高等职业教育

计算机类专业规划教材

INFORMATION TECHNOLOGY

网络安全案例教程

蒋罗生 主编
戴香玉 副主编

中国电力出版社
http://jc.cepp.com.cn

内 容 提 要

本书是高等职业教育计算机类专业规划教材。

全书通过大量实例，系统地介绍了计算机网络安全的基本概念、基本原理和主要技术。全书共分为五章，主要内容包括网络安全概述、安全使用个人电脑、局域网安全技术、Internet/Intranet 网络安全技术、电子商务安全技术。此外，附录 A 和附录 B 分别收录了计算机网络安全法律法规汇编和实习指导书。

全书理论讲解适中，重在培养读者的实际动手能力。本书既可作为高职高专类计算机及相关专业“网络安全”课程的教材，也可供网络安全爱好者参考。

图书在版编目（CIP）数据

网络安全案例教程/蒋罗生主编. —北京：中国电力出版社，2010.2

高等职业教育计算机类专业规划教材

ISBN 978-7-5123-0058-3

Ⅰ. ①网… Ⅱ. ①蒋… Ⅲ. ①计算机网络－安全技术—高等学校：技术学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 016141 号

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://jc.cepp.com.cn）

航远印刷有限公司印刷

各地新华书店经售

*

2010 年 3 月第一版 2010 年 3 月北京第一次印刷

787 毫米×1092 毫米 16 开本 19.25 印张 466 千字

印数 0001—3000 册 定价 **30.80** 元

前言

计算机网络作为20世纪最伟大的科学发明，已经成为当前社会发展的重要推动力。社会经济发展、国防信息建设以及与人们生活息息相关的各行各业，对计算机网络的依赖程度都在不断增大。尤其是电子商务迅猛发展的今天，网络技术已经深入我们的学习、生活、工作，网络已经改变了人们的生产和生活方式，成为现代社会生活和工作不可或缺的重要组成部分。

网络在给人们带来各种便利的同时，也向人们提出了严峻的挑战。以2009年上半年为例，我国网民规模达到3.38亿人，据有关资料显示，有1.95亿网民上网时遇到过病毒和木马的攻击，1.1亿网民遇到过账号或密码被盗的问题。与此相对应的是，2009年3月25日，中国互联网络信息中心（CNNIC）发布的《2008年中国网民信息网络安全状况研究报告》显示，尚未安装安全软件的网民数量超过1000万。这也进一步说明，普及全民的网络安全意识仍然任重道远。

本教材作为计算机网络安全的入门教材，结合国内高职高专学生的实际情况，着重从实践角度讲解计算机网络安全的基本概念、基本原理和技术方法。内容的编排依据用户类型进行，目的是为读者可以根据需要进行取舍。

注意：作为一种新的尝试，内容编排的合理性还有待实践检验，另外，各章节的知识点具有继承性，教学过程中不宜简单切割。

在网络安全的研究和教学过程中，“攻与防”一直是一对矛盾，只有了解攻击的原理、方法，才能够更好地进行防范。但是在讲解与“攻”相关内容之前，一定要增强学生的法律意识，加强学生的思想道德教育，避免学生因好奇而触犯法律。同时，在讲解与“攻”相关内容时，要适当、适度，尽量避免可能出现的负面效果。

本书由蒋罗生任主编，戴香玉任副主编；第1～2章及附录由蒋罗生编写，第3章由吕晨编写，第4章由戴香玉编写，第5章由董国香、王湘灵、徐星编写。全书由蒋罗生拟定大纲，戴香玉统一书稿。在编写过程中，参考了大量的书籍和互联网上的资料，在此，谨向这些书籍和资料的作者表示感谢。

网络安全是一门涉及计算机科学、通信技术、密码技术、应用数学、社会学等多门学科的交叉学科，同时在应用上，网络安全技术和产品发展很快，因此这本书的编写思想是，理论讲解简洁化，应用实例新颖化，操作步骤详细化，以实训引导学生理解理论，从而达到应用的目的。当然，在采用本书时，各学校也可根据具体情况采用大家熟悉的实例。

限于编者水平，书中难免有疏漏和不妥之处，恳请广大读者和专家批评指正。

编　者

2010年2月

目 录

第1章 网络安全概述

在社会日益信息化的今天，信息已成为一种重要的战略资源，信息的应用也从原来的军事、科技、文化和商业渗透到当今社会的各个领域，其在社会生产、生活中的作用日益显著。传播、共享和增值是信息的固有属性，与此同时，又要求信息的传播是可控的，共享是授权的，增值是确认的，因此，信息的安全和可靠在任何状况下都是必须要得到保证的。

