北京市高等教育精品教材立项项目
计算机网络技术与应用系列教材

计算机网络安全

Network Security

戴　红　王海泉　黄　坚　编著

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

内 容 简 介

本书全面系统地介绍计算机网络安全的基本概念、基本状况、基本理论与原理、基本技术及其实现方法。主要内容包括：加密技术（包括对称加密技术、不对称加密技术和单向哈希函数），数字签名的实现，密钥管理技术，网络攻击关键技术，身份认证技术，防火墙技术，入侵检测技术，VPN 技术等安全技术，以及与 Internet 提供的主要服务（WWW 服务、电子邮件服务、电子商务服务）相关的安全问题，网络操作系统 Windows NT、Windows 2000 和 UNIX 的安全性问题，计算机病毒基础知识及常规病毒防治方法，数据备份系统的组成、设备选择、备份方式及常用备份实施方法，网络管理的相关概念及网络管理协议——简单网络管理协议等内容。

本书以注重实用为原则，将理论知识与实际技术实现相结合，力图做到易懂、易学、易用。本书可作为高等院校高职高专、本科计算机及相关专业的课程教材，也可供网络工程、网络管理、信息管理等相关领域的工程技术人员参考。

图书在版编目（CIP）数据

计算机网络安全/戴红，王海泉，黄坚编著. —北京：电子工业出版社，2004.9
（计算机网络技术与应用系列教材）
ISBN 7-121-00273-6

Ⅰ. 计… Ⅱ. ①戴…②王…③黄… 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（2004）第 086339 号

责任编辑：冉 哲
印 刷：
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
经 销：各地新华书店
开 本：787×980 1/16 印张：14.25 字数：312 千字
印 次：2004 年 9 月第 1 次印刷
印 数：5 000 册 定价：18.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。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。

前　言

随着计算机网络技术的广泛应用和飞速发展，计算机信息网络已成为现代信息社会的基础设施。它作为进行信息交流、开展各种社会活动的基础工具，已深入到人们工作和生活当中。同时，计算机安全问题也随之日益突出，计算机病毒扩散、网络黑客攻击、计算机网络犯罪等违法事件的数量迅速增长。安全问题已成为人们普遍关注的问题。

本书是“北京市高等教育精品教材立项项目”——《计算机网络技术与应用系列教材》中的一本。本书分5大部分共10章。第1部分为概述。其中第1章介绍计算机网络安全的基本概念、基本术语，目前网络系统自身的不安全因素及所面临的威胁，主要防范措施和策略，以及计算机网络安全的评价和管理标准。第2部分为密码学。其中第2章介绍密码学基础知识，包括对称加密技术、不对称加密技术和单向哈希函数3种加密技术，以及数字签名的实现和密钥管理技术的基本概念和方法。第3部分为网络安全。其中第3章介绍网络攻击技术的基本原理和关键技术；第4章介绍现有网络安全技术所能解决的问题和适用情况，以及身份认证技术、防火墙技术、入侵检测技术、加密/解密技术、VPN技术及其他安全技术的基本概念和实现方法；第5章介绍WWW服务、电子邮件服务、电子商务服务的工作原理和安全机制及它们存在的安全问题和解决防护策略，并描述了安全电子交易模型及其工作过程；第6章介绍网络管理的相关概念及目前广泛运用的网络管理协议——简单网络管理协议。第4部分为系统安全。其中第7章介绍网络操作系统Windows NT、Windows 2000和UNIX系统的安全性及如何进行基本的安全设置；第8章介绍计算机病毒的基础知识及常规的病毒防治方法；第9章介绍数据备份的概念、方法及企业和个人用户的数据备份策略。第5部分为无线网络安全。其中第10章对无线网络的基本概念、基本安全技术、安全漏洞及安全措施进行了简单阐述。为了配合教学，本书在每章后都附有复习题和实训题，以巩固学习效果。

