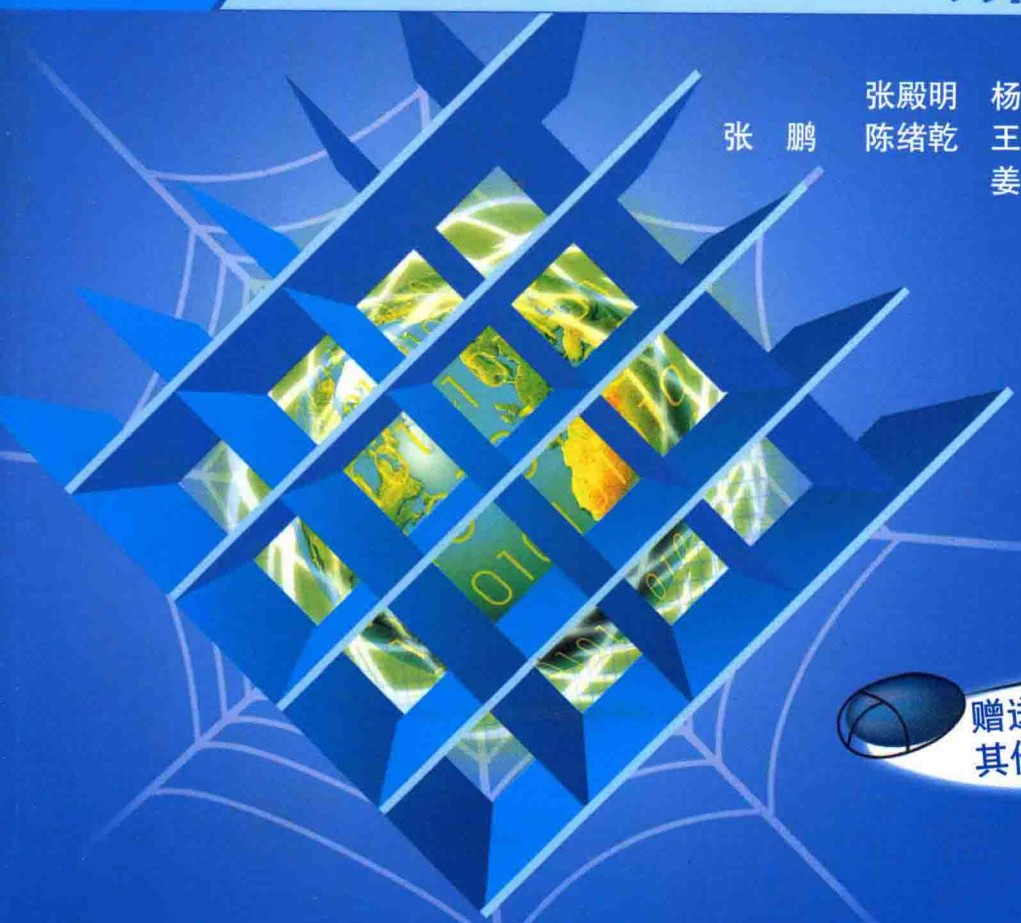
高职高专立体化教材计算机系列

# 计算机网络安全

（第2版）

张殿明　杨　辉　主　编
张　鹏　陈绪乾　王　妍　副主编
姜芳艽　主　审



赠送电子课件及
其他立体化资源

清华大学出版社

## 高职高专立体化教材计算机系列

- 网络互联及路由器技术（第2版） 姜大庆
- C语言程序设计（第2版） 李泽中
- 计算机组装与维护维修（第2版） 刘 博
- CSS+DIV网页布局技术教程 黄玉春
- ASP动态网页设计（第2版） 黄玉春
- C#程序设计——Windows项目开发（第2版） 邵顺增
- SQL Server 2005数据库管理 刘 勇
- Photoshop平面设计项目实用教程（第2版） 卢宇清
- 网站规划建设与管理维护（第2版） 张殿明
- 中小企业网络设备配置与管理 王新风
- 数据结构（C语言版） 郝春梅
- 综合布线系统设计与施工 姜大庆
- SQL Server 2008案例教程 高晓黎
- 计算机网络安全（第2版） 张殿明
- 局域网组建与维护实用教程 傅晓锋
- 网络工程规划与设计 张殿明
- 多媒体技术与应用 李 竺
- 计算机网络技术基础 王树军
- 数据库原理与应用（Access） 张 巍
- 网页制作与设计 高晓黎
- JAVA程序设计 高晓黎
- 网络安全管理与维护 付忠勇
- Linux操作系统 胡剑锋
- ERP原理、实施与案例（第2版） 肖 玉
- 办公自动化技术教程（第2版） 梁建卿
- JSP编程技术（第2版） 杨学全

本丛书免费提供以下配套教学资源

- 电子教案：包括每章的教学重点、难点、授课内容等。
- 习题库：提供多种形式的习题，并配有习题答案或要点分析，部分图书还提供了模拟试卷。
- 案例库：提供丰富的教学案例，并给出分析内容或提示。
- 专题拓展：因限于篇幅等原因不能在纸质教材中讲授的知识点，将在网络中得到补充或扩展。

清华大学出版社数字出版网站
WQBook 书文同泉
www.wqbook.com

ISBN 978-7-302-35559-5
9 787302 355595 >
定价：38.00元

高职高专立体化教材　计算机系列

# 计算机网络安全
# (第2版)

张殿明　杨　辉　主　编
张　鹏　陈绪乾　王　妍　副主编

清华大学出版社
北　京

