

<<网络安全>>

图书基本信息

书名：<<网络安全>>

13位ISBN编号：9787030270177

10位ISBN编号：7030270177

出版时间：2010-4

出版时间：科学出版社

作者：刘天华，孙阳，朱宏峰 编著

页数：344

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>

<<网络安全>>

前言

计算机网络就像一把双刃剑，它在实现信息交流与共享，极大便利和丰富社会生活的同时，由于网络本身的脆弱性加上人为攻击与破坏，因此而产生的计算机网络安全问题是各国政府有关部门、各大行业以及每个计算机用户都十分关注的重要问题。

在高等院校，对计算机专业以及相关专业的学生需要开设计算机网络安全技术课程，普及计算机网络安全知识，提高我国的计算机网络安全技术水平，保护我国信息的安全。

为了适应当前计算机网络安全技术发展的需要，解决实际计算机网络中存在的安全问题，更好地培养高素质的计算机网络安全人才，增强技术人员的实践能力，我们编写了这本书。

本书经过作者多年的教学实践与科研经验，内容结构逻辑性强，关注各个环节的安全问题，涵盖了计算机网络安全需要的多方面的基础理论和实践技术。

本书以学以致用为原则，从工程应用的角度出发，注重知识的实用性，将理论与实际相结合，在全面介绍计算机网络安全理论的基础上，充分阐述了网络安全的相关技术，选取典型网络安全问题进行方案设计，使读者在系统把握网络安全技术的基础上，正确有效地运用网络安全技术解决实际问题。

本书最突出的特点就是应用性强，在网络安全技术相关的章节后面，都有一个针对本章内容的典型项目方案设计，这个方案设计综合了相关技术知识，可在工程应用中进行灵活运用。

本书结构可分为3个部分。

第1部分：基础篇（第1~5章），介绍了网络安全的技术基础。

这部分内容对计算机网络安全的范畴进行总体把握，注重基础知识的阐述，主要突出计算机网络的和管理和技术两个方面，其中技术侧重于加强安全系统的自我完善，预防安全问题的发生。

第2部分：应用篇（第6~11章），介绍了网络安全技术。

这部分内容对计算机网络安全涉及的技术进行全面介绍，关注工程上应用广泛的网络技术及其可能遇到的安全问题，侧重于提高安全系统的被动防御和主动防御能力，阻止安全问题的发生。

第3部分：设计篇（第12~13章），介绍了网络安全检测与评估技术以及网络安全系统的设计。

这部分内容给出了对具体计算机网络安全问题进行检测与评估的相关技术，以便对具体计算机网络进行分析，将结果作为反馈信息，进一步完善和提高网络的安全性，达到设计更安全的系统的目的。

本书具有教材和技术资料的双重特征，既可作为计算机相关专业的本科生教材，也可作为信息管理与信息系统相关专业的参考书，亦可供安全管理人员参考使用。

阅读本书之前需要具备操作系统、数据库系统和计算机网络技术的预备知识，主要包括常用的操作系统的配置、关系数据库管理系统的管理、计算机网络应用层协议的实现等。

<<网络安全>>

内容概要

本书以构建计算机网络安全体系为框架，全面介绍了网络安全的基本概念、网络安全体系结构以及网络安全管理的各项内容和任务。

全书共13章，内容涵盖了网络安全的概念、网络安全体系结构、网络实体安全、网络安全协议、密码与认证技术、操作系统与数据库安全、应用系统安全、访问控制与VPN技术、防火墙与隔离网闸技术、入侵检测技术、计算机病毒与恶意代码防范技术、网络安全检测与评估技术等。

本书注重知识的实用性，将理论与实际相结合，在全面介绍计算机网络安全理论的基础上，充分阐述了网络安全的相关技术，选取典型网络安全问题进行方案设计，使读者在系统把握网络安全技术的基础上，正确有效地运用网络安全技术解决实际问题。

本书可作为计算机相关专业的本科生教材，或信息管理与信息系统相关专业的参考书，也可作为安全管理人员、网络与信息系统管理人员、IT咨询顾问与IT技术人员的参考手册和培训教材。

