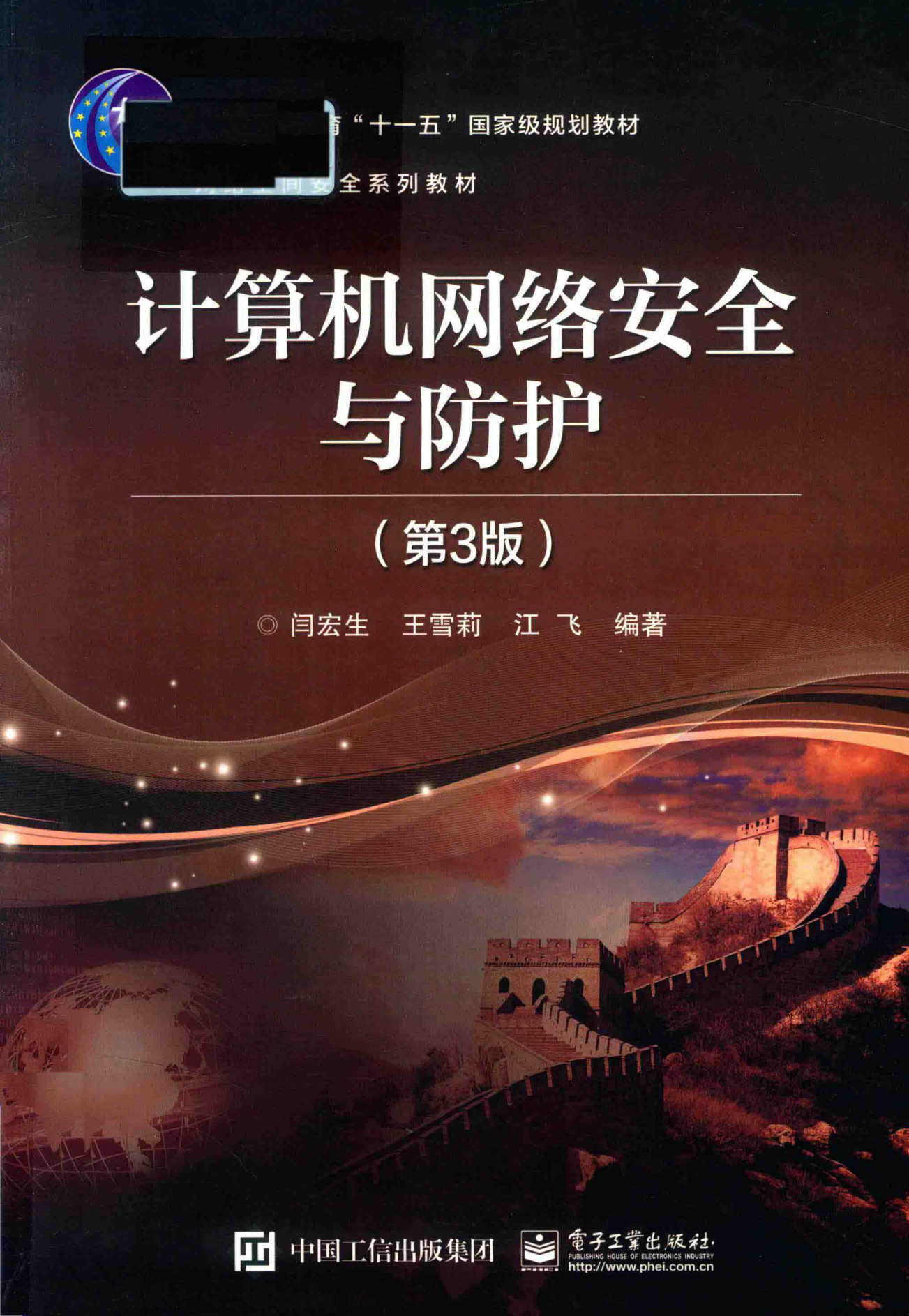

“十一五”国家级规划教材

全系列教材

计算机网络安全与防护

（第3版）

◎ 闫宏生　王雪莉　江 飞　编著

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

普通高等教育“十一五”国家级规划教材
网络空间安全系列教材

计算机网络安全与防护

（第3版）

闫宏生　王雪莉　江　飞　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书是普通高等教育“十一五”国家级规划教材，主要介绍计算机网络安全基础知识、网络安全体系结构、网络攻击，以及密码技术、信息认证技术、访问控制技术、恶意代码防范技术、防火墙技术、入侵检测技术、虚拟专用网技术、网络安全扫描技术、网络隔离技术、信息隐藏技术、无线局域网安全技术、蜜罐技术等，同时介绍网络安全管理的概念、内容、方法。全书内容广泛，注重理论联系实际，设计了 10 个实验，为任课教师免费提供电子课件。

本书适合普通高等院校计算机、网络空间安全、通信工程、信息与计算科学、信息管理与信息系统等专业本科生和硕士研究生使用。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

计算机网络安全与防护/闫宏生，王雪莉，江飞编著. —3 版. —北京：电子工业出版社，2018.7

ISBN 978-7-121-34445-9

Ⅰ. ① 计… Ⅱ. ① 闫… ② 王… ③ 江… 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（2018）第 119819 号

策划编辑：章海涛
责任编辑：章海涛
印　　刷：北京七彩京通数码快印有限公司
装　　订：北京七彩京通数码快印有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　　印张：17.5　　字数：440 千字
版　　次：2007 年 8 月第 1 版
　　2018 年 7 月第 3 版
印　　次：2018 年 7 月第 1 次印刷
定　　价：52.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：192910558（QQ 群）。

