新世纪高等学校规划教材 · 网络工程系列

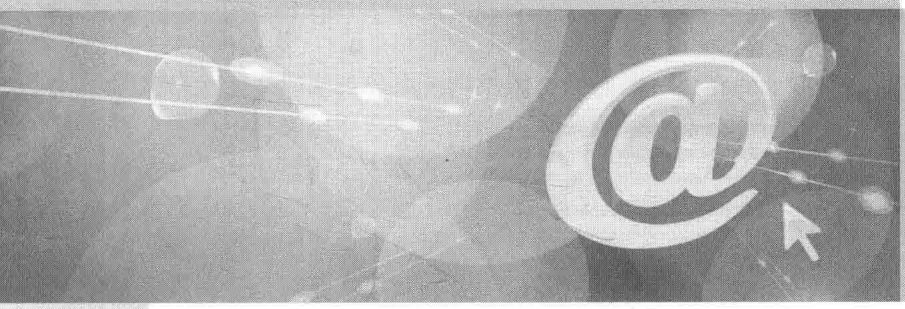
网络信息安全

主　编◎王小英
副主编◎刘庆杰　潘志安
参　编◎庞国莉　孙晓玲　陈玉伟

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

新世纪高等学校规划教材 · 网络工程系列

WANGLUO XINXI ANQUAN



网络信息安全

主　编◎王小英
副主编◎刘庆杰　潘志安
参　编◎庞国莉　孙晓玲　陈玉伟

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

图书在版编目（CIP）数据

网络信息安全／王小英主编．—北京：北京师范大学出版社，2017.4

新世纪高等学校规划教材·网络工程系列

ISBN 978-7-303-21772-4

Ⅰ．①网… Ⅱ．①王… Ⅲ．①计算机网络－信息安全－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（2016）第 301857 号

营 销 中 心 电 话 010-62978190 62979006
北师大出版社科技与经管分社网 www.jswsbook.com
电 子 信 箱 jswsbook@163.com

出版发行：北京师范大学出版社 www.bnupg.com
北京市海淀区新街口外大街 19 号
邮政编码：100875

印 刷：北京京师印务有限公司
经 销：全国新华书店
开 本：787 mm × 1092 mm 1/16
印 张：21.5
字 数：468 千字
版 次：2017 年 4 月第 1 版
印 次：2017 年 4 月第 1 次印刷
定 价：46.00 元

策划编辑：李 丹 责任编辑：李 丹
美术编辑：刘 超 装帧设计：刘 超
责任校对：毛姗姗 责任印制：赵非非

前　言

网络信息安全问题已经成为网络用户面临的一大挑战，如何在网络的海洋中安全遨游，已成为每个网络用户必须要思考的问题。那么作为计算机专业的学生，尤其是维护网络安全的学生，掌握网络安全知识尤为重要。

作者从事网络安全教学近 10 年，根据多年教学的经验和总结，编写本教材。

本书针对应用型本科学生的特点组织编写，注重理论与实践相结合，从网络攻击和防护的角度阐述网络安全原理与实践。在网络防护部分，主要介绍原理和方法，并简要介绍原理与技术的具体应用。在网络攻击部分，主要介绍方法和实践，披露一些“黑客秘技”，并给出大量的实验操作过程和代码供使用者参考，兼顾到教材的实用性和可读性。

本书将网络安全所涉及的各个知识点进行了详细的归纳总结，并以工程案例为主线，将理论知识融入工程案例中，便于学生的理解、学习和掌握。

本书共分 14 章。第 1 章主要介绍网络安全的概念、体系结构等；第 2 章主要介绍网络安全协议；第 3 章主要介绍操作系统安全的配置；第 4 章主要介绍数据库安全；第 5 章主要介绍信息加密技术中的 DES 和 RSA 的算法；第 6 章主要介绍密码算法在数字签名过程中的应用；第 7 章主要介绍常见的计算机病毒及其防范技术；第 8 章主要介绍网络攻击的全过程以及防御的流程；第 9 章和第 10 章主要介绍网络安全防御的技术，即防火墙技术和入侵检测技术；第 11 章主要介绍 VPN 的相关技术；第 12 章主要介绍无线网安全的相关技术；第 13 章主要介绍电子商务的安全技术；第 14 章主要介绍网络安全评估的技术和流程。

