普通高等教育“十一五”国家级规划教材

高等学校规划教材

计算机网络安全与防护

闫宏生　王雪莉　杨　军　等编著

网络工程与信息安全

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
高等学校规划教材

计算机网络安全与防护

闫宏生　王雪莉　杨　军　等编著

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

内 容 简 介

本书主要介绍计算机网络安全基础知识、网络安全体系结构、远程攻击与防范，以及密码技术、信息认证技术、访问控制技术、网络病毒与防范、防火墙、网络安全扫描技术、网络入侵检测技术、安全隔离技术、电磁防泄漏技术、蜜罐技术、虚拟专用网技术等，同时还介绍了网络安全管理的内容，简要分析了计算机网络战的概念、特点、任务和发展趋势。

全书涉及内容广泛，注重理论联系实际，设计了多个实验、并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、信息安全、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。

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，杨军等编著. —北京：电子工业出版社，2007.8
高等学校规划教材
ISBN 978-7-121-04644-5

Ⅰ.计… Ⅱ.①闫…②王…③杨… 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（2007）第 096670 号

策划编辑：童占梅
责任编辑：王 纲
印 刷：北京季蜂印刷有限公司
装 订：三河市万和装订厂
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：18 字数：460.8 千字
印 次：2007 年 8 月第 1 次印刷
定 价：26.00 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。

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。

服务热线：（010）88258888。

前　言

随着信息技术的迅速发展，计算机网络在改变和影响着人们的工作、生活方式和观念的同时，也极大地改变着现代战争的形态和面貌。黑客攻击、病毒侵袭、电磁泄漏等，无时无刻不在威胁着我国民用和军用信息系统的安全。因此，计算机网络安全与防护已成为影响社会稳定和国家安全的战略性问题。

本书在总结近年来教学经验的基础上，对 2002 年 7 月由军事科学出版社出版的同名专著进行改编，针对普通高等院校信息管理、信息安全等专业本科生和硕士研究生的特点，一方面在内容上根据网络安全技术的最新发展进行了修订；另一方面也**增加了部分实验和习题**，力求通俗易懂、深入浅出、理论联系实际。本书入选了**普通高等教育“十一五”国家级规划教材**。

本书首先介绍了计算机网络安全基础知识、网络安全体系结构及远程攻击与防范的基本手段，然后重点介绍了密码技术、信息认证技术、访问控制技术、网络病毒与防范、防火墙、网络安全扫描技术、网络入侵检测技术、安全隔离技术、电磁防泄漏技术、蜜罐技术、虚拟专用网技术等，最后阐述了网络安全管理的内容，分析了计算机网络战的概念、特点、任务和发展趋势，向读者展现了与其他网络安全方面书籍不同的特点。全书涉及内容十分广泛，各院校可根据需要在内容、重点和深度方面予以取舍，学时可安排 60～100 小时。**为方便教师使用，我们还制作了电子课件并免费提供下载**。本书适合普通高等院校计算机、信息安全、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。

本书由通信指挥学院军队信息化建设教研室组织编写，闫宏生副教授担任主编，对全书进行审校并编写了第 1，2，9，10，11 章，王雪莉副教授编写了第 4，6 章，杨军、何立新、樊月波、陈刚等同志分别编写了本书第 3，5，7，8 章。

本书在申报和出版过程中，得到了电子工业出版社的大力支持和指导；学院通信与信息系统专业首席专家及燕丽教授在百忙之中审阅了全书，并提出了许多建设性意见；硕士研究生李灿对书稿进行了认真校对；本科生朱琳琳、孙婷、邵平、侯赫等在毕业设计期间协助制作了部分教学课件，在此一并表示衷心感谢。

网络安全技术被人们称为“高科技中的高科技”，“博大精深”，发展又十分迅速，编写组人员现有水平有限，很难全面、准确地将其全貌反映出来，疏漏甚至错误之处在所难免，恳请广大读者不吝指正。

作者联系方式：yanhs@public.wh.hb.cn。

编著者

2007 年 6 月

目　录

第1章 绪 论

当前，世界各国都以巨大的热情和兴趣关注着信息时代的到来，全世界几乎所有国家的传媒都充斥了关于“信息高速公路”（NII）和计算机网络的报道。美国政府于 1994 年初，将其“全国信息基础设施计划”向全世界宣布，引起强烈反响。其他各国纷纷效仿，制定对策，以适应信息时代的挑战。与此同时，在一片繁荣景象的背后，潜伏着一场具有巨大威力的殊死搏斗，这就是越来越受到全人类关注的计算机网络安全问题。在 2007 年 1 月召开的达沃斯世界经济论坛上，有专家指出，在目前全世界接入国际互联网的大约 6 亿台计算机中，有大约 1.5 亿台或多或少地受到黑客的控制，更令人感到不安的是，上述 1.5 亿台计算机的所有者经常无法意识到他们的机器正在被别人非法地利用，国际互联网目前所造成的危害已超过了其所带来的益处。

