介绍系统安全的必备基础知识，由第 1~3 章构成；第二部分为核心篇，介绍系统的核心内容，由第 4~8 章构成；第三部分为拓展篇，介绍向应用推进的系统安全内容，由第 9~10 章构成。

信息安全基本认识是系统安全课程的开端，是学习第 1 章要达到的主要目的。计算机系统基础是建立系统安全思想的根基，第 2 章通过回顾计算机硬件、操作系统和数据库系统等方面的基本内容来巩固。第 3 章介绍的可信计算平台通过安全芯片提供基本的安全功能，可以作为系统安全的硬件基础。

操作系统安全性和数据库系统安全性是系统的核心内容，值得分别从基础安全性和增强安全性两个层面去把握，第 4~7 章的篇幅专门为此目的进行设置。第 8 章介绍的系统完整性保护是系统安全核心内容的另一个重要方面，它不但可以体现在操作系统安全性和数据库系统安全性中，还可以体现在硬件的安全支持和应用系统的安全需求中。

操作系统和数据库系统在系统中处于核心地位，其核心意义主要体现在它们对于确保应用系统的安全性上具有不可或缺的重要作用。应用系统的安全性是用户希望实现的根本目标。基于主机的入侵检测和计算机病毒原理及其防治是系统安全由核心层向应用层延伸的重要内容，分别在第 9 章和第 10 章介绍。

如前所述，本书不求内容的全面性，但求知识的系统性。我们着力给读者讲授计算机主机系统安全的统一知识体系，引导读者领略系统安全知识框架的整体概貌，掌握系统安全的基础知识和关键技术，为读者学习信息安全知识、掌握信息安全技术、解决信息安全问题及进一步从网络安全等其他方面充实信息安全学识打下坚实的基础。

本书的编著工作得到了国家 863 高技术研究发展计划课题（2007AA01Z414）和国家自然科学基金项目（60373054，60703102，60703103）的资助，在此，我们向国家的相关机构表示衷心的感谢。

在本书的编著过程中，我们参考了大量的技术文献、著作和教材，这些文献、著作和教材的作者的智慧结晶和出版机构的贡献使我们受益匪浅，为本书的编写奠定了宝贵的基础，在此，我们向相关作者和出版机构致以崇高的敬意和诚挚的谢意。

由于我们的学识和水平有限，书中难免有错误和不妥之处，敬请读者批评指正。关于本书的任何问题，都欢迎通过下面的电子邮箱与我们联系。同时，希望本书能为信息安全教育做出新的贡献。

电子邮箱：[syssecbook@gmail.com](mailto:syssecbook@gmail.com)。

石文昌  
2008 年 11 月  
于中国人民大学



## 反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任 and 行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396；(010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市海淀区万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036