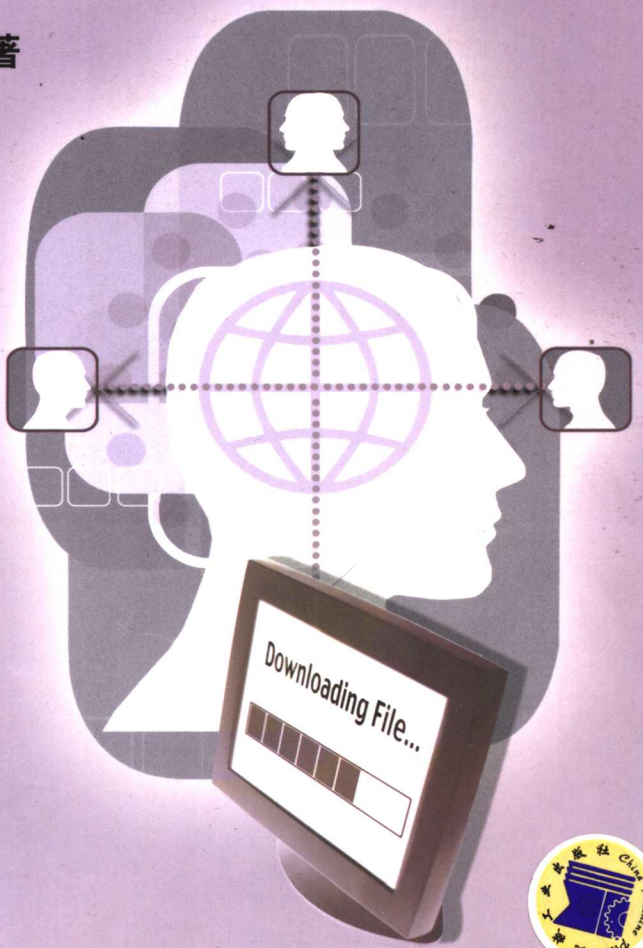
高等院校信息安全专业规划教材

计算机网络安全技术教程

- 密码学和PKI基础
- 防火墙安全技术
- 入侵检测安全技术
- 计算机病毒防治
- 系统安全

谢冬青　冷健　熊伟　编著



机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

计算机网络安全技术教程

谢冬青　冷　健　熊　伟　编著

机 械 工 业 出 版 社

本书系统全面地介绍了计算机网络安全技术的主要内容。全书共分五个部分，内容包括：密码学和 PKI 基础，防火墙安全技术，入侵检测安全技术，计算机病毒防治，系统安全。

本书适合作为电子、计算机、信息安全、电子商务等专业本科生教材，也可供从事网络与信息安全的科技人员与管理人员、研究生自学使用。对程序设计开发人员也有一定的参考价值。

图书在版编目（CIP）数据

计算机网络安全技术教程/谢冬青，冷健，熊伟编著. —北京：机械工业出版社，2007.1
（高等院校信息安全专业规划教材）
ISBN 7-111-19957-X

Ⅰ. 计… Ⅱ. ①谢… ②冷 ③熊… Ⅲ. 计算机网络－安全技术－高等学校－教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2006)第 113932 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)
策 划：胡毓坚
责任编辑：陈振虹
责任印制：洪汉军

三河市宏达印刷有限公司印刷
2007 年 1 月第 1 版·第 1 次印刷
184mm×260mm·25 印张·618 千字
0001—5000 册
定价：34.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话：(010)68326294
编辑热线电话：(010)88379739
封面无防伪标均为盗版

高等院校信息安全专业规划教材

编委会成员名单

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2. 系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3. 系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4. 注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

1984 年 11 月，国际密码学会主席 J. L. Massey 在北京、西安分别做了分组密码的学术讲座。这是中国和国际密码界的第一次公开学术交流。自此，中国的大学和研究机构逐步地开展了密码学的讨论。随着互联网业务的蓬勃开展，人们的兴趣也从密码学转向网络安全，这是网络业务强烈的需求带动的。根据中国互联网信息中心(CNNIC)2005 年 7 月发布的第 16 次中国互联网发展状况统计报告，上网用户总数为 10300 万，上网计算机总数为 4560 万台，我国 CN 下注册的域名数 622534 个，国际出口带宽总量为 82617Mbit/s，而用户对网络的安全性感到“非常满意”和“比较满意”的分别只占 2.3% 和 16.8%。

网络设计的局限性和网络的开放性、共享性、广泛的互联性，使网络在为人们提供便利的同时，承受着多方面的威胁。随着安全事件数量不断上升，损失、影响越来越大。传统的方法，只是针对出现的问题予以解决，属于事后、被动的防护方法，缺少系统的考虑。同时，网络安全的问题也不仅仅是一个技术问题，涉及政策、法规、管理、标准技术等方方面面。

