

<<网络安全与管理>>

图书基本信息

书名：<<网络安全与管理>>

13位ISBN编号：9787811237436

10位ISBN编号：7811237431

出版时间：2010-10

出版时间：陈红松 清华大学出版社，北京交通大学出版社（2010-10出版）

作者：陈红松

页数：308

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>

## &lt;&lt;网络安全与管理&gt;&gt;

## 前言

随着计算机和网络通信技术的快速发展,网络的开放性、互连性、共享程度的提高,来自外部的黑客攻击和内部的威胁使网络安全及管理问题日益突出,网络安全正面临重大挑战。

本书首先介绍了网络安全与管理的基本概念、产生背景、特点及设计原则,从系统工程的角度介绍了网络安全管理的体系结构,分析了构建网络安全管理体系的必要性,注重各安全技术之间的相互作用与联系;从网络攻击技术出发,逐层次介绍了网络安全与管理的相关技术理论与标准规范。

本书紧密结合当前网络信息安全领域的发展动态,体现学科前沿和研究成果,并且注重一定的实践性和创新性,每章后面都有相应习题供学生总结和复习所学知识,兼顾知识体系的完整性与系统性,本书很多内容来自编者的科研工程项目及课堂教学实践。

本书共分13章。

第1章介绍网络安全与管理的基本概念、产生背景、特点及设计原则;第2章介绍网络安全与管理的体系规范与标准;第3章介绍网络攻击的概念,网络风险的识别与安全评估方法;第4章介绍网络安全的密码学基础;第5章介绍网络安全所涉及的身份认证技术与相关协议;第6章介绍防火墙的概念与原理、指标与选型、发展趋势等;第7章介绍虚拟专用网的关键技术及发展趋势,其中包括基于不同协议的VPN技术等;第8章介绍入侵检测与防护系统的关键技术以及蜜罐蜜网技术等;第9章介绍了面向内容的网络安全监控技术,并给出了论坛类网站内容安全监控模型;第10章介绍了电子商务中的安全机制及安全电子商务协议;第11章介绍了无线网络安全技术,包括移动Adhoc网络及无线传感器网络的安全机制;第12章介绍了网络管理原理及技术,包括SNMP / OSI网络管理框架以及新型网络管理模型;第13章介绍了网络信息安全的法律法规体系及国内外网络安全立法框架。

本书既可作为高等院校信息安全、计算机等相关专业的本科生和研究生相关课程的教材,也可作为网络安全管理工程技术人员的参考书。

## <<网络安全与管理>>

### 内容概要

《网络安全与管理》介绍计算机网络安全与管理技术，是面向信息安全与计算机专业的教材。

《网络安全与管理》首先从整体上介绍了网络安全与管理的基本概念、产生背景、特点及设计原则，从系统工程的角度介绍了网络安全管理的体系结构。

从网络攻击技术出发，逐层次介绍了网络安全与管理的相关技术理论与标准规范。

《网络安全与管理》共分13章，内容包括网络安全与管理概述、相关规范、网络攻击与安全评估、网络安全的密码学基础、身份认证与网络安全、防火墙技术、vpn技术、入侵检测技术、面向内容的网络信息安全、电子商务安全、无线网络安全技术、网络管理原理与技术及网络信息安全的法律法规体系。

