教育部高职高专电子信息类专业教学指导委员会规划教材
JIAOYUBU GAOZHIGAOZHUAN DIANZIXINXILEIZHUANYE JIAOXUEZHIDAOWEIYUANHUI GUIHUAJIAOCAI

“高职高专电子信息类专业（信息安全专业）课程建设”研究成果
"GAOZHIGAOZHUAN DIANZIXINXILEIZHUANYE (XINXIANQUANZHUANYE) KECHENGJIANSHE" YANJIUCHENGGUO

操作系统安全

Caozuo Xitong Anquan

张波云 鄢喜爱 范强 主编
史伟奇 副主编

人民邮电出版社
POSTS & TELECOM PRESS

教育部高职高专电子信息类专业教学指导委员会规划教材

操作系统安全

张波云　鄢喜爱　范　强　主编

史伟奇　副主编

人民邮电出版社

北京

图书在版编目（CIP）数据

操作系统安全 / 张波云，鄢喜爱，范强主编. -- 北京 : 人民邮电出版社，2012.8
教育部高职高专电子信息类专业教学指导委员会规划教材
ISBN 978-7-115-26612-5

Ⅰ. ①操… Ⅱ. ①张… ②鄢… ③范… Ⅲ. ①操作系统－安全技术－高等职业教育－教材 Ⅳ. ①TP316

中国版本图书馆CIP数据核字(2011)第273705号

内 容 提 要

操作系统的安全性在计算机信息系统的整体安全性中具有至关重要的作用，没有操作系统提供的安全性，计算机系统的安全性是没有基础的。本书全面介绍了操作系统安全的基本理论和关键技术，包括安全操作系统的研究发展历程、安全策略、安全模型和安全机制、安全体系结构、知名安全操作系统介绍、安全操作系统测评以及安全操作系统的应用等，同时注重理论联系实际，重点介绍了当前主流操作系统的安全设置和安全管理及安全增强技术。

本书可作为高职高专信息安全专业、计算机相关专业学生的教材，也可作为广大计算机用户、系统管理员、计算机安全技术人员的技术参考书。同时，也可作为计算机信息安全职业培训的教材。

教育部高职高专电子信息类专业教学指导委员会规划教材

操作系统安全

◆ 主　　编　张波云　鄢喜爱　范　强
副 主 编　史伟奇
责任编辑　丁金炎
执行编辑　洪　婕

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：18.25　　2012 年 8 月第 1 版
字数：440 千字　　2012 年 8 月北京第 1 次印刷

ISBN 978-7-115-26612-5

定价：35.00 元

读者服务热线：(010)67132746　印装质量热线：(010)67129223
反盗版热线：(010)67171154
广告经营许可证：京崇工商广字第 0021 号

资源建设委员会

教育部高等学校高职高专
电子信息类专业教学指导委员会规划教材

主　任：高　林

副主任：温希东　周　明　滕　伟　曾德华　鲍　洁

委　员：（按姓氏笔画排列）

方四平　王应海　王传臣　王晓丹　王海平

王萍辉　尹　洪　叶曲炜　包华林　成立平

孙利梅　孙昕伟　孙晓雷　杨秀英　李国祯

李泽国　李慧敏　严晓舟　来建良　吴升刚

吴明华　吴家礼　张明伯　张　勇　张基宏

陈西玉　陈丽能　陈健民　武马群　胡毓坚

俞　宁　贾文胜　唐瑞海　曹建林　曹　毅

盛鸿宇　梁永生　程庆梅　熊发涯　魏文芳

教育部高等学校高职高专
电子信息类专业教学指导委员会规划教材

编审委员会

主　编：高　林

副主编：温希东　鲍　洁

编　委：（按姓氏笔画排列）

于　京　王　芳　乔江天　刘　松　杨欣斌

吴弋旻　余红娟　张　勇　张馨月　陈西玉

武春岭　郑士芹　郝　军　倪　勇　曹建林

盛鸿宇　韩毓文　曾照香

“高职高专电子信息类专业（信息安全专业）
课程建设”课题研究成果系列教材

编审委员会

主　编：郑士芹

编　委：（按姓氏笔画排列）

丁金炎　于　鑫　冯秀彦　史伟奇　吕秀鉴

张　军　张波云　武春岭　范　强　洪　婕

黄　峰　鄢喜爱　褚云霞

总序

《国家中长期教育改革和发展规划纲要（2010—2020）》确立了职业教育发展目标：到2020年，形成适应经济发展方式转变和产业结构调整要求、体现终身教育理念、中等和高等职业教育协调发展的现代职业教育体系，满足人民群众接受职业教育的需求，满足经济社会对高素质劳动者和技能型人才的需要。

