《计算机网络安全的理论与实践》

图书基本信息

书名：《计算机网络安全的理论与实践》

13位ISBN编号：9787040201413

10位ISBN编号：7040201410

出版时间：2006-10

出版社：高教

作者：王杰

页数：213

《计算机网络安全的理论与实践》

前言

网络安全是计算机科学的新分支，也是信息产业的新领域。它的产生源于网络通信的保密需要，它的发展得益于人们为应对侵犯网络通信和连网计算机系统的各种攻击所做出的锲而不舍的努力。随着互联网应用的深入和普及，如何不断地采取最有效的安全措施保护网络通信内容不被窃取、篡改和伪造以及保护连网计算机系统免受侵扰已变得至关重要。除军事和金融通信以外，网络安全如今已成为电子商务、信息管理及资源共享等领域不可缺少的工具和保障，因而也越来越受到政府、商业及家庭计算机用户的重视。毫无疑问，网络安全将继续成为计算机科学研究与应用中一个举足轻重的领域。互联网是在有线电话网的基础上发展起来的，由于当初在设计互联网通信协议时忽视了安全因素，导致互联网通信存在许多本来可以避免的缺陷和漏洞。为了解决互联网技术中的一系列问题，包括网络安全问题，美国国家科学基金会已号召研究人员探索和开发新一代互联网技术，研究互联网如果从零开始应该有怎样的体系结构才能更好地适应今后的发展和解决现有的网络安全问题。无论结果如何，维护网络安全的努力将是持续不断的，原因包括以下几点：第一，旧的网络安全机制可能由于计算理论的进展、计算机性能的提高或新技术的产生而不再有效。第二，旧的网络安全问题解决之后，新的网络安全问题又将不断出现。第三，新的应用可能需要新的安全措施加以保护。比如近年来出现的网络安全攻击，特别是对大型企业计算机系统的攻击，已从几年前用蠕虫和服务阻断所进行的撒网式攻击变成更具针对性的攻击了。经过多年的努力，特别是最近十几年的研究与实践，网络安全已逐渐形成了一些成熟的理论和有效的方法。学习这些理论与方法将为今后研究网络安全和开发安全系统打下良好的基础，同时也为系统安全管理提供牢靠的依据。因此，网络安全已成为美国各大学计算机科学系本科生与研究生的主要课程。中国的大学近年来也开始逐渐重视网络与信息安全的教学。

《计算机网络安全的理论与实践》

内容概要

《计算机网络安全的理论与实践》主要围绕着两条主线展开。第一条主线是以计算机密码学为根基而建立起来的各种安全协议和相应的工业化标准，第二条主线是为弥补通信协议缺陷和系统漏洞而发展出来的防火墙、抗恶意软件和入侵检测等技术。这两条主线相互交织，形成维护网络安全的防御体系，缺一不可。《计算机网络安全的理论与实践》以此为指导思想，用较短的篇幅向读者深入浅出、系统地介绍计算机网络安全理论与实践的主要研究成果和发展动向，使读者在一个学期的学时之内既学到理论知识又学到实用的安全技术。《计算机网络安全的理论与实践》内容包括网络安全概论，标准常规加密算法，公钥密码体系，密钥的产生、输送与管理方法，公钥证书，数据认证方法，实用网络安全协议及无线网安全协议，防火墙原理，抗恶意软件，万维网安全和入侵检测系统。《计算机网络安全的理论与实践》还包括相当数量的实际操作练习。《计算机网络安全的理论与实践》可作为高等院校本科高年级学生和一年级研究生的“计算机网络安全”教材，亦可作为计算机工作者和系统管理人员的参考书和自修读物。

《计算机网络安全的理论与实践》

作者简介

王杰（原名王洁），1961年8月生于广州，祖籍湖南。1982年和1984年分别获得中山大学计算数学理学学士和软件工学硕士学位，毕业后留校任教。1986年获美国波士顿大学校长奖学金赴美，1990年获波士顿大学计算机科学哲学博士学位。现任美国马萨诸塞大学罗威尔分校计算机科学系教授和网络与信息安全中心主任。曾任美国第一联合银行总部网络安全顾问，并在北卡罗来纳州议会的技术委员会做过数字签名和网络身份诈骗的专题报告，协助该州议会制定数字签名的法规。主要研究方向为平均计算复杂性理论、网络与系统安全、应用算法以及无线传感器网络通信。多次获得美国自然科学基金会及美国IBM公司和英特尔公司的资助。曾发表论文78篇，著书一本，编书两本。

《计算机网络安全的理论与实践》

书籍目录

《计算机网络安全的理论与实践》

章节摘录

插图：密码猜测“ 密码猜测 ”顾名思义就是猜测用户所使用的登录密码。如果用户选取的密码太短或太常见，则其密码便很有可能被他人猜出。如果用户没有更改系统默认密码或不经常更换密码，则其密码也很有可能被他人猜出。字典攻击字典攻击通常针对存储在计算机系统内的用户登录密码进行。比如在uNIX和I,inux操作系统中，用户登录密码经过加密后存放在一个密码文件内。在这些操作系统的早期版本中，用户的登录名及其加密后的登录密码均可被用户读到。又比如，微软公司Windows NT／xP操作系统将用户登录名和加密后的登录密码保存在系统的注册表中。这些信息虽然不是保存在一个文件内，但仍可被专门软件（如pwdump）读出。由于不少用户习惯使用单词、地名、人名或日期来设置登录密码，因此攻击者可先设法窃取存储在计算机系统内的登录密码文件，然后用系统所用的加密算法逐一加密所有单词、日期和各种常用名，将其密文与盗来的密文进行比较，找出相同者便可获得登录密码。为了防止字典攻击，UNIX和Linux操作系统的后期版本已不再将登录密码的密文在任何相应的文件上显示出来了（参见习题1.6）。

《计算机网络安全的理论与实践》

编辑推荐

《计算机网络安全的理论与实践》为高等教育出版社出版发行。

《计算机网络安全的理论与实践》

精彩短评

1、挺不错的一本书，内容很专业，要有一定基础才能读懂。

《计算机网络安全的理论与实践》

版权说明