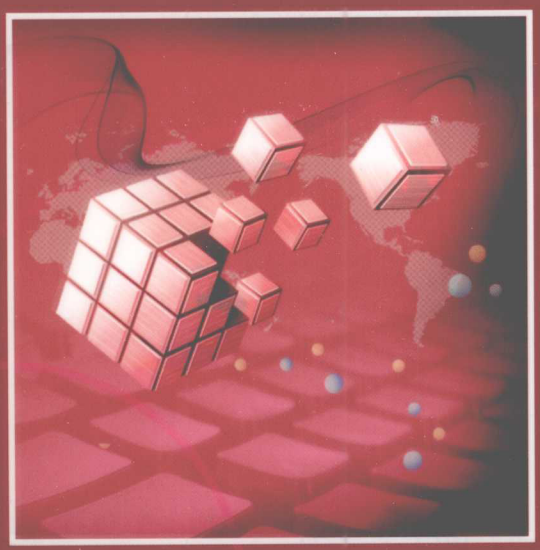
普通高等教育“十一五”计算机类规划教材

网络安全技术

刘化君 编著



免费电子课件

机械工业出版社
CHINA MACHINE PRESS

普通高等教育“十一五”计算机类规划教材

网络安全技术

刘化君　编著

机械工业出版社

本书内容共9章，包含网络安全理论基础、网络攻击与防护、网络安全应用及网络安全实验4个部分。网络安全理论基础部分讲解了网络安全的基础知识、网络安全体系结构、网络协议的安全性以及网络系统平台安全，使读者初步了解网络安全并掌握网络安全技术的架构。网络攻击与防护部分从攻与防两个角度讲解网络安全技术，包括网络攻击原理及技术、网络安全防护技术。网络安全应用部分讲解了密码技术在网络安全中的应用、网络安全应用。网络安全实验部分从搭建网络安全实验环境开始，分11个项目比较全面地讲解了攻与防等实验，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完美的结合，给读者以实用和最新的网络安全技术。

本书适用范围广，既可以作为高等院校网络安全课程的教材和教学参考书，又可作为网络安全培训教材或自学参考书；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。

为方便教师教学，本书配有免费电子课件，欢迎选用本书作为教材的教师发邮件到 llm7785@ sina. com 索取。

图书在版编目（CIP）数据

网络安全技术/刘化君编著. —北京：机械工业出版社，2010.5
普通高等教育“十一五”计算机类规划教材
ISBN 978-7-111-30466-1

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（2010）第 071856 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 版式设计：张世琴
责任校对：李秋荣 封面设计：张 静 责任印制：乔 宇
北京机工印刷厂印刷（兴文装订厂装订）
2010 年 6 月第 1 版第 1 次印刷
184mm × 260mm · 25.25 印张 · 622 千字
标准书号：ISBN 978-7-111-30466-1
定价：39.80 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
社服务中心：(010)88361066
销 售 一 部：(010)68326294
销 售 二 部：(010)88379649
读者服务部：(010)68993821

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

封面无防伪标均为盗版

前　言

随着网络系统及其应用逐渐复杂和庞大，网络攻击和破坏行为也日益普遍和多样化，并不断产生大量新颖的攻击形式，网络安全面临严峻挑战。网络安全不仅是国内外研究的重大科学问题之一，也已成为影响社会经济发展和国家发展战略的重要因素。“国之大事，死生之地，存亡之道，不可不察也”（摘自《孙子兵法》）。正因为如此，网络安全技术教学如何与时俱进，如何使初学者不仅能够较快地达到一个较高的水准，并使其知识和技能与业界当前技术状况和未来发展趋势相一致，已成为一个越来越不容易达到但又必须为之努力追求的目标。

本书面向初学者，以将读者最终引领到一个较高水准为目标，把网络安全理论、安全技术与安全工具几方面的内容有机地结合在一起，通过大量的实例讨论网络安全理论与技术，并对当前网络安全领域所遇到的一些典型问题及解决这类问题的典型方法做了较深入的讨论与阐述。在力求系统讲解网络安全知识的基础上，理论基础方面的选材和阐述原则是“够用”；技术性内容的选材原则是“典型”和“有发展潜力”，强调的是技术和应用。学习本书虽不需要读者具备任何网络安全基础知识，但考虑到网络安全是一个高度综合的领域，与计算机科学与技术的其他分支密不可分，建议读者先修读操作系统、计算机网络与通信以及有关网络编程方面的知识。通过阅读本书，读者不仅可以从理论上对网络安全有较深刻的理解，而且可以根据应用实例对网络安全攻击、防护技术有更直观的认识。

网络安全是一门综合性很强的新兴学科，涉及的内容较多。本书按照网络安全理论基础、网络攻击与防护、网络安全应用和网络安全实验4个部分架构了一个网络安全知识体系，共包含9章内容。

第1部分为网络安全理论基础，包含第1~4章，主要介绍了网络安全的基本概念、网络安全体系结构、网络协议的安全性以及网络系统平台安全。作为实例，介绍了Windows系列操作系统的安全配置与操作。

