<<网络安全基础教程>>

图书基本信息

书名：<<网络安全基础教程>>

13位ISBN编号：9787115202154

10位ISBN编号：711520215X

出版时间：2009-11

出版时间：人民邮电出版社

作者：张仕斌 等编著

页数：335

前言

随着Internet的普及和Internet技术的不断发展，网络已经影响到政治、经济、文化、军事和社会生活的各个方面，已成为全球信息基础设施的主要组成部分。
网络作为一把双刃剑，在加快人类社会信息化进程的同时，也给保障信息安全带来了极大的挑战。
一方面，私人数据、重要的企业资源、政府机密信息等被暴露在公共网络空间中，而Internet的开放性使得这些重要信息很容易被获取；另一方面，计算机病毒的种类和数量也在迅猛增长，并且其借助网络传播的速度越来越快，危害面越来越广，破坏程度也越来越大。
在人类社会进入信息化时代的今天，人们对信息的安全传输、安全存储、安全处理的要求越来越迫切，而且显得尤为重要，它不仅关系到每个人的切身利益，甚至也关系到国家的安危、科技的进步、经济的发展。
因此，网络安全已成为社会各界关注的热点问题。
当前，我国网络安全正面临着严峻的考验：一方面，随着电子政务、电子商务、电子现金、数字货币、网络银行、网络证券等的广泛应用，网络安全的需求更加严格和迫切；另一方面，黑客攻击、病毒传播以及形形色色的网络攻击曰益增加，网络安全防线十分脆弱。
因此，加快培养网络安全应用型人才、普及网络安全知识和掌握网络安全技术迫在眉睫。
本书是在广泛调研和充分论证的基础上，结合当前应用最为广泛的操作平台和网络安全规范，并通过研究实践编写而成的。
在写作中，作者始终遵循这样一个原则：为网络安全领域提供一本既可以作为教学用书，也可以作为专业技术人员的参考书.本书特别强调理论与实践相结合，具有科学严谨的体系结构，内容全面，深入浅出，构思新颖，突出实用，系统性强，并利用通俗的语言全面阐述了网络安全理论与实践技术。
每章在授课中融合了实践内容，使理论联系实际，并配有相应的习题。
全书内容包括网络安全基础知识、密码技术、信息隐藏技术、数字签名技术、认证技术、网络入侵与攻击技术、网络安全防范技术、操作系统安全技术、数据与数据库安全技术、软件安全技术、Web安全技术、网络互连安全技术等。
为了便于多媒体教学，本书配有相应的电子教案。
本书由张仕斌组织编写及统稿工作，其中第1-6章由张仕斌编写，第7章由陈麟和谭三编写，第8章由陈敏和彭城编写，第9章由方睿编写，第10章由安宇俊编写，第11章由付林编写，第12章由黄南铨编写。
为了便于多媒体教学，本书配有电子教案，订购本教材的教师可到人民邮电出版社教学服务与资源网（www.ptpedu.corn.cn）上下载。
由于作者水平有限，加上时间仓促，书中难免有不足和错误之处，欢迎广大读者批评指正。

<<网络安全基础教程>>

内容概要

网络安全理论与技术是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全理论与技术等多学科的综合性学科。
本书用通俗的语言全面阐述了网络安全理论与技术。
全书内容包括网络安全基础知识、密码技术、信息隐藏技术、数字签名技术、认证技术、网络入侵与攻击技术、网络安全防范技术、操作系统安全技术、数据与数据库安全技术、软件安全技术、Web安全技术、网络互连安全技术等。

本书内容全面，深入浅出，构思新颖，突出实用，系统性强，可作为普通高等院校计算机、通信、网络工程、信息安全等相关专业的教材，也可供计算机、通信、信息等领域研究人员和专业技术人员参考。

<<网络安全基础教程>>

书籍目录

章节摘录

插图：它们彼此目的相反、相互独立，但在发展中又相互促进。
密码编码学的任务是寻求生成高强度密码的有效算法，以满足对信息进行加密或认证的要求；密码分析学的任务是破译密码或伪造认证密码，为相关研究工作提供依据和参考。
对一个保密系统采取截获密文进行分析的方法来进行攻击称为被动攻击；非法入侵者采用删除、更改、添加、重放、伪造等手段向系统注入假信息的攻击称为主动攻击。
进攻与反进攻、破译与反破译是密码学中永无止境的矛与盾的竞技。
现代密码学除了包含密码编码学和密码分析学外，还包括近些年来才形成的新分支——密钥密码学，它是以密钥（也是现代密码的核心部分）作为研究对象的学科。
密钥管理包括一系列规程，它包括了密钥的生成、使用、存贮、备份、恢复以及销毁等环节，涵养了密钥的整个生存周期，在保密系统中至关重要。
以上三个分支学科构成了现代密码学的主学科体系。
现代密码学不仅可以实现信息的保密性，而且还可以实现信息的真实性、完整性和不可抵赖性等。
3.密码技术的应用随着计算机科学的蓬勃发展，人类社会已经进入信息时代.信息一方面为人们的生活和工作提供了很大的方便，另一方面也提出了许多急需解决的问题，其中信息的安全是当前最突出的问题。
因此随着计算机网络技术的迅速发展以及电子商务和电子政务的兴起，密码技术及其应用得到了飞速的发展。
现代密码技术已经深入到信息安全的各个环节，其应用已不仅仅局限于政治、军事等领域，其商用价值和社会价值也得到了人们的充分肯定。
当前，计算机网络的广泛应用产生了大量的电子数据，这些数据需要传输到网络的各个地方并存储起来.这些数据有的可能具有重大的经济价值，有的可能关系到国家、军队或企业的命脉甚至生死存亡。
对于这些数据，有意的计算机犯罪或无意的数据破坏都可能会造成不可估量的损失。
对于这些犯罪行为，光靠法律和相应的的监督措施很难满足现实的需要，必须进行数据的自我保护。
因此，理论和事实说明，密码技术是一种进行数据保护的实用而有效的方法。
这也是现代密码技术得到快速发展和广泛应用的原因。

<<网络安全基础教程>>

版权说明