“十二五”职业教育国家规划教材

网站建设与管理专业

Website Construction and Management

网络信息安全

主编　张砚春　赵立军　苑树波

北京出版社
山东科学技术出版社

中等职业学校网站建设与管理专业教材

网络信息安全

主 编　张砚春　赵立军　苑树波

北京出版社
山东科学技术出版社

图书在版编目（CIP）数据

网络信息安全 /张砚春，赵立军，苑树波主编. —济南：山东科学技术出版社，2016.12
ISBN 978-7-5331-8229-8

Ⅰ. ①网… Ⅱ. ①张… ②赵… ③苑… Ⅲ. ①计算机—网络—安全技术—中等专业学校—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2016)第 091757 号

网络信息安全

主编　张砚春　赵立军　苑树波

主管单位：北京出版集团有限公司
山东出版传媒股份有限公司
出 版 者：北京出版社
山东科学技术出版社
地址：济南市玉函路 16 号
邮编：250002　电话：(0531) 82098088
网址：www.lkj.com.cn
电子邮件：sdkj@sdpress.com.cn
发 行 者：山东科学技术出版社
地址：济南市玉函路 16 号
邮编：250002　电话：(0531) 82098071
印 刷 者：山东金坐标印务有限公司
地址：莱芜市嬴牟西大街 28 号
邮编：271100　电话：(0634) 6276023

开本： 787mm×1092mm　1/16
印张： 13.25
字数： 306 千
印数： 1-2000
版次： 2016 年 12 月第 1 版　2016 年 12 月第 1 次印刷

ISBN 978-7-5331-8229-8
定价：29.8 元

编审委员会

编写说明

随着科技和经济的迅速发展，互联网已成为生产和生活必不可少的一部分，社会、行业、企业对网站建设与管理人才的需求也与日俱增。如何培养满足企业需求的人才，是职业教育所面临的一个突出而又紧迫的问题。目前中职教材普遍存在理论偏重、偏难以及操作与实际脱节等弊端，突出的是以“知识为本位”而不是以“能力为本位”的理念，与就业市场对中职毕业生的要求相左。

为进一步贯彻落实全国教育工作会议精神、《国务院关于加快发展现代职业教育的决定》（国发［2014］19号）、《现代职业教育体系建设规划（2014－2020年）》（教发［2014］6号），北京出版社联合山东科学技术出版社结合网站建设与管理各中职学校发展现状及企业对人才的需求，在市场调研和专家论证的基础上，打造了反映产业和科技发展水平、符合职业教育规律和技能人才培养要求的专业教材。

本套专业教材以该专业教学标准及教学课程目标为指导思想，以中职学生实际情况为根据，以中职学校办学特色为导向，与具体的专业紧密结合，按照“基于工作流程构建课程体系”的建设思路（单元任务教学）编写，根据网站建设与管理的总体发展趋势和企业对高素质技能型人才的要求，构建与网站建设管理专业相配套的内容体系。本系列教材涵盖了专业核心课的各个方向。

本套教材在编写过程中着力体现了模块教学理念和特色，即以素质为核心、以能力为本位，重在知识和技能的实际灵活应用；彻底改变传统教材的以知识为中心、重在传授知识的教育观念。为了完成这一宏伟而又艰巨的任务，我们成立了教材编写委员会，委员会的成员由具有多年职业教育理论研究和实践经验的教育行政人员、高校教师和行业企业一线专业人士担任。从选题到选材，从内容到体例，都以职业化人才培养目标为出发点，制定了统一的规范和要求，为本套教材的编写奠定了坚实的基础。

本套教材的特点具体如下。

一、教学目标

在教材编写过程中明确提出以教育部“工学结合，理实一体”为编写宗旨，以培养知识与技能为目标，避免就理论谈理论、就技能教技能，要做到有的放矢。打破传统的知识体系，将理论知识和实际操作合二为一，理论与实践一体化，体现“学中做”和“做中学”。让学生在做中学习，在做中发现规律、获取知识。