<<网络安全>>

书籍目录

第1章 网络安全概述 1.1 计算机网络安全的概念 1.1.1 计算机网络安全的定义 1.1.2 计算机网络安全
的含义 1.1.3 计算机网络安全的主要内容 1.2 计算机网络面临的主要威胁 1.2.1
网络实体威胁 1.2.2 网络系统威胁 1.2.3 恶意程序威胁 1.2.4 网络的其他威胁
1.2.5 影响网络安全的因素 1.3 计算机网络安全的3个层次 1.3.1 安全立法 1.3.2 安全管
理 1.3.3 安全技术措施 1.4 计算机网络安全的法律和法规 1.4.1 国外的相关法律和法规
1.4.2 我国的相关法律和法规 1.5 小结 1.6 习题第2章 网络安全体系结构 2.1 安全模型
2.1.1 P2DR模型 2.1.2 PDRR模型 2.2 网络安全体系结构 2.2.1 Internet网络体系层次结
构 2.2.2 网络安全体系结构框架 2.3 安全策略与运行生命周期 2.3.1 安全策略定义
2.3.2 安全系统的开发与运行 2.3.3 安全系统的生命周期 2.4 小结 2.5 习题第3章 网络
实体安全 3.1 计算机网络机房与环境安全 3.1.1 机房的安全等级 3.1.2 机房的安全保护
3.1.3 机房的三度要求 3.1.4 机房的电磁干扰防护 3.1.5 机房接地保护与静电保护
3.1.6 机房电源系统 3.1.7 机房的防火、防水与防盗 3.2 计算机网络机房存储介质防护 3.3
安全管理 3.3.1 安全管理的定义 3.3.2 安全管理的原则与规范 3.3.3 安全管理的主要
内容 3.3.4 健全管理机构 and 规章制度 3.4 机房设计依据的规范标准 3.5 小结 3.6 习题第4
章 网络安全协议 4.1 数据链路层安全通信协议 4.1.1 PPP协议 4.1.2 PPTP协议 4.1.3
L2TP协议 4.2 网络层安全通信协议 4.3 传输层安全通信协议 4.3.1 SSL / TLS协议簇
4.3.2 SSL / TLS应用.....第5章 密码与认证技术第6章 操作系统与数据库安全 第7章 应用系统
安全 第8章 访问控制与VPN技术第9章 防火墙与隔离网闸第10章 入侵检测技术第11章 计算机
病毒、恶意代码及防范第12章 网络安全检测与评估技术第13章 网络安全方案设计附录 国际及国
家网络安全相关标准参考文献

章节摘录

插图：Internet的广泛应用使人们在生产方式、生活方式及思想观念等方面都发生了巨大变化，推动了人类社会的发展和人类文明的进步，把人类带入了崭新的信息化时代。

计算机网络就像一把双刃剑，它在实现信息交流与共享、为人们带来极大便利和丰富社会生活的同时，由于网络本身的脆弱性加上人为攻击与破坏，也对国家安全、社会公共利益以及公民个人合法权益造成了现实危害和潜在威胁。

因此，加强对信息网络安全技术和管理的研究，无论是对个人还是组织、机构，甚至国家、政府都有非同寻常的重要意义。

1.1 计算机网络安全的概念1.1.1 计算机网络安全的定义安全是指不发生意外事故，不出现意外情况。

从这个角度来说，计算机网络安全是指为了使计算机网络运行正常，通过采用全方位的管理措施和强有力的技术手段，保证在一个网络环境里，使经过计算机网络的数据具有机密性、完整性和可用性。

国际标准化组织（ISO）将计算机安全定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。

”美国国防部国家计算机安全中心将计算机安全定义为：“一般说来，安全的系统会利用一些专门的安全特性来控制对信息的访问，只有经过适当授权的人，或者以这些人的名义进行的进程可以读、写、创建和删除这些信息。

”我国公安部计算机管理监察司将计算机安全定义为：“计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害。

”上面是狭义的计算机网络安全的内容。

广义上讲，凡是涉及网络上信息的机密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络信息安全所要研究的领域。

广义的计算机网络安全还应该包括网络实体安全，如机房的安全保护、防火措施、防水措施、静电防护、电源系统保护等。

1.1.2 计算机网络安全的含义计算机网络安全是一门综合性学科，涉及计算机科学、网络技术、通信技术、密码与认证技术等多个领域的知识。

<<网络安全>>

编辑推荐

《网络安全》：以学以致用为原则，从工程应用的角度出发，注重知识的实用性，理论与实际相结合详细介绍计算机网络安全理论的基础，充分阐述网络安全的相关技术，选取典型网络安全问题进行方案设计在网络安全技术章节，都有一个针对该章内容的典型项目方案设计，可在实际工程中灵活运用
适用对象·高等院校计算机、信息安全、信息管理与系统等相关专业·安全管理人员、网络与信息系
统管理人员·IT咨询顾问与技术人员·计算机培训学校

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>