1.1 计算机网络安全面临的挑战

自 Internet 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。近年来，各种计算机病毒和网上黑客对 Internet 的攻击越来越猛烈，网站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得到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的攻击，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”，打入了政府许多非保密性的敏感计算机网络，查询并修改了工资报表和人员数据。

1999 年 5 月，美国参议院、白宫和美国陆军网络，以及数十个政府网站都被黑客攻陷。

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”。

近年的《网络安全工作报告》显示，2002 年、2003 年、2004 年、2005 年国家计算机网络应急技术处理协调中心收到的网络安全事件报告分别是 1761，13 430，64 686，123 473 件，数字增长的速度相当惊人。

2005 年 8 月 4 日，IBM 公司公布的全球业务安全指数（Global Business Securty Index）报告显示，上半年，全球针对政府部门、金融及工业领域的电子网络攻击增加了 50%，约 23 700 万起。其中政府部门位列“靶首”，有 5400 万起；其次是工业部门，3600 万起；金融部门有 3400 万起；卫生部门有 1700 万起。这些电子攻击的目的主要是为了窃取重要资料、身份证明或金钱。而美国是大部分电子网络攻击的源头，全球遭受的电子网络攻击案中，共有 1200 万起源于美国，120 万起源于新西兰，100 万起源于我国。

由国内安全厂商金山公司发布的《2005 年网络安全报告》显示，2005 年网络威胁呈现多样化的特点，传统的病毒、垃圾邮件还没有销声匿迹，危害更大的间谍软件、广告插件、网络钓鱼等新兴威胁又不请自来，纷纷加入到危害网络安全者的行列。而 IBM 公司公布的《2005 年全球商务安全指数报告》指出，2005 年虽然全球大部分 IT 威胁的严重程度处于“中等”级别，然而垃圾邮件、恶意软件和其他 IT 威胁的犯罪意图越来越明显。种种迹象表明，网络犯罪正在发生根本性的变化，即从全球范围的普遍爆发，转向瞄准具体组织进行敲诈勒索的小范围、更秘密的攻击。带有犯罪意图的网络攻击将愈演愈烈，而终端用户将成为攻击的焦点。

1.2 威胁计算机网络安全的主要因素

从技术角度上看，Internet 的不安全因素，一方面由于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的。因此，尽管 Internet 已从过去用于科研和学术目的的阶段进入到商用阶段，但是它的技术基础仍是不安全的。从一般意义上讲，我们可以认为，计算机网络安全所面临的威胁主要可分为两大类：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：此类攻击可以分为两种，一种是主动攻击，它的目的在于篡改系统中所含信息，或者改变系统的状态和操作，它以各种方式有选择地破坏信息的有效性、完整性和真实性；另一种是被动攻击，它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，它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。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。

（3）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以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，人的思想最为活跃，不可能完全用静止的方法和法律、法规加以防护，这是计算机网络安全所面临的最大威胁。

要保证信息安全就必须设法在一定程度上克服以上种种威胁，学会识别这些破坏手段，以便采取技术、管理和法律制约等方面的努力，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。安全是相对的，不安全才是绝对的。

1.3 计算机网络安全的本质

计算机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，信息数据的保密性、完整性、可用性、可控性和真实性受到保护。网络安全防护的根本目的是防止计算机网络存储、传输的信息被非法使用、破坏和篡改。计算机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 3 个方面。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。为保证计算机系统的硬安全，除网络规划和场地、环境等要求之外，还要防止系统信息在空间的扩散。

2. 软安全

软安全包括信息完整性、保密性、可用性、可控性和真实性，也称信息安全。软安全的范围要比硬安全更为广泛，它包括了信息系统中从信息的产生直至信息的应用这一全部过程。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，或者根据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。从某种程度上可以说，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，信息安全的内涵在不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和真实性，进而又发展为“攻（攻击）、防

（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

1.4 计算机网络安全的管理策略

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3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，然后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、企业和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。

网络安全管理策略是指在一个网络中关于安全问题采取的原则，对安全使用的要求，以及如何保护网络的安全运行。制定网络安全管理策略首先要确定网络安全管理要保护什么，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，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，对每一台网络设备要确定哪些人能够修改它的配置；更进一步要明确的是，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，并确定对每一设备或资源，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。