本书由北京联合大学应用文理学院教师戴红编写第1章、第5章、第7章和第10章，由北京航空航天大学软件学院教师王海泉、黄坚分别编写第2章、第3章、第4章、第6章和第8章、第9章，全书由戴红审核统稿。在本书的编写过程中，得到了北京市高等教育精品教材指导委员会和北京联合大学应用文理学院教材指导委员会的大力支持，在此表示衷心感谢。

由于作者水平有限，时间仓促，书中难免会有错误和不妥之处，恳请读者批评指正。

作　者

2004年8月

目　录

第 1 部分　概　述

第 2 部分　密　码　学

第 3 部分 网 络 安 全

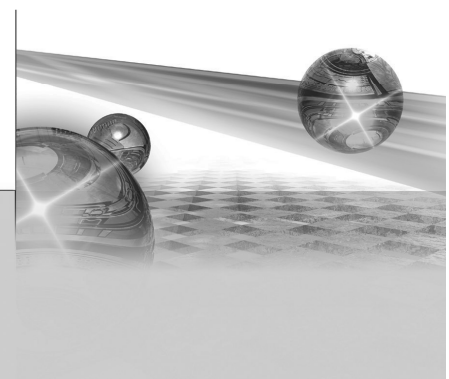
第 4 部分 系 统 安 全

第 5 部分　无线网络安全

当今世界处于信息时代，计算机和信息技术的发展成为这个时代前进的主要推动力之一。随着计算机和信息技术的发展，特别是计算机网络技术的发展和广泛应用，计算机系统的安全、信息的安全及网络系统的安全问题正越来越受到人们的普遍关注。尤其是在人们享受着网络带来的资源共享和信息交换便利的同时，也承受着因人为的蓄意攻击、人为的失误和自然灾害等不安全因素所造成的损失、混乱和破坏。在网络系统下的信息安全问题已成为社会各界所关注的热点问题。

第 1 部分

概　　述



第 1 章　计算机网络安全概述

本章介绍计算机网络安全的基本概念、基本术语，列举目前计算机网络系统自身的不安全因素及其所面临的威胁，对计算机网络安全的研究内容进行探讨。另外，还介绍目前计算机网络安全所采取的主要防范措施和策略，以及计算机网络安全的评价、管理标准和相关法律法规。

1.1　计算机网络安全简介

作为信息时代的主角——信息已成为人类最宝贵的资源之一，经济的发展、社会的进步、国家的安全都越来越依赖于对信息资源的占有和保护。而以 Internet 为代表的网络系统已成为承载、传播信息的主要媒体。网络的开放性、自由性和全球性使我们在最大限度拥有信息的同时，也为如何确保网络系统的安全以及其上的信息自身的安全，提出了新的课题。我们来看一些数据。

1996 年初，美国旧金山的计算机安全协会与联邦调查局在一次联合调查统计中称：有 53%的企业受到过计算机病毒的侵害，42%的企业的计算机系统在过去的 12 个月被非法使用过。而五角大楼的一个研究小组称美国一年中遭受的攻击就达 25 万次之多。

1996 年 2 月，刚开通不久的 CHINANET 受到某高校的一个研究生的攻击，且攻击得逞。

1996 年 8 月 17 日，美国司法部的网络服务器遭黑客入侵，并将其主页上的“美国司法部”改为“美国不公正部”，将司法部部长的照片换成了阿道夫·希特勒，将司法部徽章换成了纳粹党徽。

1996 年 9 月 18 日，黑客再次光顾美国中央情报局的网络服务器，将其主页上的“中央情报局”改为“中央愚蠢局”。

1996 年 12 月 29 日，黑客侵入美国空军的全球网网址，将其主页中有关空军介绍、新闻发布等内容改为一段简短的黄色录像，并声称美国政府所说的一切都是谎言，迫使美国国防部的其他 80 多个军方网站一度关闭。