计算机网络是信息社会的基础，然而，网络本身的开放性在给人们带来极大便利的同时，也带来了一些不容忽视的问题，如信息篡改、敏感信息泄露、数据破坏、恶意信息发布、计算机病毒发作等，由此造成的经济损失和社会不良影响难以估计。全世界计算机犯罪正以每年高于100%的速度增长，网络的黑客攻击事件也以每年10倍的速度递增，网络的安全问题正面临着日益严重的威胁，计算机网络的安全性也成为信息化建设的一个核心问题。

引　　例

（1）2009年5月19日，“暴风门”事件导致全国性断网，10余个省市不同程度地受到影响，其中江苏、安徽、广西、海南、甘肃、浙江等6省出现“断网”。

（2）2009年7月，深圳警方破获一起利用计算机网络信息系统技术恶意篡改开奖的彩票数据，欲诈骗彩票奖金3305万元的案件。

（3）下面再列举一些大家都有可能见到的网络安全问题，如

1）不久前，某校一台交换机连续两次被雷电击坏，导致学校数十天无法访问因特网。

2）今年暑假，笔者的一个学生用QQ发来信息，邀请笔者访问一个网站，并给出了访问地址。开学后，笔者询问该学生，她却告知笔者整个假期从来没有上过QQ。

3）打开邮箱，常常看到邮箱中塞满了各种垃圾邮件，更糟糕的是，打开其中一些邮件时，电脑中的防病毒软件弹出警告框，告诉我们检测到病毒。

4）某日收到一陌生人的信息，通知笔者已经获奖，要在指定的网站中填写QQ的昵称及密码和发过来的验证码领取奖品，笔者多次随便填写了QQ资料和验证码，均通知已中二等奖，奖品是一台三星笔记本。

案例思考题：

（1）以上现象说明了什么问题？

（2）试列举你所见过的或在你的周围发生的关于网络安全方面的问题。

（3）如何解决引例中所列举的这些问题？

1.1 网络安全简介

随着 Internet 的飞速发展，网络上的信息资源越来越丰富。这一方面给用户带来了极大的便利，另一方面也给计算机用户的安全带来严峻的考验。由于 Internet 的开放性和超越组织与国界等特点，使其存在安全隐患。因此，研究网络安全、探讨网络安全的成因、了解网络安全的现状及发展趋势、学习网络安全的基础知识、掌握有效的防范方法，对任何计算机用户都是非常重要和十分必要的。

1.1.1 网络安全的定义

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、信息科学、社会学等多种学科的综合性学科。国际标准化组织（ISO）对计算机系统安全的定义：为数据处理系统建立和采用的技术及管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此，可以将网络的安全理解为通过采取各种技术和管理措施，使网络系统正常运行，从而确保网络数据的保密性、完整性、可用性、可控性和可审查性。

网络安全的定义从狭义的保护角度来看，是指计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害；从广义的保护角度来说，网络安全包括网络硬件资源和信息资源的安全。硬件资源包括通信线路、通信设备（交换机、路由器等）、主机等，要实现信息快速、安全地交换，一个可靠的物理网络是必不可少的。信息资源则包括维持网络服务运行的系统软件和应用软件，以及在网络中存储和传输的用户信息数据等，信息资源的保密性、完整性、可用性和真实性是网络安全研究的重要课题。

从技术角度来说，网络信息安全主要表现在系统的可靠性、可用性、保密性、完整性、可控性、不可否认性等方面。

1. 可靠性

可靠性是网络信息系统能够在规定条件下和指定的时间内完成规定任务的特性。可靠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。网络信息系统的可靠性测度主要有三种：抗毁性、生存性和有效性。其中，抗毁性是指系统在人为破坏下的可靠性，如部分线路或节点失效后，系统是否仍然能够提供一定程度的服务；生存性是在随机破坏下系统的可靠性，这里，随机性破坏是指系统部件因为自然老化等造成的自然失效；有效性是一种基于业务性能的可靠性，主要反映在网络信息系统的部件失效情况下，满足业务性能要求的程度。

