

## <<计算机网络安全与防护>>

### 图书基本信息

书名：<<计算机网络安全与防护>>

13位ISBN编号：9787121120770

10位ISBN编号：7121120771

出版时间：2010-11

出版时间：电子工业出版社

作者：闫宏生 等编著

页数：275

字数：456000

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>

## <<计算机网络安全与防护>>

### 前言

2003年9月，中共中央办公厅印发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发27号）中，提出要在5年内建设国家信息安全保障体系，实现其目标就是大力增强国家信息安全的保障能力，特别是要积极跟踪、研究和掌握国际信息安全领域的先进理论、前沿技术和发展动态，抓紧开展对信息技术产品漏洞、后门的发现研究，掌握核心安全技术，提高关键设备装备能力，促进我国信息安全技术和产业的自主发展。

除此之外文件明确规定把信息安全人才培养作为加强国家信息安全保障的一项重要任务。

信息安全人才是国家建设信息安全保障体系和社会信息化健康发展的重要保证，而教材建设又是人才培养中一项十分重要的环节。

2007年8月，在电子工业出版社的大力支持下，我们编写的《计算机网络安全与防护》教材被教育部选为普通高等教育“十一五”国家级规划教材正式出版；2008年11月，以该书为主教材建设的《信息网络安全防护》课程被总参通信部评为首批精品课程；2009年3月，该书获湖北省第六次高等教育优秀研究成果教材类二等奖。

出版三年多来，得到许多高等院校同仁和学生的支持、鼓励和厚爱，先后印刷3次，许多读者还给我们写来热情洋溢的信件，提出了许多宝贵的意见和建议，使我们深受感动和鼓舞，在此谨向他们表示衷心的感谢。

网络安全技术发展十分迅速，原教材已不能准确反映网络安全领域的发展前沿，今年以来，我们组织人员对原教材内容进行了梳理论证，提出了修订意见，并取得了出版社的支持，在对原有内容进行适当修订的基础上，增加了近年来发展迅猛的无线局域网安全技术和信息隐藏技术的介绍，使之更具时代特色。

## <<计算机网络安全与防护>>

### 内容概要

本书是普通高等教育“十一五”国家级规划教材的修订版和总参通信部精品课程教材。

主要介绍计算机网络安全基础知识、网络安全体系结构、远程攻击与防范,以及密码技术、信息认证技术、访问控制技术、网络病毒与防范、防火墙、网络安全扫描技术、网络入侵检测技术、安全隔离技术、电磁防泄漏技术、蜜罐技术、虚拟专用网技术、无线局域网安全技术、信息隐藏技术,同时还介绍了网络安全管理和计算机网络战的概念、特点、任务和发展趋势。