《网络安全与管理》既可作为高等院校信息安全、计算机等相关专业的本科生和研究生相关课程的教材，也可作为网络安全管理工程技术人员的参考书。

## 书籍目录

第1章 网络安全与管理概述与规划1.1 网络安全与管理概述1.1.1 网络安全与管理的基本概念1.1.2 网络安全与管理的定义1.1.3 网络安全与管理的基本属性1.2 网络安全与管理问题的产生背景1.2.1 网络安全问题是国际性问题1.2.2 网络安全问题的根源1.2.3 网络安全威胁的发展趋势1.2.4 我国网络安全与管理现状1.2.5 网络安全管理的必要性1.3 网络安全与管理的特点及设计原则1.3.1 网络安全与管理的特点1.3.2 网络安全管理的设计原则1.3.3 信息安全管理的原则1.4 网络安全管理设计规划与实施案例1.4.1 网络安全系统的设计规划步骤1.4.2 银行系统网络安全设计与实施案例小结习题第2章 网络安全与管理的体系规范2.1 网络安全防范体系2.2 开放系统互联安全体系结构2.2.1 安全服务2.2.2 特定的安全机制2.2.3 普遍性安全机制2.2.4 安全管理2.3 Internet网络安全体系结构2.3.1 IPSEC安全协议2.3.2 SSL安全协议2.4 信息保障技术框架2.5 ISO / IEC18028-2网络安全框架2.6 Bs7799信息安全管理规范小结习题第3章 网络攻击与安全评估3.1 网络攻击的概念及分类3.1.1 网络攻击的基本概念3.1.2 网络攻击的分类3.2 计算机及网络的漏洞分析3.2.1 漏洞的基本概念及分类3.2.2 网络漏洞3.2.3 漏洞分级3.2.4 漏洞的发现3.3 网络脆弱性的评估技术3.3.1 网络脆弱性的概念3.3.2 网络脆弱性的评估3.3.3 评估网络脆弱性的准则3.4 信息系统安全风险的概念与评估3.4.1 风险的基本概念3.4.2 信息系统安全风险的概念3.4.3 信息安全风险评估3.4.4 风险评估指标体系的设计原则3.5 网络与信息安全的风险管理3.5.1 网络风险管理3.5.2 信息安全风险管理小结习题第4章 网络安全的密码学基础4.1 密码学概述4.1.1 密码学起源及发展阶段4.1.2 密码学的基本概念4.2 密码系统的设计与分析4.2.1 密码系统的设计原则4.2.2 密码分析的概念与方法4.3 对称密码体制4.3.1 对称密码体制的基本概念4.3.2 对称密码体制的分类4.3.3 DES密码算法分析4.4 公钥密码体制4.4.1 公钥密码体制的基本概念4.4.2 公钥密码体制的特点及应用4.4.3 RSA密码算法分析4.5 散列函数4.5.1 散列函数的基本概念4.5.2 散列函数的构造方法4.5.3 散列函数的密码分析4.6 数字签名4.6.1 数字签名的基本概念4.6.2 常用的数字签名算法简介4.6.3 数字签名的系统描述4.6.4 数字签名及验证过程4.6.5 数字签名的分类4.6.6 RSA数字签名算法4.7 密钥管理4.7.1 密钥管理的基本概念4.7.2 密钥的使用阶段4.7.3 密钥的有效期4.7.4 密钥托管4.8 密码学与安全协议4.8.1 安全协议的基本概念4.8.2 安全协议的安全性质4.8.3 安全协议的缺陷分析4.8.4 安全协议的分析4.9 密码学在网络安全中的应用4.9.1 认证的应用4.9.2 电子邮件安全4.9.3 IP层安全4.9.4 Web安全小结习题第5章 身份认证与网络安全5.1 身份认证技术5.1.1 身份认证技术简介5.1.2 身份认证系统的特征5.1.3 用户身份认证的分类5.2 基于口令的身份认证5.2.1 口令的存储5.2.2 口令机制5.2.3 对口令协议的基本攻击5.2.4 口令认证的安全性5.3 双因素认证技术5.3.1 双因素认证原理5.3.2 动态口令的产生5.3.3 客户端软件代理5.3.4 管理服务器5.3.5 双因素身份验证系统的几个要点5.4 基于x.509证书的身份认证5.4.1 X.509证书的格式及含义5.4.2 基于X.509证书的双向认证过程5.5 安全认证协议5.5.1 NS认证协议5.5.2 Kerberos认证协议5.5.3 PAP认证协议5.5.4 CHAP认证协议5.5.5 RADIUS认证协议5.6 UsbKey身份认证5.6.1 UsbKey身份认证的原理5.6.2 UsbKey身份认证的特点5.7 基于生物特征的身份认证5.7.1 基于生物特征的认证方式5.7.2 与传统身份认证技术的比较5.8 零知识认证技术5.8.1 零知识证明5.8.2 零知识身份认证协议5.9 身份认证与授权管理小结习题第6章 防火墙技术6.1 防火墙的概念与原理6.1.1 防火墙的基本概念及工作原理6.1.2 防火墙的发展历程6.1.3 防火墙的主要功能6.1.4 防火墙的局限性6.2 防火墙的分类6.2.1 按软硬件的实现形态分类6.2.2 按防火墙的实现技术分类6.2.3 按防火墙结构分类6.2.4 按防火墙的应用部署位置分类6.2.5 按防火墙性能分类.....第7章 虚拟专用网技术 7.1 vpn概述 7.2 vpn的分类 7.3 vpn的设计 7.4 vpn的安全性分析 7.5 基于pptp / l2tp的vpn技术 7.6 基于ipsec的vpn技术 7.7 基于ssl的vpn技术 7.8 基于mpls的vpn技术 小结 习题 第8章 入侵检测技术 8.1 入侵检测概述 8.2 入侵检测系统的分类 8.3 入侵检测系统的部署 8.4 入侵检测系统的关键技术 8.5 入侵检测系统的标准化 8.6 入侵防护 8.7 蜜罐与蜜网技术 8.8 snort简介 小结 习题 第9章 面向内容的网络信息安全 9.1 网络内容安全的概念与意义 9.2 网络内容安全监控的功能 9.3 网络信息内容安全监测的关键技术 9.4 面向内容的网络安全监控模型 9.5 网络内容安全中的数据挖掘与知识发现 9.6 论坛类网站内容安全监控模型 小结 习题 第10章 电子商务安全 10.1 安全电子商务概述 10.2 电子商务中的安全机制 10.3 电子商务的支付系统 10.4 set协议 10.5 ssl协议 小结 习题 第11章 无线网络安全技术 11.1 无线网络概述 11.2 无线网络安全概述 11.3 无线局域网安全技术 11.4 无线移动网络安全技术 11.5 无线adhoc网络的安全技术 11.6 传感器网络的安全技术 小结 习题 第12章 网络管理原理与技术 12.1 网络管理原理及技术概论 12.2 snmp网络管理框架