前　言

2014 年 2 月，在中央网络安全和信息化领导小组第一次会议上，习近平总书记以“没有网络安全就没有国家安全，没有信息化就没有现代化”的重要论断，提出了建设网络强国的战略目标。在其后一系列国际国内相关会议上，习近平总书记的网络安全观逐渐清晰。习近平总书记的网络安全观包括主权观、国家观、发展观、法治观、人才观、人民观、国际观、辩证观等方面，为建设网络强国，深化细化网络安全工作指明了方向。

2015 年，教育部将网络空间安全列为一级学科，学科建设迫切需要尽快形成成熟的课程教学体系，建设一批配套的精品教材，以适应网络安全人才培养与网络空间快速发展的需求。2016 年 4 月 19 日，习总书记在“网络安全和信息化工作座谈会”上指出，网络空间的竞争归根结底是人才竞争，建设网络强国，要聚天下英才而用之，为网信事业发展提供有力人才支撑。2016 年 11 月 7 日，全国人大正式通过了《中华人民共和国网络安全法》，将网络安全人才培养纳入其中。

2007 年 8 月，本书第 1 版出版，后来被教育部评为**普通高等教育“十一五”国家级规划教材**；2008 年 11 月，“信息网络安全防护”课程被**原总参通信部评为首批精品课程**，本书则是该课程的教学成果的凝结；2009 年 3 月，教材**获湖北省第六次高等教育优秀研究成果教材类二等奖**。2010 年在第 1 版基础上进行了修订。出版以来，教材得到了许多高等院校同仁和学生的支持、鼓励和厚爱，许多读者给我们写来热情洋溢的信件，提出了许多宝贵意见和建议，使我们深受感动和鼓舞，在此谨向他们表示衷心的敬意和感谢。

网络安全威胁不断出现新的变化，技术发展十分迅速，教材建设也要与时俱进，才能适应形势发展。我们组织人员对教材内容进行了梳理论证，提出了修订意见。第 3 版对第 2 版教材内容进行了适当调整，使之更具时代特色，更便于学生理解，更具实际操作性。全书内容广泛，注重理论联系实际，设计了适量习题和 10 个实验，并提供电子课件。任课老师可通过华信教育资源网（http://www.hxedu.com.cn），注册后免费下载课件。

本书由国防科技大学信息通信学院信息通信管理系网络安全技术与管理教研室组织编写，闫宏生教授担任主编，王雪莉、江飞、蔡均平、何俊、陈刚、李云凡、杨军、郭连城、瞿志强、代威等同志参与了修订工作。