结合作者多年教学、科研和工程项目的经验，本书试图全面介绍网络安全的主要原理，基本方法和实践经验，并力图体现如下特点：

1. 内容全面，体系结构合理。

2. 实践性强，具有很强的针对性。

3. 充分反映发展迅速的国际标准和主要技术。

本书共分 5 篇。其中第 1 篇密码学和 PKI 基础，主要对密码学基本概念和经典密码算法作了介绍，并系统地讲述了公钥基础设施(PKI)。第 2 篇防火墙安全技术，对防火墙原理、分类、设计、体系结构作了系统的介绍，并讨论了 Linux 操作系统下的防火墙技术和实现、构建技术。第 3 篇入侵检测安全技术，介绍了入侵检测的概念、作用，数据包的截获与分析，入侵检测专家系统，规则语言设计，最后系统介绍了强大的 Snort 入侵检测系统。第 4 篇计算机病毒防治，着重病毒产生原因、特点、分类及其预防、检测和清除。第 5 篇系统安全，包括操作系统、数据库和网络站点的安全。为了方便读者，附录中给出了常用的网络安全政策法规网址，常用的网络安全相关网址和常见的网络安全工具网址。

全书由谢冬青、冷健、熊伟编写。谢冬青负责体系结构，章节安排，并编写第 1 篇和第 2 篇，熊伟编写了第 3 篇和第 4 篇，冷健编写了第 5 篇。

网络安全内容庞杂，发展迅速，书中谬误之处，请读者指正。

谢冬青

目　录

第 2 篇 防火墙安全技术

第 3 篇 入侵检测安全技术

第 4 篇 计算机病毒防治

第 5 篇 系 统 安 全

第 1 篇　密码学和 PKI 基础

第 1 章　网络信息安全与密码算法

1.1　网络信息安全概述

网络和信息系统是现代社会最重要的信息基础设施，是知识经济的基础载体和支撑环境。信息化工作是一项涉及国家经济和社会发展全局的战略性工作，信息化将改变人们的生产、生活、工作、学习方式，意义重大，影响深远。信息安全关系到国家的存亡，经济的发展，社会的稳定，民族文化的继承和发扬。从现在到 2010 年是我国信息化建设的高潮阶段，国家在经济、金融、商务、工业、文化、教育、国防和安全以及公民在教育、就业、医疗等社会保障方面的信息均将有效地组织起来，构成若干国家信息基础设施。运行在信息基础设施上的信息是社会发展的重要战略资源，它经过网络计算和处理，将直接为社会各种需求提供服务。

网络作为信息产业的基础，其安全重要性是不言而喻的，除了保证在网络上各种增值业务的加载业务运行畅通外，另一个重要指标就是信息安全，这里所指的信息安全，主要指网络信息安全。据相关统计资料显示，在信息安全事故中，发生在网络环境中的占 80%，而网络内部人员的违法犯罪造成的危害最大，所以做好网络的安全建设和管理，是保证信息安全的根本措施，必须引起高度重视。

1.1.1　网络发展历史

1. 互联网起源

互联网(Internet)是目前世界上最大的计算机网络，更确切地说是网络的网络(或者互联的网络)，几乎覆盖了整个世界。该网络组建的最初目的是为研究部门和大学服务，便于研究者及其学生探讨学术方面的问题，因此有科研教育网(或国际学术网)之称。进入 20 世纪 90 年代，互联网向社会开放，利用该网络开展商贸活动成为热门话题，人力和财力的投入，使得互联网得到迅速的发展。在我国，进入互联网成为国家电信部门近年来主要抓的大事之一，是组建 Chinanet 的主要目标。许多企业也逐步意识到进入互联网的重要性，不仅可以从网上索取大量的商业信息，更可以通过互联网向国际社会展现自己。

2. 中国网络发展

我国信息化建设的目标是：初步形成一定规模和比较完整的国家信息化体系；到 2010 年，将建立起健全的、具有相当规模的、先进的国家信息化体系。国家信息化体系由下列六个要素组成，即信息资源、国家信息网络、信息技术应用、信息技术与产业、信息化人才、信息化政策法规和标准。

可以看出,我国的信息化与外国的信息高速公路和国家信息基础设施有所不同。我国强调信息化体系六个要素之间的紧密关系,将信息资源开发利用放在核心地位。近年来,中国信息产业发展速度超过了国民经济的增长速度。中国通信网基本上实现了数字化和程控化。全国已经初步建成以光缆为主,以数字微波和卫星通信为辅,多种手段并用的网络。

1.1.2 网络和信息安全需求

网络安全需求定义为三个部分:网络安全硬件、网络安全软件、网络安全服务。网络安全硬件包括:防火墙和虚拟专用网(VPN)、独立的 VPN、入侵检测系统、认证令牌和卡、生物识别系统、加密机和芯片;网络安全软件包括:安全内容管理、防火墙/VPN、入侵检测系统、安全 3A(根据 IDC,3A 是 administration, authorization, authentication 三个英文单词的缩写)、加密,其中安全内容管理包括防病毒、网络控制和邮件扫描,安全 3A 包括授权、认证和管理;网络安全服务包括:顾问咨询、设计实施、支持维护、教育培训、安全管理。

