普通高等教育“十三五”计算机类规划教材

网络安全技术

◎ 刘化君　等编著

Wangluo
Anquan Jishu

第2版

机械工业出版社
CHINA MACHINE PRESS

普通高等教育“十三五”计算机类规划教材

网络安全技术

第2版

刘化君　等编著

机械工业出版社

本书内容共9章，包含网络安全理论、网络攻击与防护、网络安全应用及网络安全实验4个部分。网络安全理论部分介绍网络安全的基础知识、网络安全体系、TCP/IP的安全性以及系统平台安全等。网络攻击与防护部分从攻与防两个角度讨论网络安全技术，包括网络侦察、DoS/DDoS攻击、缓冲区溢出、欺骗攻击、防火墙、入侵检测、恶意代码防范与应急响应，以及网络攻击取证与安全审计等。网络安全应用部分讨论密码技术在网络安全中的应用、IP安全、VPN、安全电子邮件、Web安全技术和云计算安全。网络安全实验部分从搭建网络安全实验环境开始，分11个实验项目比较全面地呈现攻与防技术，使课程理论与实践紧密地结合起来。

本书内容丰富，技术性强，实现了网络安全理论与应用的完美结合，给读者以实用和最新的网络安全技术。

本书适用范围广，既可作为高等院校网络安全课程的教材和教学参考书，又可作为政府、企事业单位网络安全培训教材或参考书；对于具有一定网络管理、网络安全基础，并希望进一步提高网络安全技术水平的读者，也是一本理想的技术参考书。

图书在版编目(CIP)数据

网络安全技术/刘化君等编著. —2版. —北京：机械工业出版社，2015.4
普通高等教育“十三五”计算机类规划教材
ISBN 978-7-111-49936-7

Ⅰ.①网… Ⅱ.①刘… 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（2015）第074369号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)
策划编辑：刘丽敏 责任编辑：刘丽敏 吴晋瑜 吴超莉
版式设计：赵颖喆 责任校对：聂美琴
封面设计：张 静 责任印制：刘 岚
北京圣夫亚美印刷有限公司印刷
2015年6月第2版第1次印刷
184mm×260mm · 27印张 · 735千字
0001—2000册
标准书号：ISBN 978-7-111-49936-7
定价：55.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务 网络服务
服务咨询热线：010-88379833 机 工 官 网：www.cmpbook.com
读者购书热线：010-88379649 机 工 官 博：weibo.com/cmp1952
教育服务网：www.cmpedu.com
封面无防伪标均为盗版 金 书 网：www.golden-book.com

前　言

网络安全正面临着严峻的挑战，一方面是互联网规模扩大和关键应用的剧增，如电子政务、电子商务、电子支付与网络银行等网络应用业务的飞速发展，对网络安全的需求提高；另一方面是网络安全攻击的持续不断，安全威胁形式变化多样，给网络应用的健康发展带来巨大障碍。因此，网络安全问题已成为人们普遍关注的问题，网络安全技术也成为信息技术领域的重要研究课题。为适应网络安全技术发展及其课程教学需要，决定对《网络安全技术》第1版进行全面修订。

考虑到网络安全技术的新发展，结合一线教师和学生的反馈意见，本书第2版对上一版教材的内容进行了适当的调整和补充，主要包括：对内容的系统性进行了修订，如调整了网络安全体系结构，使之在体系上更科学，在逻辑上更合理；针对网络安全对内容实效性要求高的特点，对网络安全技术的实效性进行检查和更新，删除了一些陈旧的知识点，增加了当前最新的技术和发展动态，包括网络访问控制、网络存储备份、云计算安全，以及软件定义网络（SDN）的安全、物联网安全保障等，保持了网络安全技术的先进性；更加突出实验、实践能力的培养，将原第3章网络协议的安全性改写为网络协议安全性分析，更新了网络安全实验题目和方法，进一步凸显了理论与实践的紧密结合，使读者能够更好地结合实际应用进行学习。

本书仍然保持了第1版的内容体系结构，内容共9章，分为网络安全理论、网络攻击与防护、网络安全应用、网络安全实验4个大部分，涵盖了攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）等多方面的基本理论和技术。网络安全理论部分介绍网络安全的基础知识、网络安全体系结构、网络协议安全性分析、网络系统平台安全等。网络攻击与防护部分从攻与防两个角度讨论网络安全技术，包括网络信息收集技术、欺骗攻击及防范、DoS/DDoS攻击、缓冲区溢出攻击、网络资源访问控制、防火墙技术、入侵检测技术、恶意代码防范与应急响应，以及网络攻击取证与安全审计等内容。网络安全应用部分首先介绍密码技术在网络安全中的应用，然后重点讨论IP安全、虚拟专用网技术（VPN）、Web安全技术、云计算安全。网络安全实验部分从搭建网络安全实验环境开始，分11个实验项目介绍网络攻与防实验技术，使课程理论与实践紧密地结合起来。

本书这次修订在保持第1版体例结构、编著特色的基础上，进一步彰显了理论与实际紧密结合的工程应用性特色，主要特点如下。

1）内容丰富，科学合理，搭建了一个有机的知识体系。在教学内容选取方面进行了深入的考虑，遵照循序渐进的基本原则构建了一条知识链；在协调内容的深度、广度、难度的关系时，充分考虑学生的基础和能力，使之能够适应普通高等教育专业教学需要；在理论与应用知识的比例方面，在保持科学性和实用性的同时，使理论与技术相得益彰。

2）理论与实践密切结合，侧重实践能力的培养。网络安全课程的宗旨是培养学生在信息存储、传输和处理过程中所应具备的解决安全问题的能力，是一门实践性很强的课程。本书将大量网络安全实例融合到理论阐释之中，实现了理论指导下的实践，实践基础上的理论提升。更为重要的是精选了11个实验项目并单列一章，从实验环境搭建到网络安全攻防多个层面，将网络安全实践能力培养提高到了一个新的水平。