1997 年初，北京某 ISP 被黑客成功侵入，并在清华大学“水木清华”BBS 站的“黑客与解密”讨论区张贴有关如何免费通过该 ISP 进入 Internet 的文章。

1997 年 4 月 23 日，美国得克萨斯州内查德逊地区西南贝尔互联网公司的某个 PPP 用户侵入中国互联网信息中心的服务器，破译该系统的 ShutDown 账户，把中国互联网信息中心的主页换成了一个笑嘻嘻的骷髅头。

2000 年 3 月，攻击者针对 Microsoft（微软）的以色列网站发起了一次拒绝服务型攻击。

2000 年 3 月，美国中央情报局主管未否认名为 ECHELON 的大规模情报收集系统的存在。

2000 年，包括微软的 Internet Explorer 5.0、ISS（互联网安全系统）公司的 RealSecure 网络入侵检测软件在内的多种软件被公布存在缺陷和漏洞。

2001 年，我国有 73%的计算机曾感染病毒，到了 2002 年上升到近 84%，2003 年上半年又增加到 85%。而微软的官方统计数据称，2002 年因网络安全问题给全球经济造成的直接损失高达 130 亿美元。

2003 年 8 月 12 日，一种叫做“ 冲击波 ”的计算机病毒开始袭击计算机用户，有数字统计表明，至少有数十万台计算机受到袭击。

……

这些数字可谓触目惊心。人类发展史上技术最先进、破坏最严重的安全问题在网络上威胁着人们的工作和生活。

1. 信息系统安全的 6 大基本要素

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等的综合性学科。网络安全是一个内涵丰富的概念，从不同的角度和不同的应用环境有不同的解释。本质上来说，网络安全就是网络系统上的信息安全。信息系统的安全性应包括以下 6 个基本要素。

1）保密性

保密性是指确保信息不暴露给未授权的人或程序。换句话说，信息除拥有者和被授权使用的人外，其他人不能有意或无意地获取。某些信息，如个人私有信息和企业内部资料、有关政府和国家的机密等，对保密性的要求尤为重要。

2）完整性

完整性也称真实性，是指只有得到授权的人或程序才能修改数据，同时能够识别数据是否已经被修改。当信息在网络上存储、传输时，确保不被有意或无意地插入、删除、修改、伪造、重排、重放等。交通运输、金融贸易等应用场合中信息的完整性若遭受破坏，就可能会造成重大的经济损失。

3）可用性

可用性是指得到授权的人或程序可以按照需要访问数据，即使在网络部分受损或需要降级使用时，仍能为授权用户提供有效服务。

4）可控性

可控性是指可以控制授权范围内的信息流向及行为方式，对网络信息的传播及内容具有控制能力。用户对网络信息系统所提供的服务具有随机性、实时性和多角度等要求，网络系统除了能够对用户的身份进行识别及确认外，还应对用户的访问

权限和方式进行控制。

5）可靠性

可靠性是指网络信息系统能够在规定条件下和规定的时间内完成规定功能的特性，是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

6）可审查性

可审查性是指对出现的网络安全问题提供调查的依据和手段。其最为重要的组成特点之一就是不可抵赖性，也称为不可否认性，是指在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。用户在系统进行某项运作后，若事后能提出证明，而无法加以否认，便具备不可否认性。

2. 计算机网络安全的定义

计算机网络安全是计算机安全概念在网络环境下的扩展。因此，在介绍计算机网络安全以前首先需要了解计算机安全的基本概念。

1）计算机安全

国际标准化组织曾建议将计算机安全定义为：“计算机系统受到保护，计算机系统的硬件、软件、数据不被偶然或故意地泄露、更改和破坏。”计算机系统安全可以分为实体安全、运行安全和信息安全 3 个方面。

- 实体安全包括环境安全、设备安全和媒体安全 3 个方面。
- 运行安全包括风险分析、审计跟踪、备份与恢复、应急处理 4 个方面。
- 信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密和鉴别 7 个方面。