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。实际使用中，硬件可靠性和软件可靠性较易受到重视，而人员可靠性和环境可靠性则极易被忽视。事实上，人员可靠性在整个系统可靠性中扮演重要角色，系统失效的大部分是人为差错造成的；环境可靠性也极为重要，良好自然环境和电磁环境是保障网络成功运行的关键。

2. 可用性

可用性是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，确保为授权用户提供有效服务的特性。

可用性是衡量网络信息系统面向用户的一种安全性能，应满足身份识别与确认、访问控制、业务流控制、路由选择控制、审计跟踪等要求。

3. 保密性

保密性是网络信息不被泄漏给非授权的用户、实体或过程，或供其利用的特性，即杜绝信息泄漏给非授权个人或实体，强调信息只为授权用户使用的特性。

保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。常用的保密技术包括防侦收、防辐射、信息加密、物理保密等。

4. 完整性

完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储、交换或传输过程中，保持不被偶然或恶意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样性，使信息能正确生成、存储、传输，这是最基本的安全特征。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的因素主要有设备故障、误码、人为攻击、计算机病毒等。

保障网络信息完整性的主要方法有以下五种。

（1）协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。

（2）纠错编码方法：由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法。

（3）密码校验和方法：它是抗篡改和传输失败的重要手段。

（4）数字签名：保障信息的真实性。

（5）公证：请求网络管理或中介机构证明信息的真实性。

5. 可控性

可控性指对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。

6. 不可否认性

不可否认性也称不可抵赖性，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。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

网络安全的具体含义会随着“角度”的变化而变化。常见的有如下几种。

1. 从用户（个人、企业等）的角度

用户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，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，对未授权的内容进行访问和破坏。

2. 从网络运行和管理者角度

管理者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、拒绝服务和网络资源非法占用和控制等威胁，制止和防御网络黑客的攻击。

3. 从安全保密部门角度

安全保密部门希望对非法的、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，给国家造成巨大损失。

4. 从社会教育和意识形态角度

从社会教育和意识形态角度来看，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，因此必须对其进行控制。

1.1.2 影响网络安全的主要因素

计算机网络安全的脆弱性伴随着计算机网络的诞生而产生、伴随着计算机网络的飞速发展而凸显。在网络建设中，网络的特性决定了不可能无条件、无限制地提高其安全性能。既要方便快捷，又要安全可靠，这是一个计算机网络建设中的“两难选择”，网络安全技术就是要在这对矛盾中寻求统一，在这种“两难选择”中寻找支撑点。因此，可以说任何一个计算机网络都不是绝对安全的。

1. 互联网具有的不安全性

由于互联网是对全世界所有国家开放的网络，任何团体或个人都可以利用它方便地传送和获取各种各样的信息，具有开放性、国际性和自由性的特征。互联网的不安全性主要表现在如下几个方面。

（1）由于网络互联技术是全开放的，使得网络所面临的破坏和攻击更加复杂。破坏和攻击可能来自多方面，如可能来自物理传输线路，也可能来自对网络通信协议，还可能是对软件和硬件设施的攻击。

（2）互联网的国际性意味着网络的攻击可以来自世界上的任何一台机器，也就是说，网络安全面临的是国际化的挑战。

（3）网络的自由性意味着对用户的使用并没有提供严格的技术约束，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。另外，互联网使用的基础协议 TCP/IP、FTP 以及 E-mail、RPC、NFS 等标准不仅是公开的，而且都存在一些安全漏洞。

2. 操作系统存在的安全问题

操作系统软件自身的不安全性，以及系统设计时的漏洞（BUG），都给计算机网络留下了安全隐患。

导致操作系统不安全的主要原因有两个：一是由于操作系统体系结构造成的；二是操作系统的进程管理机制所造成的。另外，操作系统的一些功能也有安全隐患，例如支持在网络上传输可以执行的文件映像、网络加载程序等。

3. 数据的安全问题

网络中的数据存放在数据库中，通过 B/S 或 C/S 方式供不同的用户共享。然而，数据库存在许多不安全因素。如授权用户超出权限进行数据的修改；非法用户窃取信息资源等。数据库的安全就是要保障数据的安全可靠和正确有效，即确保数据的安全性、完整性和并发控制；就是要防止数据库被恶意破坏和非法存取。数据的完整性是指防止数据库中存在不符合语义的数据，防止由于错误信息的输入、输出造成无效操作和错误结果；并发控制是指在多个用户程序并行存取数据时，保证数据库的一致性。