本书在修订和出版过程中，得到了电子工业出版社的大力支持和指导；学院张旭院长、王梦麟副院长、教务处张炎明处长以及信息通信管理系沈建军主任等都对教材修订工作非常关注，提出了许多好的建议，在此一并表示衷心感谢。

作　者

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章 绪 论

伴随信息技术的飞速发展，计算机网络已经成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域，全面改变着人们的生产生活方式，深刻影响着人类社会历史发展进程。据中国互联网信息中心的最新调查报告，2017年年底我国网民规模已达到7.72亿人，普及率达55.8%，中国互联网呈现出前所未有的发展与繁荣。快速发展的计算机网络在给人们带来极大便利的同时，其安全问题更加凸显，如不及时采取积极有效的应对措施，必将影响我国信息化的深入持续发展，对经济社会的健康发展带来不利影响。2014年2月，在中央网络安全和信息化领导小组第一次会议上，习近平总书记指出，“没有网络安全就没有国家安全，没有信息化就没有现代化”，把网络安全上升到国家安全战略地位来看待，提出了建设网络强国的战略目标。进一步加强网络安全工作，创建一个健康、和谐的网络环境，需要我们不断深入研究，坚持积极防御、综合防范的原则，建立稳固的网络安全保障体系。

1.1 计算机网络安全的本质

计算机网络是指地理上分散布置的多台独立计算机通过通信线路互相连接所构成的网络，进一步说，还包括由大量计算机、数据库和通信线路构成的、提供各种信息服务的大型信息网络，包括多个相同或不同类型网络组成的网络系统。为叙述方便，本书中所称网络均特指计算机网络。根据2017年颁布的《中华人民共和国网络安全法》，网络安全是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。网络安全防护的根本目的是防止网络存储、处理、传输的信息被非法使用、破坏和窜改。网络安全的内容应包括两方面，即硬安全（物理安全）和软安全（逻辑安全）。

1. 硬安全

硬安全指系统设备及相关设施受到物理保护，免于破坏、丢失等，也称为系统安全。保障硬安全的目的是，保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限，防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

硬安全主要包括环境安全、设备安全和媒体安全三方面。环境安全是指对系统所在环境的安全保护，如区域保护和灾难保护。设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。媒体安全包括媒体数据的安全及媒体本身的安全。为了保证计算机系统的硬安全，除网络规划和场地、环境等要求外，还要防止系统信息在空间的扩散。

此为试读，需要完整PDF请访问：www.ertongbook.com

2．软安全

软安全包括信息完整性、保密性、可用性、可控性和抗抵赖性，也称为信息安全。软安全的范围要比硬安全更广泛，包括信息系统中从信息的产生直至信息的应用这一全过程。如果非法用户获取系统的访问控制权，从存储介质或设备上得到机密数据或专利软件，或者为了某种目的修改了原始数据，那么网络信息的保密性、完整性、可用性、可控性和真实性将遭到严重破坏。如果信息在通信传输过程中受到不同程度的非法窃取，或者被虚假的信息和计算机病毒以冒充等手段充斥最终的信息系统，使得系统无法正常运行，造成真正信息的丢失和泄露，会给使用者带来经济或政治上的巨大损失。

综上所述，保护网络的信息安全是最终目的。从某种程度上说，网络安全的本质就是信息安全。随着信息技术的发展与应用，信息安全的内涵也在不断延伸，从最初的信息保密性发展到信息完整性、可用性、可控性和抗抵赖性，进而发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”多方面的基础理论和实施技术。

1.2 计算机网络安全面临的挑战

自互联网问世以来，资源共享和信息安全一直作为一对矛盾体存在着，计算机网络资源共享的进一步加强所伴随的信息安全问题也日益突出，各种计算机病毒和网上黑客对互联网的攻击越来越猛烈，网络遭受破坏的事例不胜枚举。