第2部分由第5章和第6章组成，主要讨论网络攻击与防护技术。首先详细介绍了网络攻击技术“五部曲”（信息收集、获得系统或管理员权限、攻击、种植后门、在网络中隐身）。然后就网络侦察、拒绝服务攻击、缓冲区溢出、欺骗攻击、服务端口管理等内容进行了比较全面的讲解。关于网络防护，主要讨论了防火墙技术、入侵检测技术、恶意代码防范与应急响应等内容。最后，简单介绍了网络攻击取证与安全审计等网络安全监控技术。

第3部分为第7章和第8章，这两章以网络的安全应用为主题，讲解了数据加密与解密技术在网络安全中的应用、认证技术及公开密钥基础设施（PKI），并就作者在信息隐藏方面的研究成果做了简单介绍。然后讨论了IP安全、虚拟专用网（VPN）、安全电子邮件和Web安全技术等内容。

最后一部分为第9章，即网络安全实验，主要包括操作系统安全配置、网络攻击和网络安全防护等方面的内容，共计11个实验项目。这些实验项目使课程理论与实践紧密地结合在一起，所讨论的内容主要是为了提高网络安全实践能力，强化理论与实践相结合而设置

的。

另外，在本书的有关章节中，还介绍了一些相对深入的网络安全技术和新的研究成果，包括作者自己的部分研究工作，例如信息隐藏算法、网络安全风险评估等相关内容。

虽然，本书所选择的典型问题具有引导初学者入门的性质，但并不希望因此而使读者远离网络安全技术前沿。鉴于这一考虑，本书对每类问题的讨论都试图达到一定的深度，并在每章末附有小结与进一步学习建议以及一定数量的思考与练习题，进一步学习建议旨在能为读者进一步开阔视野提供一些帮助，思考与练习题与章节内容密切相关，以帮助读者巩固和复习有关概念，切实掌握网络安全技术知识。

本书内容翔实、结构合理、概念清楚、语言精练、实用性强，既可以作为高等院校网络安全课程的教材和教学参考书，又可作为网络安全培训教材或自学参考书；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。

本书由南京工程学院杨洁执笔编写第4、9章，以及第7章中的部分内容，其余各章节由刘化君执笔编写；全书由刘化君统编定稿。本书作者的研究工作得到了江苏省高校自然科学基础项目“短波环境下透明语言伪装通信技术的研究（07KJB510037）”及应用型本科院校“十一五”国家课题“我国高校应用型人才培养模式研究”子项目“通信与电子信息类专业课程体系研究与建设（FIB070335－A7－08）”的资助支持；在编写过程中得到了刘枫、解玉洁等老师及许多同学的支持和帮助；在此一并表示衷心感谢！

随着互联网技术及应用的飞速发展，网络安全理论与技术也必将随之发展变化。在编写过程中，我们力求精益求精，及时吸纳最新的网络安全研究成果及技术，但囿于编者理论水平和实践经验所限，错误与不妥之处在所难免，恳请广大读者不吝赐教，批评斧正。

编　者

此为试读，需要完整PDF请访问：www.ertongbook.com

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，轻者给个人或机构带来信息损害、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，涉及到诸多因素，包括技术、产品和管理。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；然后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。当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，给社会造成难以估量的巨大损失。网络安全越来越成为关系国计民生的大事，已经引起了全社会的高度重视。网络安全涉及到网络和通信，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，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”。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。在远古时代，就有了信息安全的概念。早期，所有的资产都是物理的，重要的信息也是物理的，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，可将之称为物理安全。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，则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），报文即使被截获也无法读懂。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，将每个字符编码后再放入报文传输；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。这个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。

第二阶段是计算机系统信息安全时期。当计算机技术普及应用之后，信息开始以电子形式移植到计算机系统中，计算机系统上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，简称为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。

信息安全的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，且迅速发展起来。网络安全的主要任务是：解决在分布式网络环境中，对信息载体及其运行提供安全保护问题；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，是第四阶段。物联网被称为是继计算机、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统统交给人工智能去处理，从而从繁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个新兴的学科，而且是一门边缘交叉性学科，涉及到通信技术、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。该定义则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；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

在美国国家信息基础设施（NII）的文献中，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，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看做是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，涉及到多个方面。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，应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，以防止数据、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，避免他人利用窃听、冒充、篡改、抵赖等手段侵犯用户利益。

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、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

此为试读，需要完整PDF请访问：www.ertongbook.com

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相互交错与关联的。

网络安全涉及的内容既有安全理论、安全应用技术和安全管理方面的问题，还有社会、教育、法律等问题，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。既便是窃听者截获报文，由于报文在一定程度上进行了加密处理，即进行了数据伪装，使得截获者不能解密（即理解）所截获的报文含义。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及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）也称做不可抵赖性。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，也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，有许多网络故障与软件可靠性、人员可靠性和环境可靠性有直接关系。

（7）可控性

可控性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、认证和不可否认将在相当长的时期内仍是安全通信的关键组成部分。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. 网络安全的进一步讨论

