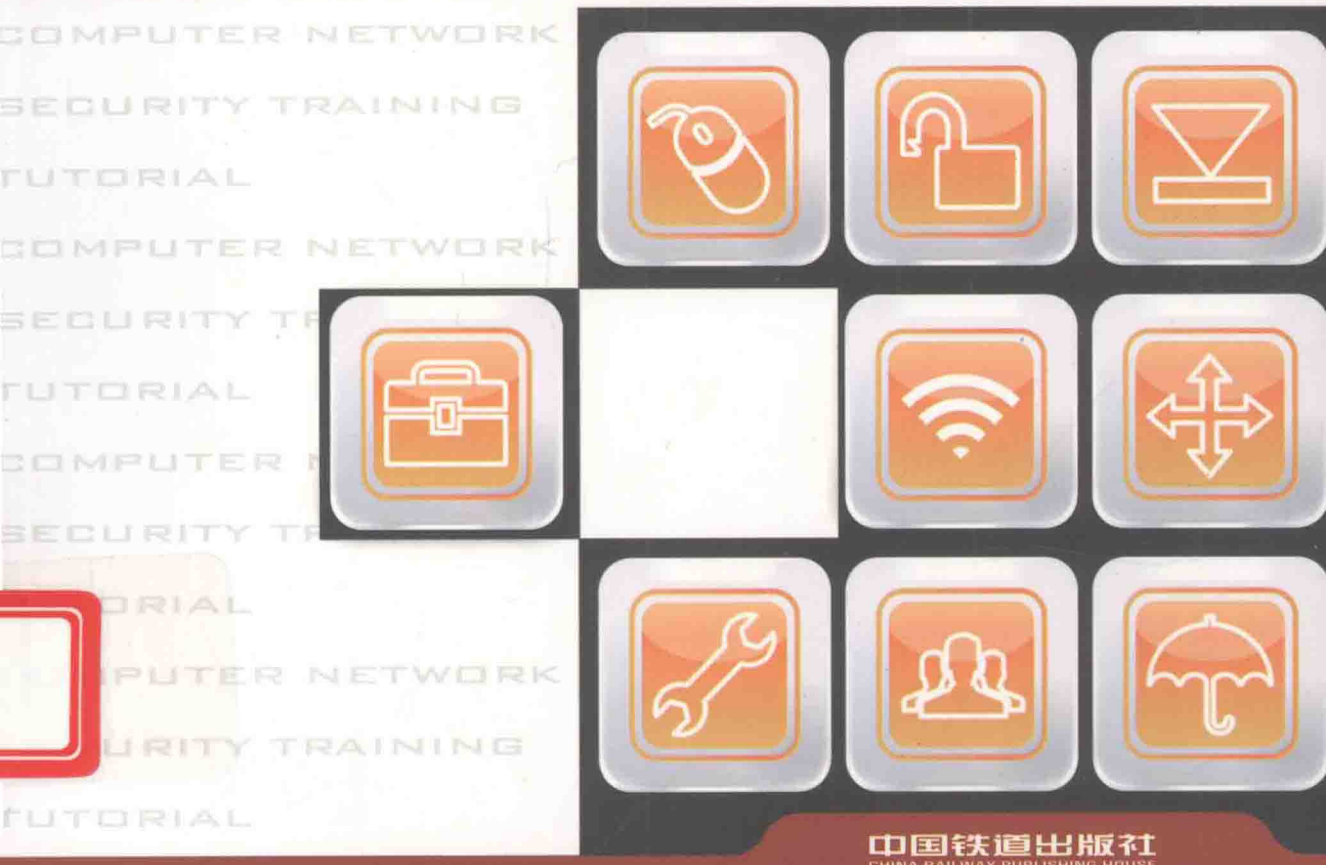
国家社会科学基金(教育学科)"十一五"规划课题研究成果

全国高等职业院校计算机教育规划教材

计算机网络安全实训教程

COMPUTER NETWORK SECURITY TRAINING TUTORIAL

贺广生　武书彦　吴慧玲　主编



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

国家社会科学基金（教育学科）“十一五”规划课题研究成果
全国高等职业院校计算机教育规划教材

计算机网络安全实训教程

主编　贺广生　武书彦　吴慧玲

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书遵循“理论知识以够用为度，重在实践应用”的原则，通俗地阐述了网络安全的基础知识，主要内容包括计算机网络安全知识、计算机病毒防治、黑客攻防技术、操作系统安全、信息加密技术基础、数字签名与数字证书、防火墙技术、电子商务的安全等。

