21世纪高等院校计算机网络工程专业规划教材

基于案例的网络安全技术与实践

朱宏峰 朱丹 孙阳 刘天华 编著

可下载教学资料
http://www.tup.tsinghua.edu.cn

清华大学出版社

21世纪高等院校计算机网络工程专业规划教材

基于案例的网络安全技术与实践

朱宏峰 朱丹 孙阳 刘天华 编著

清华大学出版社
北京

内 容 简 介

本书主要介绍了研究和掌握网络安全技术必备的基本数学方法、安全协议以及相关的网络安全典型知识，主要内容包括密码学数学基础、古典密码、计算密码、物理密码、基本安全协议、N 方安全协议、网络安全体系结构、网络实体安全、网络安全协议、访问控制与 VPN、防火墙与隔离网闸、入侵检测技术、计算机病毒等方法与技术，并同步介绍了这些方法与技术在实际应用中的典型案例。

本书适用于计算机专业本科生以及对当前密码学与网络安全感兴趣的技术人员。

图书在版编目(CIP)数据

基于案例的网络安全技术与实践/朱宏峰等编著. --北京：清华大学出版社，2012.12
21 世纪高等院校计算机网络工程专业规划教材
ISBN 978-7-302-30245-2

Ⅰ. ①基… Ⅱ. ①朱… 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(2012)第 233157 号

责任编辑：闫红梅　李　晔
封面设计：何凤霞
责任校对：李建庄
责任印制：何　芊

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：北京密云胶印厂
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**：24.25　　**字　　数**：608 千字
版　　次：2012 年 12 月第 1 版　　**印　　次**：2012 年 12 月第1 次印刷
印　　数：1～3000
定　　价：39.00 元

产品编号：047110-01

前　言

《基于案例的网络安全技术与实践》涉及网络中的各个层次，犹如血液一般渗透到计算机实际应用过程中的各个环节。为了对整体有一个清晰的把握，通常可以把计算机系统划分为5个纵向层次：硬件材料→硬件设计与实现→操作系统→系统软件→应用软件，类似地，网络安全系统也可以分成一个5层体系：数学基础→密码学→安全协议→网络安全→应用安全，本书着重阐述中间3层内容。

本教材编写的出发点主要针对3种“问题”学生：一是“高分低能”型，其核心问题是“重知识而轻能力”；二是“眼高手低”型，其核心问题是“知其然而不知其所以然”；三是“小学生”型，其核心问题是“无兴趣则不学”，传统教学方法无效。

为了解决上述问题，我们编写了基于“兴趣”的启发式网络工程教材：《基于案例的网络安全技术与实践》。由于这门课程的特殊性（与密码和安全相关的有趣实例非常多），可以基于“兴趣”进行展开，每章都可以从一个趣味盎然的实例开始阐述，然后进行启发式的讲解，一环套一环，吸引学生一步步进入教师节奏，从而达到良好的教学效果。因此，教材每一章编写的基本思路是：实例（吸引读者）→分析（为什么这样做?）→原理（具体怎么做?）→实践（实验）→总结（形成体系）→习题（锻炼思维），其中，习题部分将突出批判精神，引导学生以辩证思维方式看问题，进而将学生培养成为能够善于独立思考、有创造力的复合型人才。

此外，本书还具备以下特点：

（1）整体的连贯性。本书整体上按照网络安全系统从低到高的层次阐述，重点针对“密码学→安全协议→网络安全”3个层次进行展开，且前者都是作为后者的“黑盒”来体现，使条理更为清晰。“数学基础”部分只给出简明扼要的知识点，而“应用安全”则适度的分布在各个章节以及实验练习中。

（2）案例的趣味性。本书图文并茂，深入浅出。采用简单有趣的案例来说明其实质，然后再将问题的“计算”或“规模”复杂化，叙述过程中的“对比”、“流程”、“交互”等问题将以图表的形式体现。同时抓住时机，引出知识点。

（3）知识的系统性。本书最终目的是培养学生的能力与创造力，因此在全书选材上不仅注意理论与实际的结合，更加注重对兴趣的培养，在基本知识掌握的基础上，适当给出当前的发展方向，从而培养出大局观思维与微创新能力“双强”的优秀毕业生。

目　录

第一篇　引　言

第二篇 密码学——奠基之石

第三篇　安全协议——衔接之桥

第一篇

引　言

第1章 网络安全概述

如果把一封信锁在保险柜中，把保险柜藏在纽约的某个地方……然后告诉你去看这封信，这并不是安全，而是隐藏。相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全的概念。

——Burce Schneier

Internet的广泛应用使人们在生产方式、生活方式及思想观念等方面都发生了巨大变化，推动了人类社会的发展和人类文明的进步，把人类带入崭新的信息化时代。

计算机网络就像一把双刃剑，它在实现了信息交流与共享、极大便利和丰富了社会生活的同时，由于网络本身的脆弱性加上人为攻击与破坏，也对国家安全、社会公共利益以及公民个人合法权益造成现实危害和潜在威胁。因此，加强对信息网络安全技术和管理的研究，无论是对个人还是组织、机构，甚至国家、政府都有非同寻常的重要意义。

1.1 计算机网络安全的概念

1.1.1 计算机网络安全的定义

“安全”一词在字典中被定义为“远离危险的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击或逃跑而采取的措施”。从这个角度来说，计算机网络安全是指为了使计算机网络运行正常，通过采用全方位的管理措施和强有力的技术手段，保证在一个网络环境里，使得经过计算机网络的数据保持保密性、完整性和可用性。

国际标准化组织(ISO)将计算机安全定义为“为数据处理系统和采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露”。美国国防部国家计算机安全中心将计算机安全定义为：“一般说来，安全的系统会利用一些专门的安全特性来控制对信息的访问，只有经过适当授权的人，或者以这些人的名义进行的进程可以读、写、创建和删除这些信息”。我国公安部计算机管理监察司将计算机安全定义为“计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害”。

上面是狭义的计算机网络安全的内容。广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络信息安全所要研究的领域。广义的计算机网络安全还应该包括网络实体安全，如机房的安全保护、防火措施、防水措施、静电防