本书由王小英、刘庆杰、潘志安、庞国莉、孙晓玲、陈玉伟共同编写。最后由王小英统稿，刘庆杰审定。

在编写本书过程中，白张旋、刘凯峰、苏旺、梁亚鑫、张晓东等多位同学帮助验证实验步骤，在此对给予帮助和支持的同人表示深深的感谢。

由于作者水平有限，书中不足之处在所难免，敬请读者批评指正。

目　录

第 1 章　网络安全概论

教学目标

通过本章的学习使学生掌握网络安全的含义、网络安全威胁；了解 OSI 安全服务、OSI 安全机制和 OSI 安全服务的层配置；掌握网络安全体系结构的基本模型。

教学要求

知 识 要 点	能 力 要 求
网络安全的含义	掌握网络安全的基本概念
网络安全威胁	掌握网络安全面临的威胁
OSI 安全服务	了解 OSI 安全服务
OSI 安全机制	了解 OSI 安全机制
OSI 安全服务的层配置	了解 OSI 安全服务的层配置
网络安全体系结构模型	掌握网络安全体系结构模型

网络安全是什么？每个接触计算机的人都会这么问，本章将详细给大家介绍网络安全的概念、特征及常遇到的网络安全威胁，网络安全体系结构及模型等知识，让大家对网络安全有一个初步的认识和了解。

1.1　网络安全概述

以 Internet 为代表的全球性信息化浪潮所带来的影响日益深刻，信息网络技术的应用正日益普及，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型的、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要因素，而 Internet 所具有的开放性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在以下两个方面。

1. 开放性

网络技术是全开放的，任何组织和个人都可能获得，因而网络所面临的破坏和攻击可能是多方面的。例如，任何具有不良企图的黑客可以对物理传输线路实施攻击，也可以对网络通信协议实施攻击；可以对软件实施攻击，也可以对硬件实施攻击。网络的国际化还意味着网络的

攻击不仅仅来自本地网络用户，它可以来自 Internet 上的任何一台主机，也就是说，网络安全所面临的是一个国际化的挑战。

2. 自由度

自由度意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而不受任何的法律限制。

开放的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得人们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力，同时人们又要面对网络开放带来的数据安全的新挑战和新危险。如何保护内部机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所必须考虑的重要事情之一。

1.1.1 网络安全案例

安全性是互联网技术中最关键也最容易被忽视的问题。许多组织都建立了庞大的网络体系，但在多年的使用中从未考虑过安全问题，直到网络安全受到威胁，才不得不采取安全措施。随着计算机网络的广泛使用和网络之间数据传输量的急剧增长，网络安全的重要性愈加突出。

2014 年 1 月 21 日下午 3 点 10 分左右，国内通用顶级域的根服务器忽然出现异常，导致众多知名网站出现 DNS 解析故障，用户无法正常访问。虽然国内访问根服务器很快恢复，但由于 DNS 缓存问题，部分地区用户“断网”现象仍持续数小时，至少有 2/3 的国内网站受到影响。微博调查显示，“‘1·21’全国 DNS 大劫难”影响空前。事故发生期间，超过 85% 的用户遭遇了 DNS 故障，引发网速变慢和打不开网站的情况；4 月 8 日，Open SSL 爆出本年度最知名的安全漏洞 Heart bleed，被形象地形容为致命的“心脏出血”。利用该漏洞，黑客坐在自己家里的计算机前，就可以实时获取约 30% 的 https 开头网址的用户登录账号和密码，其中包括网民最常用的购物、网银、社交、门户、微博、微信、邮箱等知名网站和服务，影响至少两亿中国网民。Open SSL 的“心脏出血”再一次把网络安全问题推到了公众面前。

