<<计算机网络安全>>

图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787302203971

10位ISBN编号：7302203970

出版时间：2009-9

出版时间：清华大学出版社

作者：沈鑫剡

页数：287

前言

目前计算机网络安全教材是百花齐放，各有特色，但总体上可以分成三类，第一类着重讨论加密、认证算法及其他安全协议，这一类教材的特点是比较详细地讲述网络安全理论，尤其对各种算法和协议做了深入讨论，但缺乏和当前主流安全技术的结合，很难让读者学以致用。
第二类主要讨论黑客攻击手段和防御技巧，这一类教材不介绍系统、完整的网络安全理论，有点像黑客攻防大全。
第三类把操作系统安全机制、应用程序安全机制和网络安全机制放在一起讨论，当然，所有内容都是浅尝辄止。
这三类教材虽然侧重点不同，但有着同样的问题，一是不对当前主流网络安全技术进行深入讨论，二是不在具体网络环境下讨论安全网络的设计方法和过程，对许多问题只是空对空地介绍一些基本概念和方法，没有具体结合目前面临的网络安全问题。
因此，难以培养读者解决网络安全问题的实际能力。
对于一本真正以实现将读者领进计算机网络安全知识殿堂为教学目标的教材，一是必须提供完整、系统的网络安全理论，这样才能让读者理解网络安全技术的实现机制，具有进一步研究网络安全技术的能力。
二是必须深入讨论当前主流网络安全技术，同时，结合网络安全理论讨论这些安全技术的实现原理，让读者知其所以然，也让读者具备用主流网络安全技术解决实际网络安全问题的能力。
三是需要在具体网络环境下讨论运用网络安全技术设计安全网络的方法和过程，给读者提供解决实际网络安全问题的方法和思路，解决读者学以致用的问题。
作为计算机网络安全教材，应该着重讨论和网络有关的安全问题，与操作系统及应用程序有关的安全问题应该在《操作系统》和《算法与程序设计》课程中予以解决，因为离散地讨论一些安全问题会降低该教材的系统性和连贯性，同时，不和整个操作系统结构和程序设计环境结合来讨论操作系统和应用程序安全问题的解决机制，也不利于读者理解、掌握。
计算机网络安全教材不可避免地会涉及黑客攻击和防御，但必须从网络总体结构出发，讨论防御黑客攻击的技术，而不是逐个列出攻击手段和防御方法，将教材变成黑客攻防大全，背离了教材着重于基本理论、基本技术和基本方法的宗旨。
本教材的特色在于: 一是为读者提供完整、系统的网络安全理论；二是详细讨论当前主流网络安全技术，并结合网络安全理论讨论这些安全技术的实现原理；三是在实际网络环境下给出运用当前主流安全技术设计安全网络的方法和过程；四是通过构建防御黑客攻击的网络安全体系，讨论运用网络安全技术全方位防御黑客攻击的方法；五是通过门户网站这样的技术给出了精确控制网络资源访问过程的方法。
全书内容安排如下: 第1章概论，着重讨论了目前存在的安全问题、解决安全问题的基本方法和构建网络安全体系的必要性。
第2章黑客攻击机制，详细讨论了黑客攻击类型、主要攻击步骤及运用网络安全技术防御黑客攻击的基本思路。
第3章网络安全基础，详细讨论了加密算法、报文摘要算法、认证协议、IP Sec等网络安全基础理论。
第4章安全网络技术，详细讨论了几种广泛应用的网络安全技术及这些网络安全技术防御黑客攻击的机制。
第5章无线局域网安全技术，详细讨论了WEP安全机制及存在的安全缺陷，802.11i安全机制解决无线局域网通信安全的原理。
第6章虚拟专用网络，详细讨论了第2层和第3层隧道实现数据跨公共分组网络安全传输的方法和过程。
第7章防火墙，详细讨论了无状态分组过滤器、有状态分组过滤器及堡垒主机对网络资源访问过程实施严格控制的机制。
统一访问控制动态配置网络资源访问控制策略的机制。
第8章入侵防御系统，详细讨论了主机入侵防御系统和网络入侵防御系统防御黑客攻击的机制。
第9章网络管理和监测，详细讨论了网络管理系统的安全问题和解决方法，监测网络安全状态的机制

。
第10章安全网络设计实例，详细讨论了运用主流网络安全技术、防火墙、入侵防御系统、网络综合监测系统设计一个实现预定安全目标的安全网络的过程。
第11章应用层安全协议，详细讨论了Web安全机制、电子邮件安全传输协议和门户网站精致控制网络资源访问过程的机制。
在教材编写过程中，解放军理工大学工程兵工程学院计算机应用教研室的俞海英、伍红兵、胡勇强、魏涛和龙瑞对教材内容提出了许多很好的建议和意见，其他同事也给予了很多帮助和鼓励，在此向他们表示衷心的感谢。
作为一本无论在内容组织、叙述方法还是教学目标都和传统计算机网络安全教材有一定区别的新教材，错误和不足之处在所难免，殷切希望使用该教材的老师和学生批评指正，也殷切希望读者能够就教材内容和叙述方式提出宝贵建议和意见，以便进一步完善教材内容。

<<计算机网络安全>>

内容概要

这是一本既注重网络安全基础理论，又着眼培养读者解决网络安全问题能力的教材，书中详细讨论了加密算法、报文摘要算法、认证协议等网络安全基础理论，黑客攻击方法和过程，目前主流的网络安全技术，如以太网安全技术、安全路由、信息流管制、VPN、防火墙、入侵防御系统和安全无线局域网等，以及这些防御黑客攻击技术的原理和案例，安全网络的设计方法和过程，安全应用层协议及应用等。