1991 年，美国国会总审计署宣布，在海湾战争期间，几名荷兰少年黑客侵入美国国防部的计算机，修改或复制了一些与战争相关的敏感情报，包括军事人员、运往海湾的军事装备和重要武器装备开发情况等。

1994 年，格里菲斯空军基地和美国航空航天局的计算机网络受到两名黑客的攻击。同年，一名黑客用一个很容易破解的密码发现了英国女王、梅杰首相和其他几位军情五处高官的电话号码，并把这些号码公布在互联网上。美国一名 14 岁少年通过互联网闯入我国中科院网络中心和清华大学的主机，并向系统管理员提出警告。

1998 年，国内各大网络几乎都不同程度地遭到黑客攻击，8 月，印尼事件激起中国黑客集体入侵印尼网点，造成印尼多个网站瘫痪。与此同时，国内部分站点遭到印尼黑客的报复。同年，美国国防部宣称黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”，侵入了政府许多非保密性敏感计算机网络，查询并修改了工资报表和人员数据。

2000 年 2 月，在 3 天时间里，黑客使美国数家顶级互联网站雅虎、亚马逊、电子港湾、CNN 陷入瘫痪。同年 2 月 8 日至 9 日，我国门户网站新浪网遭到黑客长达 18 小时的袭击，其电子邮箱系统完全陷入瘫痪。

2001 年，从 4 月 30 日晚开始，由中美撞机事件引发的中美网络黑客大战的战火愈烧愈烈。短短数天时间，国内有逾千家网站被黑，其中近半数为政府（.gov）、教育（.edu）及科研（.ac）网站。11 月 1 日，国内网站新浪网被一家美国黄色网站攻破，以致沾染“黄污”。

2007 年 1 月初，一个名为“熊猫烧香”的病毒肆虐网络，可以使中毒计算机出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象，造成国家直接和间接经济损失达到 76 亿元人民币。

2009 年 5 月 19 日，由于暴风影音网站的域名解析系统受到网络攻击出现故障，导致电信运营商的服务器收到大量异常请求而引发拥塞，我国江苏、安徽、广西、海南、甘肃、浙

江等省份出现罕见断网故障。6月25日，搜狗发动了有史以来最大黑客攻击，导致腾讯所有的服务器全部瘫痪，所有腾讯产品均无法使用。7月7日，韩国总统府、国防部、外交通商部等政府部门和主要银行、媒体网站同时遭分布式拒绝服务（DDoS）攻击，瘫痪时间长达4小时，据统计共有12000台韩国境内的计算机和8000台韩国境外的计算机被病毒攻击，2万台计算机沦为“肉鸡”。

2010年1月12日，全球用户访问百度公司网站（baidu.com）出现异常，网站无法登录。

最近几年，全球网络安全威胁呈现出一些新的变化，新型网络威胁正呈现全球蔓延的态势，APT（Advanced Persistent Threat，高级持续性威胁）攻击者长期持续地对特定目标进行精准的打击，各领域的计算机犯罪和网络侵权等，无论数量、手段，还是性质、规模，都已经到了令人咂舌的地步。

2016年7月，美国三大政府网站congress.gov、美国国会图书馆网站、美国版权局均遭到DDoS攻击；10月，美国主要DNS服务器提供商Dyn Inc.的服务器遭遇大规模DDoS攻击，导致美国东海岸地区包括Twitter、CNN、华尔街日报在内的上百家网站无法访问，媒体将此次事件成为“史上最严重DDoS攻击”。

2016年发生了数十起数据泄露事件，2.7亿Gmail、Yahoo和Hotmail账号遭泄露；超过3200万Twitter账户密码泄露；超过3.6亿MySpace账户密码泄露。在大数据时代，数据泄露使得每个网民如同“透明人”毫无隐私可言。

2017年年初，国际上连续爆出多家知名企业用户信息泄露事件，其中包括全球四大会计师事务所之一的Deloitte（德勤）、加拿大电信巨头贝尔公司、知名教育平台Edmodo、知名云服务商Cloudflare等。泄露的信息主要为用户的隐私信息、私人账户信息、企业内部敏感文件与公司内往来邮件内容等，总计影响全球超2亿用户。