2015 年 1 月，俄罗斯约会网站 Topface，2000 万用户名和电子邮件地址被盗。2 月，优步（Uber）披露，5 万名优步司机的个人信息被不知名的第三方人士获取，包括社保码、司机相片、车辆登记号等信息。3 月，医保提供商 Premera 蓝十字披露，1100 万客户的医疗和财务数据泄露；牙齿医疗机构 Advantage Dental 约 15 万患者信息泄露，包括姓名、住址、出生日期、电话和社保码。4 月，360 补天平台披露，遍布 19 个省份的社保系统相关信息泄露达 5279.4 万条，其中包括个人身份证、社保参保信息、财务、薪酬、房屋等敏感信息；美国 Metropolitan State 大学 16 万学生个人信息泄露，包括出生日期、家庭住址、电话、个人成绩。5 月，全球知名成人约会网站 Adult Friend Finder 390 万用户信息泄露，包括电子邮件、IP 甚至是性偏好信息；手机监听软件制造商 mSpy 约 40 万用户信息泄露，包括电子邮件、短信、照片、付款记录和跟踪数据；美国国税局超过 10 万名纳税人的财务信息泄露。7 月，内衣制造商 Hanesbrands 客户订单数据库被黑，约 90 万网络和电话用户信息泄露，包括地址、电话和信用卡后四位数字；Fire Keepers Casino 酒店披露 8.5 万信用卡和借记卡信息在 2014 年泄露，包括银行卡号、姓名、验证码和卡终止日期等信息。8 月，在线票务销售平台大麦网 600 余万用户账户和密码泄露并在黑色产业论坛公开售卖；英国电信运营商 Carphone Warehouse 约 240 万在线用户个人信息泄露，包括姓名、地址、出生日期和加密的信用卡数据。10 月，音乐众筹网站 Patreon 超过 16GB 的文档资料泄露，包括 230 万个用户的电子邮件地址；为美国移动电话服务公司 T-Mobile 提供数据服务的 Experian 遭到黑客入侵，导致 T-Mobile 的 1500 万用户个人信息泄露，包括用户姓名、出生日期、地址、社会安全号、ID 号码等；英国电信运营商 Talktalk 120 万用户信息泄露，包括电子邮件、名字和电话号码，以及数万银行账户信息；美国网络券商史考特超过 460 万客户的联系人信息被攻击者获取，泄露的信息为客户姓名与地址；乌云平台曝光网易用户数据库“疑

似泄露”，数量近 5 亿条。虽然至今没有证据证明这个数字，但许多普通网民纷纷表示自己的邮箱被登录篡改，甚至由于用网易邮箱注册苹果账户，而导致手机被网络犯罪分子锁住，也是一个不争的事实。11 月，喜达屋集团旗下 54 家酒店发现窃取信用卡信息的恶意软件，包括客户名称、信用卡号码、信用卡安全码和到期日期等信息泄露，泄露数量尚未公布；香港早教电子设备公司伟易达（VTech）500 万用户和 600 万儿童的个人信息泄露，包括登录密码、IP 地址、照片、聊天记录姓名、性别等。12 月，英国快餐连锁店 Waterspoons 65 万顾客信息泄露，包括姓名、出生日期、电子邮件和电话号码。

2016 年 7 月 16 日，四川广电主站文件上传漏洞导致服务器宕机。

2016 年 7 月 17 日，新浪某重要域名被入侵；星巴克某处泄露导致公司员工信息泄露；新疆交通信息网可控服务器权限受到威胁；花旗集团软件 Bug 存在 15 年，导致大量交易数据缺失，遭美证券交易委员会罚款 700 万美元。

据不完全统计，我国的网络安全问题近年来呈逐年上升趋势。2000 年公安部有关部门受理网络犯罪案件仅 2700 多起，2005 年增至 4500 多起，2010 年剧增为 7300 多起，2015 年至 2016 年，网络入侵事件天天都在发生，增速惊人。

有关黑客威胁的报道屡见不鲜，而内部工作人员的疏忽甚至有意充当间谍对网络安全已构成更大的威胁。内部工作人员能较多地接触内部信息，工作中的任何大意都可能给信息安全带来威胁。无论是有意的攻击，还是无意的误操作，都会给系统带来不可估量的损失。虽然目前大多数的攻击者只是恶作剧似的使用篡改网站主页、拒绝服务等攻击，但当攻击者的技术达到某个层次后，他们就可以窃听网络上的信息，窃取用户密码、数据库等信息，还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，可以删除数据库内容、摧毁网络节点、释放计算机病毒等。

