

《操作系统安全设计》

图书基本信息

书名：《操作系统安全设计》

13位ISBN编号：9787111432159

10位ISBN编号：7111432150

出版时间：2013-9

出版社：机械工业出版社

作者：沈晴霓,卿斯汉

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《操作系统安全设计》

内容概要

信息安全基础设施的关键是操作系统安全，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。本书融入了作者多年来对操作系统安全设计领域的研究和工程实践的成果，旨在通过本书进一步推动此领域的人才培养，加强我国信息安全基础设施相关领域的研究和实践能力，提高我国在基础软件安全方面的国际竞争力。

【本书特色】

内容全面系统。本书内容由浅入深，分为“基础篇”、“理论篇”、“实践篇”、“趋势篇”四部分，详细介绍了经典的操作系统安全设计的相关概念、理论和实践技术，也包括业界开源操作系统安全的研究成果，帮助读者全面掌握操作系统安全设计的知识。

理论与实践结合。本书不仅阐述了操作系统安全设计的理论内容，还以我国自主研发的安胜安全操作系统的设计与实现作为案例介绍操作系统安全设计的实践，更涵盖了未来云操作系统在安全方面的考虑。

紧跟领域前沿。本书作者均为国内知名操作系统安全专家，长期从事此领域的研究和工程实践，并主持我国自主研发的高安全等级操作系统，保证本书内容既有坚实的理论基础，又充分反映领域的最新进展。

操作系统安全是计算机系统安全的基础，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。

本书从操作系统基本安全概念、通用安全需求、安全标准和必要的安全机制入手，阐述了操作系统安全建模理论、安全体系结构设计思想，以及安全保证技术和方法，以自主研发的安胜安全操作系统的设计与实现为案例介绍安全操作系统的应用实践，并就业界关注的最新的可信计算技术、系统虚拟化技术，以及云操作系统安全实践进行介绍。

本书适合作为从事操作系统安全领域工作的学生、研究人员、工程技术人员的参考书，也可供从事信息安全领域工作人员阅读。

《操作系统安全设计》

作者简介

卿斯汉 国际知名信息安全专家。中国科学院软件研究所首席研究员，中国科学院信息工程研究所信息安全国家重点实验室首席研究员，北京大学软件与微电子学院信息安全系首届系主任，教授，博士生导师，享受国家特殊津贴。现国家保密局技术顾问、中国科学院“十二五”信息安全工程监理组组长、全国信息安全标准化技术委员会委员、可信计算工作组组长、亚洲密码学会执行委员会委员、微软公司全球专家委员会（TCAAB）委员等。主持国家重大攻关项目、国务院信息办重点攻关项目、973项目、863项目等80多项。获得国家科技进步奖2次、中科院科技进步奖3次，排名均为第一。

沈晴霓 北京大学副教授，硕士生导师。先后担任北京大学软件与微电子学院信息安全系副系主任，软件技术与服务工程学科组副组长。我国自主研发的“结构化保护级”安胜安全操作系统的主要完成人之一。近年来主要研究方向包括：操作系统与虚拟化安全，云计算和大数据安全、可信计算等，主持和参加多项国家自然科学基金重点、核高基重大专项、国家973、863项目。申请国内外发明专利20多项，已登记国家软件著作权5项。