2017年3月，美国中央情报局数千份“最高机密”文档泄露，不仅暴露了全球窃听计划，还泄露了一个可入侵全球网络节点和智能设备的庞大黑客工具库。

2017年5月，一款名为“WannaCry”的蠕虫勒索软件袭击全球网络，通过加密计算机文档向用户勒索比特币。这被认为是迄今为止最大的勒索病毒事件，至少150个国家、30万用户中招，造成损失达80亿美元。中国部分Windows操作系统用户遭受感染，某些大型企业的应用系统和数据库文件被加密勒索，影响巨大。

2017年10月，用于保护Wi-Fi网络安全的WPA2安全加密协议被不法黑客破解。这意味着用户连接的绝大多数Wi-Fi处于易受攻击的状态，信用卡、密码、聊天记录、照片、电子邮件等重要信息随时有可能被不法黑客窃取。涉及平台包括Android系统、iOS系统以及Windows操作系统。

截至2017年12月底，针对中国境内目标发动攻击的境内外APT组织有38个，全年发动的攻击行动至少影响了超过万台计算机，攻击范围遍布国内31个省级行政区。

网络安全形势日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络上的合法权益面临严峻风险与挑战。

网络渗透危害政治安全。政治稳定是国家发展、人民幸福的基本前提。利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权，以及大规模网络监控、网络窃密等活动严重危害国家政治安全和用户信息安全。

网络攻击威胁经济安全。网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫

痪，造成灾难性后果，严重危害国家经济安全和公共利益。

网络有害信息侵蚀文化安全。网络上各种思想文化相互激荡、交锋，优秀传统文化和主流价值观面临冲击。网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息侵蚀青少年身心健康，败坏社会风气，误导价值取向，危害文化安全。网上道德失范、诚信缺失现象频发，网络文明程度亟待提高。

网络恐怖和违法犯罪破坏社会安全。恐怖主义、分裂主义、极端主义等势力利用网络煽动、策划、组织和实施暴力恐怖活动，直接威胁人民生命财产安全、社会秩序。计算机病毒、木马等在网络空间传播蔓延，网络欺诈、黑客攻击、侵犯知识产权、滥用个人信息等不法行为大量存在，一些组织肆意窃取用户信息、交易数据、位置信息以及企业商业秘密，严重损害国家、企业和个人利益，影响社会和谐稳定。

由于我国大部分网民缺乏网络安全防范意识，且各种操作系统及应用程序的漏洞不断出现，我国已经成为最大的网络攻击受害国。加之 CPU 芯片、操作系统、数据库和网关软件等大多依赖进口，支持互联网世界域名分配和解析的 13 台互联网域名根服务器全部设在以美国为代表的西方国家手里，这些因素使我国网络的安全性能大大降低，网络处于被窃听、干扰、监视和欺诈等安全威胁中，网络安全极度脆弱，互联网安全形势非常严峻。

1.3 威胁计算机网络安全的主要因素

从技术角度上看，Internet 拥有很多不安全因素，一方面，它是面向所有用户的，所有资源通过网络共享；另一方面，它的技术是开放和标准化的。因此，Internet 的技术基础仍是不安全的。从威胁对象讲，计算机网络安全所面临的威胁主要分为两大类：一是对网络中信息的威胁，二是对网络中设备的威胁。从威胁形式上讲，自然灾害、意外事故、计算机犯罪、人为行为、“黑客”行为、内部泄露、外部泄密、信息丢失、电子谍报、信息战、网络协议中的缺陷等，都是威胁网络安全的重要因素。从人的因素考虑，影响网络安全的因素还存在着人为和非人为两种情况。

1. 人为情况包括无意失误和恶意攻击

① 人为的无意失误。操作员使用不当，安全配置不规范造成的安全漏洞，用户安全意识不强，选择用户口令不慎，将自己的账号随意转告他人或与别人共享等情况，都会对网络安全构成威胁。