本书的特色在于书中提供了大量的实训例子，能够帮助读者理解和掌握计算机网络安全的基本原理与技术。每章后面都附有习题，有利于教师的授课和学生的学习。

本书适合高职高专计算机及相关专业的学生使用，也可作为对计算机网络安全技术感兴趣的读者的实训参考书。

图书在版编目（CIP）数据

计算机网络安全实训教程 / 贺广生，武书彦，吴慧玲主编. -- 北京：中国铁道出版社，2011.2
国家社会科学基金（教育学科）“十一五”规划课题研究成果. 全国高等职业院校计算机教育规划教材
ISBN 978-7-113-12172-3

Ⅰ. ①计… Ⅱ. ①贺… ②武… ③吴… 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（2011）第 012646 号

书　　名：计算机网络安全实训教程
作　　者：贺广生　武书彦　吴慧玲　主编

策划编辑：翟玉峰
责任编辑：翟玉峰　　**读者热线电话：400－668－0820**
特邀编辑：梁卫红　　**编辑助理：包　宁　巨　凤**
封面设计：付　巍　　**封面制作：白　雪**

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号）　邮政编码：100054
印　　刷：河北新华第二印刷有限责任公司
版　　次：2011 年 2 月第 1 版　　2011 年 2 月第 1 次印刷
开　　本：787mm × 1092mm　1/16　印张：14　字数：334 千
印　　数：3 000 册
书　　号：ISBN 978-7-113-12172-3
定　　价：22.00 元

国家社会科学基金(教育学科)“十一五”规划课题研究成果
全国高等职业院校计算机教育规划教材

编审委员会

主　任：邓泽民

副主任：（按姓氏笔画排序）

吕一中　严晓舟　李　雪　汪燮华　张洪星
张晓云　武马群　赵凤芝　段银田　宣仲良
姚卿达　聂承启　徐　红　彭　勇　蒋川群

委　员：（按姓氏笔画排序）

王浩轩　邓安远　邓璐娟　白延丽　包　锋
朱　立　任益夫　刘志成　刘晓川　孙街亭
延　静　李　洪　李　洛　李　新　李学相
李洪燕　杨立峰　杨永娟　杨志茹　杨俊清
连卫民　吴晓葵　沈大林　宋海军　张　伦
张世正　张晓蕾　张新成　欧阳广　周国征
赵传慧　赵轶群　段智毅　贺　平　秦绪好
袁春雨　徐人凤　徐布克　黄丽民　梅创社
崔永红　梁国浚　蒋腾旭　蔡泽光　翟玉峰

序

PREFACE

国家社会科学基金（教育学科）“十一五”规划课题“以就业为导向的职业教育教学理论与实践研究”（课题批准号 BJA060049）在取得理论研究成果的基础上，选取了高等职业教育十个专业类开展实践研究，高职高专计算机类专业是其中之一。

本课题研究发现，高等职业教育在专业教育上承担着帮助学生构建起专业理论知识体系、专业技术框架体系和相应职业活动逻辑体系的任务，而这三个体系的构建需要通过专业教材体系和专业教材内部结构得以实现，即学生的心理结构来自于教材的体系和结构。为此，这套高职高专计算机类专业系列教材的设计，依据不同教材在其构建知识、技术、活动三个体系中的作用，采用了不同的教材内部结构设计和编写体例。

承担专业理论知识体系构建任务的教材，强调了专业理论知识体系的完整与系统，不强调专业理论知识的深度和难度，追求的是学生对专业理论知识整体框架的把握，不追求学生只掌握某些局部内容的深度和难度。

承担专业技术框架体系构建任务的教材，注重让学生了解这种技术的产生与演变过程，培养学生的技术创新意识；注重让学生把握这种技术的整体框架，培养学生对新技术的学习能力；注重让学生在技术应用过程中掌握这种技术的操作，培养学生的技术应用能力；注重让学生区别同种用途的其他技术的特点，培养学生职业活动过程中的技术比较与选择能力。

承担职业活动体系构建任务的教材，依据不同职业活动对所从事人特质的要求，分别采用了过程驱动、情景驱动、效果驱动的方式，形成了“做学”合一的各种的教材结构与体例，诸如：项目结构、案例结构等。过程驱动培养所从事人的程序逻辑思维；情景驱动培养所从事人的情景敏感特质；效果驱动培养所从事人的发散思维。