3）言简意赅，清楚易懂，理论阐述严谨、透彻，技术讨论翔实、细致。在编写过程中，融入学科方法论，倡导科学的思维方法，通过大量的图表，形象直观地讲解了知识概念。

本书可作为高等院校信息安全、计算机类、电子信息类各专业本科生和研究生的教材或教学参考书，也可作为政府、企事业单位网络安全培训教材或参考书；对于具有一定网络管理、网络安全基础，并希望进一步提高网络安全技术水平的读者，仍是一本理想的技术参考书。

本书由杨洁（南京工程学院）执笔编写第4章、第9章，并对本书提出了许多具体的修订意见，钱骁执笔撰写第6章中的网络访问控制部分的初稿，顾礼峰执笔改写了第9章中的9.1节和实验11基于路由器VPN安全配置等内容，其余各章节由刘化君执笔编撰。全书由刘化君统编定稿。在编写过程中，许多研究生如邓大为等同学也参与了相关工作。在本书编写过程中参阅了大量中外文献及安全网站，从中获得了许多启示和帮助，在此一并表示衷心感谢！

网络安全是一个内容广博、不断发展的技术领域。在本书的编撰过程中，尽管编者力求精益求精，及时吸纳最新的网络安全研究成果及技术，但由于编者理论水平和实践经验所限，书中的疏漏和不足之处在所难免，敬请广大读者批评指正。

编 者

目　录

第1章 绪 论

信息网络的迅速发展普及应用，在给人们的工作、生活带来巨大便利的同时，也带来了许多安全隐患，出于政治、经济、文化等利益的需要或者好奇心的驱动，网络攻击事件层出不穷、屡见不鲜，且有愈演愈烈之势；轻者会给个人或机构带来信息损害和经济利益损失，重者将会影响国家的政治、经济和文化安全。因此，信息网络安全问题已成为国内外重大的研究课题之一。

信息网络安全是一个非常复杂的综合性问题，涉及包括技术、产品和管理在内的诸多因素。网络安全主要研究信息网络的安全理论、安全应用和安全管理技术，确保网络免受各种威胁和攻击，以便能够正常工作。本章主要介绍网络安全的基本概念、网络安全风险及其评估、网络安全策略；并讨论信息网络安全研究的主要内容、关键技术以及发展趋势。

1.1 何谓网络安全

互联网技术的普及应用，使得信息突破了时间和空间上的障碍，信息的价值在不断提高。然而，计算机技术、网络技术及信息技术也与其他科学技术一样是一把双刃剑。在大部分人使用信息技术提高工作效率，为社会创造更多财富的同时，也有一些人在利用信息技术做着相反的事情。他们非法侵入他人的计算机系统窃取机密信息、篡改和破坏数据，给社会造成了难以估量的巨大损失。网络安全日渐成为关系国计民生的大事，已经引起了全社会的高度重视。网络安全涉及网络和通信，并不像初次接触这个领域的人想象的那样简单。网络安全所涉及的内容很多，下面先介绍一些有关信息安全、网络安全的基本概念。

1.1.1 安全的历史回顾

“安全”一词通常被理解为“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”。这是在广泛意义上对安全的表述。对信息技术而言，纵观其快速发展与广泛的应用，信息安全的含义也有一个不断丰富和发展的过程。根据社会对信息安全的需求，它经历了三个重要的发展阶段。

第一个阶段是通信安全阶段，这一历史时期比较长。早在远古时代，就有了信息安全的概念。那时，所有资产都是物理的，重要的信息也是物理的，如将文字刻在石头上、竹片上，到后来写在纸张上。保护这种信息，也是采取一些物理性的手段，如深藏密宫、护卫把守等。这时信息传递通常也只能用信使完成，飞鸽传书也算是一种信息传递方式。物理安全存在许多安全缺陷，如果报文在传递过程中被截获，报文的信息就会被敌人知悉，因此产生了通信安全问题。早在公元前600年，Julius Caesar发明了凯撒密码（Caesar Cipher），从此，敌方即使截获了报文，也无法读懂。此后，加密报文这个概念得到了迅速发展与应用，一直到目前的量子密码。与此同时，军事通信也开始使用密码技术，即将每个字符编码后放入报文传输。敌人即使通过无线电通信手段窃听、截获到报文，也无法识别其含义。在这一时期，通信安全的主要任务是解决数据传输的安全问题，所采取的主要措施是密码技术。

到了20世纪中期，在广泛使用计算机等数据处理设备之前，主要依靠物理和行政手段来保障重要信息的安全。所采用的物理手段主要是将重要的文件资料存放在带有密码锁的文件柜或保

密室里；行政手段则是通过制订强有力的管理措施，对工作人员加强检查和限制。这时的信息安全技术尚处于原始工具阶段。

第二个阶段是计算机系统信息安全时期。当计算机技术普及之后，信息被以电子形式移植到计算机系统中，而计算机系统中的信息对任何访问者都是开放的。显然，存放在计算机系统中的文件和其他一些信息，需要一种自动工具来保护。这些自动工具（诸如分时共享系统、通过公共电话网或互联网可访问的系统等）可作为保护数据信息和阻止攻击者实施破坏行为的工具，因此便产生了计算机系统信息安全，简称计算机安全或信息安全。计算机安全的主要任务是解决计算机信息载体及其运行的安全问题；采取的主要措施是根据主、客体的安全级别，正确实施主体对客体的访问控制。