4. 传输线路的安全问题

尽管在光缆、同轴电缆、微波、卫星通信中窃听其中指定一路的信息是很困难的，但是

从安全的角度来看，没有绝对安全的通信线路。

5. 网络安全管理问题

网络系统缺少安全管理人员，缺少安全管理的技术规范，缺少定期的安全测试与检查，缺少安全监控，是网络最大的安全问题之一。

1.1.3 网络安全的重要性

尽管网络的重要性已经被广泛认同，但对网络安全的忽视仍很普遍，缺乏网络安全意识的状况仍然严峻。不少企事业单位极为重视网络硬件的投资，但没有意识到网络安全的重要性，对网络安全的投资较吝啬。这也使得目前不少网络信息系统都存在先天性的安全漏洞和安全威胁，有些甚至产生了非常严重的后果。下面是2005年以后的一些典型案例。

2005年，韩国一名未满17岁的少年，使用“黑客软件”获取他人的密码之后，从受害人银行账户中转走5000万韩元（约5万美元）。

2006年，成都一名电子商务专业在校学生，利用互联网多次搜索他人身份证号码和招商银行卡卡号，并通过身份证测试银行卡密码，用这一方法窃得苏州某高校44名学生的银行卡内存款51 619.12元。

2006年，“熊猫烧香”木马致使我国数百万计算机用户受到感染，并波及周边国家。2007年2月，“熊猫烧香”作者李俊被捕。

2007年，美国五角大楼的一个电子邮件系统遭黑客入侵，迫使美国国防部1500个邮件账户被脱机停用。

2007年，美国政府招聘人员的专用网站遭黑客入侵，大约14.6万名用户的数据被盗取，以致该网站被迫关闭。

2007年，俄罗斯黑客成功劫持Windows Update下载器。

2008年，一名黑客入侵了美国两家大型连锁超市Hannaford和Sweetbay，盗窃了1800份完整信用卡资料和420万个信用卡的部分资料。

2008年，一个叫Kryogeniks的黑客组织劫持了comcast.net，使得comcast.net的访问者跳转到该黑客组织的网站。Comcast是美国著名企业，为数千万的美国客户提供互联网接入服务。

2008年，一个全球性的黑客组织，利用ATM欺诈程序在一夜之间从世界49个城市的银行中盗走了900万美元。

2009年5月，山西人唐某入侵了开发和经营网络游戏的苏州某网游数码科技公司，盗窃了虚拟货币“银子”超过50亿两，造成公司百万以上的直接经济损失。

2009年7月7日，韩国遭受有史以来最猛烈的一次黑客攻击。韩国总统府、国会、国情院和国防部等国家机关，以及金融界、媒体和防火墙企业网站遭受攻击。7月9日，韩国国家情报院和国民银行网站无法被访问。韩国国会、国防部、外交通商部等机构的网站也一度无法打开。

以上仅仅是一些个案，事实上，这样的案例不胜枚举，而且计算机犯罪案件有逐年增加的趋势。据美国的一项研究显示，全球互联网每39s就发生了一次黑客事件，其中大部分黑客没有固定的目标。

因此，网络系统必须有足够强大的安全体系。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。

1.2 网络安全现状

目前，网络安全已经引起了各国的高度重视，主要体现在网络安全标准和网络安全立法两个方面。

1.2.1 网络安全标准

一、国外网络安全标准的现状

针对日益严峻的网络安全形势，许多国家和标准化组织纷纷出台了相关的安全标准，我国也制定了相应的安全标准，这些标准既有很多相同的部分，也有各自的特点，其中以美国国防部制定的可信计算机安全标准（TCSEC）及其改进版本应用最广泛。

考虑到 TCSEC 主要只考虑了保密性，各国和各标准化组织都在致力制定新的标准用以替代 TCSEC。20 世纪 90 年代初，英、法、德、荷四国联合提出了包括保密性、完整性、可用性概念的《信息技术安全评价准则（nSFC）》，但是该准则并没有给出综合解决上述问题的理论模型和方案。近年来，六国七方（美国国家安全局和国家技术标准研究所、加拿大、英国、法国、德国、荷兰）共同提出了《信息技术安全评价通用准则》，该准则综合了国际上已有的评审准则和技术标准的精华，给出了框架和原则要求。然而，这一准则仍然缺少综合解决信息多种安全属性的理论模型依据。更重要的是，他们的高安全级别的产品对我国是封锁禁售的。

