

<<信息安全>>

图书基本信息

书名：<<信息安全>>

13位ISBN编号：9787560629155

10位ISBN编号：7560629156

出版时间：2013-2

出版时间：西安电子科技大学出版社

作者：马建峰

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：<http://www.tushu007.com>

## <<信息安全>>

### 内容概要

《信息安全(新世纪计算机类专业规划教材)》编著者马剑峰。

《信息安全(新世纪计算机类专业规划教材)》共8章,内容分别为信息安全概述和发展趋势、密码学与密码技术、网络安全技术、网络基本安全防护、信息系统可信性、可信软件和恶意软件防范、信息安全应用、无线网络安全技术。

相对于传统的信息安全教材,本书添加了对信息系统可信性、可信软件、系统分区等技术的介绍,并在此基础上,从多个方面系统地阐述了信息安全的具体应用以及无线网络安全技术。

本书可作为高校有关专业本科生和研究生的教材,也可作为通信工程师和计算机系统安全工程师的参考书。

## 书籍目录

第1章 信息安全概述和发展趋势 1 1.1 信息安全概述 1 1.1.1 信息的定义与性质和特征 1 1.1.2 信息安全的基本概念 2 1.1.3 信息安全的目标 3 1.2 安全攻击与防御 3 1.2.1 计算机系统中的安全威胁 4 1.2.2 网络系统中的安全威胁 5 1.2.3 数据的安全威胁 5 1.2.4 事务安全 5 1.2.5 技术防护 6 1.3 信息安全发展趋势 7 1.3.1 密码理论与技术研究的现状及发展趋势 7 1.3.2 安全协议理论与技术的研究现状及发展趋势 8 1.3.3 安全体系结构理论与技术的研究现状及发展趋势 8 1.3.4 信息对抗理论与技术的研究现状及发展趋势 9 1.3.5 网络安全与安全产品的研究现状及发展趋势 9 1.4 人为和社会因素 10 1.5 信息安全与法律 11 1.5.1 网络立法的现状与思考 11 1.5.2 计算机记录的法律价值 11 1.5.3 用户的行为规范 12 思考题 12 参考文献 12 第2章 密码学与密码技术 14 2.1 传统密码技术 14 2.1.1 单表代换密码 14 2.1.2 多表代换密码 15 2.1.3 多字母代换密码 16 2.1.4 转轮密码 17 2.2 对称密码算法 17 2.2.1 分组密码DES 17 2.2.2 国际数据加密算法(IDEA) 25 2.2.3 RC5算法 27 2.3 非对称密码算法 29 2.3.1 用于构造公钥密码的单向函数 29 2.3.2 RSA密码体制 31 2.3.3 Rabin密码体制 32 2.3.4 ElGamal密码体制 33 2.3.5 基于椭圆曲线的公开密钥密码体制 33 2.4 消息认证码MAC和散列函数Hash 38 2.4.1 消息认证码 39 2.4.2 散列函数 41 2.5 密码技术应用 43 2.5.1 数字签名 44 2.5.2 PKI及其应用 46 2.5.3 数字水印 47 思考题 51 参考文献 52 第3章 网络安全技术 53 3.1 密钥管理 53 3.1.1 概论 53 3.1.2 密钥的组织结构 54 3.1.3 密钥管理的基本内容 54 3.2 身份认证 55 3.2.1 认证的基本原理 55 3.2.2 认证协议 56 3.2.3 应用举例 64 3.3 访问控制 70 3.3.1 访问控制的基本概念 70 3.3.2 自主访问控制(DAC) 71 3.3.3 强制访问控制(MAC) 73 3.3.4 基于角色的访问控制 74 3.4 公钥基础设施 77 3.4.1 需要解决的问题 77 3.4.2 信任模型与PKI体系结构 78 3.4.3 证书 81 3.5 授权管理基础设施 87 3.5.1 授权管理基础设施的基本概念 87 3.5.2 PMI技术的授权管理模式及其优点 88 3.5.3 PMI系统的架构及需求 89 3.5.4 PMI的应用 91 3.6 IP安全技术 92 3.6.1 概述 92 