第三个发展阶段是信息安全保障，即网络系统安全阶段。当通过网络把分布在不同地理位置的计算机系统连接起来后，网络用户也来自社会各个阶层与部门，如何保护在网络中大量存储和传输的数据就越来越重要了，因此网络安全应运而生，并迅速发展起来。网络安全的主要任务是解决计算机信息载体及其运行的安全问题；采取的主要措施是提供完整的信息安全保障体系，包括防护、检测、响应和恢复。

实际上，对于计算机安全和网络安全并没有明确的界限，例如，对信息系统最常见的攻击是计算机病毒，它可能已经感染移动存储介质（如磁盘、U盘），然后再加载到计算机上，从而进入系统；也可能是通过互联网进入系统。无论哪一种情况，一旦病毒驻留在计算机系统中，就需要内部计算机安全工具来查杀病毒并恢复数据。

信息安全的继续发展是物联网的安全保障，即物联网安全阶段，也就是第四个阶段。物联网被称为继计算机、互联网与移动通信网之后的又一次信息产业浪潮。在物联网时代，人类会将基本的日常管理交给人工智能去处理，继而从烦琐的低层次管理中解脱出来，将更多的人力、物力投入到新技术的研发中。因此，物联网的信息安全也将更为重要。

1.1.2 信息安全

进入21世纪，信息技术给人们的生活、工作带来了数不尽的便捷和好处。与此同时，网页篡改、计算机病毒、系统非法入侵、信息泄漏、网站欺骗、拒绝服务、非法利用漏洞等信息安全事件时有发生，从而不断突显出信息安全的重要性。信息与信息系统安全现在已经成为一门新兴学科，而且是一门边缘交叉性学科，涉及通信技术、计算机科学、计算机网络、信息论、数论、密码学、人工智能及社会工程学等。

1. 信息安全的定义

由信息安全技术的发展过程可以知道，信息安全的内涵是在不断丰富和发展的。国际标准化组织（ISO）将计算机系统信息安全（Computer System Security）定义为“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然和恶意的原因而遭到破坏、更改和泄露”，这一定义偏重于静态信息保护。因此，可将计算机系统信息安全进一步定义为“计算机的硬件、软件和数据得到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，保障系统连续正常运行”，这一定义侧重了动态意义的描述。显然，“安全”一词是指将服务与资源的脆弱性降到最低限度，其中脆弱性是指计算机信息系统的任何弱点。

信息安全涵盖的内容比较丰富，包括操作系统安全、网络安全、病毒查杀、访问控制、加密与认证以及数据库安全等多个方面。

2. 信息安全的属性

美国国家信息基础设施（NII）的文献给出了信息安全的5个属性：可用性、可靠性、完整

性、机密性和不可抵赖性。这5个属性适用于国家信息基础设施的教育、娱乐、医疗、运输、国家安全、电力供给及分配、通信等广泛领域。

1.1.3 网络安全

20世纪90年代以来，计算机网络技术得到了飞速发展，信息的处理和传输突破了时间和地域的限制，网络化与全球化成为不可抗拒的世界潮流，互联网进入了社会生活的各个领域和环节。随着计算机的网络化和全球化，人们日常生活中的许多活动已逐步转移到网络中，然而，安全却是计算机网络尤其是互联网技术中的一个薄弱环节。

1. 网络安全的定义

假若A和B要应用网络进行通信，并希望该网络及其通信过程是“安全”的。在这里，A和B可以是两台需要安全交换路由表的路由器，也可以是希望建立一个安全传输连接的客户机和服务器，或者是交换安全电子邮件的应用程序，因此，可把A和B看作两个网络通信实体，即应用进程。A和B要进行网络通信并希望做到“安全”，那么，此处的安全意味着什么呢？显然，这个“安全”的内涵是丰富多彩的，且涉及多个方面。譬如，A和B希望存储在客户机或服务器中的数据不被破坏、篡改、泄露；它们之间的通信内容对于窃听者是保密的，而且在通信时，的确是在与真实的对方在进行；它们还希望所传输的内容即使被窃听者窃取了也不能理解其报文的含义；还要确保它们的通信内容在传输过程中没有被篡改；即使被篡改了，也应该能够检测到该信息已经被篡改、破坏。由此归纳起来，可以给出网络安全（Network Security）的定义：网络安全就是在分布式网络环境中，对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防数据、信息内容遭到破坏、更改、泄露，或网络服务中断或拒绝服务或被非授权使用和篡改。

对网络安全内涵的理解会随着“角色”的变化而有所不同，而且在不断地延伸和丰富，比如，从用户（个人、企业等）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，避免被他人利用窃听、冒充、篡改、抵赖等手段侵犯自身利益。

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（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。

可见，网络安全的内涵与其保护的信息对象有关，但本质都是在信息的安全期内保证在网络上传输或静态存放时允许授权用户访问，而不被未授权用户非法访问。因此，网络安全与信息安全的研究领域是交错与关联的。

网络安全涉及的内容既有安全理论、安全应用技术等方面的问题，还有社会、教育、法律等管理问题，这几个方面相互补充，缺一不可。技术方面主要侧重于防范非法用户的攻击，管理方面则侧重于防范人为因素的破坏。如何更有效地保护重要的数据信息、提高网络系统的安全意识，已经成为网络安全必须考虑和解决的重要问题之一。

2. 网络安全的特性

网络安全具有信息安全的基本属性。从其本质上来讲，网络安全就是要保证网络上信息存储

和传输的安全性。根据网络安全的定义，网络的安全具有下述几个特性。

（1）机密性

机密性（Confidentiality）是指网络通信中的信息，仅能由发送者和预定的接收者所理解。即便窃听者截获了报文，也会因为报文在一定程度上进行了加密处理（即进行了数据伪装）而不能解密（即理解）所截获报文的含义。这里所指的报文不但包括国家秘密，而且也包括各种社会团体、企业组织的工作秘密、商业秘密和个人私密（如浏览习惯、购物习惯）。防止信息失窃和泄露的保障技术称为保密技术。在网络的不同层次上，有不同的机制来保障机密性；在物理层上，主要是采取电磁屏蔽技术、干扰及跳频技术来防止电磁辐射造成的信息外泄；在网络层、传输层及应用层，主要采取加密、访问控制、审计等方法来保障信息的机密性。