12.3 osi网络管理框架 12.4 电信管理网 12.5 新型网络管理模型 12.6 cmip、snmp和corba的安全性比较 小结 习题 第13章 网络信息安全的法律法规体系 13.1 网络信息安全法制建设的必要性 13.2 网络信息安全法律的特点 13.3 国外网络安全立法分析 13.4 我国网络安全立法体系框架 13.5 网络安全相关法律法规的制定与分析 小结 习题 参考文献

## 章节摘录

插图：5.可控性可控性是对网络信息的传播及内容具有控制能力的特性。

概括地说，网络信息安全与保密的核心，是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储消息的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等。后来，美国计算机安全专家又在CIA安全三要素的基础上提出了一种新的安全框架，包括保密性、完整性、可用性、真实性（Authenticity）、实用性（Utility）、占有性（Possession），即在原来的基础上增加了真实性、实用性、占有性，认为这样才能解释各种网络安全问题。

网络信息的真实性是指信息的可信度，主要是指信息的完整性、准确性和对信息所有者或发送者身份的确认，它也是一个信息安全性的基本要素。

网络信息的实用性是指信息加密密钥不可丢失（不是泄密），丢失了密钥的信息也就丢失了信息的实用性。

占有性是指存储信息的主机、磁盘等信息载体被盗用，导致对信息占用权的丧失。

保护信息占有性的方法有使用版权、专利、商业秘密、提供物理和逻辑的访问限制方法，以及维护和检查有关盗窃文件的审计记录、使用标签等。

1.2 网络安全与管理问题的产生背景网络安全已经成为人类共同面临的挑战，我国网络安全问题日益突出，互联网向社会控管能力的挑战已经成为信息时代政治、经济、军事、文化斗争的新领域。

本节将主要介绍网络安全的国际性问题、产生根源、发展趋势、特点及必要性。

1.2.1 网络安全问题是国际性问题由于网络建立开始只考虑方便性、开放性，并没有考虑总体安全构架，因此开放性的网络导致网络的技术是全开放的，任何一个人或者团体都可能接入，因而网络所面临的破坏和攻击可能是多方面的。

正如一句非常经典的话：“Internet的美妙之处在于你和每个人都能互相连接，Internet的可怕之处在于每个人都能和你互相连接。

”网络安全成为信息时代人类共同面临的挑战，美国前总统克林顿在签发《保护信息系统国家计划》的总统咨文中陈述道：“在不到一代人的时间里，信息革命以及计算机进入了社会的每一领域，这一现象改变了国家的经济运行和安全运作乃至人们的日常生活方式，然而，这种美好的新时代也带有它自身的风险。

所有计算机驱动的系统都很容易受到侵犯和破坏。

对重要的经济部门或政府机构的计算机进行任何有计划的攻击都可能产生灾难性的后果，这种危险是客观存在的。

过去敌对力量和恐怖主义分子毫无例外地使用炸弹和子弹，现在他们可以把手提电脑变成有效武器，造成非常巨大的危害。

如果人们想要继续享受信息时代的种种好处，继续使国家安全和经济繁荣得到保障就必须保护计算机控制系统。

使它们免受攻击。

”

<<网络安全与管理>>

编辑推荐

《网络安全与管理》：高等学校信息安全类专业系列教材。

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>