本套教材从课程标准的开发、教材体系的建立、教材内容的筛选、教材结构的设计，到教材素材的选择，均得到了信息技术产业专家的大力支持，他们根据信息技术行业职业资格标准和各类技术在我国应用的广泛程度，提出了十分有益的建议；国内知名职业教育专家和一百多所高职高专院校参与本课题研究，他们对高职高专信息技术类人才培养提出了可贵意见，对高职高专计算机类专业教学提供了丰富的素材和鲜活的教学经验。

这套教材是我国高职教育近年来从只注重学生单一职业活动逻辑体系构建，向专业理论知识体系、技术框架体系和职业活动逻辑体系三个体系构建的转变的有益尝试，也是国家社会科学研究基金课题“以就业为导向的职业教育教学理论与实践研究”研究成果的具体应用之一。

本套教材如有不足之处，敬请各位专家、老师和广大同学不吝赐教。希望通过本套教材的出版，为我国高等职业教育和信息技术产业的发展做出贡献。

2009 年 8 月

前言

FOREWORD

互联网的迅猛发展正在改变着人们的工作、学习和生活方式，同时互联网的不安全也正在影响着社会政治、经济、文化和生产的各个领域，网络安全越来越成为全社会关注的焦点。如何维护我们的网络免受黑客及不安全因素的攻击，如何保证计算机网络处于一个安全稳定的工作环境，是计算机网络专业人士都在思考的重要问题。

计算机网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术等多种学科和技术的综合性学科，课程的理论性强，涉及的知识面宽，对学生的理论与实践两方面的要求均较高。本书基于高职高专层次的读者，遵循“理论知识以够用为度，重在实践应用”的原则，在简单介绍计算机网络安全理论知识的基础上，从实训和应用的角度出发，使读者了解一般计算机网络安全的基础理论和技术原理，能够理解和掌握计算机网络安全的实质，了解涉及网络不安全的主要因素有哪些，如何构建一个安全稳定的网络安全环境。本书每章配有大量的实训例子，以培养学生的动手能力和提高学生的综合运用能力；此外，每章后面都配有相应的练习，为学生课后巩固课堂知识提供方便，并在附录中给出了部分试题的参考答案。本书实训用到的工具相对来讲都是比较新的版本，都可以从互联网上免费下载。本书完全从实用的角度出发，用较少的理论和大量的实训来讲解当前网络安全解决方案中用到的技术。

本书共分 9 章，主要内容如下：

第 1 章是网络安全概述，主要介绍计算机网络安全的现状、计算机网络安全的定义和网络信息安全的特征等知识。

第 2 章主要介绍操作系统的安全配置方法，包括如何配置账户安全、系统安全、服务安全，以及如何有效地维护注册表安全。

第 3 章主要介绍 Web 服务的安全及 Web 浏览器的安全性。

第 4 章主要介绍电子商务的安全知识，包括电子商务的现状、电子商务涉及的安全问题及电子商务的两种安全协议等。

第 5 章主要介绍密码学的基础知识，包括密码学的基本概念、密码学的对称加密算法和非对称加密算法及数据传输加密技术等。

第 6 章主要介绍数字签名及数字证书的基础知识，包括什么是数字签名、数字签名的原理、数字签名的过程及数字证书的使用。

第 7 章主要介绍计算机病毒的分类、特征，计算机病毒的入侵途径及其危害，计算机病毒的检测及防范技术等。

第 8 章主要介绍黑客攻击网络的一些知识，从黑客如何攻击网络的角度告诉读者如何发现网络的不安全因素。

第 9 章主要介绍防火墙技术，包括防火墙满足的条件及防火墙自身的局限性、防火墙的几种技术、防火墙的体系结构和防火墙产品的选购等。

本书涉及的内容实践操作性强，建议在学习时可多安排实训操作课时，并要求学生写好实训报告。对本书理论如需要进一步加深学习，可参考其他理论知识比较强的书。建议本课程的教学课时安排 60 学时，其中理论部分安排 26 学时，实训部分安排 34 学时。建议第 1、4 章分别安排 4 学时，第 6、7、9 章分别安排 6 学时，第 2、3、5 章分别安排 8 学时，第 8 章安排 12 学时。