目前，最主要的网络国际安全标准有如下几个。

1. 美国 TCSEC

该标准是美国国防部制定的，它将网络安全分为 4 个方面：安全政策、可说明性、安全保障和文档。又分为 7 个安全级别，从低到高依次为 D1、C1、C2、B1、B2、B3 和 A1 级。

2. 欧洲 ITSEC

ITSEC 与 TCSEC 不同，它并不把保密措施直接与计算机功能相联系，而是只介绍技术安全的要求，把保密作为安全增强功能。另外，TCSEC 仅将保密作为安全的重点，而 ITSEC 则将完整性、可用性与保密性作为同等重要的因素。

3. 加拿大 CTCPEC

该标准将安全需求分为 4 个层次：机密性、完整性、可靠性和可说明性。

4. 美国联邦准则（FC）

该标准参照了 CTCPEC 及 TCSEC，其目的是提供 TCSEC 的升级版本。FC 是一个过渡标准，后来结合 ITSEC 发展为联合公共准则。

5. 联合通用准则（CC）

CC 的目的是把现有的安全准则结合成一个统一的标准。该计划从 1993 年开始执行，1996 年推出第一版，但目前仍未付诸实施。

6. ISO 安全体系结构标准

在安全体系结构方面，ISO 制定了国际标准 ISO 7498-2-1989《信息处理系统・开放系统互连、基本模型第 2 部分安全体系结构》。该标准为开放系统标准建立了一个框架，其任务是提供安全服务与有关机制的一般描述，确定在参考模型内部可以提供这些服务与机制的位置。

近 20 年来，人们一直在努力发展安全标准，并将安全功能与安全保障分离，制定了复杂而详细的条款。但真正实用、在实践中相对易于掌握的还是 TCSEC 及其改进版本。在现实中，安全技术人员也一直将 TCSEC 的 7 级安全划分当作默认标准。

二、我国网络安全研究的瓶颈

我国信息安全研究经历了通信保密及计算机数据保护两个发展阶段，现正进入网络信息安全的研究阶段。虽然通过学习、吸收、消化 TCSEC 的原则进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受制于人，而国外产品又不断更新升级，所以我国目前的网络安全成果很难保证没有漏洞，也很难得到推广应用。虽然在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、入侵检测系统、系统脆弱性扫描软件等，但是，这些产品安全技术的完善性、规范化和实用性还存在诸多不足。特别是在多平台的兼容性、多协议的适应性、多接口的满足性方面与国际水平相比存在一定的差距，而且，理论基础和自主的技术手段也需要发展和强化。

总的来说，我国的网络安全研究起步较晚，与国外的先进技术相比有一定的差距，特别是在系统安全和安全协议方面的工作与国外差距明显。在我国研究和建立创新性安全理论及系列算法，仍是一项艰巨的任务。然而，我国的网络信息安全研究已具备了一定的基础和条件，尤其是在密码学研究方面积累较多，基础较好，可以期待取得实质性进展。

1.2.2 网络安全立法

随着计算机诞生并在军事和科学、工程领域广泛应用，计算机犯罪也随之出现。从 1966 年美国查处的第一起计算机犯罪案件起，计算机犯罪以惊人的速度增长。有资料显示，目前计算机犯罪的年增长率高达 30%，其中发达国家和一些高新技术地区的增长率还远远超过这个比率，如法国达 200%，美国的硅谷地区达 400%。

与传统的犯罪相比，计算机犯罪所造成的损失要严重得多。例如，美国的统计资料表明：平均每起计算机犯罪造成的经济损失高达 45 万美元，而传统的银行欺诈与侵占案平均损失只有 1.9 万美元，银行抢劫案的平均损失不过 4900 美元，一般抢劫案的平均损失仅 370 美元。更可怕的是，如果攻击者利用计算机盗窃国家机密、军事情报或进行恐怖活动等犯罪，后果无法想象。因此，对计算机犯罪及其防治予以高度重视，已成各国不争的事实。

为有效防止计算机犯罪，除建立有效的网络安全防范体系和切实可行的安全标准之外，为了有效惩治和防范计算机犯罪，各国纷纷加快这方面的立法步伐。

1973 年，瑞典通过了世界上第一部计算机保护法律《瑞典国家数据保护法》，对数据的未经许可访问、收集、处理、复制、存储、传输、使用、修改、销毁的定罪等做了法律规定。

