21st CENTURY
实用规划教材

21世纪全国高职高专
计算机系列实用规划教材

网络安全基础
教程与实训

主　编　杨　诚　尹少平
副主编　刘华谱　张恒杰

内容特点：

- 本书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。
- 各章配有习题，大部分章节配有相应的实训，便于教学和自学。
- 可作为高职高专院校计算机及相关专业的学生教材，也可作为计算机网络安全类的技术参考书或培训教材。

北京大学出版社
PEKING UNIVERSITY PRESS

21 世纪全国高职高专计算机系列实用规划教材

网络安全基础教程与实训

主　编　杨　诚　尹少平
副主编　刘华谱　张恒杰
参　编　李　磊　张　军

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

网络安全基础知识是网络安全教育和培训过程中首先要学习和掌握的内容，本教材全面介绍了网络安全的基本框架、网络安全的基本理论以及计算机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、IP 数据报结构、密码技术、Windows 2000 系统安全、病毒分析与防御、应用服务安全、网络攻击与防范、VPN 技术、防火墙技术、入侵检测系统。

本教材注重实践技能的培养，以实训为依托，深入浅出地讲解理论知识，因此既可作为高职高专院校计算机及相关专业的学生教材，也可作为计算机网络安全类的技术参考书或培训教材。

图书在版编目(CIP)数据

网络安全基础教程与实训/杨诚，尹少平主编. —北京：北京大学出版社，2005.9

(21 世纪全国高职高专计算机系列实用规划教材)

ISBN 7-301-09667-4

Ⅰ.网… Ⅱ.①杨…②尹… Ⅲ. 计算机网络—安全技术—高等学校：技术学校—教材

Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2005)第 103339 号

书　　名：网络安全基础教程与实训

著作责任者：杨诚　尹少平　主编

责 任 编 辑：李彦红

标 准 书 号：ISBN 7-301-09667-4/TP・0816

出 版 者：北京大学出版社

地　　址：北京市海淀区中关村北京大学校内　100871

网　　址：http://cbs.pku.edu.cn　http://www.pup6.com

电　　话：邮购部 62752015　发行部 62750672　编辑部 62750667

电 子 信 箱：pup_6@163.com

排 版 者：北京东方人华北大彩印中心　　电话：62754190

印 刷 者：涿州市星河印刷有限公司

发 行 者：北京大学出版社

经 销 者：新华书店

787 毫米×1092 毫米　16 开本　19.75 印张　474 千字

2005 年 9 月第 1 版　　2005 年 9 月第 1 次印刷

定　　价：26.00 元

信息技术的职业化教育

(代丛书序)

刘瑞挺/文

北京大学出版社第六事业部组编了一套《21 世纪全国高职高专计算机系列实用规划教材》。为此，制订了详细的编写目的、丛书特色、内容要求和风格规范。在内容上强调面向职业、项目驱动、注重实例、培养能力；在风格上力求文字精练、图表丰富、脉络清晰、版式明快。

一、组编过程

2004 年 10 月，第六事业部林章波主任、葛昊晗副主任开始策划这套丛书，分派编辑深入各地职业院校，了解教学第一线的情况，物色经验丰富的作者。2005 年 1 月 15 日在济南召开了“北大出版社高职高专计算机规划教材研讨会”。来自 13 个省、41 所院校的 70 多位教师汇聚一堂，共同商讨未来高职高专计算机教材建设的思路和方法，并对规划教材进行了讨论与分工。2005 年 6 月 13 日在苏州又召开了“高职高专计算机教材大纲和初稿审定会”。编审委员会委员和 45 个选题的主、参编，共 52 位教师参加了会议。审稿会分为公共基础课、计算机软件技术专业、计算机网络技术专业、计算机应用技术专业 4 个小组对稿件逐一进行审核。力争编写出一套高质量的、符合职业教育特点的精品教材。

二、知识结构

职业生涯的成功与人们的知识结构有关。以著名侦探福尔摩斯为例，作家柯南道尔在“血字的研究”中，对其知识结构描述如下：

- 文学知识——无；
- 哲学知识——无；
- 政治学知识——浅薄；
- 植物学知识——不全面。对于药物制剂和鸦片却知之甚详。对毒剂有一般了解，而对于实用园艺却一无所知；
- 化学知识——精深；
- 地质学知识——偏于应用，但也有限。他一眼就能分辨出不同的土质。根据裤子上泥点的颜色和坚实程度就能说明是在伦敦什么地方溅上的；
- 解剖学知识——准确，却不系统；
- 惊险小说知识——很渊博。似乎对近一个世纪发生的一切恐怖事件都深知底细；
- 法律知识——熟悉英国法律，并能充分实用；
- 其他——提琴拉得很好，精于拳术、剑术。

事实上，我国唐朝名臣狄仁杰，大宋提刑官宋慈，都有类似的知识结构。审视我们自己，每人的知识结构都是按自己的职业而建构的。因此，我们必须面向职场需要来设计教材。

三、职业门类

我国的职业门类分为 18 个大类：农林牧渔、交通运输、生化与制药、地矿与测绘、材料与能源、土建水利、制造、电气信息、环保与安全、轻纺与食品、财经、医药卫生、旅游、公共事业、文化教育、艺术设计传媒、公安、法律。