（2）认证

认证（Authentication）是指发送者和接收者都应该能证实网络通信过程中所涉及的另一方，确信通信的另一方确实具有它们自己所声称的身份。人类面对面通信可以通过视觉很轻松地解决这个问题，但当通信实体在不能看到对方的媒体上交换信息时，认证就比较复杂了。认证是网络通信系统安全的基础。

（3）完整性

完整性（Integrity）是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被篡改，即信息的内容不能被未授权的第三方修改；数据在存储或传输的过程中不被修改、破坏，不出现数据包的丢失、乱序等。

（4）不可否认性

不可否认性（Non-Repudiation）也称为不可抵赖性。不可否认性是面向通信双方（人、实体或进程）信息真实统一的安全要求，它包括收、发双方均不可抵赖。一是源节点发送证明，它是提供给信息接收者的证据，使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞；二是交付证明，它是提供给信息发送者的证据，使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

（5）可用性

可用性（Availability）是指可被授权实体访问并按需求使用的特性。安全通信的一个关键要求就是首先能够进行通信，无论在何时，只要用户需要，网络通信系统必须是可用的，也就是说，网络通信系统不能拒绝服务。然而，用户的通信需求是随机的、多方面的（语音、数据、文字和图像等），有时还要求时效性，网络必须随时满足用户通信的要求。攻击者通常采用占用资源的手段阻碍授权者的工作，例如，网络环境下的拒绝服务、破坏网络系统的正常运行等都属于对可用性的攻击。可以使用访问控制机制阻止非授权用户进入网络，从而保证网络系统的可用性。增强可用性还包括如何有效地避免因各种灾害（战争、地震等）造成的系统失效。

（6）可靠性

可靠性（Reliability）是指系统在规定条件下和规定时间内完成规定任务的概率。可靠性是网络安全最基本的要求之一，网络不可靠，故障不断，就谈不上网络的安全。目前，对于网络可靠性的研究基本上偏重于硬件的可靠性。除了研制高可靠性的元器件设备以外，采取合理的冗余备份措施仍是最基本的可靠性对策。另外，许多网络故障与软件可靠性、人员可靠性和环境可靠性也有直接关系。

（7）可控性

可控性（Controllability）是指网络对信息的传播应具有控制能力，确保仅允许拥有适当访问

权限的实体以定义明确的方式，对访问权限内的资源进行访问。

机密性、完整性、认证和不可否认性将在相当长的时期内仍是安全通信的关键特性。可用性、可靠性和可控性则是对安全通信概念的最新扩展，是为保证网络基础设施安全免受攻击而提出的。

3. 网络安全是一个系统

由上述对网络安全定义及其特性的讨论可知，网络安全的内涵主要集中在对通信和网络资源的保护方面。实际上，网络安全不仅涉及安全防护，还涉及入侵检测、应急响应以及数据灾难备份与恢复等内容。在许多情况下，作为对攻击的响应，网络管理员需要设置附加的保护机制和措施。同时，网络攻击技术也应包含在网络安全研究的范畴之中。只有对网络攻击技术有比较深刻的了解，才能做好网络安全工作。因此，ITU-T X.800 标准认为：网络安全包括安全攻击（Security Attack）、安全服务（Security Service）和安全机制（Security Mechanism）等方面，并在逻辑上分别进行了定义。安全攻击是指损害机构所拥有信息安全的任何行为；安全服务是指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全性的服务；安全机制是指用于检测、预防安全攻击或者恢复系统的机制。在这种意义上，网络安全是通过循环往复的保护、攻击、检测和响应而实现的。

由此看来，网络安全不仅研究安全防护技术，还研究网络攻击技术以及用于防御这些攻击的对策。从网络系统安全的角度考虑，网络安全攻防技术包括防护技术和攻击技术两大类，如图 1-1 所示。

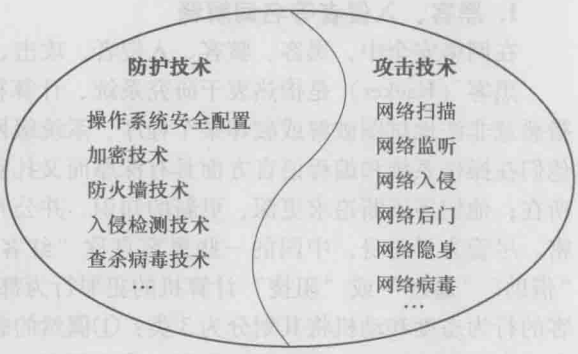

图 1-1 网络安全攻防技术

对于不同环境和应用中的网络安全，还可以将其划分为以下几个方面。

1）运行系统安全，即保证数据处理和传输系统的安全。它侧重于保证系统的正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的数据造成破坏和损失；避免由于电磁泄漏，产生信息泄露，干扰他人或受他人干扰。