从中国网络安全服务市场状况来看,尚处在起步阶段。这个市场有 2170 万美元的市场规模,还比较小,但它却有着非常高的市场增长潜力,预计到 2006 年能达到 2.65 亿美元,平均的增长率达到 65%,高出整个网络安全产品市场的平均数。更多的厂商和用户开始重视网络安全服务,一些成熟的行业如金融、电信行业在使用网络安全产品时,也意识到要为网络安全服务付费。目前中国客户还享受免费的服务,但随着安全服务的发展,相信还是会支付服务费用的。截止到 2001 年底,中国和信息安全相关的注册就有 1500 多家;具有研发能力的厂商有 350 家;有自己产品的厂商有 187 家,防火墙的厂商有 100 多家,而有成熟产品的厂商只有近 80 家。整个市场 80% 的利润,只来源于 20% 的厂商,可见中国的众多安全产品厂商举步维艰。

防火墙和防病毒产品被用户普遍认为是最需要的安全产品,其次依次是 IDS、加密、网络 3A。网络安全的迅猛发展为安全产品厂家也创造了市场机会,如关键行业的网络安全加固与更新;基于宽带的网络安全;移动网络的安全;个人网络安全;生物及个人安全认证;安全内容管理中的 email 扫描、IAC/EIM 等,还有为数最多的中小企业的网络安全,都将为安全产品厂商的发展提供难得的机会。

网络安全市场的威胁主要来自于用户对信息系统的依赖程度低;粗制滥造的产品流向市场,很多软件只是从网络上直接下载使用;网络安全产品的价格战;用户议价能力的提高等。

1.2 网络与信息安全分类

1.2.1 网络安全

网络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。网络安全是指网络系统的硬件、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。其重要性正随着全球信息化步伐的加快而变得越来越重要。从其本质上来讲,网络安全就是网络上的信息安全。从广义来说,凡是涉及到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安全的研究领域。网络安全的具体含义会随着"角度"

的变化而变化。比如:从用户的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免他人利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者角度说,他们希望对本地网络信息的访问、读写等操作受到保护和控制,避免出现"陷门"、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁,制止和防御网络黑客的攻击。对安全保密部门来说,他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵,避免机要信息泄露,避免对社会产生危害,对国家造成巨大损失。从社会教育和意识形态角度来讲,网络上不健康的内容,会对社会的稳定和人类的发展造成阻碍,必须对其进行控制。

21 世纪全世界的计算机都将通过 Internet 联到一起,信息安全的内涵也就发生了根本的变化。它不仅从一般性的防卫变成了一种非常普通的防范,而且还从专门的领域变成了无处不在。一个国家的信息安全体系实际上包括国家的法规和政策,以及技术与市场的发展。我国在构建信息防卫系统时,应着力发展自己独特的安全产品,我国要想真正解决网络安全问题,最终的办法就是通过发展民族的安全产业,带动我国网络安全技术的整体提高;建立起一套完整的网络安全体系,特别是从政策上和法律上建立起有中国自己特色的网络安全体系。

网络安全产品有自身的特点:网络安全来源于安全策略与技术的多样化,如果采用一种统一的技术和策略也就不安全了;网络的安全机制与技术要不断地变化;随着网络在社会各个方面的延伸,进入网络的手段也越来越多,因此,网络安全技术是一个十分复杂的系统工程。为此建立有中国特色的网络安全体系,需要国家政策和法规的支持及集团联合研究开发。安全与反安全就像矛盾的两个方面,总是不断地向上攀升,所以安全产业将来也是一个随着新技术发展而不断发展的产业。

1.2.2 信息安全

1. 信息安全的含义

信息安全(Information Security)是指信息的保密性(Confidentiality)、完整性(Integrity)和可用性(Availability)的保持。保密性是保障信息仅仅为那些被授权使用的人获取。完整性是保护信息及其处理方法的准确性和完整性。可用性意指保障授权使用人在需要时可以获取信息和使用相关的资产。信息的保密性针对信息被允许访问(Access)对象的多少而不同,所有人员都可以访问的信息为公开信息,需要限制访问的信息一般为敏感信息或秘密,秘密可以根据信息的重要性及保密要求分为不同的密级,例如国家根据秘密泄露对国家经济、安全利益产生的影响(后果)不同,将国家秘密分为秘密、机密和绝密三个等级,组织可根据其信息安全的实际,在符合《国家保密法》的前提下将其信息划分为不同的密级;对于具体信息的保密性有时效性,如秘密到期解密等。信息完整性一方面是指信息在利用、传输、储存等过程中不被篡改、丢失、缺损等,另一方面是指信息处理的方法的正确性。不正当的操作,如误删除文件,有可能造成重要文件的丢失。信息的可用性是指信息及相关的信息资产在授权人需要的时候,可以立即获得。例如通信线路中断故障会造成信息在一段时间内不可用,影响正常的商业运作,这是对信息可用性的破坏。不同类型的信息及相应资产的信息安全在保密性、完整性及可用性方面关注点不同,如组织的专有技术、市场营销计划等商业秘密对组织来讲保守机密尤其重要;而对于工业自动控制系统,控制信息的完整性相对其保密性重要得多。