美国也极重视网络安全立法。1965 年，美国总统办公室发布计算机安全保护的法规；1970 年，美国颁布了《金融秘密权利法》；1978 年，美国的佛罗里达州制定了《佛罗里达计算机犯罪法》，该法明确了对计算机犯罪的惩处：知识产权、侵犯计算机装置和设备、侵犯计算机用户等犯罪；1984 年 8 月，美国通过了《伪造存取手段及计算机诈骗与滥用法》，将非法使用计算机和损坏资料的行为规定为犯罪；另外，美国关于网络安全的法律法规还有《通信秘密法》、《计算机安全法》和《计算机病毒消除法》等。

其他国家也参照美国法律，制定了相应的法律或法规。如德国、日本等国均在刑法中规定了多项计算机犯罪及处罚。而英国则试图将计算机犯罪用传统犯罪来解释，主要着眼于犯

罪所引发的结果，以及是否被传统犯罪类型所覆盖，而不以其犯罪手法和工具而定。但由于对于计算机程序等是否属于无形财产没有明确立法规定，因此也仅部分立法。如 1984 年颁布的《数据保护法》、《治安与犯罪证据法》；1985 年修订的《著作权法》和 1990 年制定的《计算机滥用法》等。

虽然一些国家重视计算机立法，但总体而言，和当今计算机犯罪日益猖獗的现状相比，立法相对滞后。还有一些国家没有进行相关的立法，有的国家虽然制定有相关法律但力度较薄弱，不足以遏制计算机犯罪。

我国于 1986 年首次发现计算机犯罪，截止到 1990 年，共发现并破获计算机犯罪 130 余起。进入 20 世纪 90 年代，随着我国计算机应用和普及程度的提高，计算机犯罪呈迅猛增长态势，例如，1993～1994 年，全国的计算机犯罪发案数就达 1200 多例。为了有效遏制计算机犯罪，1994 年 2 月 18 日，我国国务院令第 147 号发布了《中华人民共和国计算机信息系统安全保护条例》。该条例是我国历史上第一个规范计算机信息系统的安全管理、惩治侵害计算机安全的违法犯罪的法规，在我国网络安全立法史上具有里程碑的意义。由于网络犯罪的新发展，自 1997 年开始国务院陆续颁布了《计算机信息网络国际联网安全保护管理办法》、《互联网信息服务管理办法》、《互联网电子公告服务管理规定》、《互联网上网服务营业场所管理条例》等行政法规。1997 年刑法修订时新增了第 285 条、第 286 条、第 287 条，增设了非法侵入计算机信息系统罪和破坏计算机信息系统罪，2000 年 12 月 28 日全国人大常委会通过了《关于维护互联网安全的决定》。至此，我国通过行政法规和刑法，建立了较完备的网络安全法律法规体系，虽然这一法律体系随着互联网的发展需要继续改进、完善，但就目前来说，已经基本上能满足维护网络安全的需要。

1.3 网络安全的主要威胁

1.3.1 网络安全的层次结构

网络安全的结构层次有物理安全、安全控制和安全服务等。

1. 物理安全

物理安全是指在物理介质层次上对存储和传输信息的安全保护。也就是保护计算机网络设备、设施以及其他媒体，免遭灾难性环境事故、人为操作失误或错误及各种计算机犯罪行为导致的破坏。物理安全是网络安全的最基本保障。物理安全主要包括环境安全、设备安全、媒体安全等。

目前，物理介质层次上常见的不安全因素主要有如下几种。

（1）自然灾害、物理损坏、设备故障等。这类不安全因素具有突发性、自然性、非针对性等特点。这类因素对网络信息的完整性和可用性威胁最大，而对保密性的影响较小。防范此类不安全隐患的有效方法是采取各种有效的防护措施、制定切实可行的安全规章、及时数据备份等。

（2）电磁辐射、乘虚而入、痕迹泄露等。此类不安全因素具有隐蔽性、人为实施的故意性、信息无意泄露性等特点。这种不安全因素主要破坏网络信息的保密性，而对完整性和可用性影响不大。防范此类不安全隐患的有效方法是采取辐射防护、屏幕口令、隐藏销毁等手段。