本书由贺广生（解放军信息工程大学）、武书彦（郑州牧业工程高等专科学校）、吴慧玲（郑州牧业工程高等专科学校）任主编，张新成（开封大学）、张辉（黄河水利职业技术学院）、耿丽（河南省财经学校）任副主编，张思胜（郑州牧业工程高等专科学校）、焦晖（郑州轻工业学院民族职业学院）、曾赟（黄河水利职业技术学院）、马金素（郑州牧业工程高等专科学校）、何保荣（郑州牧业工程高等专科学校）、王辉（郑州牧业工程高等专科学校）参与了编写工作。本书由贺广生统稿并定稿。在本书的编写过程中，还得到了解放军信息工程大学沈建京教授的大力支持，在此表示衷心的感谢！本书在编写过程中参考了大量的有关资料、文献，一些资料来自互联网和一些非正式出版物，书后的参考文献无法一一罗列，在此一并表示诚挚的感谢！

由于编写水平及时间所限，书中难免有疏漏和不足之处，恳请专家和广大读者批评指正。

编 者

2010 年 10 月

目录

CONTENTS

第1章 网络安全概述

学习目的

- 了解网络安全的现状，掌握网络安全的定义及实质，掌握网络信息安全的特征。
- 理解计算机网络系统面临的几种威胁，了解安全威胁存在的根源。
- 掌握网络安全的防范技术。
- 了解网络安全威胁的发展趋势。

1.1 网络安全简介

1.1.1 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，大到国际间的合作、全球经济的发展，小到购物、聊天、游戏，所有社会中存在的活动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重要。据中国互联网络信息中心（CNNIC）发布的《第26次中国互联网络发展状况统计报告》显示，截至2010年6月底，我国网民规模已达4.2亿人，互联网普及率持续上升增至31.8%。互联网在中国已进入高速发展时期，人们的工作、学习、娱乐和生活已完全离不开网络。

但与此同时，互联网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，因而操作系统、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、内部攻击及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、软件下载及即时通信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Hotmail、谷歌、雅虎等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，木马病毒井喷式大肆传播，而且传播途径千变万化让人防不胜防。

计算机网络已成为敌对势力、不法分子的攻击目标；成为很多青少年吸食网络毒品（主要是不良信息，如不健康的网站图片和视频等）的滋生源；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。

1.1.2 网络安全的定义

网络安全从狭义角度来分析，是指计算机及其网络系统资源和信息资源（即网络系统的硬件、软件和系统中的数据）受到保护，不受自然和人为有害因素的威胁和危害；从广义上讲，凡是涉及计算机网络信息的保密性、完整性、可用性、真实性和不可抵赖性的相关技术和理论都是计算机网络安全的研究领域。

网络安全问题实际上包括两方面的内容：一是网络的系统安全；二是网络的信息安全。网络安全从其本质上来讲就是网络上信息的安全，它涉及的内容相当广泛，既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于如何防范外部非法攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据，提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题。

1.1.3 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过程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具备五大核心要素：

1. 保密性

保密性是防止信息泄露给非授权个人或实体，只允许授权用户访问的特性。保密性是一种面向信息的安全性，它建立在可靠性和可用性的基础之上，是保障网络信息系统安全的基本要求。

2. 完整性

完整性是指网络中的信息安全、准确、有效，不因人为的因素而改变信息原有的内容、形式与流向，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输，也就是信息在生成、存储或传输过程中保证不被偶然或蓄意地删除、修改、伪造、乱序、插入等破坏和丢失的特性。

3. 可用性

可用性即网络信息系统在需要时，允许授权用户或实体使用的特性；或者是网络信息系统在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的特性。

4. 真实性

真实性是确保网络信息系统的访问者与其声称的身份是一致的；确保网络应用程序的身份和功能与其声称的身份和功能是一致的；确保网络信息系统操作的数据是真实有效的数据。

5. 不可抵赖性

不可抵赖性也称做不可否认性，即在网络信息系统的信息交互过程中所有参与者都不可能否认或抵赖曾经完成的操作的特性。

1.2 网络安全面临的威胁

当前威胁网络安全的因素很多，通常分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。

从其表现形式上看，凡是涉及自然灾害、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威胁。

从技术角度来分析，网络存在的安全威胁原因在于：一方面由于网络的所有资源可以为所有用户共享，这不可避免地留给不法分子可乘之机；另一方面是因为网络的技术是开放和标准的，研制者当初并没有刻意考虑网络的安全性能，因此才造成了今天网络面临的各种威胁。

从人为的恶意攻击行为上分析，可以将网络安全威胁分为两类：一类为主动攻击，其目标在于篡改系统中的信息，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，并通过对信息的破译以获得重要的机密信息。

