<<网络安全原理与应用>>

图书基本信息

书名：<<网络安全原理与应用>>

13位ISBN编号：9787030114501

10位ISBN编号：7030114507

出版时间：2003-5

出版时间：科学出版社

作者：张世永 编

页数：418

字数：620000

前言

随着信息化的普及和发展，互联网络已覆盖了社会政治、经济、文化、生产的各个领域，网络安全也越来越成为全社会关注的焦点，并成为网络发展的重要课题。
提高全社会网络安全意识，是保障我国信息化建设健康稳定发展的长期重点工作之一。
从20世纪90年代以来，我们在网络信息安全领域开展了广泛而卓有成效的科研工作，取得了一定的成果，荣获了数十项重大成果，包括国家科技进步二等奖、三等奖各1项，部委科技进步一等奖、二等奖各2项，上海市科技进步二等奖4项、三等奖8项，国家计委重大科技成果奖3项，机电部重大科技成果奖3项等。
本书不仅是在跟踪国内外网络信息安全方面的最新研究成果，同时也是对我们该领域的实践经验与科研成果的一点总结。
我们的目标是为网络信息安全领域提供一本既可作教科书，又可作专业人员全面参考的手册性书籍。
本书为21世纪复旦大学研究生教学用书，属于上海市学位委员会研究生学位课程教材建设项目，在本书的写作过程中，除了介绍了作者自身的大量研究内容及成果之外，还参考了众多国内外论文、书籍以及其他一些在互联网上公布的相关资料，我们尽量在每章后面都列出，但由于网上资料数量众多且杂乱，可能无法把所有文献都一一注明出处。
这些资料来源于众多的大学、研究机构：安全团体、安全网站、商业公司以及一些研究计算机及网络安全问题的个人，对于他们在推动安全事业发展的过程中所做的工作和努力，再次表示衷心的感谢。
写作过程中所参考的这些书籍资料，其原文版权属于原作者，特此声明。
本书具有科学严谨的体系结构，内容深入浅出，新颖而全面，涉及广泛，全书在结构上分为网络安全概述、安全框架与评估标准、密码学理论、安全技术和产品四大部分，全面介绍网络信息安全的基本原理和应用实践技术，基本遍及了网络信息安全的各个方面，侧重于基本原理和实践技术，特别是较为系统全面的给出了目前网络信息安全的各种技术，反映了网络信息安全领域的最新研究成果和新趋势，并融进作者近年来在该领域的实践经验与科研成果。
此外从教材使用的角度考虑，在每章后面给出了习题作为巩固知识之用，书中还给出了大量的参考文献。
作为“21世纪复旦大学研究生教学用书”之一，本教材的目的同样是为提高研究生的培养质量，把创新能力和创新精神的培养放到突出位置上而出版的适应新的教学和科研要求的有复旦特色的教材。

<<网络安全原理与应用>>

内容概要

本书为复旦大学研究生教学用书，书中全面介绍网络信息安全的基本原理和实践技术。
在第一部分“网络安全概述”中先简介TCP/IP协议，然后分析目前常见的各种安全威胁，指出问题根源，提出网络安全的任务；第二部分“安全框架与评估标准”介绍一些经典的网络安全体系结构，并介绍了国际和国内对网络安全的评估标准和有关法规；第三部分“密码学理论”着重介绍密码学，从传统密码技术到对称密码体系、公钥密码体制以及密钥分配与管理、数字签名、数据隐写与电子水印等；第四部分为“安全技术和产品”，全面介绍身份认证、授权与访问控制、PKI/PMI、IP安全、E-mail安全、Web与电子商务安全、防火墙、VPN、安全扫描、入侵检测与安全审计、网络病毒防范、系统增强、安全应急响应、网络信息过滤、网络安全管理等技术，内容基本涵盖目前主要的安全技术。
在每章后面给出了习题作为巩固知识之用，还给出了大量的参考文献。
本书可作为高等院校计算机、通信、信息等专业研究生和高年级本科生的教材，也可作为计算机、通信、信息等领域研究人员和专业技术人员的参考书。

<<网络安全原理与应用>>

书籍目录

章节摘录

插图：本章我们首先介绍一下密码学的起源和发展以及它的应用，密码学是伴随着现代科学以及实践发展的实际需要而发展起来的，并且它正得到越来越广泛的应用。
然后我们简要介绍一下密码学的基础及组成部分，一次一密系统的基本原理和密码分析，这是密码学系统最基本的基础，也是深入了解密码学的前提知识。
随后我们回顾了传统密码学的知识，这是传统密码学发展中的精粹，包括换位密码和代替密码以及它们的实现工具——转轮机。
最后我们着重介绍了两种基本的密码系统——流密码和分组密码，其中详细介绍了同步流密码，它是流密码中的代表，关于分组密码应用很广泛，在此我们仅仅介绍它的基本概念和要求，在下一章我们将详细介绍DES（数字加密标准）。

编辑推荐

《网络安全原理与应用》由科学出版社出版。

<<网络安全原理与应用>>

版权说明