## 内 容 简 介

本书从网络安全的角度出发，全面介绍网络安全的基本理论以及网络安全方面的管理、配置和维护。全书共分 10 章，主要内容包括网络安全概述、网络攻击与防范、拒绝服务与数据库安全、计算机病毒与木马、安全防护与入侵检测、加密技术与虚拟专用网、防火墙、网络应用服务安全配置、无线网络安全以及移动互联网安全的相关知识。各章后都编排了习题，供学生课后复习与巩固所学知识。

本书注重实用性，实例丰富、典型，实训内容和案例融合在课程内容中，从而将理论知识与实践操作可以很好地结合起来。

通过本书的学习，读者可以对网络安全有一个基本和较全面而系统的认识，同时可以学会使用网络安全工具。本书可作为高职高专计算机、网络技术、电子商务等相关专业学生的教材，也可作为相关技术人员的参考书或培训教材。



**图书在版编目(CIP)数据**

计算机网络安全/张殿明主编. --2 版. --北京：清华大学出版社，2014
(高职高专立体化教材　计算机系列)
ISBN 978-7-302-35559-5
Ⅰ. ①计… Ⅱ. ①张… Ⅲ. ①计算机网络—安全技术—高等职业教育—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 040132 号

**责任编辑**：桑任松
**封面设计**：刘孝琼
**责任校对**：周剑云
**责任印制**：王静怡

**出版发行**：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62791865

**印 刷 者**：三河市君旺印装厂
**装 订 者**：三河市新茂装订有限公司
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　　张**：22.25　　**字　　数**：541 千字
**版　　次**：2010 年 4 月第 1 版　2014 年 5 月第 2 版　　**印　　次**：2014 年 5 月第1 次印刷
**印　　数**：1～3000
**定　　价**：38.00 元

产品编号：054176-01

# 《高职高专立体化教材　计算机系列》

# 丛　书　序

## 一、编写目的

关于立体化教材，国内外有多种说法，有的叫“立体化教材”，有的叫“一体化教材”，有的叫“多元化教材”，其目的是一样的，就是要为学校提供一种教学资源的整体解决方案，最大限度地满足教学需要，满足教育市场需求，促进教学改革。我们这里所讲的立体化教材，其内容、形式、服务都是建立在当前技术水平和条件基础上的。