二、教学内容

一方面根据教学目标综合设计新的知识能力结构及其内容，另一方面还要结合新知识、新技术的发展要求增删、更新教学内容，重视基础内容与专业知识的衔接。这样学生能更有效地建构自己的知识体系，更有利于知识的正迁移。让学生知道“做什么”“怎么做”“为什么”，使学生明白教学的目的，并为之而努力，这才能切实提高学生的思维能力、学习能力、创造能力。

三、教学方法

教材教法是一个整体，在教材中设计“单元—任务”方式，通过案例载体来展开，以任务的形式进行项目落实。每个任务以“完整”的形式体现，即完成一个任务后，学生可以完全掌握相关技能，以提升学生的成就感和兴趣。体现以学生为主体的教学方法，做到形式新颖。通过“教、学、做”一体化，按教学模块的教学过程，由简单到复杂开展教学，实现课程的教学创新。

四、编排形式

教材配图详细、图解丰富、图文并茂，引入的实际案例和设计等教学活动具有代表性，既便于教学又便于学生学习；同时，教材配套有相关案例、素材、配套练习及答案光盘以及先进的多媒体课件，强化感性认识、强调直观教学，做到生动活泼。

五、编写体例

每个单元都是以任务驱动、项目引领的模块为基本结构。具体栏目包括任务描述、任务目标、任务实施、任务检测、任务评价、相关知识、任务拓展、综合检测、单元小结等。其中，“任务实施”是教材中每一个单元教学任务的主题，充分体现“做中学”的重要性，以具有代表性、普适性的案例为载体进行展开。

六、专家引领，双师型作者队伍

本系列教材由北京出版社和山东科学技术出版社共同组织国家示范中等职业学校双师型教师编写，参加的学校有中山市中等专业学校、山东省淄博市工业学校、滨州高级技工学校、浙江信息工程学校、河北省科技工程学校等，并聘请山东省教研室主任助理杜德昌、山东师范大学教授刘凤鸣担任教材主审，感谢浪潮集团、星科智能科技有限公司给予技术上的大力支持。

本系列教材，各书既可独立成册，又相互关联，具有很强的专业性。它既是网站建设与管理专业教学的强有力工具，也是引导网站建设与管理专业的学习者走向成功的良师益友。

前　言

随着信息技术和网络技术的快速发展，计算机网络在政治、经济、教育、军事等诸多领域得到了广泛应用。计算机网络在为人们提供便利、带来效益的同时，也使人类面临着信息安全的巨大挑战。如何保护个人、企业和国家的大量重要信息不被入侵和破坏，如何保证网络系统安全、不间断地工作，是网络建设必须考虑的重要问题。因此，使计算机网络系统免遭破坏，提高系统的安全可靠性，已成为人们关注和急需解决的问题。每个单位的网络管理与维护人员、网络系统用户和工程技术人员都应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全稳定地运行并提供正常而安全的服务。

本书全面介绍了网络安全基础理论和网络安全应用技术，共分为9个单元：网络信息安全概述，信息加密技术，网络协议基础，计算机病毒及其防范，防火墙与入侵检测技术，网络攻击技术及防范，网络安全策略，网络故障排除与维护，无线网络安全技术。

书中各单元不仅讲述了网络安全的理论知识和应用技术，同时详细介绍了许多实例的具体操作步骤，使读者能在最短的时间内学以致用，而且还配有一定数量的练习题供读者学习使用。

本书由张砚春、赵立军、苑树波主编，王忠、毛岳军、马书波、王嘉怡、隆方红、吴海梅、王乐乐、吴倩任副主编，侯根合、胡珍珍、高瑶瑶参与编写。

由于编写时间仓促，编者水平有限，缺点和错误在所难免，恳请有关专家批评指正，以便出版时修正。

编　者

目 录
CONTENTS

第一单元　网络信息安全概述

单元概述

我们现在生活在各类电子信息和网络环境中，如：办公和家庭计算机，数据库服务器，电话系统，全球定位系统，无线通信系统，公用信息系统，智能卡系统，等等。在享受网络丰富信息资源给我们带来的方便的同时，计算机病毒、黑客及木马控制、垃圾邮件等也给我们带来了越来越多的麻烦。因此，保证互联网的健康发展，网络信息安全是首先要解决的问题。本单元将系统地阐述计算机网络安全的基本知识、计算机网络安全技术、网络安全策略等相关概念、技术和应用，可以帮助我们全面地学习和理解网络安全方面的专业知识，提高网络安全防范的意识。