但网络安全威胁的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。就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，再加上基于网络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，尤其是网络已不仅作为信息传递的平台和工具，而且还担当起了控制系统的中枢，那些与网络密切相关的政治、经济、军事、文化和金融、通信、电力、交通、油气等国家的战略命脉，也必然地处于相对的威胁之中。

1.3 网络安全问题的根源

前面我们分析了网络安全的主要威胁，下面了解一下这些安全问题存在的根源。大体上网络安全问题有物理安全问题、方案设计的缺陷、系统的安全漏洞、TCP/IP 协议的安全和人的因素等几个方面。

1.3.1 物理安全问题

物理安全问题除了物理设备本身的问题外，还包括设备的位置安全、限制物理访问、物理环境安全和地域因素等。物理设备的位置极为重要，所有基础网络设施都应该放置在严格限制来访人员的地方，以降低出现未经授权访问的可能性。

物理设备也面临着环境方面的威胁，这些威胁包括温度、湿度、灰尘、供电系统对系统运行可靠性的影响。另外，电磁辐射也可以造成信息泄露，自然灾害（如地震、闪电、风暴等）也能对系统造成破坏等。

此外，还有地域因素，互联网络往往跨越城际、国际，地理位置错综复杂，通信线路质难以保证，这样，一方面在其上传输的信息会遭到损坏、丢失，同时也给那些“搭线窃听”黑客以可乘之机，增加更多的安全隐患。

1.3.2 系统安全问题

随着软件系统规模的不断增大，系统中的安全漏洞或后门也不可避免地存
常用的无论是网络版还是单机版的操作系统，无论是 Windows 还是 Linux 几
的安全漏洞，众多的各类服务器，最典型的如微软的 IIS 服务器、浏览器

存在有安全隐患。可以说任何一个软件系统都可能因为程序员的一个疏忽、设计中的一个缺陷等原因而存在安全漏洞，这也是网络安全问题的主要根源之一。

1.3.3 方案设计问题

有一类安全问题的根源在于方案设计时的缺陷。由于在实际中，网络的结构往往比较复杂，为了实现异构网络间信息的通信，往往要牺牲一些安全机制的设置和实现，因而会提出更高的网络开放性的要求。而开放性和安全性往往是互为矛盾的，因为特定的环境往往会有特定的安全需求，所以不存在可以到处通用的解决方案，往往需要制定不同的方案。如果设计者的安全理论与实践水平不够，那么设计出来的方案经常会出现很多漏洞，这也是安全威胁的根源之一。

1.3.4 协议安全问题

因特网最初的设计考虑是该网并不会因局部故障而影响信息的传输，所以基本没有考虑信息安全问题，因此它在安全可靠、服务质量、带宽和方便性等方面存在着严重的不适应性。尤其是作为因特网灵魂的 TCP/IP，更存在着很大的安全隐患，它缺乏强健的安全机制，这也是网络不安全的主要因素之一。

本文主要以 TCP/IP 的主要协议之一——IP，作为例子来说明这个问题。IP 依据 IP 头中的目的地址项来发送 IP 数据包，如果目的地址是本地网络内的地址，则该 IP 包就被直接发送到目的地；而如果目的地址不在本地网络内，则该 IP 包就会被发送到网关，再由网关决定将其发送到何处，这是 IP 路由 IP 包的方法。我们发现，IP 协议在路由 IP 包时对 IP 头中提供的 IP 源地址不做任何检查，并且认为 IP 头中的 IP 源地址即为发送该包的机器的 IP 地址。当接收到该包的目的主机要与源主机进行通信时，它以接收到的 IP 包中 IP 源地址作为其发送的 IP 包的目的地址，来与源主机进行数据通信。IP 的这种数据通信方式虽然非常简单和高效，但它同时也是 IP 的一个安全隐患，常常会使 TCP/IP 网络遭受两类攻击：最常见的一类就是拒绝服务攻击（DoS），另一类最常见的攻击是劫持攻击。

1.3.5 人的因素

人是信息活动的主体，因此人的因素是网络安全问题的最主要因素，这主要体现在以下 3 个方面：

1. 人为的无意失误

如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

人为的恶意攻击

意攻击也就是黑客攻击，这是计算机网络所面临的最大威胁。此类攻击又可以分一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是在不影响网络正常工作的情况下，进行截获、窃取和破译以获得重要机密信息。计算机网络造成极大的危害，并导致机密数据的泄露。

