计算机系列教材

网络安全原理与实践

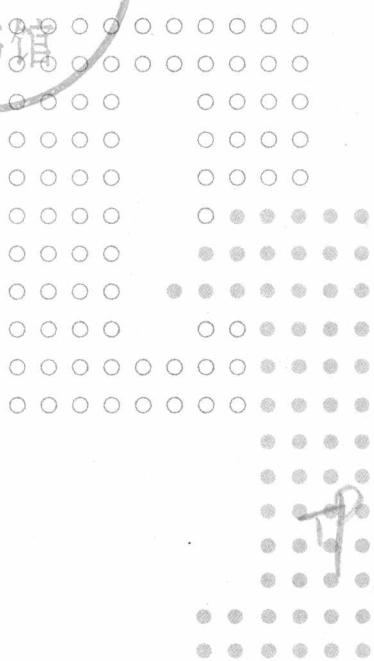
陈伟 李频 编著

清华大学出版社

计算机系列教材

陈伟 李频 编著

网络安全原理与实践



清华大学出版社
北京

内 容 简 介

本书围绕网络安全技术体系的建立，系统介绍了计算机网络安全知识和理论，全书共分 17 章，内容包括网络安全基础、网络安全威胁、密码学概述、对称加密、公钥密码、消息认证和散列函数、鉴别和密钥分配协议、身份认证和访问控制、PKI 技术、IPSec 协议、电子邮件安全、Web 安全、防火墙技术、虚拟专用网、入侵检测系统和网络诱骗系统、无线网络安全、恶意代码。本书既重视基础原理和基本概念的阐述，又紧密联系当前的前沿科技知识，注重理论和实践的统一，可以有效加深学生对于网络安全的理解，培养学生的创新能力。

本书可作为信息安全、计算机、信息管理、电子商务等专业本科生和研究生的教材，也可供从事相关专业的教学、科研和工程人员参考。

图书在版编目（CIP）数据

网络安全原理与实践/陈伟，李频编著. —北京：清华大学出版社，2014
计算机系列教材
ISBN 978-7-302-35654-7

Ⅰ. ①网…　Ⅱ. ①陈…　②李…　Ⅲ. ①计算机网络－安全技术－高等学校－教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 053008 号

责任编辑：白立军　顾　冰
封面设计：常雪影
责任校对：梁　毅
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：20.5　　**字　数**：511 千字
版　　次：2014 年 7 月第 1 版　　**印　次**：2014 年 7 月第1次印刷
印　　数：1～2000
定　　价：34.50 元

产品编号：054620-01

《网络安全原理与实践》前言

随着计算机网络的发展，信息安全越来越受到人们的关注，信息安全已成为发展最为迅速的学科领域之一。人员、技术和管理是信息安全保障的三大要素，虽然人员和管理在安全领域所扮演的角色非常重要，但技术要素才是基础，一个信息安全工程师首先必须对安全技术的功能和其弱点有深入的理解。对于信息安全专业人才培养来说，使学生掌握信息安全技术理论和应用是关键。

2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业，我国从此开始了信息安全本科生的培养。2002 年又批准了 18 所高等学校建立信息安全本科专业，之后信息安全本科人才培养进入热潮阶段。在信息安全本科生培养初期，教材比较匮乏，一般信息安全专业课使用各个学校的内部讲义或面向研究生的教材，2007 年后出现了大量的信息安全本科专业教材，课程涵盖密码学、系统安全、网络安全、网络攻防、信息安全实验等。

南京邮电大学 2002 年获批建立信息安全本科专业，在信息安全学科专业领域，特别是网络安全方向拥有一支学术水平较高的专家队伍，承担了网络安全领域的多项科研课题，能够从事本科至博士生的多层次人才培养。我们在十多年信息安全本科生人才培养的过程中积累了一点经验，通过对多种教材的使用有了一定的心得，体会到信息安全专业是一门对实践性要求很高的学科，如果在教学中不能将理论与实践相结合，学生难以有效地掌握知识点。在编写本书之前，我们将本书定位为适应本科生教学使用，偏向网络安全、理论与实践相结合的教材。编写时以网络安全理论为本位，以实际能力为目标，注意原理联系实践，尽量多介绍一些实际问题，让读者增加感性认识。