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保护，还包括了入侵检测、应急响应以及数据灾难备份与恢复。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：网络安全包含了安全攻击（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，还要研究网络攻击技术以及用于防御这些攻击的对策。从系统安全的角度考虑，网络安全攻防技术体系的组成如图 1-1 所示。

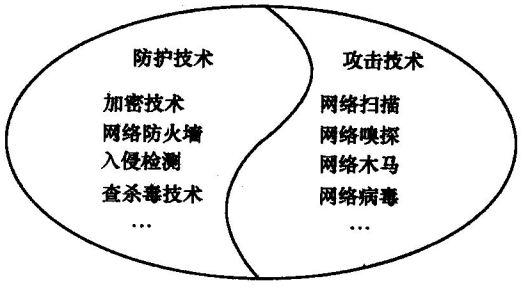


图 1-1 网络安全攻防技术体系

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，网络安全问题最终可归纳为网络的系统安全和网络的信息安全两大类，而保护网络的信息安全是网络安全的关键和终极目标。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。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和技术都属于网络安全的研究范畴。

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

自从1988年莫里斯蠕虫病毒发作以来，重大网络安全事故连续不断发生，每年都导致数百亿美元的损失。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，网络犯罪也开始顺应这一发展趋势，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、入侵者、攻击、威胁等是使用频率比较高的名词术语。

黑客（Hacker）是指对于任何计算机操作系统奥秘都有强烈兴趣的人。大多数黑客都是程序员，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，一般没有破坏数据的企图。黑客的特点是喜欢破译解密。为了正身，中国的一些黑客自称为“红客（Honker）”。美国警方还是把所有涉及到“利用”、“借助”、“通过”或“阻挠”计算机的犯罪行为都定义为Hacking。因此，人们一般也以黑客的行为态度和动机将其划分为三类：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，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，因此在使用时往往不加区别。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、网络僵尸、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 20 秒钟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，如图 1-2 所示，主要可以归纳为以下几种情况。

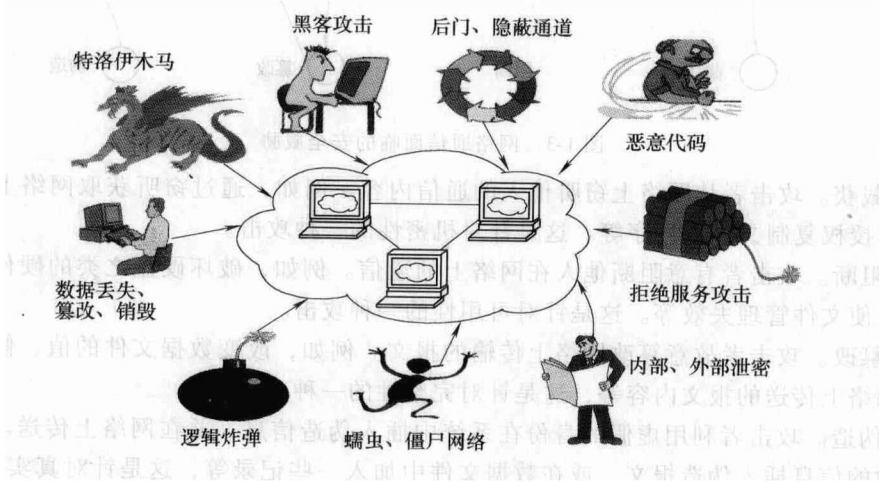


图 1-2 网络系统面临的安全威胁

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 蠕虫等安全问题对社交网站用户形成的安全威胁。这些恶意软件首先感染用户计算机，然后再窃取信息。此类恶意软件一旦植入到社交网站内部，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。

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或进行欺诈性的认证等。

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；或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）隐藏某些恶意信息于其他通信之中，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，使软件功能异常改变，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；或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，如上所述一些安全威胁或者说网络攻击实例屡见不鲜，难以数清。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。

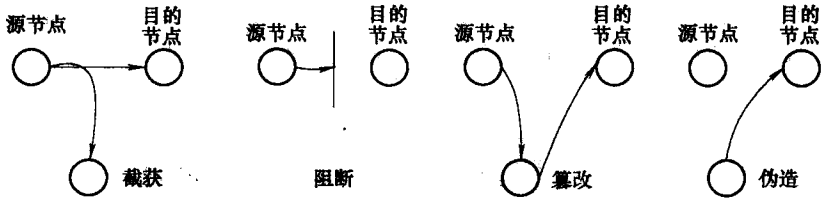


图 1-3　网络通信面临的安全威胁

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。

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之外，针对网络系统的安全威胁主要来自以下几个方面。

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，以及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协议是在可信环境下，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。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有各种漏洞。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。然而，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部分都是因为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。

1.2.3 网络安全风险评估

网络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，如何应对多种网络安全威胁？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低到最低程度。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很困难。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，以便实现有效地网络安全风险管理。

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。譬如说，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，或者说如何确认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。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

此为试读，需要完整PDF请访问：www.ertongbook.com