2）计算机网络安全

计算机网络安全（简称网络安全）是指网络系统的硬件、软件及其系统中的数据受到保护，不被偶然或者恶意地破坏、更改、泄露，系统连续可靠地正常运行，网络服务不中断。对于一般用户而言，是指保证其在网络上的私人信息或商业信息内容的安全保密性和完整性；对于网络运行和管理者而言，网络安全的侧重点为信息处理和传输系统的安全性、网络信息的可用性和可控性；对于安全保密部门而言，则注重的是信息的机密性和可控性；而从社会、道德和教育的角度来说，对网络信息内容的可控性，是目前要解决的主要问题。

总之，凡涉及到网络上信息的保密性、完整性、可用性、可控性和可审查性及网络

系统自身的可靠性的相关技术和理论都是网络安全所要研究的领域。其涉及层面包含技术和管理两个方面，技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。

在评估网络的安全性时，因其是计算机安全概念在网络环境下的扩展，所以往往要先假设其安全性完全依赖于计算机系统的安全性，再根据计算机系统安全性的准则确定网络的安全级别。

在 1989 年提出的 ISO 7498—2 标准中，ISO 提出了层次型的安全体系模型结构（如图 1.1 所示），成为网络安全的经典模型。

安全 OSI 或 ODP（开放分布式处理）系统
安全应用程序
安全服务
安全机制

图 1.1　ISO 安全体系的层次模型

3. 计算机网络安全的发展过程

自第一代电子计算机出现以来，随着计算机技术的发展和应用领域的扩大，计算机系统及其相关系统的安全性问题逐渐引起人们的注意。

20 世纪 50 年代，计算机尚未普及，安全问题并未受到重视。

到了 20 世纪 70 年代，计算机得到广泛应用。一些重要信息开始采用计算机来处理，开始出现以窃取信息为目的的计算机犯罪，人们开始意识到安全的重要性，研究并制定了一系列的计算机安全法律、法规和防护手段。1976 年，美国学者提出的公开密钥密码体制在克服了网络信息系统密钥管理困难的同时，解决了数字签名问题，并可用于身份认证，它是当前研究的热点。1977 年，美国国家标准局（NBS）颁布了国家数据加密标准（DES）。

20 世纪 80 年代，美国国防部基于军事计算机系统的保密需要，在 20 世纪 70 年代的基础理论研究成果——计算机保密模型（Bell & Lapadula 模型）的基础上，制定了《可信计算机系统评价准则》（TCSEC），形成了安全信息系统体系结构的最早原则。

20 世纪 90 年代以来，计算机网络安全问题得到进一步的深化。英、法、德、荷 4 国提出了包括保密性、完整性、可用性概念在内的“信息技术安全评价准则”（TISFC）。

近年来，6 国 7 方（美国国家安全局和国家技术标准研究所、加、英、法、德、荷）共同提出了《信息技术安全评价通用准则》（The Common Criteria for Information Technology Security Evaluation，简称通用准则或 CC）。CC 综合了国际上已有的评审准则和技术标准的精华，给出了安全评价的框架和原则要求。

1.2 计算机网络所面临的威胁

网络系统正面临着各种各样的危险。攻击者的目的有很多种，例如，造成整个系统瘫痪，造成间歇停机，造成随机数据差错，盗窃大量信息，盗用服务，进行非法监视和收集情报，引入假电文和提取数据用于欺诈等。

目前，计算机网络系统所面临的威胁主要表现为两大类。

1.2.1 人为威胁

1. 人为的无意失误

1）安全配置不当造成的安全漏洞

系统管理员设置资源访问控制的失误，会导致一些资源被偶然或故意地破坏。另外，用户安全意识不强、口令选择不慎、将自己的账号随意转借或与别人共享等都会给网络安全造成威胁。