立体化教材是一个“一揽子”式的，包括主教材、教师参考书、学习指导书、试题库在内的完整体系。主教材讲究的是“精品”意识，既要具备指导性和示范性，也要具有一定的适用性，喜新不厌旧。那种内容越编越多，本子越编越厚的低水平重复建设在“立体化”的世界中将被扫地出门。和以往不同，“立体化教材”中的教师参考书可不是千人一面的，教师参考书不只是提供答案和注释，而是含有与主教材配套的大量参考资料，使得老师在教学中能做到“个性化教学”。学习指导书更像一本明晰的地图册，难点、重点、学习方法一目了然。试题库或习题集则要完成对教学效果进行测试与评价的任务。这些组成部分采用不同的编写方式，把教材的精华从各个角度呈现给师生，既有重复、强调，又有交叉和补充，相互配合，形成一个教学资源有机的整体。

除了内容上的扩充，立体化教材的最大突破还在于在表现形式上走出了“书本”这一平面媒介的局限，如果说音像制品让平面书本实现了第一次“突围”，那么电子和网络技术的大量运用就让躺在书桌上的教材真正“活”了起来。用 PowerPoint 开发的电子教案不仅大大减少了教师案头备课的时间，而且也让学生的课后复习更加有的放矢。电子图书通过数字化使得教材的内容得以无限扩张，使平面教材更能发挥其提纲挈领的作用。

CAI 课件把动画、仿真等技术引入了课堂，让课程的难点和重点一目了然，通过生动的表达方式达到深入浅出的目的。在科学指标体系控制之下的试题库既可以轻而易举地制作标准化试卷，也能让学生进行模拟实战的在线测试，提高了教学质量评价的客观性和及时性。网络课程更厉害，它使教学突破了空间和时间的限制，彻底发挥了立体化教材本身的潜力，轻轻敲击几下键盘，你就能在任何时候得到有关课程的全部信息。

最后还有资料库，它把教学资料以知识点为单位，通过文字、图形、图像、音频、视频、动画等各种形式，按科学的存储策略组织起来，大大方便了教师在备课、开发电子教案和网络课程时的教学工作。如此一来，教材就“活”了。学生和书本之间的关系不再像领导与被领导那样呆板，而是真正有了互动。教材不再只为教师们规定什么重要什么不重要，而是成为教师实现其教学理念的最佳拍档。在建设观念上，从提供和出版单一纸质教材转向提供和出版较完整的教学解决方案；在建设目标上，以最大限度满足教学要求为根本出发点；在建设方式上，不单纯以现有教材为核心，简单地配套电子音像出版物，而是

以课程为核心，整合已有资源并聚拢新资源。

网络化、立体化教材的出版是我社下一阶段教材建设的重中之重，作为以计算机教材出版为龙头的清华大学出版社确立了“改变思想观念，调整工作模式，构建立体化教材体系，大幅度提高教材服务”的发展目标。并提出了首先以建设“高职高专计算机立体化教材”为重点的教材出版规划，希望通过邀请全国范围内的高职高专院校的优秀教师，在2008年共同策划、编写这一套高职高专立体化教材，利用网络等现代技术手段实现课程立体化教材的资源共享，解决国内教材建设工作中存在教材内容的更新滞后于学科发展的状况。把各种相互作用、相互联系的媒体和资源有机地整合起来，形成立体化教材，把教学资料以知识点为单位，通过文字、图形、图像、音频、视频、动画等各种形式，按科学的存储策略组织起来，为高职高专教学提供一整套解决方案。

## 二、教材特点

在编写思想上，以适应高职高专教学改革的需要为目标，以企业需求为导向，充分吸收国外经典教材及国内优秀教材的优点，结合中国高校计算机教育的教学现状，打造立体化精品教材。

在内容安排上，充分体现先进性、科学性和实用性，尽可能选取最新、最实用的技术，并依照学生接受知识的一般规律，通过设计详细的可实施的项目化案例(而不仅仅是功能性的小例子)，帮助学生掌握要求的知识点。

在教材形式上，利用网络等现代技术手段实现立体化的资源共享，为教材创建专门的网站，并提供题库、素材、录像、CAI 课件、案例分析，实现教师和学生在更大范围内的教与学互动，及时解决教学过程中遇到的问题。