盖了所有的操作系统，包括 UNIX、Windows、Linux 等。黑客攻击比病毒

破坏更具目的性，因而也更具危害性。更为严峻的是，黑客技术逐渐被越来越多的人掌握和发展。目前，世界上有上千万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用及系统的一些漏洞，因而系统、站点遭受攻击的可能性就更大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性好、杀伤力强，并成为网络安全的主要威胁之一。

3. 管理上的因素

网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于安全方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90%的 IT 企业对黑客攻击准备不足。目前，美国 75%～85%的网站都抵挡不住黑客的攻击，约有 75%的企业网上信息失窃。此外，管理的缺陷还可能造成系统内部人员泄露机密或外部人员通过非法手段截获而导致机密信息的泄露，从而为一些不法分子制造了可乘之机。

1.4 确保网络安全的主要技术

网络安全是一个相对概念，不存在绝对的安全，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。应对网络安全威胁则需要不断提升防范的技术和加强安全管理，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。目前广泛运用和比较成熟的网络安全技术主要有：信息加密技术、数字签名技术、防病毒技术、防火墙技术、入侵检测技术等，以下将对这几项技术分别进行简单的分析。

1.4.1 信息加密技术

信息加密技术是利用数学或物理手段，对信息在传输过程中和存储体内进行保护，以防止泄露的技术。加密就是通过密码算术对数据进行转化，使之成为没有正确密钥任何人都无法读懂的报文，而这些以无法读懂的形式出现的数据一般被称为密文。为了读懂报文，密文必须重新转变为它的最初形式——明文，而用来以数学方式转换报文的双重密码就是密钥。在这种情况下即使一则信息被截获并阅读，这则信息也是毫无利用价值的。

按照国际上通行的惯例，将信息加密技术按照双方收发的密钥是否相同的标准划分为两大类：

一种是对称加密算法，其特征是收信方和发信方使用相同的密钥，即加密密钥和解密密钥是相同或等价的。比较著名的对称加密算法有：美国的 DES 及其各种变形，欧洲的 IDEA，日本的 RC4、RC5 及以代换密码和转轮密码为代表的古典密码等。在众多的对称加密算法中影响最大的是 DES 对称加密算法。对称加密算法的优点是有很强的保密强度，且可以经受住时间检验和攻击，但其密钥必须通过安全的途径传送。因此，其密钥管理成为系统安全的

另一种是公钥加密算法，也叫非对称加密算法。其特征是收信方和发信方使用相同，而且几乎不可能从加密密钥推导出解密密钥。比较著名的公钥密码算法有码、McEliece 密码、Diffe Hellman、Rabin、椭圆曲线、EIGamal 算法等。最有算法是 RSA，它能抵抗到目前为止已知的所有密码攻击。

1.4.2 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，或是对数据单元所作的密码变换。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（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，签名消息能在通信网络中传输。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。

数字签名技术主要解决以下信息安全问题：

- 否认：事后发送者不承认文件是他发送的。
- 伪造：有人自己伪造了一份文件，却声称是某人发送的。
- 冒充：冒充别人的身份在网上发送文件。
- 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。

1.4.3 防病毒技术

随着计算机技术的不断发展，计算机病毒变得越来越复杂，它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 上，它对本地和本地工作站连接的远程资源采用分析扫描的方式进行检测、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。

1.4.4 防火墙技术

网络防火墙技术是一种用来加强网络之间访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络，访问内部网络资源，保护内部网络操作环境的特殊网络互连设备。它对两个或多个网络之间传输的数据包（如链接方式）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。

目前的防火墙产品主要有堡垒主机、包过滤路由器、应用层网关（或代理服务器）及电路层网关、屏蔽主机防火墙、双宿主机等类型。

防火墙处于 5 层网络安全体系中的最底层，属于网络层安全技术范畴，负责网络间的安全认证与传输。但随着网络安全技术的整体发展和网络应用的不断变化，现代防火墙技术已经逐步走向网络层之外的其他安全层次，不仅要完成传统防火墙的过滤任务，同时还能为各种网络应用提供相应的安全服务。另外，还有多种防火墙产品正朝着数据安全与用户认证、防止病毒和黑客入侵等方向发展。

侵检测技术

技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术，包侵和内部用户的非授权行为进行检测。进行入侵检测的软件与硬件的组合便trusion Detection System，IDS）。入侵检测系统能够实现以下的主要功能：