2）无意的信息泄露

合法用户进入安全进程后中途离开而给非法用户提供可乘之机，口令密钥等保管不善而为他人非法获得，造成网络信息保密性的破坏。

3）操作失误

删除文件、格式化硬盘、线路拆除等操作失误，系统掉电、“死机”等系统崩溃引起信息缺失，从而造成网络信息完整性和可用性的破坏。

2. 人为的恶意攻击

这是计算机网络所面临的最大威胁，对手的攻击和计算机犯罪同属此类。此类攻击又可以分为两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性，是纯粹的信息破坏。这类积极攻击者通常截取网上信息包，对其进行更改使之失效，或者故意篡改信息，或者登录系统占用大量网络资源从而导致资源消耗，损害合法用户的利益。这类攻击者的破坏作用最大。另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息，这类攻击者称为消极攻击者。两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。人为恶意攻击具体可表现在以下几个方面。

1）非授权访问

未经同意而使用网络或计算机资源被看做非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或者擅自扩大权限，越权访问信息等。其主要表现形式有：假冒，身份攻击，非法用户进入网络系统进行违法操作，合法用户以未授权方式进行操作等。

2）信息泄露或丢失

是指敏感数据在有意或无意中被泄露出去或丢失，通常包括：信息在传输中丢失或泄露（如“黑客”利用电磁泄露或搭线窃听等方式截获机密信息，或者通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等重要信息），以及信息在存储介质中丢失或泄露等。

3）破坏数据完整性

以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

4）拒绝服务攻击

不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入网络系统或不能得到相应的服务。

5）利用网络传播病毒

通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

3. 威胁的来源（对手）

1）黑客

黑客（Hacker）是指一类为满足智力上的挑战、心理上的好奇和纯粹的快感而对系统的局限性进行实验的人。他们往往具备特别的技能却不注重伦理道德。黑客攻击网络的手段可分为非破坏性攻击和破坏性攻击两大类。非破坏性攻击一般是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹一类的特殊工具软件，在短时间内向目标服务器发送大量超出系统负荷的信息，消耗可用系统、带宽资源，最后致使网络服务瘫痪。破坏性攻击则采用穷举搜索法发现后门程序，并利用其侵入他人计算机系统，盗窃系统保密信息，破坏系统数据，或者采用网络监听的方法截获网上传输的信息。

2）恶意的内部人员

黑客入侵增强了人们对来自于外部的安全威胁的注意程度，但目前，来自于“内部”的威胁越来越受到人们的注意。内部人员（Insider）可以是授权用户、CERT 人员、网络管理员、系统维护人员、系统管理员、建筑物维修人员、信息安全官员或建筑物安全人员等。内部人员犯罪具有“危害大、难抵御、难发现”的特点，他们最容易接触核心数据资源，威胁的针对性强，而且防不胜防。同时，他们对要攻击的目标非常熟悉，使攻击性行为具有隐蔽性，很难被发现。

3）商业间谍

2000 年 10 月 27 日（星期五），微软公司受到黑客攻击。其源代码被窃取的新闻充斥各大媒体的版面。据路透社报道，微软公司将这一事件称为“商业间谍的可怕行为”。知识产权窃取所带来的损失在不断上升。商业间谍的攻击是具有明确动机的，即通过窃取

竞争对手的商业机密而获得竞争优势。

4）新闻机构

新闻机构可以认为是商业间谍的一种，他们攻击的动机是最大限度地获取具有“价值”的新闻。他们会利用所有可利用的资源和高科技手段，甚至不惜冒风险（如美国的水门事件的报道者）以达到其认为“正确”的目标。

5）军事情报部门

美国的 CIA（中央情报局）、NSA（国家安全局）等情报组织，以获取军事信息、武器设计信息、外交信息等为目的，采用一整套先进的调查研究方法、设备，及训练有素的人员，成为网络安全最强大的威胁。

