<<信息安全原理及应用>>

图书基本信息

书名：<<信息安全原理及应用>>

13位ISBN编号：9787302191070

10位ISBN编号：7302191077

出版时间：2009-4

出版时间：清华大学出版社

作者：熊平　主编

页数：309

前言

当今时代是信息的时代，信息成为社会发展的重要战略资源。
信息的安全交换、存储和保障能力成为综合国力和经济竞争力的重要组成部分。
我国政府把信息安全技术与产业列为今后一段时期的优先发展领域。
信息安全教育在我国高等教育中正在逐步展开。
教育部继2001年批准在武汉大学开设信息安全本科专业之后，又先后批准了几十所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。
另外，教育部2005年7号文件出台了“关于进一步加强信息安全学科、专业建设和人才培养工作的意见”，并将建立国家网络信息安全保障体系确定为国家发展的基本战略目标之一。
目前有关信息安全的书籍很多，其中不乏精品。
然而，由于信息安全所涵盖的内容非常广泛，要想在一部教材中介绍信息安全的方方面面是不切实际的，在内容安排上都会做适当的取舍。
笔者在实际教学过程中发现，正是这种取舍造成目前信息安全基础教材普遍存在两个方面的缺憾。
其一，对密码学基础理论缺乏比较系统的介绍。
密码学是信息安全的基石，信息安全理论与技术大多建立在密码学基础之上，但遗憾的是，目前信息安全基础教材大多突出密码学的应用，而忽视了对基础知识的介绍。
其二，没有与信息安全理论相应的实验内容。
实验教学是信息安全基础教学中不可缺少的内容，但目前的信息安全基础教材要么没有实验内容，要么有实验内容但对实验环境要求较高，在实际教学中没有可操作性。
因此，在本书的内容编排上，力求理论与实践相结合，包含了密码学基础理论、密码学应用机制、实用安全技术及相关实验内容，使读者更清晰地从信息安全体系的层面掌握信息安全的基础理论和应用技术。
本书内容共分为15章。
第1章介绍信息安全的基本概念、发展历史、实现的目标以及主要的研究内容。
第2－4章介绍密码学基础理论：第2章对密码学进行综述，介绍了密码学的基本概念、密码系统及其分类，并对经典密码学的基本方法进行了阐述；第3章介绍对称密码体制，包括分组密码和序列密码，并对代表性的对称密码DES、AES、RC4等进行了阐述；第4章对公钥密码体制进行了介绍，包括数论基础、公钥密码体制的基本原理，并对代表性的RSA密码及其他公钥密码进行了阐述。
第5－7章介绍密码学应用机制：第5章介绍了用于解决信息安全完整性的消息认证机制，重点包括消息认证码和Hash函数；第6章介绍了身份认证与数字签名技术，其中，身份认证是实现访问控制的基本前提，而数字签名则用于解决信息安全的抗否认性。
第7章介绍了密钥管理机制，包括对称密码体制下的密钥管理和公钥密码体制下的密钥管理，重点是公钥证书的管理及PKI。
第8－12章介绍安全保障技术：第8章介绍访问控制技术，包括访问控制策略和常用的网络访问控制方法；第9章介绍了常用的网络攻击技术和相应的防范方法；第10章介绍了恶意代码分析技术，根据对恶意代码的分类，逐一介绍了各类恶意代码及其防范方法；第11章介绍了防火墙系统，包括防火墙的原理与分类、基本技术，以及在实际部署中的体系结构；第12章介绍了入侵检测系统，包括入侵检测系统的分类和主要检测方法，并以Snort为例阐述了入侵检测系统的基本结构。
第13章介绍安全协议，对TCP/IP体系结构进行了安全分析，并从网络体系结构上分别介绍了网络层、传输层及应用层的安全协议IPSec、SSL和SET。
第14章介绍了评估信息系统安全的国内外标准，包括TCSEC、CC及国内标准。
第15章是实验部分，由8个实验组成，包括数据加密、认证和签名、访问控制、网络扫描、协议分析、远程控制、防火墙及入侵检测系统的配置等内容。
本书由熊平担任主编，朱天清参与了各章内容的讨论、安排与编写工作。
由于作者自身水平有限，本书定有不妥甚至错误之处，恳请读者及专家提出宝贵意见。

<<信息安全原理及应用>>

内容概要

本书共15章。
第1章介绍信息安全的基本概念、目标和研究内容；第2章介绍密码学的基本概念，是信息安全的基础理论；第3～4章介绍两种重要的密码实现体制，即对称密码体制和公钥密码体制；第5～7章介绍了密码学理论的应用机制，分别是消息认证、身份认证与数字签名、密钥管理；第8章介绍访问控制技术；第9～10章从安全技术人员的角度介绍网络攻击技术和恶意代码分析；第11～12章介绍两种应用广泛的安全防护系统，即防火墙和入侵检测系统；第13章从网络体系结构上分别介绍网络层、传输层及应用层的安全协议；第14章介绍评估信息系统安全的国内外标准；第15章编制了8个信息安全实验，使读者通过实际操作加深对基础理论与技术的理解。
本书可作为信息安全，计算机应用、信息管理等相关专业本科生或研究生的教材和参考书，也可供从事安全技术和管理工作人员参考。

<<信息安全原理及应用>>

书籍目录

章节摘录

插图：第1章　信息安全概述在全球信息化的推动下，实现政府管理信息化、企业经营信息化以及国防信息化已经成为时代不可抵挡的潮流。
信息技术和信息产业以前所未有之势，渗透到各行各业和社会生活当中，正在逐渐改变着人们的生产和生活方式，推动着社会的进步。
但是，在信息网络的作用不断扩大的同时，信息网络的安全也变得日益重要，网络系统一旦遭到破坏，其影响和损失也将十分巨大。
信息安全不仅关系到普通民众的利益，也是影响社会经济发展、政治稳定和国家安全的战略性问题。因此，信息安全问题已经成为国内外专家学者广泛关注的课题。
1.1 信息安全的概念要了解信息安全，首先要了解什么叫信思。
信息(information)是经过加工（获取、推理、分析、计算、存储等）的特定形式数据，是物质运动规律的总和。
信息的主要特点具有时效性、新知性和不确定性，信息是有价值的。
给信息安全下一个确切的定义是比较困难的，主要是因为它包含的内容太过广泛，如国家军事政治等机密安全，防范商业企业机密泄露，防范青少年对不良信息的浏览，防范个人信息的泄露等。
信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。
信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。
从广义来说，凡是涉及信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是信息安全的研究领域。

<<信息安全原理及应用>>

编辑推荐

《信息安全原理及应用》可作为信息安全、计算机应用、信息管理等相关专业本科生或研究生的教材和参考书，也可供从事安全技术和管理工作人员参考。
内容包括：信息安全的基本概念、目标和研究内容，密码学的基本理论与应用；访问控制技术、从安全技术人员的角度介绍网络攻击技术和恶意代码分析；防火墙和入侵检测系统；评估信息系统安全的国内外标准；八个信息安全实验。

<<信息安全原理及应用>>

版权说明