高等职业教育是我国职业教育体系中的重要组成部分，具有高等教育和职业教育双重属性，其主要任务是培养生产、服务、管理第一线的高素质技能型专门人才。在建设现代职业教育体系中发挥引领、示范和骨干作用。1998年以来，我国高职院校培养的毕业生已经超过了1300万人，目前全国高等职业院校共有1200余所，年招生规模达到310万人，在校生达900万人。随着我国《国家“十二五”规划纲要》、《国家中长期教育改革和发展规划纲要（2010—2020）》、《人才规划纲要》、《科技规划纲要》的颁布实施，我国经济社会发展进入新的时期。面对当前的新形势、国家发展战略对高等职业教育改革提出的新需求，高等职业教育必须坚持以服务为宗旨、以就业为导向，走产学研结合发展道路的办学方针，以提高质量为核心，以增强特色为重点，创新体制机制，深化教育教学改革，抓住机遇、迎接挑战。进一步明确经济社会发展和高素质技能型专门人才培养对高等职业教育提出的新期望，进一步准确把握高等职业教育在建设现代职业教育体系中的时代定位，进一步明确新时期赋予高等职业教育的新任务，推动高等职业教育事业在新时期实现科学发展，努力办出中国特色、世界水准的高等职业教育。

教育部高等学校高职高专电子信息类专业教学指导委员会（以下简称电子信息教指委）致力于推动高职高专电子信息类专业的教学改革，面向我国电子信息产业的发展与人才需求，积极借鉴国外先进的课程理念，探索具有中国特色的高职课程改革开放模式，根据教育部的工作部署和电子信息教指委的工作计划，切实落实《关于全面提高高等职业教学教学质量的若干意见》教高[2006]16号文件及教育部近年有关高职教育教学等重要会议和相关文件精神，强化内涵，突出特色，把提高质量与促进发展作为高职电子信息类专业规范建设与改革创新的主线。在电子信息教指委第一批专业教学改革立项课题结题成果和《高职高专电子信息类指导性专业规范（Ⅰ）》研制、发布基础上，2009年电子信息教指委再次立项，进一步开展电子信息类专业教学改革研究，重点结合高职高专电子信息类专业在目前形势下教学改革中亟待解决的热点、难点问题，立足于深入贯彻专业规范，引领专业改革和教学资源建设，并为《高职高专电子信息类教学指导性专业规范（Ⅱ）》的研制奠定坚实的基础。经过专家和电子信息教指委推荐，院校申请，并经专家研讨和审核之后，电子信息教指委批准确立第二批教学改革研究项目50个，共有31个单位参加项目的研究工作。

电子信息类教指委推动专业教学改革主要包含两个方面的内容：第一方面是专业和课程教学内容的改革；第二方面是专业人才培养模式的改革。

首先电子信息产业是发展非常快的朝阳产业，这主要得益于电子信息技术的发展，电子

信息技术具有研发创新周期短，新技术应用变化快的时代特点，要求从业人员能实时跟进电子信息技术发展和电子信息基本技能的发展要求，这就要求高职电子信息类专业和课程内容要针对高素质技能型专门人才的职业工作需要及时变化教学内容和基本技能训练内容，以反映电子信息新技术发展和技术应用要求。电子信息教指委重点推进的基本技能训练包括电子电路设计与制作技术、芯片级检测与维修技术、编码与程序设计技术；重点推进的新技术应用包括嵌入式技术、信息安全技术、3G 技术、新一代企业信息化应用技术、物联网技术、新能源电子技术。同时，推动这些新技术应用尽快反映在教材中，从而尽快引进专业教学。

无论是新技术引进，还是原有课程内容都需要进行改革，使其适应高等职业教育的规律，体现高等职业教育的特色。电子信息教指委在人才培养模式改革和专业课程体系建设，遵循产学合作、工学结合的指导思想，将职业竞争力导向的“工作过程—支撑平台系统化课程”模式作为电子信息类专业教学改革指导性课程模式。这一模式是在学习借鉴德国设计导向基于工作过程课程模式和国内外高职教学改革经验基础上，由原北京联合大学高等技术与职业教育研究所提出，经电子信息教指委在电子信息类专业教学改革中实践应用和不断完善，从而形成的一个科学先进、实用可行、体现中国特色和适应电子信息类专业需求的人才培养模式和系统化的课程开发方法，在众多高职院校电子信息类专业受到欢迎并得到应用。这一模式具有以下特点：