2）网络系统信息的安全，包括用户口令认证、用户存取权限控制、数据存取权限、访问方式控制、安全审计、安全问题跟踪、计算机病毒防治和数据加密等。

3）网络信息的健康性，包括信息过滤等，主要指防止和控制非法、不健康的信息自由传输，抑制公用网络信息传输失控。

4）网络上信息内容的安全，主要侧重于保护信息的机密性、真实性（认证）和完整性。避免攻击者利用系统漏洞实施篡改、泄露、窃听、冒充、欺骗等破坏行为。

根据以上对网络安全定义的讨论可知，网络安全是一个系统。它不是防火墙、不是入侵检测、不是虚拟专用网，也不是加密、认证、授权以及审计。安全也不是网络设备公司及其任何合作伙伴或竞争对手能够为用户提供的任何东西。尽管这些产品、技术在其中扮演着十分重要的角色，但网络安全的概念更为宽泛。网络安全始于安全策略，还涵盖了必须遵守这些安全策略的人以及实施这些策略的人。那么，对于网络安全来说什么是系统呢？网络安全系统是指通过相互协作的方式为信息资产提供安全保障的全体网络产品、技术、策略以及最优做法的集合。因此，从狭义的角度看，网络安全是指防护网络系统和信息资源不受自然和人为有害因素的威胁和危害。若从广义的角度讲，凡是与网络上信息的机密性、完整性、认证、可用性、可控性、不可否认性

等相关的理论、技术和产品都属于网络安全的研究范畴。若从社会学的角度看，网络安全是一个系统，涵盖网络安全战略布局、安全文化、人才培养、产业发展等方面。

1.2 网络安全风险分析与评估

在明确了网络安全的含义之后，接下来考察网络究竟面临着哪些安全性威胁，影响网络安全的因素有哪些？并对网络攻击的类型、方式、手段以及网络安全风险进行分析讨论。网络安全风险分析与评估就是通过对网络系统的安全状况进行安全性分析，发现并指出存在的安全漏洞，将风险降低到可接受的程度。

1.2.1 网络面临的安全性威胁

自1988年莫里斯蠕虫病毒爆发以来，重大网络安全事故连续不断发生，每年都造成巨额的经济损失。更为值得注意的是，不但网络攻击的复杂性在持续增加，而且新型网络应用的发展又带来了新的安全性威胁，譬如，已经开始有越来越多的IT功能通过云计算来提供，网络犯罪也开始借此趋势，使用基于云计算的工具，部署远程攻击，甚至借此大幅拓展攻击范围。

1. 黑客、入侵者等名词解释

在网络安全中，黑客、骇客、入侵者、攻击、威胁等是使用频率较高的名词术语。

黑客（Hacker）是指热衷于研究系统、计算机及网络内部运作的人，骇客（Cracker）则是指恶意非法地试图破解或破坏某个程序、系统级网络安全的人。大多数黑客、骇客都是程序员，他们在操作系统和编程语言方面具有深厚而又扎实的专业知识，熟知网络系统中的漏洞及其原因所在；他们还不断追求更深、更新的知识，并公开他们的发现。黑客和骇客的特点是喜欢破译解密。尽管为了正身，中国的一些黑客自称“红客（Honker）”，但美国警方把所有涉及“利用”“借助”“通过”或“阻挠”计算机的犯罪行为都定义为Hacking。因此，人们一般也以黑客和骇客的行为态度和动机将其划分为3类：①偶然的破坏者。这类黑客喜欢进入他人主机系统，但没有一定的明确目标，多数是恶作剧。②入侵者（Cracker）。入侵者一般是指怀有不良企图，侵入甚至破坏远程主机系统完整性的人。这类黑客具有明确的破坏目的，并会给主机系统带来巨大的甚至是毁灭性的破坏。入侵者很容易识别，因为他们的目的是恶意的。③间谍。这类黑客以窃取他人私密信息或单位的商业资料为目的，或摧毁网络服务，对资源不加限制地访问等。

在RFC 2828中，对攻击的定义是：对系统安全的攻击，它来自于一种具有智能的威胁。也就是说，攻击是指有意违反安全服务和侵犯系统安全策略的（特别是方法或技巧的）智能行为。在RFC 2828中，对威胁的定义是：侵犯安全的可能性。也就是说，威胁是利用脆弱性的潜在危险。显然，所谓网络的安全性威胁就是指某个实体（人、事件、进程等）对某一网络资源的机密性、完整性、可用性及不可否认性等造成的危害。可见，攻击和威胁这两个术语的含义通常是相同的，因此在使用时有时也不加区别。对于网络管理人员来说，一切可能使网络系统受到破坏的行为都可视为攻击。

2. 网络系统面临的安全威胁

在全球范围内，计算机病毒、大规模的蠕虫、垃圾邮件、系统漏洞、僵尸网络、虚假有害信息和网络违法犯罪等问题日渐突出。据统计，全球约20s就会发生一次网络入侵事件，互联网上的防火墙约有1/4被攻破，约有70%以上的网络主管人员曾报告因机密信息泄露而受到了损失。网络系统面临的安全威胁形式各种各样，主要可以归纳为以下几种情况，如图1-2所示。

1）获取对网络信息的非授权访问，即侵犯信息的机密性或隐秘性。典型实例如Koobface等

安全问题对社交网站用户形成的安全威胁。这些恶意软件先感染用户计算机，然后再窃取信息。此类恶意软件一旦植入社交网站内部，无论用户是否访问社交网站，黑客都能毫无限制地窃取用户的资料和登录密码。