在网络安全策略里关于用户的权利与责任中，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；希望是用户自身提供备份还是由网络服务提供者提供。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，网络安全策略中所能达到的一定只是用户希望达到绝对稳私与网络管理人员为诊断、处理问题而收集用户信息的一个折中。安全策略中必须确定在什么情况下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，例如，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，相对也就越安全。同时，还要制定对用户授权的过程设计，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。其中最好的一种处理办法是尽量只分配给用户够完成任务所需的最小权限。另外，网络安全策略中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，以进一步确定消除掉安全隐患。每一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，网络安全策略最终一定要送到每一个网络使用者手中。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，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。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；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，侧重于防止和控制非法、有害的信息进行传播，避免公用网络上大量自由传输的信息失控；信息内容的安全，侧重于保护信息的保密性、真实性和完整性，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，本质上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，但是在不同的场合下，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 系统与 Internet 连接之处部署防火墙；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。如图 1.1 所示，以某军事信息网络为例简要介绍了信息系统中常用的网络安全技术措施，具体技术将在后续章节中进行详细分析。

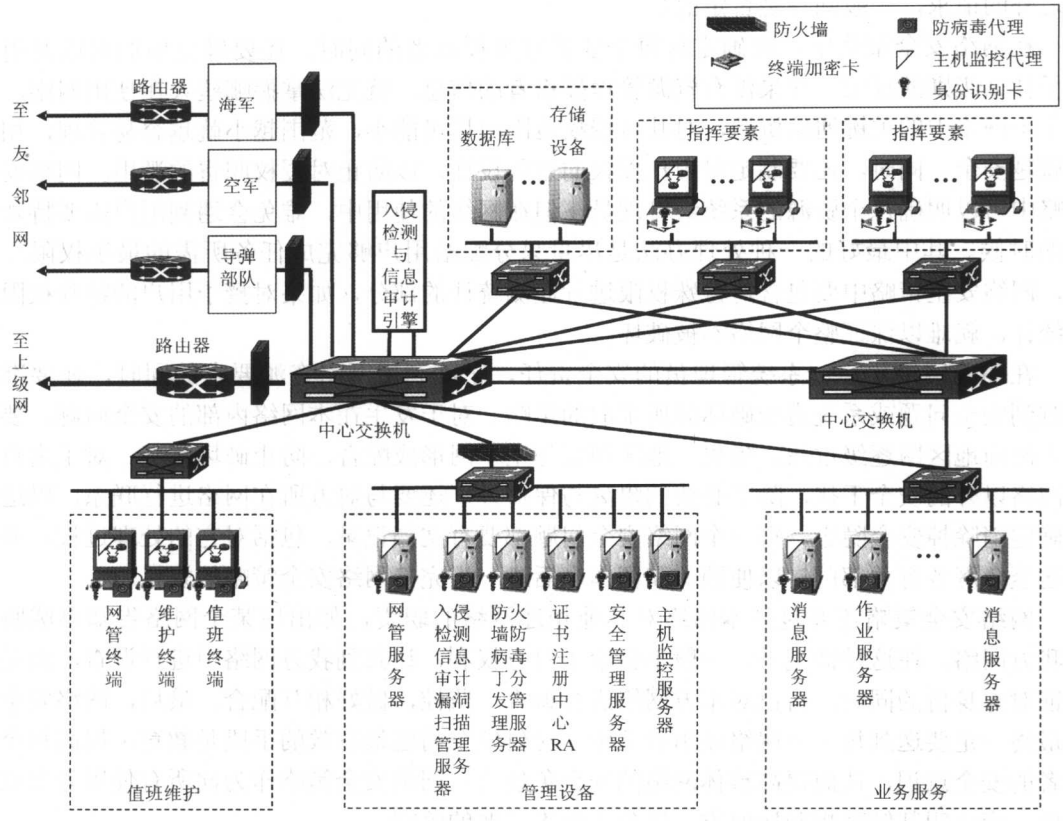

图 1.1　信息系统中常用的网络安全技术措施

本 章 小 结

本章首先分析了近年来计算机网络安全面临的挑战和主要威胁，介绍了计算机网络安全的概念，然后概要介绍了计算机网络安全的管理策略和主要技术措施，使读者对计算机网络安全建立整体认识。主要包括以下内容：

1. 威胁计算机网络安全的主要因素

计算机网络安全所面临的威胁主要可分为两大类：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。

2. 计算机网络安全的本质

计算机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，信息数据的保密性、完整性、可用性、可控性和真实性受到保护。计算机网络安全包括两个方面，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。

3. 计算机网络安全的管理策略

网络安全管理策略是指在一个网络中关于安全问题采取的原则，对安全使用的要求，以及如何保护网络的安全运行。这里着重讨论制定网络安全管理策略需要重点关注的问题。

4. 计算机网络安全的主要技术措施

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，本章首先通过实例建立了初步认识。

习 题 1

1.1 威胁计算机网络安全的主要因素有哪些？

1.2 说明计算机网络安全的内涵。

1.3 计算机网络安全包括哪两个方面？

1.4 什么是计算机网络安全管理策略？

1.5 制定计算机网络安全管理策略需要注意哪些问题？

1.6 计算机网络安全的主要技术措施有哪些？