<<网络信息安全>>

图书基本信息

书名：<<网络信息安全>>

13位ISBN编号：9787302221760

10位ISBN编号：7302221766

出版时间：2010-6

出版时间：清华大学出版社

作者：葳鹏，刘沛骞　主编

页数：305

<<网络信息安全>>

前言

随着国民经济信息化进程的推进、网络应用的发展和普及，各行各业对计算机网络的依赖程度越来越高，这种高度依赖将使社会变得十分“脆弱”，一旦计算机网络受到攻击，不能正常工作，甚至全部瘫痪时，就会使整个社会陷入危机。
人类对计算机网络的依赖性越大，对网络信息安全知识的普及要求就越高。
总之，信息安全引起了社会各界的广泛关注，面对这样的局面，高等院校开始将网络信息安全纳入主修课程，本书正是为适应这样的需求而编写的。
本书共分15章，比较全面地论述了信息安全的基础理论和技术原理。
第1章网络信息安全综述，介绍了有关网络安全的基础知识，以及网络安全研究的目标、内容、发展和意义。
第2章分组密码体制，介绍丁密码学的基本概念、经典的密码体制、分组密码体制（工）ES、AES）及其工作模式，以及流密码的基本思想。
第3章单向散列函数，介绍了Mi-）5和SHA算法，以及消息认证码。
第4章公钥密码体制，主要介绍了公钥密码的原理及相关基础知识、RSA算法、E1Gamal算法和椭圆曲线密码EC（：算法、密钥交换，以及数字签名技术与应用。
第5章密钥管理技术，主要介绍了密钥的生成、分配、存储和保护、密钥共享和托管，以及公钥基础设施PKI。
第6章信息隐藏技术，介绍了信息隐藏的基本原理、信息隐藏技术、数字水印技术，以及常用的信息隐藏算法。
第7章认证技术与访问控制，介绍了常见的身份认证技术、访问控制原理，以及访问控制策略及应用。
第8章入侵检测技术，介绍了入侵检测模型，入侵检测技术原理、分类，以及入侵检测系统的标准与评估。
第9章防火墙技术，介绍了防火墙的实现原理、体系结构，以及防火墙的部署与应用。
第10章漏洞扫描技术，介绍了安全脆弱性分析、漏洞扫描技术，以及常用的扫描工具。
第11章网络安全协议，介绍了IPSec协议、SSL协议，以及TLS协议。
第12章其他网络安全技术，主要介绍了操作系统安全、数据库安全，以及计算机病毒的基本知识.第13章应用安全，主要介绍了网络服务安全、电子邮件安全、电子商务安全，以及DNS安全。
第14章安全管理与评价标准，介绍了网络风险分析与评估、国际安全标准，以及我国的安全评价标准。
第15章简单介绍了新一代网络的安全趋势。

<<网络信息安全>>

内容概要

本书全面系统地讲述了网络信息安全的理论、原理、技术和应用。
本书主要内容有对称加密算法（DES、AES），公钥密码算法（RSA、ECC），安全散列算法（MD5、SHA），数字签名（DSS），密钥管理技术，信息隐藏技术，身份认证与访问控制，入侵检测技术，防火墙，漏洞扫描技术，网络安全协议（IPSec、SSL），操作系统安全、数据库安全以及计算机病毒，安全评估标准（TCSEC、CC、GB17859），Web安全，E-mail安全（PGP、S/MIME），电子商务安全（SET）及DNS安全等。

本书适合作为高等院校本科或研究生教材，也可作为研究人员和开发人员的参考用书。

<<网络信息安全>>

书籍目录

章节摘录

插图：2.网络安全与经济一个国家信息化程度越高，整个国民经济和社会运行对信息资源和信息基础设施的依赖程度也越高。
当计算机网络因安全问题被破坏时，其经济损失是无法估计的。
我国计算机犯罪的增长速度超过了传统的犯罪，1997年20多起，1998年142起，1999年908起，2000年上半年1420起，再后来就没有办法统计了.利用计算机实施金融犯罪已经渗透到了我国金融行业的各项业务中。
近几年已经破获和掌握100多起，涉及金额达数亿元。
3.网络安全与社会稳定互联网上的一些虚假信息、有害信息对社会管理秩序造成的危害，要比现实社会中一个谣言大得多。
1994年4月，河南商都热线一个BBS，一张说交通银行郑州支行行长携巨款外逃的帖子，造成了社会的动荡，3天10万人上街排队，一天提了十多亿元。
2001年2月8日，正值春节期间，新浪网遭受攻击，电子邮件服务器瘫痪了18个小时，造成了几百万的用户无法正常联络。
4.网络安全与军事在第二次世界大战中，美国破译了日本的作战密码，将日本的舰队几乎全歼，重创了日本海军。
目前的军事战争更是信息化战争，谁掌握了战场上的信息权，谁就将取得最后的胜利。
网络与信息安全是把双刃剑。
安全性高，固然可以保证国家和民众的财产和正常生活，可是犯罪分子也可以用它来危害社会。
有报告称，现在的恐怖分子都使用加密的电子邮件互相联络，从而难以发现他们的行踪。
著名美国学者BruceSchneier在其名著《应用密码学》中描绘了一个利用计算机密码学犯罪的场景。
当具有纸质现金特点的数字现金广泛使用时，将会出现理论上安全的犯罪。
歹徒绑架人质，然后要求以数字现金的形式支付赎金。
这种犯罪几乎绝对安全：支付赎金时没有物理接触，依靠网络和公共媒体（如报纸）完成；同时，数字现金和纸质现金一样是不可追踪的，警察不能像追踪转账支票一样来追踪数字现金。

编辑推荐

《网络信息安全》：高等学校计算机专业教材精选·网络与通信技术

版权说明