全书内容广泛,注重理论联系实际,设计了11个实验,为任课教师免费提供电子课件。

本书适合普通高等院校计算机、信息安全、通信工程、信息与计算科学、信息管理与信息系统等专业本科生和硕士研究生使用。

## &lt;&lt;计算机网络安全与防护&gt;&gt;

## 书籍目录

第1章 绪论 1 1.1 计算机网络安全面临的挑战 1 1.2 威胁计算机网络安全的主要因素 2 1.3 计算机网络安全的本质 3 1.4 计算机网络安全策略 4 1.5 计算机网络安全的主要技术措施 5 本章小结 6 习题17第2章 计算机网络安全体系结构 8 2.1 网络安全体系结构的概念 8 2.1.1 网络体系结构 8 2.1.2 网络安全需求 9 2.1.3 建立网络安全体系结构的必要性 10 2.1.4 网络安全体系结构的任务 10 2.2 网络安全体系结构的内容 11 2.2.1 开放系统互联安全体系结构 (OSI安全体系结构) 11 2.2.2 美国国防部目标安全体系结构与国防信息系统安全计划 13 2.2.3 基于TCP/IP的网络安全体系结构 15 2.3 网络安全协议与标准 16 2.3.1 网络安全协议与标准的基本概念 16 2.3.2 网络安全协议与标准举例——美军JTA信息系统安全标准 16 2.4 网络安全的评估 17 2.4.1 美国的“可信计算机系统评估准则” 17 2.4.2 我国的“计算机信息系统安全等级保护划分准则” 19 本章小结 20 习题221第3章 远程攻击与防范 22 3.1 远程攻击的步骤和手段 22 3.1.1 远程攻击的一般步骤 22 3.1.2 远程攻击的主要手段 26 3.2 远程攻击的防范 30 3.2.1 防范远程攻击的管理措施 30 3.2.2 防范远程攻击的技术措施 31 本章小结 33 实验334 实验3.1 综合扫描 34 实验3.2 缓冲区溢出攻击 34 实验3.3 账号口令破解 36 实验3.4 IPSec策略配置 38 习题339第4章 密码技术 40 4.1 密码技术的基本概念 40 4.1.1 密码系统的基本组成 40 4.1.2 密码体制分类 41 4.1.3 古典密码体制 44 4.1.4 初等密码分析 48 4.2 分组密码体制 49 4.2.1 数据加密标准 (DES) 49 4.2.2 国际数据加密算法 (IDEA) 56 4.2.3 其他分组密码算法 59 4.3 公开密钥密码体制 60 4.3.1 RSA公开密钥密码体制 60 4.3.2 ElGamal密码体制 62 4.4 密钥管理 63 4.4.1 传统密码体制的密钥管理 63 4.4.2 公开密钥密码体制的密钥管理 70 本章小结 73 实验473 实验4.1 古典密码算法 73 实验4.2 RSA密码体制 74 习题474第5章 信息认证技术 76 5.1 报文认证 76 5.1.1 报文内容的认证 77 5.1.2 报文源的认证 78 5.1.3 报文时间性认证 78 5.2 身份认证 79 5.2.1 口令验证 79 5.2.2 利用信物的身份认证 82 5.2.3 利用人类特征进行身份认证 83 5.3 数字签名 83 5.3.1 数字签名的概念 84 5.3.2 公钥密码实现数字签名的原理 85 5.3.3 利用RSA密码实现数字签名 87 5.3.4 利用ElGamal密码实现数字签名 89 5.3.5 利用椭圆曲线密码实现数字签名 91 5.3.6 美国数字签名标准 (DSS) 92 5.3.7 不可否认签名 94 5.3.8 盲签名 95 5.4 数字签名的应用 97 5.4.1 计算机公证系统 97 5.4.2 Windows系统的数字签名 99 5.5 信息认证中心 103 5.5.1 数字证书 103 5.5.2 证书管理与密钥管理 103 5.5.3 认证中心的功能 104 5.5.4 认证中心的建立 105 本章小结 107 实验5 认证、授权和计费 (AAA) 服务 107 习题5113第6章 访问控制技术 115 6.1 访问控制概述 115 6.1.1 访问控制的基本任务 115 6.1.2 访问控制的层次 117 6.1.3 访问控制的要素 118 6.1.4 访问控制策略 119 6.2 访问控制的类型 120 6.2.1 自主访问控制 121 6.2.2 强制访问控制 127 6.2.3 基于角色的访问控制 129 6.3 访问控制模型 130 6.3.1 BLP模型 130 6.3.2 Biba模型 131 6.3.3 角色模型 132 6.4 访问控制模型的实现 135 6.4.1 访问控制模型的实现机制 135 6.4.2 访问控制模型的实现方法 137 本章小结 138 习题6139第7章 网络病毒与防范 140 7.1 网络病毒及其特征 140 7.1.1 网络病毒的概念 140 7.1.2 网络病毒的主要特点 141 7.1.3 网络病毒实例 144 7.2 网络反病毒原则与策略 154 7.2.1 防重于治, 防重在管 155 7.2.2 综合防护 155 7.2.3 最佳均衡原则 155 7.2.4 管理与技术并重 156 7.2.5 正确选择网络反病毒产品 156 7.2.6 多层次防御 156 7.2.7 注意病毒检测的可靠性 157 7.3 网络防治病毒的实施 157 7.3.1 病毒诊断技术原理 157 7.3.2 网络反病毒技术的主要能力 159 7.3.3 网络反病毒的基本技术措施 161 7.3.4 网络反病毒技术体系 163 7.3.5 主流反病毒产品介绍 166 本章小结 170 实验7 网络蠕虫病毒及防范 171 习题7173第8章 防火墙 175 8.1 防火墙的基本原理 175 8.1.1 防火墙的概念 175 8.1.2 防火墙的模型 175 8.1.3 防火墙的安全策略 176 8.2 防火墙的分类 177 8.2.1 包过滤防火墙 177 8.2.2 应用代理防火墙 185 8.2.3 复合型防火墙 192 8.3 防火墙体系结构 195 8.3.1 几种常见的防火墙体系结构 195 8.3.2 防火墙的变化和组合 199 8.3.3 堡垒主机 201 8.4 防火墙的选购 207 8.5 防火墙的发展趋势 209 本章小结 210 实验8 天网防火墙的配置 211 习题8212第9章 其他网络安全技术 213 9.1 安全扫描技术 213 9.1.1 安全扫描技术简介 213 9.1.2 端口扫描技术 214 9.1.3 漏洞扫描技术 214 9.2 入侵检测技术 216 9.2.1 入侵检测的概念 216 9.2.2 入侵检测系统技术及分类 217 9.2.3 入侵检测的主要方法 217 9.2.4 入侵检测技术的发展方向 218 9.3 安全隔离技术 219 9.4 电磁防泄漏技术 219 9.4.1 电磁泄漏 219 9.4.2 电磁泄漏的基本途径 220 9.4.3 电磁防泄漏的主要技术 220 9.5 蜜罐技术 222 9.5.1 蜜罐的概念 222 9.5.2 蜜罐的主要技术 224 9.6 虚拟专用网