- 以产学合作、工学结合为指导思想；
- 贯彻职业竞争力导向的职业教育理念；
- 创新面向技能型专门人才的职业分析方法；
- 构建工作过程—支撑平台系统化的专业课程体系；
- 提出专业课程体系中的三种基本的课程类型。

尤其是“工作过程—支撑平台系统化课程”模式提出高等职业教育专业课程体系是由三种典型的基本课程类型构建的，第一类称为相对系统的专业知识性课程；第二类称为基本技术技能的训练性实践课程；第三类称为理论—实践一体化的学习领域课程。这三类课程有时也简称为 A、B、C 三类课程。调研显示，经过近 20 年的改革，绝大部分高等职业教育专业人才培养方案都是由这三类课程为主组成的，所以问题的关键不是存在这三类课程，而是如何改革，或是说有没有一套能按现代职业教育和中国高职教育的特点，分别设计这几类课程的系统性课程设计方法。

伴随“工作过程—支撑平台系统化课程”模式给出的工作过程—支撑平台系统化课程开发方法，对 A、B 类课程，强调基于职业分析，以支持典型工作任务完成的基础知识和基本技能构成课程主要内容，满足职业工作需要；课程和教材结构设计采用案例或任务引导，深入浅出，易于学生学习。C 类课程是以典型工作任务为载体，旨在培养综合职业能力，但不选择目前培养综合职业能力较普遍采用的综合实训课程、任务课程或项目课程等形式，而强调采用对培养综合职业能力更具优势和系统性的学习领域课程，再通过项目教学方式和行动导向的教学法完成学习领域课程教学。三类课程中每一门课程都要遵循工作过程—支撑平台系统化课程开发方法给出的设计步骤，以职业分析为起点，经过专业课程体系设计，再完成具体课程设计，设计过程和案例可参见我们编写出版的《高职高专电子信息类指导性专业规范（Ⅱ）》和《高等职业教育课程设计手册》等书。

为把电子信息教指委教学改革研究立项成果落实于教学实践中，切实提高人才培养质量，

配合电子信息教指委正在实施的优质教学资源建设工作，电子信息教指委组织了高等职业院校一线教师及行业企业专家共同开发“教育部高等学校高职高专电子信息类专业教学指导委员会规划教材”。教材开发贯彻高职课程改革的指导思想，采用职业竞争力导向的“工作过程—支撑平台系统化课程”模式和课程开发方法，学校教师、企业专家相互合作、优势互补，并且教材开发得到多家出版社支持。

“教育部高等学校高职高专电子信息类专业教学指导委员会规划教材”包括电子信息类多个专业不同类型的典型课程教材，也包括电子类和信息类专业共同的基本技术技能训练性实践课程（B 类）教材。参加编写的学校有北京信息职业技术学院、深圳信息职业技术学院等 17 所；企业有神州数码、中兴通讯等 12 家；出版社有中国铁道出版社、人民邮电出版社等 4 家。

目前，建设现代职业教育体系，创新中国特色高等职业教育人才培养模式，已成为高等职业教育发展的主流趋势。机遇与挑战并存，我们要抓住机遇，迎接挑战，培养出符合社会需求的高素质技能型专门人才。希望通过电子信息类专业规划教材的出版，大力推动我国高等职业教育改革，实现优质资源共享，提高高等职业教育人才培养质量，为我国现代经济社会发展做出应有的贡献。

教育部高等学校高职高专电子信息类专业教学指导委员会

2011.6

前　言

本书是教育部高职高专电子信息类专业教学指导委员会规划的系列教材之一，充分考虑了技能型专业人才培养目标、岗位需求和前后续课程的衔接，以“必需、够用”为度，统筹考虑和选取教学内容。书中将教、学、做相结合，强化学生能力培养，合理设计实验、实训、实习等关键环节。以理论为引导，重点以“怎么解决问题”为目标，做到深入浅出，让学生能够进行有针对性的学习和掌握解决问题的能力。

全书共 11 章，具体内容安排如下。

第 1 章是绪论，介绍操作系统面临的安全威胁、安全操作系统的研究进展以及操作系统安全的相关定义及术语，为后续学习打下基础。

第 2 章简要介绍操作系统安全理论基础，内容包括操作系统安全机制及其在主流操作系统上的应用以及操作系统安全需求、安全策略和安全模型基本概念，并对几种重要的安全模型如 Bell-Lapadula 模型等做了简要介绍，最后讲述了操作系统安全体系结构的概念和安全体系结构设计的基本原则。