3.6.2 封装安全载荷(ESP) 94 3.6.3 验证头(AH) 97 3.6.4 Internet密钥交换(IKE) 99 3.7 传输层安全 101 3.7.1 SSL协议 101 3.7.2 TLS协议 106 思考题 107 参考文献 108 第4章 网络基本安全防护 109 4.1 网络安全防护体系 109 4.1.1 网络安全体系结构的相关概念 110 4.1.2 网络安全体系的三维框架结构 110 4.1.3 安全服务之间的关系 111 4.2 防火墙 112 4.2.1 防火墙概述 112 4.2.2 网络策略 113 4.2.3 防火墙体系结构 114 4.2.4 代理服务技术 118 4.3 入侵检测 124 4.3.1 入侵检测概述 124 4.3.2 入侵检测技术分析 127 4.3.3 入侵检测系统 131 4.4 审计日志 136 4.4.1 审计内容 137 4.4.2 日志安全审计 137 4.4.3 结果响应 139 4.4.4 审计报告 139 4.5 漏洞检测技术 139 4.5.1 漏洞的定义 139 4.5.2 漏洞的分类 140 4.5.3 漏洞检测方法 140 4.5.4 漏洞检测技术 141 4.5.5 小结 142 4.6 网络故障管理探析 142 4.6.1 故障管理基本内容和检测模式 143 4.6.2 网络故障的基本检查方法 143 4.6.3 解决网络故障的一般步骤 144 4.6.4 小结 146 4.7 数据备份与恢复 146 4.7.1 数据备份 146 4.7.2 数据恢复 148 4.8 可生存性和容忍入侵 150 4.8.1 网络可生存性 150 4.8.2 容忍入侵技术 151 4.8.3 容忍入侵技术的基本理论 152 4.8.4 容忍入侵技术的实现 153 4.9 系统分区隔离 154 4.9.1 传统操作系统的隔离机制 154 4.9.2 基于沙箱的隔离机制 155 4.9.3 基于虚拟机技术的隔离机制 156 4.9.4 现有隔离机制的分析比较 157 思考题 157 参考文献 158 第5章 信息系统可信性 159 5.1 可信性概述 159 5.1.1 TCG的可信定义 161 5.1.2 TCG体系结构规范框架 161 5.2 可信度测度和评估 164 5.3 可信计算平台 167 5.3.1 安全地报告当前环境：平台状态 168 5.3.2 安全存储 171 5.4 TCG软件栈 174 5.4.1 TSS设计概况 174 5.4.2 TCG服务提供者接口(TSPi) 175 5.4.3 TSP(或TSPi)对象类型 175 5.4.4 TSS返回代码 182 5.4.5 TSS内存管理 182 5.4.6 可移植的数据设计 183 5.4.7 永久密钥存储 183 5.4.8 签名和认证 184 5.4.9 设置回调函数 184 5.4.10 TSS确认数据结构 185 5.5 TSS服务 186 5.5.1 TCS概述 186 5.5.2 选择WSDL的原因 189 5.5.3 wsdl文件的分析 190 5.5.4 复杂类型中的InParms和OutParms 192 5.5.5 消息 193 5.5.6 端口类型的操作 193 5.5.7 绑定操作 193 5.5.8 服务 194 5.5.9 与TCS相关的隐私问题 196 5.5.10 小结 197 思考题 197 参考文献 197 第6章 可信软件和恶意软件防范 198 6.1 程序安全 198 6.1.1 程序安全的概念 199 6.1.2 非恶意的程序漏洞 200 6.1.3 病毒和其他恶意代码 203 6.2 软件可靠性模型 205 6.2.1 软件可靠性模型的发展历程 206 6.2.2 软件可靠性模型分类 207 6.2.3 软件可靠性模型的作用 208 6.2.4 软件可靠性预计模型 209 6.3 软件系统排错技术 209 6.3.1 软件系统排错的目的 209 6.3.2 软件系统的排错过程 210 6.3.3 软件系统的排错方法 211 6.3.4 软件系统的排错原则 213 6.4