综上所述，网络必须有足够强大的安全措施。无论是局域网还是广域网，无论是单位还是个人，网络安全的目标是全方位地防范各种威胁以确保网络信息的保密性、完整性和可用性。

1.1.2　网络安全的含义

网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可用性受到保护。要做到这一点，必须保证网络系统软件、应用软件、数据库系统具有一定的安全保护功能，并保证网络部件（如终端、调制解调器、数据链路）的功能仅仅能被那些被授权的人访问。网络的安全问题实际上包括两方面的内容，一是网络的系统安全，二是网络的信息安全，而保护网络的信息安全是最终目的。

从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、可控性的相关技术和理论都是网络安全的研究领域。保密性指确保信息不暴露给未授权的实体或进程。完整性则意味着只有得到授权的实体才能修改数据，并且能够判别出数据是否已被篡改。可用性说明得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。可控性表示可以控制授权范围内的信息流向及行为方式。

网络安全的具体含义随观察者角度不同而不同。从用户（个人、企业等）的角度来说，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保密性、完整性和不可否认性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯，即用户的利益和隐私不被非法窃取和破坏。从网络运行和管理者角度来说，希望其网络的访问、读写等操作受到保护和控制，避免出现“后门”、病毒、非法存取、拒绝服务，网络资源非法占用和非法控制等威胁，制止和防御黑客的攻击。对安全保密部门来说，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、对社会产生危害、给国家造成损失。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威胁，必须对其进行控制。

1.1.3 网络安全的特征

要保证网络安全，最根本的就是保证网络安全的基本特征发挥作用。因此，下面先介绍信息安全的五大特征。

1. 保密性

保密性指确保信息不暴露给未授权的实体或进程。

2. 完整性

完整性指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

3. 可用性

可用性指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。比如网络环境下的拒绝服务，破坏网络和有关系统的正常运行等都属于对可用性的攻击。

4. 不可否认性

不可否认性指通信双方在信息交互过程中，确信参与者本身，以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

5. 可控性

可控性指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息要在一定传输范围和存放空间内可控。除了采用常规的传播站点和传播内容监控这种形式外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

1.1.4 网络安全威胁

网络安全威胁是指实体对网络资源的保密性、完整性和可用性在合法使用时可能造成的危害。这些可能出现的危害，是某些别有用心的人通过一定的攻击手段来实现的。网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击；网络中的敏感数据有可能泄露或被修改；从内部网向公共网传送的信息可能被他人窃听或篡改等。

1. 网络安全威胁的种类

网络安全威胁主要有以下四种：

① 截获（Interception）：攻击者从网络上窃听他人的通信内容。

② 中断（Interruption）：攻击者有意中断他人在网络上的通信。

③ 篡改（Modification）：攻击者故意篡改网络上传送的通信内容。

④ 伪造（Fabrication）：攻击者伪造网络上的通信内容并进行传送。

上述四种威胁可划分为被动攻击和主动攻击两大类，截获信息的攻击称为被动攻击；中断、篡改和伪造信息的攻击称为主动攻击。

对网络安全威胁较大的还有如下四种恶意程序，分别为计算机病毒、计算机蠕虫、特洛伊木马和逻辑炸弹。

美国基础设施保护中心（NIPC）做了一个统计，近几年，平均每个月出现 10 种以上新的攻击手段。深圳市安络科技有限公司（CNNS）特地组织安全专家对近几十年的网络安全威胁，尤其是近几年出现的新攻击手段进行分析，从图 1-1 中可以看出，基于各种攻击机制的现成攻

击工具越来越智能化，也越来越傻瓜化。虽然大多数的攻击手段都惊人地相似，无非是蠕虫、后门、Rootkits 和 DDoS 等，但这些手段都体现了强大的威力。攻击手段的新变种与以前的相比，更加智能化，攻击目标直指互联网基础协议和操作系统。同时，黑客工具应用起来也越来越简单，使很多新手也能轻易使用黑客工具，而且，攻击者入侵技术要求越来越低。