单元目标

- 能够掌握网络信息安全的定义、构成要素及面临的各种威胁
- 能够了解常见的网络安全技术，提高网络的安全意识
- 能够了解网络安全相关法规及评价标准

学习任务1 网络安全简介

任务概述

当今社会可以说是网络无处不在，我们可以网上购物，可以网银转账，但网络安全吗？什么是网络安全，它又包括哪些内容？一个安全的网络由哪些要素组成？我们在使用网络时又会面临怎样的威胁？通过本任务的学习可以初步了解有关网络安全及防范的相关专业知识，找出以上问题的答案。

任务目标

- 了解计算机网络安全的重要性
- 理解计算机网络安全的定义
- 掌握计算机网络安全的要素
- 学会分析计算机网络面临的威胁

学习内容

当今，计算机网络所具有的信息共享和资源共享等优点，日益受到人们的关注并获得了广泛的应用。同时，Internet 应用范围的扩大，使得网络应用进入到一个崭新的阶段。一方面，入网用户能以最快的速度、最便利的方式以及最廉价的花费获得最新的信息；另一方面，随着网络规模越来越大和越来越开放，网络上的许多敏感信息和保密数据难免会遭受各种主动和被动的人为攻击。也就是说，人们在享受网络提供的好处的同时，也必须要考虑如何应对网络上日益泛滥的信息垃圾和非法入侵行为，即考虑网络安全问题。

一、网络安全的重要性

伴随信息时代的来临，计算机和网络已经成为这个时代的代表和象征，政府、国防、国家基础设施、公司、单位、家庭几乎都成为一个巨大网络的一部分，大到国际的合作、全球经济的发展，小到购物、聊天、游戏，所有社会中存在的概念都因为网络的普及被赋予了新的概念和意义，网络在整个社会中的地位越来越举足轻重了。中国互联网络信息中心（CNNIC）发布的《第 34 次中国互联网络发展状况统计报告》显示，截至 2014 年 7 月底，我国网民规模达 6.32 亿人，其中手机网民达 5.27 亿人，较 2013 年底增加 2 699 万人，互联网普及率持续上升。互联网在中国已进入高速发展时期，人们的工作、学习、娱乐、生活已完全离不开网络。

但与此同时，Internet 本身所具有的开放性和共享性对信息的安全问题提出了严峻的

挑战，由于系统安全脆弱性的客观存在，操作系统、应用软件、硬件设备等不可避免地会存在一些安全漏洞，网络协议本身的设计也存在一些安全隐患，这些都为黑客采用非正常手段入侵系统提供了可乘之机，以至于计算机犯罪、不良信息污染、病毒木马、内部攻击、网络信息间谍等一系列问题成为困扰社会发展的重大隐患。便利的搜索引擎、电子邮件、上网浏览、软件下载以及即时通讯等工具都曾经或者正在被黑客利用进行网络犯罪，数以万计的电子邮件账户和密码被非授权用户窃取并公布在网上，使得垃圾邮件数量显著增加。此外，大型黑客攻击事件不时发生，木马病毒大肆传播，传播途径千变万化让人防不胜防。

计算机网络也成为敌对势力、不法分子的攻击目标，成为很多青少年网络犯罪的根源（主要是不良信息，如不健康的网站、图片、视频等），网络安全问题正在打击着人们使用电子商务的信心，这些不仅严重影响到电子商务的发展，更影响到国家政治、经济的发展。因此，提高对网络安全重要性的认识，增强防范意识，强化防范措施，是学习、使用网络的当务之急。

二、网络安全的定义

所谓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，不因偶然的或者恶意的原因而遭到破坏、更改或者泄露，系统连续、可靠、正常地运行，网络服务不中断。本质上，网络安全就是网络上的信息安全。网络安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论和信息论等多门学科的边缘学科。从技术角度看，网络安全的内容大体包括四个方面：