本书围绕网络安全体系的建立展开，第 1 章和第 2 章介绍网络安全的基本概念和目前存在的网络安全威胁，后续章节可以分为三大部分，第一部分为密码学，这部分为网络安全的基础，主要包含第 3～6 章，本书不过多讨论密码学中的算法设计和安全性证明，重点介绍各种密码的主要思想和算法特点，目标是让读者能在不同应用场景下选择合适的密码方法；第二部分为网络安全协议，由于网络技术的出现，原有的在单机上的安全保护技术遇到了挑战，网络安全协议主要解决此类问题，主要包含第 7～10 章，还有第 12 章的部分内容；第三部分为网络安全技术，相比密码学和网络安全协议，读者在现实生活中更容易接触到这些应用技术，这些技术主要会应用在网络攻防中，主要包含第 11～17 章。本书适合 32～64 学时使用，部分章节可作为选学内容。

前 言《网络安全原理与实践》

本书既注重网络安全基础理论，又着眼培养读者解决网络安全问题的实际能力。本书的特点是突出网络安全的特色，理论与实践相结合，文字简明通俗易懂，用循序渐进的方式叙述网络安全知识，对网络安全的原理与技术的难点的介绍适度，适合本科生教学使用。

本书由南京邮电大学计算机学院信息安全系组织编写，为南京邮电大学“十二五”规划教材，第3～6章、第15～17章由陈伟编写，其余章节由李频编写完成。本书在编写过程中参阅了大量文献，还参考了互联网上信息安全的相关资料，在此一并向作者表示衷心的感谢。硕士研究生杨龙、李晨阳、吴震雄、姜海东、顾杨、龚沛华、许若妹等参与部分文字的录入和插图绘制工作，此书的出版得到了多位专家的指导和帮助，在此一并表示感谢。

正如互联网的设计会存在漏洞一样，限于作者的水平，本书难以避免会存在错误，我们将会虚心聆听读者指出的任何一处错误，恳请广大读者批评指正。作者的E-mail为champway@163.com，lipin7421@163.com。

作　者

2013年10月

《网络安全原理与实践》目 录

第1章　网络安全基础

1.1　网络安全的概念

21世纪是信息的时代，信息正成为重要的战略资源，信息的获取能力、处理能力和保障能力成为一个国家综合国力的重要组成部分。一个信息技术和信息产业落后的国家，无法成为世界强国，目前信息科学和技术正处于快速发展阶段，成为促进经济发展和社会进步的重要因素。另一方面，危害信息安全的事件不断出现，人们经常在新闻中听到黑客、木马、漏洞这些与信息安全有关的名词，网络银行账号、网络游戏账号、QQ账号被盗已经不再成为新闻，网络谣言、人肉搜索等网络暴力事件已经成为常见的现象，信息安全的形势严峻，信息技术的发展改善了人们的生活，但也让人们的敏感信息变得不安全。也许几十年前，人们只要把敏感文档锁进保险箱，就可以高枕无忧，可如今大部分的信息都是以二进制的形式存储在电子产品中，通过网络进行传送，人们已经没有保险箱可以保证这些信息的安全，信息安全事关国家安全和社会稳定，必须采取措施确保我国的信息安全。

1. 信息安全的含义

目前业界关于信息安全的定义和内含，尚没有形成一个统一的说法。不同的学者根据自己的研究和理解，给出了不同的诠释。尽管这些诠释不尽相同，但其主要内容却是相同的。

信息论的知识告诉我们，信息不能脱离它的载体而孤立存在。例如，有一份重要的文档使用微软公司软件Office编辑处理，并存储在计算机的硬盘中，可以通过网络用电子邮件发送给对方。在编辑发送过程中，Office软件、硬盘、网络都是信息的载体，如果Office软件存在漏洞、计算机硬盘被偷走、网络数据被截取，这个重要的文档就会被泄密。我们不能脱离信息系统而孤立地谈论信息安全。因此，应当从信息系统安全角度来全面考虑信息安全的内含。信息系统安全主要包括四个层面：硬件安全、软件安全、数据安全和安全管理，其中的数据安全即是传统的信息安全。为了表述简单，在不会产生歧义时可以直接将信息系统安全简称为“信息安全”。

(1) 硬件安全：信息系统硬件的安全是信息系统安全的首要问题，包括硬件的稳定性、可靠性和可用性。

(2) 软件安全：如保护信息系统不被非法侵入，系统软件和应用软件不被非法复制、篡改，不受恶意软件的侵害等。

(3) 数据安全：采取措施确保数据免受未授权的泄露、篡改和毁坏，主要包括数据的机密性、完整性、不可否认性和可用性。