（3）操作失误、意外疏漏等。此类不安全因素具有人为实施的无意性、非针对性等特点。这种不安全因素主要破坏网络信息的完整性和可用性，而对保密性影响较小。解决此类不安全隐患的有效方法是状态检测、报警确认、应急恢复等。

2. 安全控制

安全控制是指在网络信息系统中对信息的操作和进程进行控制和管理，重点是在网络信息处理层次上对信息进行初步的安全保护。安全控制可以分为以下几个层次。

（1）操作系统的安全控制。包括对用户合法身份进行核实、对文件读写存取的控制等，操作系统的安全控制主要保护被存储数据的安全。

（2）网络接口模块的安全控制。在网络环境下对来自其他计算机的网络通信进程进行安全控制，包括身份认证、客户权限设置与判别、审计日志等。

（3）网络互联设备的安全控制。对整个子网内所有主机的传输信息和运行状态进行安全监控，常使用网管软件或对路由器配置来实现。

3. 安全服务

安全服务是指在应用程序层对网络信息的保密性、完整性和信源的真实性进行保护和鉴别，以满足用户的安全需求，防止和抵御各种安全威胁。安全服务可以在一定程度上弥补和完善现有操作系统和网络信息系统的安全漏洞。

安全服务的主要内容包括安全机制、安全连接、安全协议、安全策略等。

（1）安全机制。安全机制是利用密码算法对重要而敏感的数据进行处理。如以网络信息的保密性为目标的数据加密和解密；以网络信息来源的真实性和合法性为目标的数字签名和验证等。安全机制是安全服务乃至整个网络安全系统的核心和关键，现代密码学在安全机制的设计中扮演着重要的角色。

（2）安全连接。安全连接是在安全处理前与网络通信方之间的连接过程，它为安全处理进行了必要的准备工作。安全连接主要包括会话密钥的分配、生成和身份验证。

（3）安全协议。协议是多个使用方为完成某些任务所采取的一系列的有序步骤。协议的特性：预先建立、相互同意、非二义性和完整性。安全协议使网络环境下互不信任的通信方能够相互配合，并通过安全连接和安全机制的实现来保证通信过程的安全性、可靠性和公平性。

（4）安全策略。安全策略是安全体制、安全连接和安全协议的有机组合，是网络信息系统安全性的完整的解决方案。安全策略决定了网络信息安全系统的整体安全性和实用性。不同的网络信息系统和不同的应用环境需要不同的安全策略。

1.3.2 协议安全分析

网络的运行基于网络协议。由于 TCP/IP 协议在 Internet 上一统天下，使得 TCP/IP 的任何安全漏洞都会对互联网产生巨大的影响。TCP/IP 协议在设计初期并没有考虑到安全性问题，而是重点关注异构网的互联。由于用户和网络管理员没有足够的精力专注于网络安全控制，加之操作系统越来越复杂，开发人员不可能排除所有的安全漏洞，因此，接入网络的计算机系统不可避免会受到外界的恶意攻击。

1. 物理层安全

物理层安全威胁主要指由网络周边环境和物理特性引起的网络设备和线路的不可用，进而造成的网络系统的不可用。如设备老化、设备被盗、意外故障、设备损毁等。另外，由于

以太局域网中采用广播方式，因此，在某个广播域中利用嗅探器可以在设定的侦听端口侦听到所有的信息包，并且对信息包进行分析，这样，本广播域的信息传递都会暴露无遗。所以，为确保网络系统安全，很多企事业单位都将内部的信息管理系统和互联网从物理上隔断，同时保证在逻辑上两个网络能够连通。

2. 网络层安全

网络层的安全威胁主要有两类：IP 欺骗和 ICMP 攻击。

IP 欺骗是利用了主机之间的正常信任关系进行的攻击手段。IP 欺骗的技术较复杂，常用的实现方法有两种：一种是把源 IP 地址改成一个错误的 IP 地址，而接收主机不能判断源 IP 地址的正确性，由此形成欺骗；另一种是利用源路由 IP 数据包，让它仅仅被用于一个特殊的路径中传输，这种数据包被用于攻击防火墙。

ICMP（Internet 控制消息协议）用于给 IP 协议提供控制服务，允许路由器或目标主机给数据的发送方提供反馈信息。需要发送反馈信息的情况包括数据包不能被发送到目标主机，路由器缓冲区溢出导致数据包被删除，路由器想要把流量重定向到另外一个更短的路由器上等。ICMP 协议是 IP 协议的一部分，任何实现了 IP 协议的设备同时也被要求实现 ICMP 协议。