网络实体安全：包括机房的物理条件、物理环境及设施的安全标准，计算机硬件、附属设备及网络传输线路的安装及配置等。

软件安全：如保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、篡改，不受病毒的侵害等。

网络数据安全：如保护网络信息的数据不被非法存取，保护其完整一致等。

网络安全管理：运行时突发事件的安全处理，包括采取计算机安全技术，建立安全管理制度，开展安全审计，进行风险分析等内容。

三、计算机网络安全的要素

确保网络系统的信息安全是网络安全的目标，对整个网络信息系统的保护最终是为了保护信息在存储和传输过程中的安全。从网络安全的定义中，我们不难分析出网络信息安全的五大核心要素：

1. 完整性

完整性是网络数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、伪造、乱序、重放、插入等破坏和丢失的特性。它是信息安全的一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

2. 可靠性

可靠性指网络信息系统能够在规定条件下和规定时间内完成规定功能的概率。可靠性是网络安全最基本的要求之一，是所有网络系统的建设目标和运行目标。

3. 可用性

可用性是网络信息可被授权访问并按需求使用的特性，即网络信息服务在需要时允

许授权用户或实体使用的特性。可用性是网络面向用户的基本安全要求，是指信息和通信服务在需要时允许授权人或实体使用。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的、多方面的，有时还要求时效性。

4. 保密性

保密性指防止信息泄漏给非授权个人或实体，信息只为授权用户使用。保密性是面向信息的安全要求。加密是保护数据的一种重要方法，也是保护存储在系统中的数据的一种有效手段，人们通常采用加密来保证数据的保密性。要解决的问题是：如何防止用户非法获取关键的敏感信息，避免机密信息的泄露。

5. 不可抵赖性

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。

四、网络安全的威胁

当前威胁网络安全的因素很多，通常把网络安全面临的主要威胁分为两种：一是对网络中信息的威胁，二是对网络中设备的威胁。

从表现形式上看，自然灾害、意外事故、硬件故障、软件漏洞、人为失误、计算机犯罪、黑客攻击、内部泄露、外部泄露、信息丢失、网络协议中的缺陷等人为和非人为的情况，都是计算机网络安全面临的主要威胁。从攻击行为上分析，可以将网络安全面临的主要威胁分为两类：一类是主动攻击，它的目标在于篡改系统中所含的信息，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；另一类是被动攻击，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，对信息流量进行分析，并通过信息的破译以获得重要的机密信息。

但网络安全的威胁根源还是来自于网络自身的脆弱性，以及计算机基本技术自身存在的种种隐患。对计算机软件技术而言，由于现在软件设计本身的水平所限，软件设计人员不可能考虑到影响网络安全因素的每一个细节。对于网络自身而言，由于网络的开放性和其自身的安全性互为矛盾，无法从根本上予以调和，再加上诸多不可预测的人为与技术安全隐患，网络就很难实现其自身的安全了，也必然地处于相对的威胁中了。

目前，计算机网络面临的安全威胁主要有以下几个方面。

1. 黑客

电脑黑客利用系统中的安全漏洞非法进入他人计算机系统，其危害性非常大。从某种意义上讲，黑客对信息安全的危害甚至比一般的电脑病毒更为严重。

2. 软件漏洞及安全设置

每个网络软件及操作系统都不可能是无缺陷和漏洞的，这就使我们的计算机处于危险的境地，一旦链接入网，将成为众矢之的，如 Windows、UNIX 等都有数量不等的漏洞。另外，局域网内网络用户使用盗版软件、随处下载软件及网管的疏忽都容易造成网络系统漏洞，这不但影响了局域网的正常工作，也在很大程度上把局域网的安全置于危险之地，黑客利用这些漏洞就能完成密码探测、系统入侵等攻击。

操作系统或网络设备的安全配置不当也会造成安全漏洞。例如，防火墙软件的配置

不正确，那么它根本不起作用。对特定的网络应用程序，当它启动时，就打开了一系列的安全缺口，许多与该软件捆绑在一起的应用软件也会被启用，除非用户禁止该程序或对其进行正确配置，否则安全隐患始终存在。