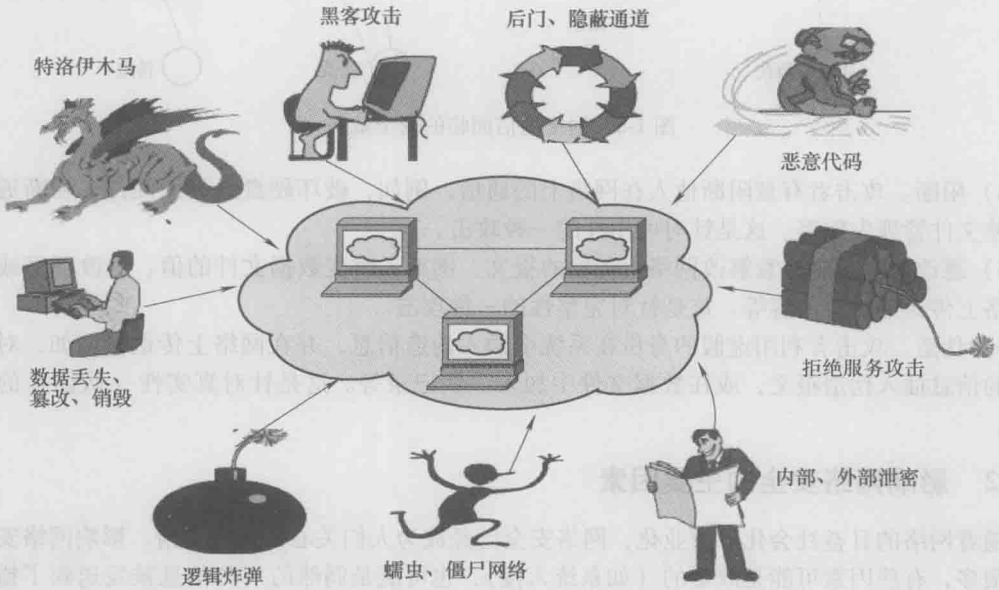

图 1-2 网络系统面临的安全威胁

2）冒充别的用户或盗用他人的合法权限，以达到制造欺诈信息、篡改合法信息、使用欺诈性的身份获取非授权访问以及进行欺诈性的认证等目的。

3）抵赖欺诈引起的责任；否认接收到了信息或接收信息的时间；否认已经给某人发送了某种信息等。

4）伪造其他用户信息，骗取信任，扩大合法访问权限，进行截获、窃取、破译，以获得重要机密信息，包括内部、外部泄密等。

5）将某些恶意信息隐藏于其他通信链路之中，或将自身作为中继插入到其他用户的通信链路中，如特洛伊木马等。

6）通过网络系统的漏洞、后门及隐蔽通道入侵他人系统，窃取机密数据或实施破坏活动。

7）通过加入一个秘密函数，使软件功能异常，破坏网络系统正常运行，如拒绝服务攻击等。

8）破坏网络通信基础设施，使网络用户无法进行通信；阻止其他用户之间的通信；特别是通过秘密介入，使合法通信被拒绝，如逻辑炸弹、蠕虫、僵尸网络等。

在现实世界中，上述安全威胁或网络攻击的实例屡见不鲜，难以数计。通常可把它们大体上分为两种：一种是对网络中信息的威胁；另一种是对网络设备的威胁。

3. 网络通信所面临的安全威胁

从网络通信的角度观察，可将网络通信安全所面临的威胁归纳为以下 4 种情况，如图 1-3 所示。

1）截获。攻击者从网络上窃听他人的通信内容，例如，通过窃听获取网络上传输的数据，或非授权复制文件或程序等。这是针对机密性的一种攻击。

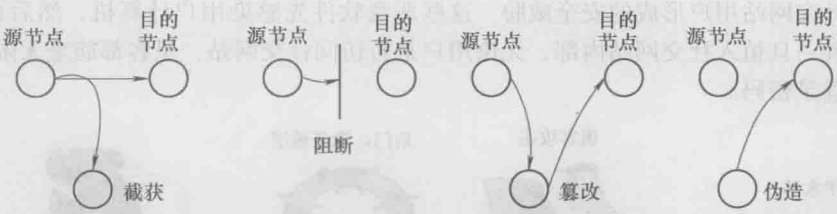

图 1-3 网络通信面临的安全威胁

2）阻断。攻击者有意阻断他人在网络上的通信，例如，破坏硬盘之类的硬件，切断通信线路，使文件管理失效等。这是针对可用性的一种攻击。

3）篡改。攻击者故意篡改网络上传输的报文，例如，改变数据文件的值、修改程序或修改在网络上传送的报文内容等。这是针对完整性的一种攻击。

4）伪造。攻击者利用虚假的身份在系统中插入伪造信息，并在网络上传送，例如，对网络传输的信息插入伪造报文，或在数据文件中加入一些记录等。这是针对真实性（认证）的一种攻击。

1.2.2 影响网络安全的主要因素

随着网络的日益社会化、商业化，网络安全已经成为人们关心的重要事情。影响网络安全的因素很多，有些因素可能是故意的（如系统入侵），也可能是偶然的（如信息被发送到了错误的地址）；可能是人为的，也可能是非人为的；还可能是外来攻击者对网络系统资源的非法使用。归纳起来，除了环境和灾难因素，诸如水灾、火灾、地震、电磁辐射等方面对网络的威胁外，针对网络系统的安全威胁主要来自于以下几个方面。

1. 人为因素

在网络安全问题中，人为因素是非常重要的。大多数网络安全事件都是人为因素造成的，不但危害性大，而且难以防御。

人为因素可分为有意和无意两种情况。有意是指人为地对网络进行恶意攻击，实施违纪、违法和犯罪活动。无意是指网络管理人员或者用户因工作疏忽大意造成的操作失误，虽然不是主观故意，但同样会对网络系统造成不良后果，例如，操作员配置不当造成的安全漏洞，用户安全意识不强、口令选择不当等引起的信息泄密，程序员开发的软件存在安全缺陷等。

2. 网络通信协议存在先天性安全漏洞

由于 TCP/IP 是在可信环境下，为网络互联专门设计的，从开始创建就缺乏安全性总体构想和设计。互联网是一个开放和自由的网络，它在增强了网络信息服务灵活性的同时，也给攻击和入侵敞开了方便之门，因而存在着许多安全隐患，所导致的结果就是，不仅传统的病毒借助互联网加快了传播速度、扩大了传播范围，而且各种针对网络协议和应用程序漏洞的新型攻击方法也层出不穷。

