<<计算机网络安全技术>>

图书基本信息

书名：<<计算机网络安全技术>>

13位ISBN编号：9787302177784

10位ISBN编号：7302177783

出版时间：2008-8

出版时间：清华大学出版社

作者：王群 编著

页数：291

前言

如今，计算机网络的应用已延伸到全球的各个角落和领域，正在对人们的工作、生活产生前所未有的影响，如同电力、交通一样日益成为人们生活中不可缺少的组成部分。
与此同时，随着网络规模的不断扩大，以及人们对网络知识的了解越来越深入，网络中的攻击等不安全因素越来越多，已经严重威胁到网络与信息的安全。
计算机网络的安全已经成为一个备受全球关注的问题。
计算机网络与信息安全技术的核心问题是对计算机和网络系统进行有效的防护。
网络安全防护涉及的面非常广，从技术层面上分，主要包括数据加密、身份认证、入侵检测、入侵保护、病毒防护和虚拟专用网等方面，这些技术中有些是主动防御，有些是被动保护，有些则是为安全研究提供支撑和平台。
本书在写作过程中强调了以下几点。
一是尽可能用通俗易懂的语言来描述晦涩的理论阐述。
在计算机网络安全这门课程中涉及到了大量的概念、理论体系、算法和协议，如何用通俗易懂的语言来描述这些抽象的专业术语是本书的一个侧重点。
为此，在写作过程中作者尽可能用简捷明快的语言来阐述理论，而不是照搬文献和标准文档。
二是通过大量直观的图例来描述复杂的工作原理和操作流程。
在一些国家的计算机专业教育中，有图解（diagram）或映像（map）这门课，旨在通过易于理解的图例来直观地描述网络的结构、工作流程及实现原理。
本书在写作过程中采用了大量的图例和表格来描述复杂的网络安全实现原理。
三是理论与实践的有机结合。
理论与实践之间的脱节是目前许多计算机专业教材普遍存在的问题，有些教材过于强调理论阐述而忽视实践操作，而有些图书则只注重讲述操作步骤而忽视了理论讲解。
本书一方面强调对基本概念、理论、算法和协议的讲解，同时尽可能地通过实际操作来验证相关的理论。
四是内容新颖翔实。
计算机网络技术的发展非常迅速，为了使学生在走出校门后能够将所学知识应用到具体工作中，在教材内容的选择上必须考虑到与实际应用之间的有机结合。
本书在写作过程中参阅了大量的研究成果和文献资料，以求内容新颖，讲解翔实。
五是注重内容讲解时的完整性。
网络安全涉及的面较广，许多应用的实现需要大量理论的支持。
本书在写作过程中充分考虑到内容完整性，对所涉及到的但在本书中没有单独讲述的内容进行了实时介绍或给出了文献出处，以便读者查阅。
本书共分为9章，主要内容包括计算机网络安全概述、数据加密技术及应用、PKI／PMI技术及应用、身份认证技术、TCP／IP体系的协议安全、计算机病毒、木马和间谍软件与防治、网络攻击与防范、防火墙技术及应用和VPN技术及应用等内容。

<<计算机网络安全技术>>

内容概要

本书是一本面向普通高等院校本科教学要求的教材，是理论与实践有机结合的研究成果，也是作者长期从事计算机网络教学、网络安全设计、网络管理与维护的经验总结。
为了使内容安排符合教学要求，并尽可能地贴近实际应用，解决实际问题，本书在内容选择上既注重基本理论和概念的讲述，又紧紧抓住目前网络安全领域的关键技术和用户普遍关注的热点问题，对内容进行了合理规划。
本书共分9章，主要内容包括计算机网络安全概述、数据加密技术及应用、PKI/PMI技术及应用、身份认证技术、TCP/IP体系的协议安全、计算机病毒、木马和间谍软件与防治、网络攻击与防范、防火墙技术及应用、VPN技术及应用等。
本书主要针对普通高等院校计算机及相关专业本科层次的教学要求而编写，其中大量的实训内容可供高职高专和有关培训机构使用，本书也可供从事网络安全设计和管理的技术人员阅读、参考。

<<计算机网络安全技术>>

书籍目录

章节摘录

插图：今天，IP网络几乎成为现代计算机网络的代名词。
IP网络存在的设计缺陷和安全隐患也逐渐暴露出来。
随着计算机网络应用范围的不断扩展，大量基于IP网络的应用层出不穷，这更加剧了网络的负担，安全问题越加突出。
本章将从网络安全概念、安全现状、安全策略和热点技术等方面，对计算机网络的安全进行综述性介绍。
1.1 计算机网络安全研究的动因现在广泛使用的基于IPv4通信协议的网络，在设计之初就存在着大量缺陷和安全隐患。
虽然下一个版本IPv6在一定程度上解决1Pv4中存在的安全问题，但是IPv6走向全面应用还需要较长的时间。
从IPv4网络的应用历史来看，许多安全问题也是随着应用的出现而暴露出来的，所以不能肯定地讲IPv6网络的应用就一定能够解决IPv4中存在的所有安全问题。
1.1.1 网络自身的设计缺陷如果对比分析PSTN、ATM和FR等网络技术，就会发现IP网络在设计上存在的不足或缺陷。
TCP/IP通信协议自20世纪60年代末诞生以来，已经历了30多年的实践检验，并成为Internet的基础。
TCP/IP通信协议的不断发展和完善促进了Internet的发展，同时Internet的发展又进一步扩大了T'CP/IP通信协议的影响。
目前，几乎所有厂商的网络产品都支持TCP/IP，如硬件厂商Cisco、IMB等，数据库0racle等，操作系统Netware等。
虽然TCP/IP取得了巨大的成功，但其存在的设计缺陷不可回避。
分析目前广泛使用的IPv4协议，在应用中主要存在以下的安全问题。
　1.协议本身的不安全性例如，在TCP/IP参考模型的传输层提供了TcP和UDP两种协议（2000年提出了SCTP协议，即流控制传输协议），其中UDP本身就是一种不可靠、不安全的协议，而TCP当初力求通过三次握手机制保障数据传输的可靠性和安全性，但近年来利用Tcp/1P三次握手出现的网络攻击现象频繁发生。
再如，目前在局域网中泛滥的ARP欺骗和DHCP欺骗，其根源是这些协议在当初设计时只考虑到了应用，而没有或很少考虑安全。
还有，如DNS、POP3、SMTP和SNMP等应用层的协议几乎都存在安全隐患。

编辑推荐

《计算机网络安全技术》的特色：教学目标明确，注重理论与实践的结合；教学方法灵活，培养学生自主学习的能力；教学内容先进，反映了计算机学科的最新发展；教学模式完善，提供配套的教学资源解决方案。

<<计算机网络安全技术>>

版权说明