② 人为的恶意攻击，可以分为两种。一种是主动攻击，其目的在于窜改系统中所含信息，或者改变系统的状态和操作，以各种方式有选择地破坏信息的有效性、完整性和真实性。主动攻击较容易被检测到，但难于防范。因为正常传输的信息被窜改或被伪造，接收方根据经验和规律能容易地觉察出来。除采用加密技术外，还要采用鉴别技术和其他保护机制和措施，才能有效地防止主动攻击。另一种是被动攻击，在不影响网络正常工作的情况下，进行信息的截获和窃取，分析信息流量，并通过信息的破译获得重要机密信息，不会导致系统中信息的任何改动，而且系统的操作和状态也不被改变，因此被动攻击主要威胁信息的保密性。被动攻击不容易被检测到，因为它没有影响信息的正常传输，发送和接收双方均不容易觉察。但被动攻击容易防止，只要采用加密技术将传输的信息加密，即使该信息被窃取，非法接收者也不能识别信息的内容。这两种攻击均可对网络安全造成极大的危害，并导致机密数据的泄露。

2．非人为因素主要指网络软件的“漏洞”和“后门”

网络软件不可能是百分之百的无缺陷和无漏洞的，如 TCP/IP 协议的安全问题。然而这些漏洞和缺陷恰恰是黑客进行攻击的首选目标，导致黑客频频攻入网络内部的主要原因就是相应系统和应用软件本身的脆弱性和安全措施的不完善。另外，软件的“后门”都是软件设计编程人员为了自便而设置的，一般不为外人所知。但是一旦“后门”洞开，将使黑客对网络系统资源的非法使用成为可能。

虽然人为因素和非人为因素都可能对网络安全构成威胁，但是相对物理实体和硬件系统及自然灾害而言，精心设计的人为攻击威胁最大。因为人的因素最为复杂，人的思想最活跃，不可能完全用静止的方法和法律、法规来防护，这是计算机网络安全面临的最大威胁。

要保证信息安全就必须设法在一定程度上消除以上种种威胁，学会识别这些破坏手段，以便采取技术、管理和法律手段，确保网络的安全。需要指出的是，无论采取何种防范措施都不可能保证网络的绝对安全，网络安全是整体的而不是割裂的，是动态的而不是静态的，是开放的而不是封闭的，是相对的而不是绝对的。

1.4 计算机网络安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。通常，计算机网络安全策略模型包括建立安全环境的三个重要组成部分。

1．严格的法规

安全的基石是社会法律、法规与手段，这部分用于建立一套安全管理标准和方法，即通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

2．先进的技术

先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，再集成先进的安全技术，形成全方位的安全系统。

3．有效的管理

各网络使用机构、企事业单位应建立相应的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

网络安全策略是指在一个网络中对安全问题采取的原则，包括对安全使用的要求，以及如何保护网络的安全运行。制定网络安全策略首先要确定网络安全要保护什么，在这一问题上一般有两种截然不同的描述原则：一种是“一切没有明确表述为允许的都被认为是禁止的”；另一种是“一切没有明确表述为禁止的都被认为是允许的”。对于网络安全策略，一般采用第一种原则来加强对网络安全的限制。对于少数公开的试验性网络可能会采用第二种较宽松的原则，在这种情况下，一般不把安全问题作为网络的一个重要问题来处理。

在确定了描述原则后，网络安全策略所要做的是确定网络资源的职责划分。网络安全策略要根据网络资源的职责确定哪些人允许使用某一设备，对每台网络设备要确定哪些人能够修改它的配置；更进一步要明确，授权给某人使用某网络设备和某资源的目的是什么，他可以在什么范围内使用，并确定对每个设备或资源，谁拥有管理权，即可以为其他人授权，使其他人能够正常使用该设备或资源，并制定授权程序。