3. 计算机硬件系统故障

任何计算机系统都存在安全性问题，可以说绝对安全的计算机系统根本不存在。显然，由计算机系统组成的网络也不可能做到绝对安全。一个计算机系统，只要使用，就或多或少存在安全性问题，只是程度不同而已。对于网络互联设备，如路由器，承担着互联网上繁重的数据交换、转发任务，功能强大而且复杂，就目前的技术而论，不可能完全避免漏洞。

4. 操作系统的先天性缺陷

操作系统本身不可避免地存在各种漏洞，例如，可以远程创建和激活进程，但所提供的安全

认证功能却很有限；为系统开放提供的无口令入口等。尽管操作系统的缺陷可以通过版本的不断升级来克服，但不断增加新功能也会带来新的漏洞。

5. 网络数据库、应用软件存在的缺陷和漏洞

网络数据库、应用软件的安全隐患来自于软件设计和软件工程，而这些漏洞和缺陷恰恰是黑客进行攻击的首选目标，许多系统入侵事件大多是由数据库或应用软件存在安全漏洞、安全措施不完善所导致的。另外，有些软件的“后门”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，然而一旦“后门”洞开，造成的后果也将不堪设想。

6. 大数据手段的综合分析与深度挖掘

云计算和大数据技术的发展应用，不仅将人们的现实行为虚拟化为数据，其强大的计算能力也为存储、分析这些数据提供了无限可能性。也就是说，在大数据时代，遍布网络上的普通信息一旦达到一定数量级，或者一些看似不相关的数据一旦被整合起来，通过大数据手段的综合分析与深度挖掘，很可能会泄露十分重要的信息。这将是影响网络安全的一种全新因素，而且是一个严峻的新挑战。

1.2.3 网络安全风险评估

安全风险评估是近年迅速发展起来的一个新兴研究课题，也是网络安全领域需要迫切解决的“热点”“难点”问题。网络安全威胁多种多样，用户应如何应对？虽然不能完全消除网络安全威胁，但可以对网络进行安全评估和风险管理，从而使得安全威胁降到最低程度。风险评估的核心不仅仅是理论，更是实践，而且评估的实践工作非常困难。据国外统计数字显示，只有60%的风险评估是成功的。国内的风险评估工作更是面临着诸多挑战。下面在讨论网络风险评估要素的基础上，根据实际需要给出风险评估的主要环节及其实用的方法，以便实现有效的网络安全风险管理。

1. 完整意义上的风险评估

何为完整意义的风险评估？网络系统的安全风险，是指由于网络存在的脆弱性，人为或自然的威胁导致安全事件发生的可能性及其造成的影响，例如，Web站点可能面临诸多安全威胁，那么如何发现Web站点的安全漏洞，或者如何确认Web站点是否存在安全漏洞和弱点呢？这就需要对Web站点进行全面的安全风险评估。网络安全风险评估是指依据有关网络安全技术标准，对网络系统及由其处理、传输和存储信息的机密性、完整性和可用性等安全属性进行科学评价的过程。

在网络风险评估中，最终要根据对安全事件发生的可能性和负面影响的评估来识别网络系统的安全风险。一个完整意义上的风险评估要素有：①使命。使命即一个单位通过网络系统实现的工作任务。使命对网络系统的依赖程度越高，风险评估的任务就越重要。②资产及其价值。资产是指通过信息化建设积累起来的网络系统、信息、生产或服务能力等；价值是指资产的敏感程度、重要程度和关键程度。③威胁。网络资产可能受到的侵害。威胁可以用多种属性来描述，如威胁的主体（威胁源）、能力、资源、动机、途径、可能性和后果。④脆弱性。网络资产及其安全措施在安全方面的不足和弱点，也常称之为漏洞。⑤事件。威胁主体利用网络资产及其安全措施的脆弱性，实际产生危害的情况。⑥风险。由于网络系统存在的脆弱性，人为或自然的威胁导致安全事件发生的可能性及其造成的影响。⑦残余风险。采取安全措施、提高网络安全保障能力之后，网络仍然存在的风险。残余风险是不可避免的。⑧安全需求。为保证使命能够正常行使，在网络安全保障措施方面提出的具体要求。⑨安全措施。应对威胁，减少脆弱性，保护资产，限制意外事件的影响，检测、响应意外事件，促进灾难恢复和打击网络犯罪而实施的各种实践、规

程和机制的总和。

2. 网络风险评估的主要环节及其方法

通过对风险评估所涵盖的要素分析可知，网络风险评估是一个复杂的过程。许多研究给出了进行网络风险评估的过程与步骤。事实上，一个风险评估涉及诸多方面，主要包含风险分析、风险评估、安全决策和安全监测4个环节，如图1-4所示。

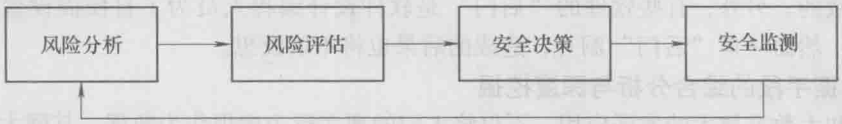

图1-4 网络安全风险评估涉及的4个环节

（1）安全风险分析

安全风险分析是风险评估的第一个环节。所谓风险就是指丢失所需要保护资产的可能性。网络安全风险分析就是估计网络威胁发生的可能性以及因系统的脆弱性而引起的潜在损失。大多数风险分析在最初要对网络资产进行确认和评估，此后再用不同的方法进行损失计算。就网络安全而言，漏洞和威胁是测定风险的两个主要对象。