3. 拒绝服务攻击

拒绝服务攻击是一种具有破坏性的攻击方式，它使用户系统不能正常处理业务，严重时会使整个系统响应缓慢甚至瘫痪，影响用户的正常使用，甚至会导致合法用户被排斥而无法进入计算机网络系统。

4. 计算机病毒

计算机病毒实际上是一段具有破坏性的程序，这种病毒程序具有极大的破坏性，其危害性已经为人们所认识。计算机病毒具有传染性、寄生性、隐蔽性、触发性、破坏性等特点。特别是通过网络传播的病毒，无论是在传播速度、破坏性，还是在传播范围等方面，都是单机病毒所无法比拟的。

5. 网络犯罪

网络犯罪是非常容易操作的，不受时间、地点、条件限制的网络诈骗、网络战简单易施、隐蔽性强，能以较低的成本获得较高的效益。再加上网络空间的虚拟性、异地性等特征，也在一定程度上刺激了犯罪的增长。尤其是受到全球经济危机的影响，网络犯罪成倍增长。除了给社会造成负面影响外，网络犯罪造成的经济损失巨大，追踪匿名网络犯罪分子的踪迹非常困难。网络犯罪已成为严重的全球性威胁。

6. 特洛伊木马

完整的木马程序一般由两个部分组成：一个是服务器端，一个是控制器端。中了木马就是被安装了木马的客户端程序。若计算机中被安装了客户端程序，则拥有相应服务器端的人就可以通过网络控制该计算机，这时计算机上的各种文件、程序，以及在计算机上使用的账号、密码就无安全可言了。

7. 安全意识不强

用户口令选择不慎，或将自己的账号随意转借他人或与别人共享等，都会对网络安全带来威胁。

学习任务2 网络安全技术

任务概述

网络安全是一个相对概念，不存在绝对安全，所以必须未雨绸缪、居安思危；并且安全威胁是一个动态过程，不可能根除威胁，所以唯有积极防御、有效应对。那么面对网络的复杂性，我们采用什么样的防范技术才能减少或者消除各种网络威胁呢？

任务目标

- 能够掌握常见的网络安全技术

学习内容

为了应对网络安全威胁，需要不断提升防范技术和组建安全管理团队，这是网络复杂性对确保网络安全提出的客观要求。从技术上讲，网络安全防护体系主要由防病毒、防火墙、入侵检测等多个安全组件组成，一个单独的组件无法确保网络信息的安全。目前广泛运用的网络安全技术主要有：防病毒技术、防火墙技术、信息加密技术、数字签名技术、入侵检测技术、系统容灾技术等，以下对这几项技术分别进行简单的分析。

一、病毒防范技术

计算机病毒实际上就是一种在计算机系统运行过程中能够传染和侵害计算机系统的功能程序。病毒经过系统穿透或违反授权攻击成功后，攻击者通常要在系统中植入木马或逻辑炸弹等程序，为以后攻击系统、网络提供方便条件。随着计算机技术的不断发展，计算机病毒变得越来越复杂和高级，对计算机信息系统构成极大的威胁。在病毒防范中普遍使用的防病毒软件，从功能上可以分为网络防病毒软件和单机防病毒软件两大类。单机防病毒软件一般安装在单台 PC 机上，对本机和本机链接的远程资源采用分析扫描的方式检测、清除病毒。网络防病毒软件则主要注重网络防病毒，一旦病毒入侵网络或者从网络向其他资源传染，网络防病毒软件会立刻检测到并加以删除。

二、防火墙(Fire Wall) 技术

防火墙技术是指网络之间通过预定义的安全策略，对内外网通信强制实施访问控制的安全应用措施。它对网络之间传输的数据包按照一定的安全策略来实施检查，以决定网络之间的通信是否被允许，并监视网络运行状态。由于它简单实用且透明度高，可以在不修改原有网络应用系统的情况下达到一定的安全要求，所以被广泛使用。

三、数据加密技术

数据加密技术就是对信息进行重新编码，从而隐藏信息内容，使非法用户无法获取信息的真实内容的一种技术手段。数据加密技术是为提高信息系统及数据的安全性和保密性，防止秘密数据被外部破译所采用的主要手段之一。