本系列教材采用案例式的教学方法，以实际应用为主，理论够用为度。

本系列教材将提供全方位、立体化的服务。网上提供电子教案、文字或图片素材、源代码、在线题库、模拟试卷、习题答案等。

在为教学服务方面，主要是通过教学服务专用网站在网络上为教师和学生提供交流的场所，每个学科、每门课程，甚至每本教材都建立网络上的交流环境。可以为广大教师信息交流、学术讨论、专家咨询提供服务，也可以让教师发表对教材建设的意见，甚至通过网络授课。对学生来说，则可以在教学支撑平台上所提供的自主学习空间上来实现学习、答疑、作业、讨论和测试，当然也可以对教材建设提出意见。这样，在编辑、作者、专家、教师、学生之间建立起一个以课本为依据、以网络为纽带、以数据库为基础、以网站为门户的立体化教材建设与实践的体系，用快捷的信息反馈机制和优质的教学服务促进教学改革。

# 前　言

计算机网络安全已引起世界各国的广泛关注，我国也在高等教育中不断增加计算机网络安全方面的基础知识和网络安全技术应用知识。随着网络高新技术的不断发展，社会经济的建设与发展越来越依赖于计算机网络。与此同时，网络中的不安全因素对国民经济的威胁，甚至对国家和地区的威胁也日益严重。加快培养网络安全方面的应用型人才、广泛普及网络安全知识和掌握网络安全技术就突显重要。本书是在广泛调研和充分论证的基础上，结合当前应用最为广泛的网络攻防技术实例，并通过研究实践而形成的一本高职高专计算机及相关专业网络安全课程的教材，全书较系统而全面地介绍了网络安全与管理方面的相关内容，并适当地安排了实训内容，旨在使读者能够综合运用书中所讲授的知识进行网络安全与管理方面的实践。

本书以培养应用型和技能型人才为根本，通过认识、实践、总结和提高这样一个认知过程，精心组织学习内容，图文并茂、深入浅出，全面适应社会发展的需要，符合高等职业教育教学改革规律及发展趋势，力求内容先进实用，并有所创新。全书共分 10 章：第 1 章全面分析计算机网络的基本安全问题，介绍网络安全的基本概念、内容和方法，以及当前病毒发展的趋势和最新的防病毒技术；第 2 章重点介绍网络攻击与防范措施；第 3 章介绍拒绝服务与数据库安全相关知识；第 4 章重点介绍计算机病毒与木马的概念，以及攻击防范技术；第 5 章重点介绍入侵与攻击的基本概念，典型的攻击方法和原理，以及入侵检测方法等基本内容；第 6 章主要介绍加密技术与虚拟专用网的相关知识；第 7 章介绍防火墙的概念、设计原理与应用案例；第 8 章介绍网络应用服务安全配置技术；第 9 章介绍无线网络安全的相关知识；第 10 章介绍移动互联网安全的相关知识。

本书第 1 版主要由山东水利职业学院的老师编写完成。本书的第 2 版在改版之初，有计划地深入互联网企业调研，收集素材，并进行分析整理；同时针对日益严峻的网络安全现状和移动互联网飞速发展的形势，更是为了在教材中融入最新的网络安全知识，邀请了几位互联网企业专家参加了教材的编写和指导工作，具体工作完成情况如下。

全书由张殿明策划、组织编写、修改校对和统稿。第 1 章由张殿明编写，第 2 章由金山安全中心张民松编写，第 3 章由陈绪乾老师与山东浪潮齐鲁软件产业股份有限公司刘伟峰共同编写，第 4 章由王妍编写，第 5 章由钱玉霞编写，第 6 章由刘春燕编写，第 7 章由黄山编写，第 8 章由张鹏编写，第 9 章由杨辉编写，第 10 章由浪潮通信信息系统有限公司杨士强编写。