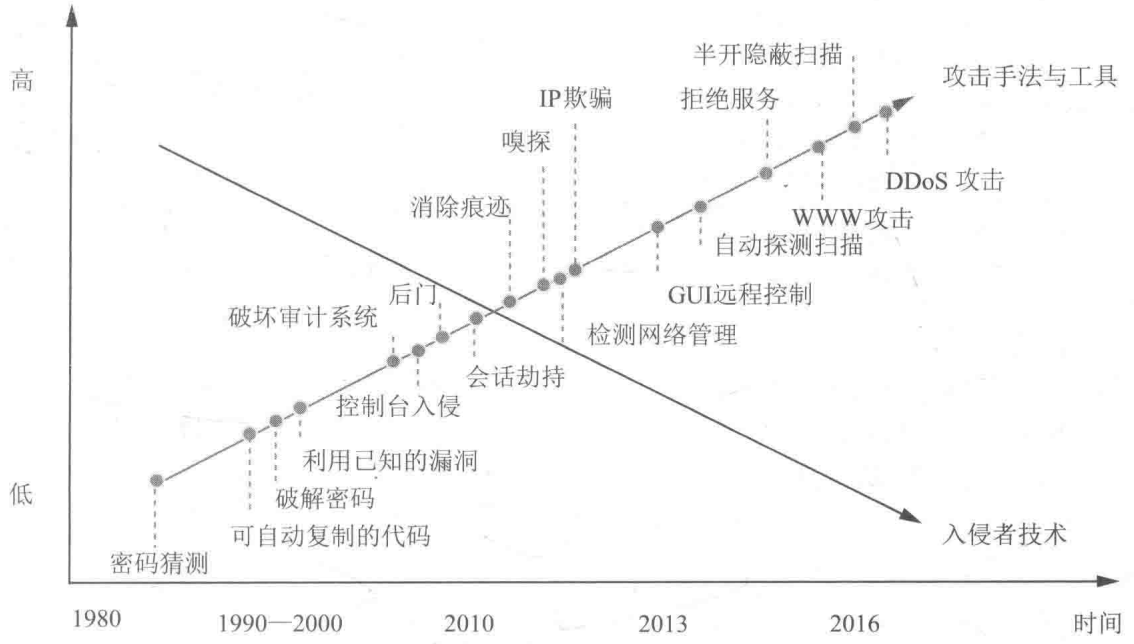


图 1-1　攻击手法与入侵者技术对比图

病毒技术与黑客技术的结合对信息安全造成更大的威胁。近年来，流行的计算机病毒无一例外地与网络结合，同时具有多种传播方法和攻击手段，一旦爆发即在网络上快速传播，难以遏制，加之与黑客技术的融合，潜在的威胁和损失巨大。从发展趋势来看，现在的病毒已经由从前的单一传播、单种行为，变成依赖互联网传播，具有电子邮件、文件传染等多种传播方式，融黑客、木马等多种攻击手段于一身的广义的“新病毒”。

2. 未来网络安全威胁的特点

今后恶意代码、网络安全威胁和攻击机制的发展将具有以下特点：

① 与互联网更加紧密地结合，利用一切可以利用的方式（如邮件、局域网、远程管理、即时通信工具等）进行传播。

② 所有的病毒都具有混合型特征，集文件传染、蠕虫、木马、黑客程序的特点于一身，破坏性大大增强。

③ 扩散极快，而且更加注重欺骗性。

④ 利用系统漏洞将成为病毒有力的传播方式。

⑤ 无线网络技术的发展使远程网络攻击的可能性加大。

⑥ 各种境外情报、谍报人员将越来越多地通过信息网络渠道收集情报和窃取资料。

⑦ 各种病毒、蠕虫和后门技术越来越智能化，并呈现整合趋势，形成混合性威胁。

⑧ 各种攻击技术的隐秘性增强，常规手段不能识别。

⑨ 分布式计算技术用于攻击的趋势增强，威胁高强度密码的安全性。

⑩ 一些政府部门的超级计算机资源将成为攻击者利用的跳板，网络管理安全问题日益突出。

3. 网络安全技术的特点

网络安全技术的发展是多维、全方位的，主要有以下几方面。