书籍目录

编委会

丛书序

前言

教学建议

第一部分 基础篇

第1章 引言??1

1.1 操作系统安全威胁与安全需求??1

1.1.1 安全威胁类型??1

1.1.2 通用安全需求??3

1.2 操作系统安全是信息系统安全的基础??6

1.3 国内外安全操作系统发展历史与现状??7

1.3.1 国外安全操作系统发展历史与现状??7

1.3.2 国内安全操作系统发展历史与现状??11

1.4 计算机系统安全等级划分与评测标准??12

1.4.1 标准发展概况??12

1.4.2 TCSEC准则??14

1.4.3 CC准则??19

1.5 相关术语??28

1.6 本章小结??29

习题1??30

参考文献??30

第2章 基本概念??31

2.1 系统边界与安全周界??31

2.2 可信软件与不可信软件??32

2.3 访问控制基本概念??32

2.3.1 主体与客体??32

2.3.2 访问控制矩阵??33

2.3.3 引用监控器??34

2.3.4 安全内核??34

2.4 构建安全的基本要素??36

2.4.1 安全策略??36

2.4.2 安全机制??37

2.4.3 安全保证??37

2.5 可信计算基??38

2.6 本章小结??39

习题2??39

参考文献??40

第3章 操作系统基本安全机制??41

3.1 硬件安全机制??42

3.1.1 存储安全??42

3.1.2 运行安全??43

3.1.3 I/O安全??45

3.2 访问控制机制??45

3.2.1 自主访问控制??45

3.2.2 客体重用??48

3.2.3 安全标记??49

3.2.4 强制访问控制??49

- 3.3 可追究机制??54
 - 3.3.1 标识与鉴别??54
 - 3.3.2 可信通路??58
 - 3.3.3 安全审计??61
- 3.4 连续保护机制??63
 - 3.4.1 系统完整性??63
 - 3.4.2 隐蔽通道分析??64
 - 3.4.3 最小特权管理??72
 - 3.4.4 可信恢复??76
- 3.5 本章小结??76
- 习题3??77
- 参考文献??77
- 第4章 通用操作系统安全机制??79
 - 4.1 UNIX/Linux操作系统安全机制??79
 - 4.1.1 系统结构??80
 - 4.1.2 安全机制??86
 - 4.2 Windows NT/XP操作系统安全机制??93
 - 4.2.1 系统结构??94
 - 4.2.2 安全模型??96
 - 4.2.3 安全机制??102
 - 4.3 本章小结??106
 - 习题4??106
 - 参考文献??107
- 第二部分 理论篇
- 第5章 安全策略与安全模型??109
 - 5.1 安全策略??109
 - 5.1.1 安全策略概述??109
 - 5.1.2 安全策略类型??110
 - 5.1.3 策略表达语言??110
 - 5.2 安全模型??111
 - 5.2.1 安全模型的作用和特点??111
 - 5.2.2 形式化安全模型设计目标与要求??111
 - 5.2.3 状态机安全模型的一般开发方法??113
 - 5.3 机密性策略与模型??114
 - 5.3.1 机密性策略目标??114
 - 5.3.2 Bell-LaPadula模型??114
 - 5.3.3 Bell-LaPadula模型分析与改进??121
 - 5.4 完整性策略与模型??123
 - 5.4.1 完整性策略目标??123
 - 5.4.2 Biba模型??123
 - 5.4.3 Clark-Wilson模型??127
 - 5.5 混合型/中立型安全策略与模型??130
 - 5.5.1 中国墙模型??131
 - 5.5.2 基于角色的访问控制模型??137
 - 5.5.3 域和型强制实施模型??140
 - 5.6 其他模型??141
 - 5.6.1 安全信息流模型??141
 - 5.6.2 无干扰安全模型??145
 - 5.7 本章小结??146

习题5??146

参考文献??147

第6章 安全体系结构??148

6.1 安全体系结构基本概念??148

6.1.1 安全体系结构定义??149

6.1.2 安全体系结构分类??149

6.2 安全体系结构设计原则与目标??150

6.2.1 设计原则??150

6.2.2 设计目标??153

6.3 GFAC通用访问控制框架??153

6.4 Flask安全体系结构与LSM框架??155

6.4.1 Flask安全体系结构??155

6.4.2 LSM访问控制框架??166

6.5 权能安全体系结构??174

6.5.1 权能与访问控制列表??174

6.5.2 EROS系统及其权能体系??176

6.6 本章小结??179

习题6??179

参考文献??179

第7章 安全保证技术??181

7.1 概述??181

7.1.1 安全保证的概念??181

7.1.2 安全保证的必要性??183

7.1.3 安全保证中需求的作用??183

7.2 安全开发生命周期??184

7.2.1 系统的生命周期??184

7.2.2 瀑布型生命周期模型??186

7.2.3 安全开发生命周期??187

7.3 安全测试技术??188

7.3.1 老虎队和善意黑客??189

7.3.2 安全测试的基本过程??189

7.4 形式化规范与验证技术??189

7.4.1 形式化方法概述??189

7.4.2 形式化方法的应用研究??191

7.4.3 常用形式化规范与验证技术??192

7.5 安全测评方法??196

7.5.1 传统安全性保证手段??196

7.5.2 操作系统安全评测方法??197

7.6 本章小结??198

习题7??198

参考文献??198

第三部分 实践篇

第8章 安全操作系统设计与实现技术??201

8.1 安全操作系统设计原则??201

8.2 安全操作系统的一般开发过程??202

8.3 安全操作系统的常用开发方法??204

8.3.1 虚拟机法??204

8.3.2 改进/增强法??204

8.3.3 仿真法??204

8.4 安全操作系统设计和实现案例??206

- 8.4.1 安全目标??206
- 8.4.2 总体结构设计??206
- 8.4.3 安全内核的开发??211
- 8.4.4 多策略安全模型??212
- 8.4.5 多级分层文件系统??217
- 8.4.6 隐蔽存储通道分析??219
- 8.4.7 安全加密文件系统??223
- 8.4.8 客体重用机制??227