关于用户的权利与责任，在网络安全策略里中需要指明用户必须明确了解他们所用的计算机网络的使用规则。其中包括：是否允许用户将账号转借给他人，用户应当将他们自己的口令保密到什么程度；用户应在多长时间内更改他们的口令，对其选择有什么限制；希望由用户自身提供备份还是由网络服务提供者提供备份。在关于用户的权利与责任中还会涉及电子邮件的保密性和有关讨论组的限制。在电子邮件组织（Electronic Mail Association）发表的白皮书中指出，Internet 中每个计算机网络都要有策略来保护职员与用户的隐私。事实上，网络安全策略中能达到的一定只是用户希望达到绝对隐私与网络管理人员为诊断、处理问题而收集用户信息的折中。安全策略中必须明确在什么情况下网络管理员可以读用户的文件，在什么情况下网络管理员有权检查网络上传送的信息。

另外，网络安全策略还应说明网络使用的类型限制。定义可接受的网络应用和不可接受的网络应用，要考虑对不同级别的人员给予不同级别的限制，但一般的网络安全策略都会声明每个用户都要对他们在网络上的言行负责。所有违反安全策略、破坏系统安全的行为都是被禁止的。在大型网络的安全管理中，还要确定是否要为特殊情况制定安全策略，如是否允许某些组织（如 CERT 安全组）来试图寻找系统的安全弱点。对于此问题，对来自网络本身之外的请求，一般的回答是否定的。

在网络安全策略中，在确定对每个资源管理授权者的同时，还要确定他们可以对用户授予什么级别的权限。如果没有资源管理授权者的信息，就无法掌握哪些人在使用网络。对于主干网络中的关键通信资源，对其可授权范围应尽可能小，范围越小就越容易管理，相对就越安全。同时，要制定对用户授权过程的设计，以防止对授权职责的滥用。网络安全策略中可以明确每个资源的系统级管理员，但在网络的使用中难免会遇到用户需要特殊权限的时候。一种好的处理办法是尽量只分配给用户能够完成任务所需的最小权限。另外，网络安全策略中还要包含对特殊权限进行监测统计的部分，如果对授予用户的特殊权限不可统计，就难以保证整个网络不被破坏。

在明确网络用户、系统管理员的安全责任，正确利用网络资源要求的同时，还要准备检测到安全问题或系统遭受破坏时所采取的策略。对于发生在本网络内部的安全问题，要从主干网向地区网逐级过滤、隔离。地区网要与主干网形成配合，防止破坏蔓延。对于来自整个网络以外的安全干扰，除了必要的隔离与保护外，还要与对方所在网络进行联系，以进一步确定消除安全隐患。每个网络安全问题都要有文档记录，包括对它的处理过程，并将其送至全网各有关部门，以便预防和留作今后进一步完善网络安全策略的资料。

网络安全策略还要包括本网络对其他相连网络的职责，如出现某个网络告知有威胁来自我方网络。在这种情况下，一般不会给予对方权利，让其到我方网络中进行调查，而是在验证对方身份的同时，自己对本方网络进行调查、监控，做好相互配合。最后，网络安全策略一定要送到每个网络使用者手中。对付安全问题最有效的手段是教育，提高每个使用者的安全意识，从而提高整体网络的安全免疫力。网络安全策略作为向所有使用者发放的手册，应注明其解释权归属何方，以免出现不必要的争端。

1.5 计算机网络安全的主要技术措施

不同环境和应用中的计算机网络安全有不同的含义和侧重，相应的技术措施也各不相同。例如：

① 运行系统的安全主要是保证信息处理和传输系统的安全，侧重保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免因电磁泄漏而产生信息泄露，干扰他人或受他人干扰。

② 系统信息的安全包括用户口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治和数据加密等措施。

③ 信息传播的安全是信息传播后果的安全，通过信息过滤等措施，侧重防止和控制非法、有害信息的传播，避免公用网络上大量自由传输的信息失控。

④ 信息内容的安全，侧重保护信息的保密性、完整性和抗抵赖性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质是保护用户的利益和隐私。