第 3 章介绍 Windows 安全模型及安全模型组件，对安全对象如进程、线程、事件和其他同步对象以及文件、目录和设备进行了简介。同时对 Windows 文件系统、域、用户、注册表、驱动程序等系统安全相关基础知识进行了介绍。

第 4 章介绍 Windows 账户安全管理。主要介绍账户的基本概念、用户账户的管理、用户组的管理、系统账户权限设置等内容。通过为用户设置相关的权限，可以实现对用户访问系统中各种资源权限的管理，以保护本地系统和服务器不被非法用户访问，达到控制系统资源分布与共享的目的。

第 5 章介绍 Windows 系统资源的安全保护，包括文件系统和共享资源的安全设置、应用程序和用户主目录的安全管理、打印机的安全管理、注册表的安全管理、审核策略和系统策略文件、用户磁盘空间的限制和数据备份等内容，系统资源的安全性是应用安全的基础。

第 6 章主要介绍 Windows 操作系统的漏洞扫描方法和测评操作系统安全的标准和方法。首先介绍了漏洞扫描系统的功能、分类，说明如何通过漏洞扫描自动评估操作系统配置方式不当所导致的安全漏洞，然后讲述了操作系统的安全级别划分、安全测评标准以及操作系统测评框架相关知识。

第 7 章系统地介绍了 Windows 系统的各项安全配置和安全加固情况。加强 Windows 系统安全、提高安全风险级别，能有效提高信息系统整体安全水平，减少黑客攻击、病毒入侵的安全漏洞隐患，信息系统整体安全水平可以得到有效提高。

第 8 章从 Linux 系统下的用户和组管理机制出发，介绍用户口令的安全性保证机制、用户和组文件的安全机制，并介绍与之相关的用户、组文件设置指令。

第 9 章从文件分区的安全策略、文件共享安全、NFS 安全、文件系统的安全加载、文件的完整性检查、文件系统的数据备份等不同角度讲述了 Linux 操作系统中的文件系统安全防护技术。

第 10 章从系统管理员的角度讨论 Linux 操作系统安全增强问题。主要内容有系统启动和登录安全性设置、网络访问安全性设置、安装系统安全补丁包、日志和审计工具的使用、入

侵检测工具如 Snort 等的配置及使用方法介绍。

第 11 章介绍安全操作系统的两种应用，即 WWW 安全与防火墙系统安全。讲述了安全 Web 服务器的概念以及多级安全机制在 Web 服务器中的整合方法。并介绍了防火墙涉及的安全技术和防火墙利用安全操作系统的保护机制。

全书由张波云教授负责统筹、规划和审稿。具体分工是：第 1 章由张波云编写，第 2 章由赵薇、赵磊编写，第 3 章由谭敏编写，第 4 章由鄢喜爱编写，第 5 章由罗熹编写，第 6 章由赵薇编写，第 7 章由范强编写，第 8 章由欧阳伟编写，第 9 章由许柯编写，第 10 章及第 11 章由唐德权编写。编者收集整理了大量资料，结合自己的教学研究工作，撰写了本书。本书从各种论文、书籍、期刊以及互联网中引用了相关资料，在此谨向原作者表示衷心的感谢。对于所引资料，我们尽量在参考文献中予以列出，如有遗漏，深致歉意。

在本书完稿之际，感谢教育部高职高专电子信息类教学指导委员会高林和鲍洁老师在写作过程中给予我们的的精心指导；感谢北京信息职业技术学院郑士芹老师在组织信息安全教学改革项目中付出的辛勤劳动，本书也是教育部电子信息类教学改革项目的研究结果；感谢公安部应用创新基金（编号 2007HNSTYYCX072 和 2011YYCXHNST072）和湖南省科技计划基金（编号 2011GK3084）的资助；感谢在写作过程中给予我们大力支持的湖南警察学院信息技术（网监）系的领导和老师们。

由于操作系统安全所涉及的内容广泛，相关技术的发展迅速，尽管编者已经尽了最大的努力，但仍感错误难免，不足之处恳请读者批评指正。如有建议，请与编者联系，电子邮箱：hnjxzby@yahoo.com.cn。另外，为方便教学，我们提供了配套电子讲义及教学素材，可从人民邮电出版社网站 www.ptpress.com.cn 下载使用。

