# <<计算机网络安全管理>>

## 图书基本信息

书名：<<计算机网络安全管理>>

13位ISBN编号：9787115219640

10位ISBN编号：7115219648

出版时间：2010-3

出版时间：人民邮电出版社

作者：王群 编著

页数：290

## 前言

随着计算机网络技术的快速发展及应用的逐渐普及，信息化已经成为推动社会发展的重要手段。
实现信息化的基础设施是计算机网络，但是由于计算机网络具有连接形式的多样性、网络系统的开放性、终端接入的任意性、用户身份的弱认证性等特征，致使网络易受黑客、病毒和其他恶意程序的攻击，信息的安全和保密成为一个至关重要的问题。
“计算机网络安全管理”以计算机网络为基础和环境，以管理为手段，以安全为目标。
网络安全与网络管理虽然在研究方法和研究内容上存在侧重点不同，但两者的实现目标是相同的，实现方法和过程是交叉的，安全离不开管理，管理的目标之一是安全。
基于这一思想，本书将网络安全与网络管理两方面的内容从知识组织、实现方法、应用特点等方面进行了有机结合，实现了在安全中融入管理，在管理中实现安全。
这一思想也符合目前计算机网络的应用现状和管理趋势。
随着网络安全在实际工作中的重要性日益凸显，目前各高职高专院校也将网络安全管理课程作为网络专业的核心课程。
本书是作者在总结了多年网络课程的教学经验和网络管理工作的基础上编写的，在内容安排上本书强调了以下3点：一是从信息安全与网络安全的关系人手，介绍了信息安全和网络安全的概念及联系，分析了网络安全所面临的主要威胁，并提出了相应的解决方法。
综合目前网络应用，提出了网络安全的发展趋势。
通过这一部分内容的学习，使读者对网络安全的概念、现状及未来发展有一个总体宏观的认识。

# <<计算机网络安全管理>>

## 内容概要

本书从信息安全与网络安全的关系入手，在介绍了信息安全和网络安全的概念及联系、网络安全所面临的主要威胁和解决方法、网络安全的发展趋势等基础知识后，重点从物理安全、计算机病毒及防范、防火墙技术与应用、入侵检测与黑客攻击防范、数据加密技术及应用、VPN技术与应用、无线网络安全、计算机网络管理等方面，系统介绍了相关技术的概念、简要工作原理、使用方法和应用特点。

同时，为便于教学工作的开展，介绍了网络安全实验环境的组建方式，并结合一个具体的网络实例，分析了安全管理方案的设计和部署方法。

本书可作为高职高专计算机系“网络安全管理”及相关课程的教材，也可作为广大计算机应用工程技术人员、网络管理人员的参考书。

# <<计算机网络安全管理>>

## 书籍目录

第1章　计算机网络安全管理技术概述　1.1　信息安全与网络安全　1.1.1　信息安全　1.1.2　网络安全　1.1.3　信息安全与网络安全之间的关系 1.2　计算机网络安全威胁　1.2.1　安全威胁及相关概念　1.2.2　典型安全威胁介绍 1.3　计算机网络安全管理需求分析　1.3.1　物理安全　1.3.2　安全隔离　1.3.3　访问控制　1.3.4　加密通道　1.3.5　入侵检测　1.3.6　入侵保护　1.3.7　安全扫描　1.3.8　蜜罐　1.3.9　物理隔离　1.3.10　灾难恢复和备份 1.4　计算机网络安全管理的法律法规　1.4.1　计算机网络安全管理中的法律问题　1.4.2　我国立法情况　1.4.3 国外立法情况 1.5　计算机网络安全管理的发展方向　1.5.1　针对网络协议漏洞的攻击越来越频繁　1.5.2　不合理的软件设计所造成的影响越来越大　1.5.3　网络攻击的利益化趋势越来越突出　1.5.4　计算机网络管理中的互动性越来越明显 本章小结 习题第2章　实验环境组建及协议分析 2.1　计算机网络安全管理模拟实验环境的组建　2.1.1　VMware Workstation的基本配置　2.1.2　在虚拟机上安装操作系统　2.1.3　VMware Workstation中主要网络功能的配置 2.2　协议分析软件的使用方法　2.2.1　Sniffer Pro的安装及基本功能介绍　2.2.2　操作实例：捕获某一台主机的数据包　2.2.3　操作实例：捕获网络用户账户信息 本章小结 习题第3章　物理安全　3.1　物理安全概述　3.1.1　物理安全的概念　3.1.2　物理安全的主要内容 3.2　物理隔离　3.2.1　物理隔离的概念　3.2.2 “ 双机双网 ”物理隔离方案　3.2.3 “ 一机双网 ”物理隔离方案　……第4章　计算机病毒及其防治方法第5章　防火墙技术及应用第6章　入侵检测与防黑客攻击技术第7章　数据加密技术及其应用第8章　VPN技术及其应用第9章　无线网络安全第10章　网络管理技术第11章　安全管理方案设计和实施

## 章节摘录

插图：访问是使信息在不同设备之间流动的一种交互方式。
访问控制决定了谁能够访问系统，能访问系统的何种资源以及如何使用这些资源。
适当的访问控制能够阻止未经允许的用户有意或无意地获取数据。
访问控制的段包括用户识别代码、口令、登录控制、资源授权（例如用户配置文件、资源配置文件和控制列表）、授权核查、日志和审计。
访问控制主要是通过防火墙、交换机或路由器的使用来实现的。
防火墙是实现网络安全最基本、最经济、最有效的安全措施之一，通过制定严格的安全策略，防火墙可以对内外网络或内部网络不同信任域之间进行隔离，使所有经过防火墙的网络通信接受设定的访问控制。
此外，通过防火墙提供的NAT功能，也可以起到网段隔离的作用（主要是局域网与广域网之间）。
另外，随着微电子技术的发展，交换机和路由器的数据处理和存储能力得到了提高。
为此，目前许多设备已集成了原来多个设备所提供的功能。
例如.现在的绝大多数防火墙已提供了原来路由器才具有的ACL（Access Control List，访问控制列表）、（Network Address Translation，网络地址转换）等功能。
同时，在一些路由器上也提供了原本由防火墙才具有的访问控制功能。

# <<计算机网络安全管理>>

## 编辑推荐

《计算机网络安全管理》：随着计算机网络技术的快速发展及应用的逐渐普及，信息化已经成为推动社会发展的重要手段。
实现信息化的基础设施是计算机网络，但是由于计算机网络具有连接形式的多样性、网络系统的开放性、终端接入的任意性、用户身份的弱认证性等特征，致使网络易受黑客、病毒和其他恶意程序的攻击，信息的安全和保密成为一个至关重要的问题。
《计算机网络安全管理》通过将网络安全与网络管理两方面的内容从知识组织、实现方法、应用特点等方面的有机结合，实现了在安全中融入管理，在管理中实现安全。
这一思想也符合目前计算机网络的应用现状和管理趋势。
基础知识与基本应用讲解浅显易懂实训操作与基本原理介绍融会贯穿教学内容与应用需求衔接有机结合

# <<计算机网络安全管理>>

## 版权说明