## &lt;&lt;计算机网络安全与防护&gt;&gt;

技术 225 9.6.1 虚拟专用网概述 225 9.6.2 VPN的工作流程 226 9.6.3 VPN的主要技术 227 9.6.4 VPN  
服务分类 228 9.7 无线局域网安全技术 229 9.7.1 无线局域网的安全缺陷 230 9.7.2 针对无线局域网的  
攻击 230 9.7.3 常用无线局域网安全技术 231 9.7.4 无线局域网的常用安全措施 233 9.8 信息隐藏技术  
235 9.8.1 信息隐藏技术的概念、分类和特点 235 9.8.2 信息隐藏技术在网络安全中的应用 237 本章小  
结 238 实验9 239 实验9.1 入侵检测系统 239 实验9.2 虚拟专用网 240 习题9 243第10章 网络安全管理  
244 10.1 网络安全管理概述 244 10.1.1 网络安全管理的内容 244 10.1.2 网络安全管理的原则 246  
10.1.3 网络安全管理的方法和手段 248 10.2 网络设施安全管理 251 10.2.1 硬件设施的安全管理 251  
10.2.2 机房和场地设施的安全管理 253 10.3 网络信息的安全管理 255 10.3.1 密钥管理与口令管理 255  
10.3.2 软件设施的安全管理 257 10.3.3 存储介质的安全管理 259 10.3.4 技术文档的安全管理 261 10.4  
网络安全运行管理 261 10.4.1 安全运行管理系统框架 261 10.4.2 安全审计 262 10.4.3 灾难恢复管理  
263 本章小结 264 习题10 265第11章 计算机网络战 266 11.1 计算机网络战的概念与特点 266 11.1.1 计  
算机网络战的概念 266 11.1.2 计算机网络战的特点 268 11.2 计算机网络战的任务 270 11.2.1 情报侦察  
与反侦察 270 11.2.2 病毒破坏与反破坏 270 11.2.3 电磁干扰与反干扰 271 11.2.4 实体摧毁与反摧毁  
271 11.3 计算机网络战的发展趋势 272 本章小结 274 习题11 274参考文献 275

## <<计算机网络安全与防护>>

### 章节摘录

插图：1.1 计算机网络安全面临的挑战自互联网问世以来，资源共享和信息安全一直作为一对矛盾体存在着，计算机网络资源共享的进一步加强所伴随的信息安全问题也日益突出，各种计算机病毒和网上黑客对互联网的攻击越来越猛烈，网站遭受破坏的事例不胜枚举。

1991年，美国国会总审计署宣布，在海湾战争期间，几名荷兰少年黑客侵入美国国防部的计算机，修改或复制了一些与战争相关的敏感情报，包括军事人员、运往海湾的军事装备和重要武器装备开发情况等。

1994年，格里菲斯空军基地和美国航空航天局的计算机网络受到两名黑客的攻击。

同年，一名黑客用一个很容易得到的密码发现了英国女王、梅杰首相和其他几位军情五处高官的电话号码，并把这些号码公布在互联网上。

美国一名14岁少年通过互联网闯入我国中科院网络中心和清华大学的主机，并向系统管理员提出警告

。1998年，国内各大网络几乎都不同程度地遭到黑客的攻击，8月，印尼事件激起中国黑客集体入侵印尼网点，造成印尼多个网站瘫痪。

与此同时，国内部分站点遭到印尼黑客的报复。

同年，美国国防部宣称黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”，打入了政府许多非保密性的敏感计算机网络，查询并修改了工资报表和人员数据。

## <<计算机网络安全与防护>>

### 编辑推荐

《计算机网络安全与防护(第2版)》：普通高等教育“十一五”国家级规划教材,总参通信部精品课程教材。

<<计算机网络安全与防护>>

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>