数据加密技术主要是通过对网络数据的加密来保障网络的安全可靠性，能够有效地防止机密信息的泄漏。另外，它也广泛地被应用于信息鉴别、数字签名等技术中，用来防止电子欺骗，对信息处理系统的安全起到了极其重要的作用。

四、数字签名技术

数字签名(Digital Signature) 技术是非对称加密算法的典型应用。所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所做的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人(例如接收者) 伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名。

数字签名技术主要用来解决以下信息安全问题:

(1) 否认: 事后发送者不承认文件是他发送的。

(2) 伪造: 有人自己伪造了一份文件，却声称是某人发送的。

(3) 冒充: 冒充别人的身份在网上发送文件。

(4) 篡改: 接收者私自篡改文件的内容。

数字签名机制可以确保数据文件的完整性、真实性和不可抵赖性。

五、入侵检测技术

入侵检测技术主要分成两大类型:

(1) 异常入侵检测: 异常入侵检测方法依赖于异常模型的建立，不同模型构成不同的检测方法。异常检测是通过观测到的一组测量值偏离度来预测用户行为的变化，然后做出决策判断的检测技术。

(2) 误用入侵检测: 误用入侵检测指的是通过对预先定义好的入侵模式与观察到的入侵发生情况进行模式匹配来检测入侵。入侵模式说明了那些导致安全突破或其他误用的事件的特征、条件、排列和关系。一个不完整的模式可能表明存在入侵的企图。

六、系统容灾技术

一个完整的网络安全体系，只有防范和检测措施是不够的，还必须具有灾难容忍和系统恢复能力。因为任何一种网络安全设施都不可能做到万无一失，一旦发生漏防漏检事件，其后果将是灾难性的。此外，天灾人祸、不可抗力等所导致的事故也会对信息系统造成毁灭性的破坏。这就要求即使发生系统灾难，也能快速地恢复系统和数据，才能完整地保护网络信息系统的安全。现阶段主要有基于数据备份和基于系统容错的系统容灾技术。数据备份是数据保护的最后屏障，不允许有任何闪失，但本地的离线介质有时也不能保证安全。数据容灾通过 IP 容灾技术来保证数据的安全。数据容灾使用两个存储器，在两者之间建立复制关系，一个放在本地，另一个放在异地。本地存储器供本地备份系统使

用,异地容灾备份存储器实时复制本地备份存储器的关键数据,二者通过 IP 相连,构成完整的数据容灾系统,也能提供数据库容灾功能。

七、漏洞扫描技术

漏洞扫描是自动检测远端或本地主机安全的技术,它查询 TCP/IP 各种服务端口,并记录目标主机的响应,收集关于某些特定项目的有用信息。这项技术的具体实现就是安全扫描程序。

扫描程序可以在很短的时间内查出现存的安全脆弱点。扫描程序开发者搜集、研究可得到的攻击方法,并把它们集成到整个扫描中,扫描后以统计的格式输出,便于参考和分析。

八、物理安全

为保证信息网络系统的物理安全,还要防止系统信息在空间的扩散。通常是在物理上采取一定的防护措施来减少或干扰扩散出去的空间信号。为保证网络的正常运行,在物理安全方面应采取如下措施:

(1) 产品保障方面: 主要指产品采购、运输、安装等方面的安全措施。

(2) 运行安全方面: 网络中的设备,特别是安全类产品在使用过程中,必须能够从生产厂家或供货单位得到迅速的技术支持服务。对一些关键设备和系统,应设置备份系统。

(3) 防电磁辐射方面: 所有重要涉密的设备都需安装防电磁辐射产品,如辐射干扰机。

(4) 保安方面: 主要是防盗、防火等,还包括网络系统所有网络设备、计算机、安全设备的安全防护。

计算机网络安全是个综合性和复杂性的问题。除了以上介绍的几种网络安全技术之外,还有一些被广泛应用的安全技术,如身份验证、存取控制、安全协议等。面对网络安全行业的飞速发展以及整个社会越来越快的信息化进程,各种新技术将会不断出现。