8.5 注意的问题??230

- 8.5.1 TCB的设计与实现??230
- 8.5.2 安全机制的友好性??241
- 8.5.3 效率和兼容性考虑??241

8.6 本章小结??241

习题8??242

参考文献??242

第9章 安全操作系统的应用??243

9.1 安全操作系统与Web服务器安全??243

- 9.1.1 Web服务器概述??243
- 9.1.2 安全Web服务器概念及解决方案??245
- 9.1.3 多级安全Web服务器??246

9.2 安全操作系统与防火墙安全??254

- 9.2.1 防火墙及其安全技术??254
- 9.2.2 基于安全操作系统的防火墙保护机制??256

9.3 安全操作系统与数据库安全??261

- 9.3.1 数据库安全威胁与安全需求??261
- 9.3.2 数据库安全与操作系统安全的关系??262
- 9.3.3 多级安全数据库??264

9.4 本章小结??273

习题9??274

参考文献??274

第四部分 趋势篇

第10章 可信计算技术??275

10.1 概述??275

- 10.1.1 可信计算的概念??275
- 10.1.2 可信计算的形成历程??276
- 10.1.3 可信计算组织TCG??278
- 10.1.4 国内外可信计算产品与技术发展??282

10.2 可信平台/密码模块TPM/TCM??284

- 10.2.1 可信平台模块TPM??284
- 10.2.2 可信密码模块TCM??286
- 10.2.3 TCM、TPM、TPM.next之间的关系??289

10.3 可信平台相关技术??290

- 10.3.1 可信平台构件??290
- 10.3.2 可信边界??291
- 10.3.3 可传递的信任??291
- 10.3.4 完整性度量??292
- 10.3.5 完整性报告??292
- 10.3.6 TCG证书机制??292

- 10.3.7 TCG密钥管理机制??295
- 10.4 基于TPM/TCM的可信操作系统??297
 - 10.4.1 主流操作系统的安全性问题??297
 - 10.4.2 可信操作系统的TPM/TCM支持要求??298
 - 10.4.3 基于TPM/TCM的可信操作系统核心机制??300
- 10.5 本章小结??304
- 习题10??304
- 参考文献??305
- 第11章 系统虚拟化技术??307
 - 11.1 概述??307
 - 11.1.1 背景介绍??307
 - 11.1.2 系统虚拟化技术的分类??309
 - 11.1.3 x86架构虚拟化实现技术??311
 - 11.1.4 支持虚拟化的硬件体系结构??313
 - 11.1.5 主流的系统虚拟化软件??314
 - 11.2 虚拟化平台安全机制??317
 - 11.2.1 安全性分析??317
 - 11.2.2 虚拟机监控器安全体系结构??319
 - 11.2.3 虚拟机迁移安全机制??322
 - 11.2.4 虚拟机安全监控技术??325
 - 11.2.5 虚拟机之间的隐蔽通道分析??327
 - 11.2.6 虚拟机之间的I/O隔离技术??330
 - 11.3 虚拟可信平台技术??332
 - 11.3.1 虚拟平台工作组简介??332
 - 11.3.2 虚拟可信平台体系架构??333
 - 11.3.3 虚拟可信平台安全问题??340
 - 11.3.4 虚拟可信平台研究进展??342
 - 11.4 本章小结??343
 - 习题11??343
 - 参考文献??343
- 第12章 操作系统进展及其安全实践??345
 - 12.1 SELinux操作系统??345
 - 12.1.1 从DTMach到SELinux??345
 - 12.1.2 SELinux的安全策略模型??346
 - 12.1.3 SELinux的安全体系结构??347
 - 12.2 Solaris 10操作系统??349
 - 12.2.1 Solaris的发展史??349
 - 12.2.2 Solaris 10的安全体系结构??350
 - 12.2.3 Solaris 10的安全特性??352
 - 12.3 Windows Vista/Windows 7操作系统??355
 - 12.3.1 Windows Vista安全体系结构??355
 - 12.3.2 Windows Vista安全机制和技术??356
 - 12.3.3 Windows 7安全改进??365
 - 12.4 未来云操作系统??367
 - 12.4.1 Google Chrome OS??367
 - 12.4.2 Windows Azure??368
 - 12.4.3 Android OS??372
 - 12.5 本章小结??374
 - 习题12??374

参考文献??374

《操作系统安全设计》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com