本教材的最大特点是将计算机网络安全理论、目前主流网络安全技术和安全网络的设计过程有机地集成在一起。

让读者既能掌握完整、系统的计算机网络安全理论，又具备运用主流网络安全技术实现安全网络的设计能力。

本教材以通俗易懂、循序渐进的方式叙述网络安全知识，并通过大量的例子来加深读者对网络安全知识的理解，内容组织严谨、叙述方法新颖，是一本理想的计算机专业本科生的计算机网络安全教材，也可作为计算机专业研究生的计算机网络安全教材，对从事计算机网络安全工作的工程技术人员，也是一本非常好的参考书。

<<计算机网络安全>>

书籍目录

第1章 概述 1.1 信息安全和网络安全 1.1.1 信息处理时的安全问题 1.1.2 信息传输时的安全问题 1.1.3 电子交易时的安全问题 1.2 信息安全目标 1.2.1 适用性 1.2.2 保密性 1.2.3 完整性 1.2.4 不可抵赖性 1.2.5 可控制性 1.3 网络安全机制 1.3.1 加密、报文摘要算法和数字签名技术 1.3.2 接入控制和认证机制 1.3.3 分组检测和信息流管制机制 1.3.4 入侵防御机制 1.3.5 应用层安全机制 1.4 网络安全体系 1.4.1 TCP/IP体系结构 1.4.2 网络安全体系结构 习题第2章 黑客攻击机制 2.1 黑客攻击类型 2.1.1 非法访问 2.1.2 窃取和中继攻击 2.1.3 拒绝服务 2.1.4 恶意代码 2.2 黑客攻击过程 2.2.1 收集信息 2.2.2 侦察 2.2.3 攻击 2.3 黑客攻击实例 2.3.1 内部网络结构 2.3.2 非法接入 2.3.3 获取DNS服务器内容 2.3.4 拒绝服务攻击 2.3.5 非法访问 2.4 网络安全和抑制黑客攻击 2.4.1 消除网络安全漏洞 2.4.2 弥补操作系统和应用程序的安全漏洞 习题第3章 网络安全基础 3.1 加密算法 3.1.1 对称密钥加密算法 3.1.2 公开密钥加密算法 3.2 报文摘要算法 3.2.1 报文摘要算法要求 3.2.2 MD5 3.2.3 SHA-1 3.2.4 HMAC 3.3 数字签名 3.3.1 基于对称密钥算法的数字签名技术 3.3.2 基于公开密钥算法的数字签名技术 3.4 认证协议 3.4.1 Kerberos 3.4.2 TLS 3.4.3 EAP和802.1X 3.4.4 RADIUS 3.5 IPSec 3.5.1 安全关联 3.5.2 AH 3.5.3 ESP 3.5.4 ISAKMP 习题第4章 安全网络技术第5章 无线局域网安全技术第6章 虚拟专用网络第7章 防火墙第8章 入侵防御系统第9章 网络管理和监测第10章 安全网络设计实例第11章 应用层安全协议附录A 英文缩写词参考文献

章节摘录

插图：1.病毒病毒是一种具有自复制能力并会对系统造成巨大破坏的恶意代码，它首先隐藏在某个实用程序中，隐藏过程可以由实用程序设计者完成，或者通过病毒感染该实用程序的过程完成。
当某个计算机下载该实用程序并运行它时，将运行隐藏在其中的恶意代码，即病毒，病毒将感染其他文件，尤其是可执行文件，并接管一些系统常驻软件，如鼠标中断处理程序。
如果病毒接管了鼠标中断处理程序，当鼠标操作激发该中断处理程序时，将首先激发病毒程序，病毒程序可以再次感染其他文件，并视情况执行破坏操作，如清除所有硬盘中的文件。
当感染了病毒的实用程序被其他计算机复制并执行时，病毒将蔓延到该计算机。
对于单台计算机，病毒传播主要通过相互复制实用程序完成，对于接入网络的计算机，从服务器下载软件、下载主页、接收电子邮件等操作都有可能感染病毒。
接入网络的计算机一旦感染病毒，安全将不复存在，存储在计算机中的信息将随时有可能被破坏，机密信息将随时外泄，非授权用户随时有可能通过远程桌面这样的工具对计算机进行非法访问。
2.非法访问非法访问是指非授权用户通过远程登录或远程桌面等工具访问计算机的资源，造成非法访问的原因有病毒、操作系统和应用程序漏洞等。
特洛伊木马病毒可以将通过网络接收到的命令作为特权用户输入的命令发送给命令解释程序，从而达到访问系统资源的目的。
操作系统和应用程序漏洞可以使普通用户获得特权用户的访问权限，从而使非授权用户访问到本不该访问的资源。

编辑推荐

《计算机网络安全》特色：完全以解决目前面临的网络安全问题，构建能够防御黑客攻击的安全网络为依据组织本教材内容，完整介绍网络安全基础理论和各种用于实现安全网络的主流网络安全技术。结合网络安全基础理论讨论目前主流网络安全技术的工作机制，在实际网络环境下讨论运用主流网络安全技术设计安全网络的方法和过程。
在网络安全体系架构下讨论各层网络安全技术相互作用、相互协调的过程，给出通过有视集成各层网络安全技术构建防御黑客攻击的立体盾牌的思路。

<<计算机网络安全>>

版权说明