基于 ICMP 的攻击可以分为三类，并且都可以归类为拒绝服务攻击：针对带宽的 DoS 攻击，利用无用的数据来耗尽网络带宽；针对主机的 DoS 攻击，攻击操作系统的漏洞；针对连接的 DoS 攻击，可以终止现有的网络连接。

3. 传输层安全

具体的传输层安全措施要取决于具体的协议。安全套接层（SSL）及其继任者传输层安全（TLS）是在互联网上提供保密安全信道的加密协议，为诸如网站、电子邮件、网上传真等数据传输进行保密。SSL 3.0 和 TLS 1.0 有轻微差别，但两种规范其实大致相同。SSL 利用密钥算法在互联网上提供端点身份认证与通信保密；TLS 在 TCP 的顶部提供了如身份验证、完整性检验以及机密性保证这样的安全服务。

4. 应用层安全

现在，应用层安全已经被分解成网络层、操作系统、数据库的安全，由于应用系统复杂多样，不存在一种安全技术能够完全解决一些特殊应用系统的安全问题。但对一些通用的应用程序，如 Web Server 程序、FTP 服务程序、E-mail 服务程序、浏览器、Microsoft Office 办公软件等，可以通过互联网扫描服务和系统扫描服务检查应用程序自身的安全漏洞和由于配置不当造成的安全漏洞，在最大程度上避免安全隐患。

1.3.3 典型的网络安全威胁

影响计算机网络安全的因素很多，有恶意的也有无意的、有人为的也有非人为的。网络安全的威胁主要见表 1-1 所示的几个方面。

表 1-1　　典型的网络安全威胁

威　胁	描　述
窃听	网络中传输的敏感信息被窃听
重传	攻击者事先获得部分或全部信息，以后将此信息发送给接收者
伪造	攻击者将伪造的信息发送给接收者

续表

威　胁	描　述
篡改	攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者
非授权访问	通过假冒、身份攻击、系统漏洞等手段获取系统访问权，从而使非法用户进入网络系统读取、删除、修改、插入信息等
拒绝服务攻击	攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁/射频截获	攻击者从电子或机电设备所发出的无线射频或其他电磁辐射中提取信息
人员疏忽	已授权人为了利益或由于粗心将信息泄漏给未授权人

网络安全威胁可分为人为的疏忽和恶意攻击两大类。

人为的疏忽包括失误、失职、误操作等。例如，操作员安全配置不当所造成的安全漏洞，用户安全意识不强，用户密码选择不慎，用户将自己的账户随意转借给他人或与他人共享等都会对网络安全构成威胁。

恶意攻击是计算机网络所面临的最大威胁。这类攻击又可以分为以下两种：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；另一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性。主动攻击又可进一步划分为三种：更改报文流，包括对连接的 PDU（协议数据单元）的真实性、完整性和有序性的攻击；拒绝报文服务，指攻击者删除通过某一连接的所有 PDU，或者将双方或单方的所有 PDU 加以延迟；伪造连接初始化，攻击者重放以前已经被记录的合法连接初始化序列，或者伪造身份而企图建立连接。

恶意攻击对计算机网络危害最大，不仅可能导致经济损失，还可能导致机密数据的泄漏。恶意攻击具有下述特性。

1. 智能性

从事恶意攻击的人员大都具有相当高的专业技术和熟练的操作技能。他们的文化程度高，在攻击前都经过了周密预谋和精心策划。

2. 严重性

尤其是对大型企业或涉及金融资产的网络信息系统恶意攻击，往往会使金融机构、企业蒙受重大损失，甚至给社会带来动荡。

3. 隐蔽性

人为恶意攻击的隐蔽性强，不易引起怀疑。一般来说，由于其作案的技术手段较先进，也容易毁灭证据，使得侦破和取证难度较大。

4. 多样性

随着计算机互联网的迅速发展，网络信息系统中的恶意攻击技术也随之发展。由于经济利益的强烈诱惑，近年来，各种恶意攻击主要集中于电子商务和电子金融领域。攻击手段日新月异，新的攻击目标包括偷税漏税、利用自动结算系统洗钱以及在网络上进行赢利性的商业间谍活动等。

恶意攻击的手段很多，下面是一些最常见的。