限于编者的水平，书中有不当甚至错误之处，诚恳广大读者提出宝贵意见。

编　者

# 目　录

# 第 1 章　网络安全概述

**【本章要点】**

通过本章的学习，可以了解网络安全的现状及发展趋势，掌握其定义。了解网络安全主要表现的几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理安全等。了解当前最先进的反病毒技术。

## 1.1　网络安全的内涵

近年来，随着计算机和网络技术在社会生活各方面的广泛应用，计算机和计算机网络已经成为人们生活中不可或缺的重要组成部分。计算机网络具有的开放性、交互性和分散性等特点，使其很容易受到干扰和攻击。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、信息安全技术、应用数学和信息论等多种学科的综合性学科，其本身包括的范围很大，大到国家军事政治机密等安全，小到防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。随着大数据时代的到来，信息量呈现高速增长，人们对网络信息安全给予了前所未有的关注。每年发生的网络信息安全事件更是不计其数，如今信息泄露、黑客攻击和病毒入侵等均成为网络安全的主要威胁。

美国的“棱镜门”事件，更是敲响了全球网络信息安全的警钟。2013 年 6 月，据《华盛顿邮报》报道，美国国家安全局(以下简称 NSA)和联邦调查局(以下简称 FBI)正在通过一个代号为 PRISM(棱镜)的机密项目，参加 PRISM 项目的科技公司包括硅谷最具主导地位的企业，这些企业的 logo 都出现在该项目的花名册上，包括微软、雅虎、谷歌、Facebook、PalTalk、AOL、Skype、YouTube 与苹果公司。

棱镜计划(PRISM)是一项由美国国家安全局(NSA)自 2007 年起开始实施的绝密电子监听计划，该计划的正式名号为 US-984XN。

据报道，PRISM 计划能够对从手机到服务器，从办公软件到操作系统，从搜索引擎到无线通信技术等进行深度的监听。许可的监听对象包括：任何在美国以外地区使用参与该计划公司服务的客户，或是任何与国外人士通信的美国公民。受到美国国家安全局监控的主要有 10 类信息：电子邮件、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料。通过 PRISM 项目，美国国家安全局甚至可以实时监控一个人正在进行的网络搜索内容。

有关PRISM的报道是在美国政府持续秘密地要求威讯(Verizon)向国家安全局提供所有客户每日电话记录的消息曝光后不久出现的。泄露这些绝密文件的是美国中情局前技术助理爱德华·斯诺登，他原本在夏威夷的国家安全局办公室工作，在 2013 年 5 月将文件复制后前往香港并将文件公开。据悉，仅 2012 年，综合情报文件(总统每日简报)就在 1 477 个计划中使用了来自 PRISM 计划的资料。

目前，美国著名 IT 公司的业务几乎渗透到了中国网络的每一个环节，鉴于上述的事件，

我们应如何来保障网络安全呢?

### 1.1.1 网络安全的定义

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受破坏、更改和泄露，网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全涉及的内容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都必须考虑和解决的一个重要问题。

### 1.1.2 网络安全的特征

网络安全一般应包括以下五个基本特征。

(1) 保密性：确保信息不泄露给非授权用户。

(2) 完整性：确保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、不被破坏和丢失的特性。

(3) 可用性：确保可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

(4) 可控性：确保对信息的传播及内容具有控制能力。

(5) 可审查性：确保出现安全问题时提供依据与手段。

## 1.2 网络安全分析

从网络运行和管理者的角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家安全的信息进行过滤和防堵，避免机要信息泄露，避免对社会造成危害、给国家造成巨大损失。从社会教育和意识形态角度来讲，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，必须对其进行控制。

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网(Intranet)、企业外部网(Extranet)、全球互联网(Internet)的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断的提高。但在连接能力信息、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理安全等。

对于网络安全问题，为了防患于未然，首先要了解网络安全的根源，然后制定相应的安全策略，做到事前主动防御、事发灵活控制和事后分析追踪。

### 1.2.1　物理安全

网络的物理安全是整个网络系统安全的前提，也是整个组织安全策略的基本元素。总体来说，物理安全的风险主要有：地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获等。因此要尽量避免网络的物理安全风险，对于足够敏感的数据和一些关键的网络基础设施，可以在物理上和多数公司用户分开，并采用增加的身份验证技术(如智能卡登录、生物验证技术等)控制用户对其物理上的访问，从而减少安全破坏的可能性。