## &lt;&lt;信息安全&gt;&gt;

软件可信运行环境 214 6.4.1 可信软件研究现状 215 6.4.2 软件可信运行保障 217 6.5 软件的完整性认证 219 6.5.1 软件完整性认证分类 219 6.5.2 软件完整性认证相关技术 220 6.5.3 软件完整性认证实例 221 6.6 计算机病毒 223 6.6.1 计算机病毒的概念 223 6.6.2 计算机病毒的特征 226 6.6.3 计算机病毒的工作原理 228 6.7 计算机蠕虫 230 6.7.1 计算机蠕虫的概念 230 6.7.2 计算机蠕虫的功能结构 234 6.7.3 计算机蠕虫的传播过程 235 6.8 特洛伊木马 236 6.8.1 特洛伊木马的概念 236 6.8.2 特洛伊木马的类型 237 6.8.3 特洛伊木马的特征 238 6.8.4 特洛伊木马的工作原理 239 6.9 其他恶意代码 240 6.9.1 陷门 240 6.9.2 逻辑炸弹 242 6.9.3 细菌 245 6.10 软件系统恢复与重构 245 6.10.1 软件系统恢复和重构的概念 246 6.10.2 逆向工程和正向工程 246 6.10.3 架构和设计恢复 247 6.10.4 架构和设计重构 250 6.10.5 系统代码重构 251 思考题 251 参考文献 252

第7章 信息安全应用 253 7.1 安全Email 253 7.1.1 Email系统概述 253 7.1.2 Email安全目标 254 7.1.3 安全Email 254 7.2 安全Web 258 7.2.1 Web服务概述 258 7.2.2 Web安全目标 259 7.2.3 安全Web 260 7.3 电子政务 264 7.3.1 电子政务的基本概念 264 7.3.2 电子政务的安全需求 265 7.3.3 电子政务的安全措施 266 7.4 电子商务 269 7.4.1 电子商务的基本概念 269 7.4.2 电子商务的安全需求 269 7.4.3 电子商务的安全措施 270 7.5 网上银行 273 7.5.1 网上银行的基本概念 273 7.5.2 网上银行的安全需求 273 7.5.3 网上银行的安全措施 274 7.6 数字版权管理 278 7.6.1 数字版权管理的应用需求 278 7.6.2 数字版权管理概述 278 7.6.3 数字版权管理的安全技术 279 7.6.4 数字版权管理标准 283 7.7 安全操作系统 284 7.7.1 操作系统安全概述 284 7.7.2 安全操作系统 285 7.7.3 主流操作系统的安全性 290 7.8 安全数据库 293 7.8.1 数据库安全概述 293 7.8.2 安全数据库 294 7.9 计算机取证 297 7.9.1 基本概念 298 7.9.2 计算机取证的原则和步骤 298 7.9.3 计算机取证技术 299 7.9.4 计算机取证工具 301 思考题 302 参考文献 302

第8章 无线网络安全技术 303 8.1 无线网络安全概述 303 8.1.1 无线网络安全简述 303 8.1.2 无线网络的安全性 303 8.2 无线网络安全威胁 306 8.2.1 无线网络的安全问题 306 8.2.2 无线网络面临的安全威胁 307 8.3 无线网络安全接入 308 8.4 集成安全接入 310 8.4.1 设计思想 310 8.4.2 体系结构方案 311 8.5 无线融合安全组网 312 8.6 WSN安全技术 313 8.6.1 WSN的体系结构 313 8.6.2 WSN的安全需求 314 8.6.3 WSN的安全威胁 315 8.6.4 WSN安全技术 316 8.7 3G和LTE安全技术 317 思考题 320 参考文献 320

编辑推荐

《信息安全(新世纪计算机类专业规划教材)》编著者马剑峰。

本教材立足学科前沿趋势，以国家战略需求为导向，为培养高层次的信息安全人才提供保障。本教材在阐述信息安全基本原理和基本概念的基础上，从密码技术和非密码技术两个方面系统地阐述信息安全技术；不拘泥于繁杂的密码算法本身，而是更关注密码学的应用，指导学生如何使用现有的密码技术和非密码技术来解决日益严重的信息安全问题；从系统的角度，阐述信息系统基本安全防护方法，增加了现有的信息安全新技术，如无线网络安全、可信计算、系统分区等内容，使得学生能够更加全面深刻地理解各种信息安全解决方案；通过介绍具体的信息系统安全解决方案，使得学生能够使用、配置和实现主流的信息安全软件，搭建基本的信息安全平台。

#### 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:<http://www.tushu007.com>