1）漏洞。漏洞是攻击的可能途径。漏洞有可能存在于计算机和网络系统中，它允许入侵者打开系统，使网络攻击得逞。漏洞也可能存在于管理过程中，使得系统环境对攻击开放。

2）威胁。威胁是一个可能破坏信息系统环境安全的动作或事件。威胁包含3个组成部分：①目标。威胁的目标通常是安全属性或安全服务，包括机密性、完整性、可用性、可审性等。一个威胁可能含有多个目标。②代理（攻击主体）。代理有访问、知识和动机3个特性。③事件（攻击行为）。事件是代理采取的行为，导致对组织的损害。例如，一个黑客通过改变一个机构网站的Web页面来伤害它。

威胁加漏洞等于风险，风险是威胁与漏洞的综合结果。没有漏洞的威胁就没有风险，没有威胁的漏洞也就没有风险。风险的度量就是确定事件发生的可能性，虽然等级化网络及信息系统安全标准研究已取得了一些成果，通常是比较复杂的，一般将风险划分成低、中、高3个级别。

（2）风险评估

在进行网络安全风险评估时，所使用方法对评估的有效性有着举足轻重的作用。评估方法的选择直接影响到评估过程中的每个环节，甚至可以左右最终的评估结果。所以需要根据网络的具体情况，选择适当的风险评估方法。风险评估的方法有很多种，概括起来可分为两大类：定量的风险评估方法和定性的风险评估方法。

定量的风险评估方法是指运用数量指标来对风险进行评估。一般使用分布状态函数，并将风险定义为分布状态函数的某一函数。典型的定量分析方法有因子分析法、聚类分析法、时序模型、回归模型等。定量的风险评估方法的优点是用直观的数据来表述评估的结果，看起来一目了然，比较客观。采用这种评估方法，可以使研究结果更加科学、严谨。

定性的风险评估方法主要是依据研究者的知识、经验、历史教训、政策走向及特殊实例等非量化资料，对系统风险状况做出判断。它主要以与调查对象进行深入访谈所做出的个案记录为基本资料，然后通过理论推导、演绎的分析，对资料进行整理，做出评估结论。定性的风险评估方法不需要知道以前事件的概率值，可以从零开始建立合理的决策模型，是一种常用的分析方法。

网络安全风险评估工作不但十分具体，有时也很困难。因为真正的威胁往往非常隐蔽，在攻击事件发生之前，并不显现出来。对网络攻击事件进行评估时，可从以下几个方面展开。

1）检测难度。检测难度是指能否检测到网络攻击的难易程度，例如，有些端口扫描器扫描频率较高，就容易被网络入侵检测系统（NIDS）检测到，而SQL注入等则相对难以察觉。

2）攻击难度。攻击难度是指实现网络攻击目的难易程度。

3）攻击频度。频度即攻击的频率。几乎每天都发生端口扫描事件，而发生SQL注入、ARP欺骗等攻击的频率则相对较低。

4）影响。影响即网络攻击事件发生后造成的后果，比如，分布式拒绝服务（DDoS）攻击对电子商务系统等产生的影响可能是经济损失；而对国防、军事等重要系统产生的影响则是数据丢失和信息泄露。

通过对以上4个方面按5分制评定分数后，可采用如下公式计算出总体评估结论：总体评估值 = 检测难度 + 攻击难度 ×2 + 攻击频度 ×3 + 影响 ×4。若总体评估值低于10，则可以不必担心这类威胁；若总体评估值高于35，则需要关注这类攻击；总体评估值高于40，则属于高危漏洞，需要及时修补。

漏洞扫描实际上就是对系统安全性能的一个评估，通过漏洞扫描可以指出哪些攻击是可能的。目前已有许多用于风险评估的软件，以帮助评估临界系统和应用程序的漏洞，例如，Nessus就是一款比较流行的风险评估软件（可从http：//www. tenable. com/products/nessus下载），它根据已知的系统漏洞和弱点，对被评估的系统进行模拟攻击，最后给出一份详细的评估报告。

值得注意的是，在云计算和大数据背景下，过去一些针对小的系统或者设备所采用的风险评估方式已不再适应网络安全形式发展的需求，需要对整个行业的大系统做综合的整体风险评估。因为在大数据时代，局部的风险一旦累加起来，零散的事件信息很可能会泄露一个重要的信息。

（3）安全决策

安全决策就是根据评估结论决定网络系统所需要采取的安全措施。风险分析与评估的目的是为了向网络管理者提供决策支持信息，进而形成合理的、有针对性的安全策略，使网络威胁得到有效控制。在安全决策的过程中，根据评估的结论可选择使用以下某一策略。

1）逃避策略。这种策略即针对现有的安全问题，不采取任何安全措施加以防范。

2）应对策略。这种策略即针对现有的安全问题，采取一定的安全措施来防止威胁的发生，尽可能减少因安全问题而造成的各种损失。

3）转移策略。这种策略的核心是“花钱买平安”，即把现有的安全问题可能造成的损失转移到别处（如保险公司）来保障自身的安全。

（4）安全监测

在网络运行期间，系统随时都有可能产生新的变化，例如增添新的网络软硬件，软件升级、设备更新等都将导致资产发生变化。这时先前的风险评估结论就失去了意义，需要重新进行风险分析、风险评估和安全决策，以适应网络系统的新变化。安全监测过程能够实时监视和判断网络系统中的各种资产在运行期间的状态，并及时记录和发现新的变换情况。

网络安全风险评估在网络安全技术中具有重要的地位，通过它可以知道一些特殊类型的资产价值以及包含这些信息的系统价值。通过风险评估及早发现安全隐患并采取相应的加固措施已成为网络安全保障体系建设必不可少的一个组成部分。风险评估的核心工作是采用多种方法对网络系统可能存在的漏洞进行检测，找出可能被黑客利用的安全隐患，并根据检测结果向系统管理者提供详细可靠的安全分析报告及漏洞修补建议，以便及早采取措施，保护网络资产免受侵害。