### 1.2.2　网络结构安全

网络拓扑结构设计也会直接影响网络系统的安全性。当外部与内部网络进行通信时，内部网络的机器安全就会受到威胁，同时也可能影响在同一网络上的许多其他系统。通过网络传播，还会影响到连上 Internet/Intranet 的其他网络；因此，我们在设计时有必要将公开服务器(WEB、DNS、EMAIL 等)和外网及内部其他业务网络进行必要的隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该被拒绝。

### 1.2.3　系统安全

系统的安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。不管基于桌面的操作系统还是基于网络的操作系统，都不可避免地存在诸多的安全隐患，如非法存取、远程控制、缓冲区溢出以及系统后门等，从各个操作系统厂商不断发布的安全公告以及系统补丁可见一二。可以确切地说，没有完全安全的操作系统。不同的用户应从不同的方面对其网络作详尽的分析，选择安全性尽可能高的操作系统。因此不但要选用尽可能可靠的操作系统和硬件平台，并对操作系统进行安全配置。而且，必须加强登录过程的认证(特别是在到达服务器主机之前的认证)，确保用户的合法性；其次应该严格限制登录者的操作权限，将其能完成的操作限制在最小的范围内。

### 1.2.4　应用系统安全

应用系统的安全跟具体的应用有关，涉及面广。应用系统的安全是动态的。应用的安全性也涉及信息的安全性，并包括很多方面。

#### 1. 应用系统的安全是动态的、不断变化的

应用程序配置和漏洞通常是恶意软件攻击或利用的目标。如攻击者可以通过诱使用户打开受感染的电子邮件附件攻击系统或使恶意软件在整个网络上传播。而其他如 WWW 服务、即时通信、FTP 服务以及 DNS 服务等都存在不同程度的安全漏洞，只有通过专业的安

全工具不断发现漏洞、修补漏洞，提高系统的安全性，才能有效防止恶意的攻击。

**2. 应用的安全性涉及信息、数据的安全性**

信息的安全性涉及机密信息泄露、未经授权的访问、假冒信息、破坏信息完整性、破坏系统的可用性等。在某些网络系统中，涉及很多机密信息，如果一些重要信息被窃取或破坏，在经济、社会和政治方面将造成严重的影响。因此，对用户使用计算机必须进行身份认证，对于重要信息的通信必须授权，传输必须加密；采用多层次的访问控制与权限控制手段，实现对数据的安全保护；采用加密技术，保证网上传输信息包括管理员口令与账户、上传信息等的机密性与完整性。

### 1.2.5 管理的安全

管理是网络安全最重要的部分。责权不明，安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。当网络出现攻击行为或网络受到其他一些安全威胁时(如内部人员的违规操作等)，无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案。因此，最可行的做法是把健全的管理制度和严格管理相结合。保障网络的安全运行，使其成为一个具有良好的安全性、可扩充性和易管理性的信息网络。一旦上述的安全隐患成为事实，所造成的对整个网络的损失都是难以估计的。因此，网络的安全建设是局域网建设过程中重要的一环。

## 1.3 网络安全的现状和发展趋势

### 1.3.1 概况

国内多家著名互联网安全企业都对 2013 年上半年互联网信息安全现状与趋势从不同的方面进行了统计、研究和分析。

**1. 360 安全中心**

仅 2013 年第二季度，360 互联网安全中心共截获新增恶意程序样本 5.27 亿个，同比增长 112.5%，环比增长 32.4%，恶意程序样本量的快速增长态势令人担忧。其中盗号木马仍然是对用户威胁最大的恶意程序。此外，流量型木马也活动猖獗，这类木马以后台静默的方式为网站刷广告，或劫持浏览器主页推广不良网址导航，这也是木马产业链的主要牟利方式。而可被黑客用于远程操控用户电脑的后门病毒也重新活跃起来，对网民上网构成了巨大的安全威胁，值得高度警惕。