编　者

2012 年 2 月

目　录

第1章 绪 论

随着社会信息化的发展，网络信息安全问题也日益突出。操作系统安全性是计算机信息系统安全的重要基础。要妥善解决日益广泛的计算机安全问题，必须有坚固的安全操作系统做后盾。安全操作系统是指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。操作系统各种安全威胁形式导致的最终后果，其实就是对一般信息系统或计算机系统应该拥有的保密性、完整性和可用性3方面的安全特性的破坏。防火墙、防病毒、入侵检测系统等安全产品采用被动防护的技术手段，所采用的思路是以共享信息资源为中心在外围对各种攻击进行封堵，以达到保护的目的。操作系统是安全的基础对象，从源头上解决信息安全问题必须依赖高安全等级操作系统。本章简要介绍了操作系统面临的安全威胁，对国内外安全操作系统的研究成果进行了综述，并对本文常见的相关专业术语给出了定义，为后续学习打下基础。

第一部分 教学组织

一、目的要求

（1）了解操作系统面临的威胁。
（2）掌握操作系统安全相关术语。
（3）了解安全操作系统的研究状况。

二、工具器材

VMware 软件，Windows 系列操作系统软件，Linux 操作系统软件。

三、学习方式建议

（1）安装不同的操作系统软件并熟练操作，增强对不同类别操作系统的感性认识。
（2）广泛查阅资料，了解当前主流操作系统面临的安全威胁。
（3）调查了解当前主流操作系统的安全漏洞及解决办法。

第二部分 教学内容

1.1 操作系统面临的安全威胁

Internet 改变了人们生活方式和工作方式，改变了全球的经济结构、社会结构。Internet

越来越成为人类物质社会的最重要组成部分，成为20世纪最杰出的研究成果。但是，在互联网高速发展的同时，信息安全问题也日益严重。

据CERT/CC（Computer Emergency Response Team/Coordination Center）报道，自1998年以来，Internet安全威胁事件逐年上升，近年来的增长态势变得尤为迅猛。1998～2003年，平均年增长幅度达50%左右，如图1.1所示。

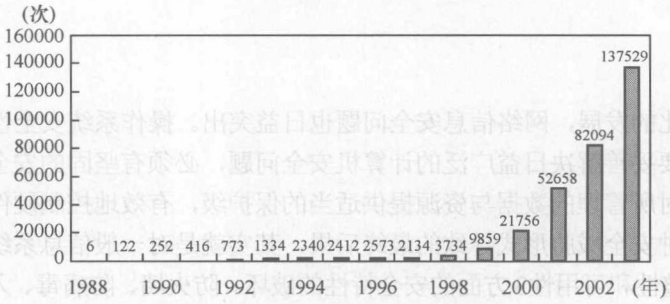

图1.1 CERT/CC安全事件报告

导致这些安全事件的主要因素是系统和信息系统安全脆弱性（Vulnerability）层出不穷。1995～2003年CERT各年度接到的脆弱性报告数逐年增多，如图1.2所示。这些安全威胁事件给Internet带来了巨大的经济损失。由于攻击数量如此之多，因此无法仅从安全事件的数量得到有关攻击范围和影响的更为有效的信息。从2004年开始，CERT/CC更为重视专门的安全事件报告。

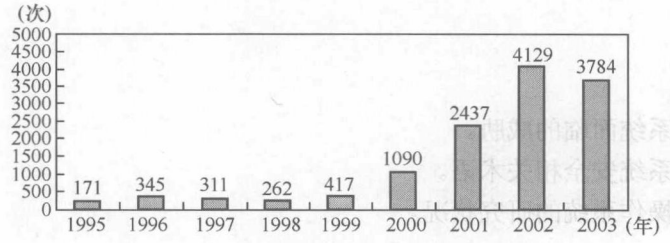

图1.2 CERT/CC安全弱点报告

随着社会信息化的发展，网络信息安全问题也日益突出。诸多信息系统尤其是大型计算机网络系统的可靠性关系到经济、政治利益乃至国家安全，这些分布式网络具有空间分布广、实时性要求高、攻防对抗性强且多为异构系统等显著特点，它们对信息安全防护技术的需求十分迫切。

1.1.1 信息安全的发展过程

对信息的安全、可靠和保障方面的考虑从自动化系统问世以来就有了。人们对信息安全的认识，经历了一个由浅入深、由片面到全面、由离散到整体的历史过程，这是在人们的实践中逐步完善的，并且与信息技术的发展相伴，受到不同历史阶段应用需求的驱动。通常认为，信息安全的发展经过了4个历史发展阶段：通信保密阶段（又称通信安全，ComSEC）、计算机安全阶段（CompuSEC）、信息安全（InfoSEC）阶段、信息安全保障（IA）阶段，如图1.3所示。在每一个阶段，信息安全都有着不同的内涵。