实际上，网络安全技术措施及相对应的控制技术种类繁多并相互交叉。虽然没有完整统一的理论基础，但是在不同场合下，为了不同的目的，这些技术确实能够发挥出色的功效。目前普遍采用的措施有：利用操作系统、数据库、电子邮件、应用系统本身的安全性，对用户进行权限控制；在局域网的桌面工作站上部署防病毒软件；在 Intranet 与 Internet 连接处部署防火墙和入侵检测系统；某些行业的关键业务在广域网上采用较少位数的加密传输，而其他行业在广域网上采用明文传输等。

近年来，随着大数据、云计算、移动互联网、物联网、区块链、人工智能技术的融合发展，给网络安全也带来了更大挑战，涌现了可信计算技术、大数据安全技术、无线局域网安全技术、云计算安全技术、物联网安全技术等。以某军事信息网络为例，信息系统中常用的网络安全技术措施，如图 1-1 所示，具体将在后续章节中详细分析。

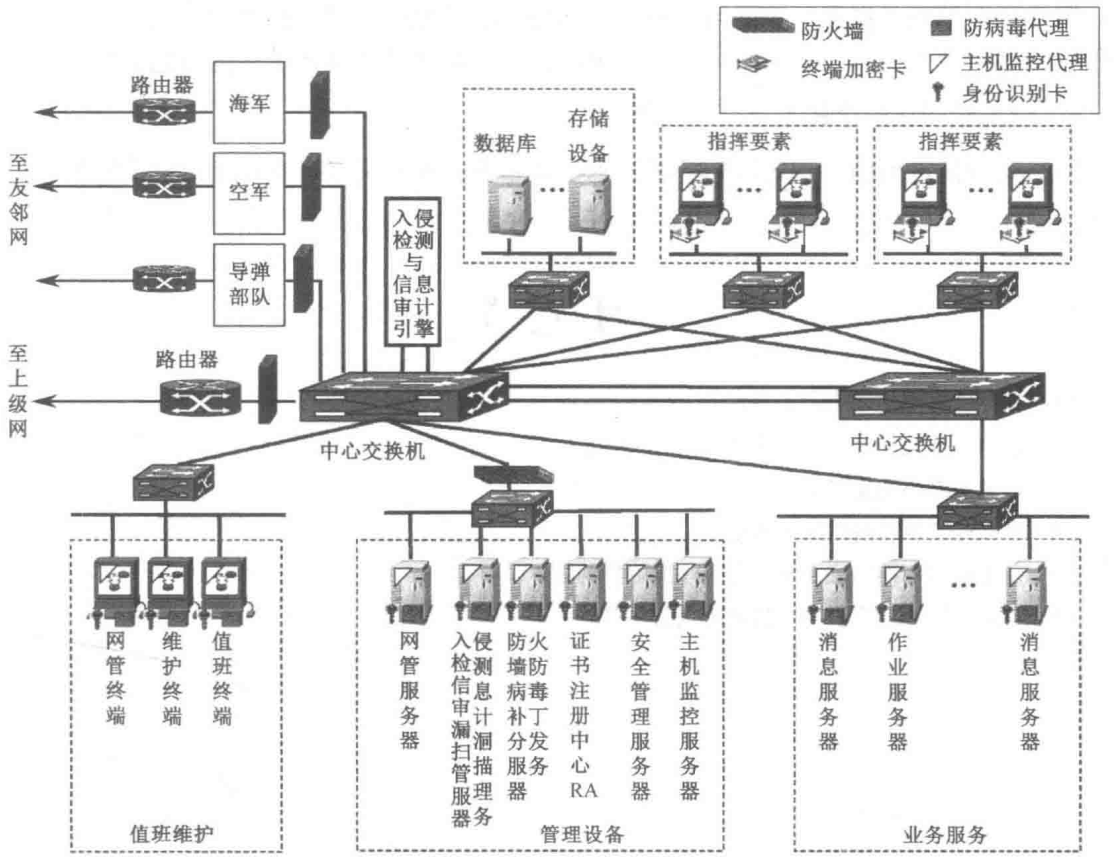

图 1-1　信息系统中常用的网络安全技术措施

此为试读，需要完整PDF请访问：www.ertongbook.com