从攻击目标来看，各种游戏盗号木马仍然是最为活跃的木马类别，这其中又以 DNF 游戏的盗号木马最为突出。

从风险人群和高危人群的比例分布上看，广东是 2013 年第二季度中国上网最不安全的

省级行政区，而香港、澳门、北京、上海和西藏是二季度中国上网最安全的省级行政区。

挂马网站数量继续减少，新增钓鱼网站数量虽然同比增长了 180.9%，但环比却下降了 34.6%；虚假购物、模仿登录和虚假中奖仍然是新增钓鱼网站的主要类型；而从单个钓鱼网站的拦截量来看，排名前 20 的钓鱼网站以境外彩票网站和假医假药网站为主。

美国仍然是中国钓鱼网站的主要源头，占比高达 38.0%；同时北美其他地区和中国内地的钓鱼网站数量增长迅速，占比分别为 30.3%和 15.7%；来自韩国的钓鱼网站数量较一季度大幅减少。

美联社 Twitter 账户被黑，IE8 爆出“劳动节水坑”漏洞以及美国黑客组织从 ATM 窃取 4 500 万美元等网络攻击事件，成为 2013 年第二季度最值得关注的国际互联网安全事件。

犯罪分子利用超级网银的安全风险进行巨额欺诈，通过 CSRF 链接攻击用户末端路由器，以及网上兼职欺诈泛滥成灾，成为 2013 年第二季度最值得关注的国内互联网安全事件。

#### 2. 瑞星公司

2013 年 1 至 6 月，病毒总体数量比去年下半年增长 93.01%，呈现出一个爆发式的增长态势。瑞星“云安全”系统截获挂马网站 246 万个(以网页个数统计)，与 2012 年下半年相比下降了 12%。同时，在报告期内，瑞星“云安全”系统共截获钓鱼网站 399 万个，比 2012 年下半年增长了 41%，帮助用户拦截钓鱼网站攻击 11 971 万人次。由此可见，现阶段挂马网站的威胁已经远远低于钓鱼网站攻击所带来的威胁。

2013 年上半年，比特币、电视选秀节目、留学生 QQ 和 Cookie 成为黑客及网络诈骗者重点关注的对象。黑客制作病毒盗取比特币，并控制用户电脑组成僵尸网络。同时，电视选秀节目类钓鱼网站开始在互联网上疯狂传播，为用户的网络生活带来巨大风险。除此之外，针对留学生的 QQ 盗号和高额诈骗在上半年频频发生，Cookie 也成为不法分子盗取用户隐私的重要途径。

在移动互联网方面，智能手机 APP 暴露出众多安全隐患。因 APP 应用设置不当造成用户人身安全的事故时有发生，同时，一些不法分子已经开始利用微博、微信等互联网社交平台的定位功能，定向追踪用户的隐私信息，为企业及个人造成巨大安全威胁。另外，2013 年上半年，多款国内外知名无线路由器也被发现存在安全漏洞，黑客可以通过该类漏洞对企业及个人用户进行终身监控。

美国 “棱镜”项目的曝光，致使国家级信息战全面爆发，我国由于过度依赖外国产品，国内企事业机关单位的办公网络目前都处于高危状态，时刻面临被第三方监控的危险。同时，各大政企内部的信息安全建设严重缺失，建立健全的信息安全体系是当务之急。除此之外，虚拟化、云应用、BYOD 设备、智能手机及可穿戴设备，也严重威胁着企业机密乃至国家机要的安全。

### 1.3.2　电脑病毒疫情统计

#### 1. 瑞星公司 2013 年上半年病毒概述

1) 病毒疫情总体概述

2013 年 1 至 6 月，瑞星“云安全”系统共截获新增病毒样本 1 633 万余个。其中木马病毒 1 172 万个，占总体病毒的 71.8%，与 2012 年情况相同，仍为第一大种类病毒。新增