1.2.2 非人为威胁

1. 天灾

天灾是指自然灾害（如地震、火灾、洪水等），物理损坏（如硬盘损坏、设备使用寿命到期、外力破损等），设备故障（如停电断电、电磁干扰）等非人为因素。其特点是发生突然，具有突发性和不可抗拒性。因其在破坏电力设备的同时一般也销毁了信息本身，所以主要是破坏了信息的完整性和可用性，而对信息的保密性影响较小。采取各种防护措施、制订安全规章、随时数据备份等都是解决这类威胁的可行办法。

2. 系统本身的脆弱性

网络软件不可能百分之百无缺陷和无漏洞，而这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件，大部分都是因为网络软件有漏洞，安全措施不完善。另外，软件的“后门”是软件公司的编程人员为自己方便而设置的，一般不为外人所知，但一旦“后门”洞开，造成的后果将不堪设想。

1）操作系统的脆弱性

- 操作系统支持系统集成和扩展的能力给系统自身留下漏洞。操作系统允许进行动态链接，I/O 驱动程序与系统服务都可以用动态链接的方式挂接到操作系统上。这种方法虽给系统的扩展和升级带来方便，但同时也为黑客和计算机病毒打开了方便之门。
- 操作系统支持在网络上传输文件，上传可执行文件为病毒和黑客程序的加载提供了方便。
- 操作系统支持创建进程，特别是支持在网络结点上进行远程进程的创建与激活，被创建的进程还可以继承创建进程的权力。将此功能与网络传输文件相结合，可实现黑客程序的远程安装。
- 操作系统的守护进程具有与操作系统核心层软件同等的权力，操作系统提供的 Debug 与 Wizard 都是黑客可以利用的程序。
- 操作系统提供远程调用 RPC 服务，该服务往往缺乏安全验证功能。

- 操作系统为系统开发人员提供的无口令便捷入口或“后门”，也是黑客可以利用的通道。

2）网络系统的脆弱性

- 网络的根本是资源共享，而这些资源本身也能为攻击者提供共享。
- 构成网络基本单元的局域网采用的是共享传输介质的广播信道，特别是无线局域网采用空间作为信道，使得消息截获相当容易。
- 网络设备存在各种安全隐患，网络设备不安全意味着整个网络的不安全。
- TCP/IP 协议的不完善，成为攻击者可利用的漏洞。
- 各种应用软件，如 FTP、E-mail、Web、CGI 的缺陷，为攻击者提供了方便。

3）数据库管理系统的脆弱性

大量信息存储在各种类型的数据库系统中，数据库系统的安全性是否与操作系统的安全性匹配是应引起重视的问题。

4）防火墙的脆弱性

- 防火墙因其自身就是基于 TCP/IP 等协议来实现的，所以无法解决 TCP/IP 等协议的漏洞。
- 防火墙无法区分恶意和善意命令。对管理员是合法的命令，黑客使用就可能是危险的。
- 防火墙无法区分恶意和善意流量。用户使用 PING 命令进行网络诊断，还是网络攻击，在流量上是没有差异的。
- 防火墙无法保证某项准许服务的安全性，服务的安全性问题必须由应用安全来解决。

5）其他方面的脆弱性

- 人们安全意识的欠缺、安全技能的匮乏、安全管理的不足，致使系统脆弱性的表现更具悲剧性。
- 计算机领域技术进步的高速性是把“双刃剑”，所谓“道高一尺，魔高一丈”，技术进步会对安全构成新的威胁，安全防范技术的发展一般总是被动地追赶威胁技术的发展。

1.3　计算机网络安全的主要研究内容

一切影响计算机信息系统资源和信息资源的安全性问题都是计算机网络安全应考虑的问题。它所研究的主要内容不仅涉及信息的安全性，更涉及系统的安全性，包括软件系统、硬件系统、网络系统及运行环境等诸多方面。

1.3.1　安全措施的研究

1. 实体安全性研究

实体安全性研究是指为了确保计算机网络设备、设施及其他媒体免遭地震、水灾、