每个职业大类又分为二级类，例如电气信息大类又分为 5 个二级类：计算机、电子信息、通信、智能控制、电气技术。因此，18 个大类共有 75 个二级类。

在二级类的下面，又有不同的专业。75 个二级类共有 590 种专业。俗话说：“三百六十行，行行出状元”，现代职业仍在不断涌现。

四、IT 能力领域

通常信息技术分为 11 个能力领域：规划的能力、分析与设计 IT 解决方案的能力、构建 IT 方案的能力、测试 IT 方案的能力、实施 IT 方案的能力、支持 IT 方案的能力、应用 IT 方案的能力、团队合作能力、文档编写能力、项目管理能力以及其他能力。

每个能力领域下面又包含若干个能力单元，11 个能力领域共有 328 个能力单元。例如，应用 IT 方案能力领域就包括 12 个能力单元。它们是操作计算机硬件的能力、操作计算软件包的能力、维护设备与耗材的能力、使用计算软件包设计机构文档的能力、集成商务计算软件包的能力、操作文字处理软件的能力、操作电子表格应用软件的能力、操作数据库应用软件的能力、连接到互联网的能力、制作多媒体网页的能力、应用基本的计算机技术处理数据的能力、使用特定的企业系统以满足用户需求的能力。

显然，不同的职业对 IT 能力有不同的要求。

五、规划梦想

于是我们建立了一个职业门类与信息技术的平面图，以职业门类为横坐标、以信息技术为纵坐标。每个点都是一个函数，即 IT(Professional)，而不是 IT+Professional 单纯的相加。针对不同的职业，编写它所需要的信息技术教材，这是我们永恒的主题。

这样组合起来，就会有 IT((328)*(Pro(590)))，这将是一个非常庞大的数字。组织这么多的特色教材，真的只能是一个梦想，而且过犹不及。能做到 IT((11)*(Pro(75)))也就很不容易了。

因此，我们既要在宏观上把握职业门类的大而全，也要在微观上选择信息技术的少而精。

六、精选内容

在计算机科学中，有一个统计规律，称为 90/10 局部性原理(Locality Rule)：即程序执行的 90%代码，只用了 10%的指令。这就是说，频繁使用的指令只有 10%，它们足以完成 90%的日常任务。

事实上，我们经常使用的语言文字也只有总量的 10%，却可以完成 90%的交流任务。同理，我们只要掌握了信息技术中 10%频繁使用的内容，就能处理 90%的职业化任务。

有人把它改为 80/20 局部性原理，似乎适应的范围更广些。这个规律为编写符合职业教育需要的精品教材指明了方向：坚持少而精，反对多而杂。

本系列教材编写目的和教学服务

本系列教材在遍布全国的各位编写老师的共同辛勤努力下，在编委会主任刘瑞挺教授和其他编审委员会成员的指导下，在北京大学出版社第六事业部的各位编辑刻苦努力下，本系列教材终于与广大师生们见面了。

教材编写目的

近几年来，职业技术教育事业得以蓬勃的发展，全国各地的高等职业院校以及高等专科学校无论是从招生人数还是学校的软、硬件设施上都达到了相当规模。随着我国经济的高速发展，尽快提高职业技术教育的水平显得越来越重要。教育部提出：职业教育就是就业教育，也就是说教学要直接面对就业，强调实践。不但要介绍技术，更要介绍具体应用，注重技术与应用的结合。本套教材的主要编写思想如下。

1．与发达国家相比，我国职业技术教育教材的发展比较缓慢并且滞后，远远跟不上职业技术教育发展的需求。我们常常提倡职业教育的实用性，但在课堂教学中仍然使用理论性和技术性教材进行职业实践教学。针对这种现状，急需推出一系列切合当前教育改革需要的高质量的优秀职业技术实训型教材。

2．本套教材总结了目前优秀计算机职业教育专家的教学思想与经验，与广大职业教育一线老师共同探讨，最终落实到本套教材中，开发出一套适合于我国职业教育教学目标和教学要求的教材，它是一套能切实提高学生专业动手实践能力和职业技术素质的教材。

3．社会对学生的职业能力的要求不断提高，从而催化出了许多新型的课程结构和教学模式。新型教学模式是必须以工作为基础的模仿学习，它是将学生置于一种逼真的模拟环境中，呈现给学生的是具有挑战性、真实性和复杂性的问题，使学生得到较真实的锻炼。

4．教材的结构必须按照职业能力的要求创建并组织实施新的教学模式。教学以专项能力的培养展开，以综合能力的形成为目标。能力的培养既是教学目标，又是评估的依据和标准。

5．本套的重点是先让学生实践，从实践中领悟、总结理论，然后再学习必要的理论，用理论指导实践。从这一个循环的教学过程中，学生的职业能力将得到极大的提高。

教学服务

1. 提供电子教案

本系列教材绝大多数都是教程与实训二合一，每一本书都有配套的电子教案，以降低任课老师的备课强度，此课件可以在我们网站上随时下载。

2. 提供教学资源下载

本系列教材中涉及到的实例(习题)的原始图片和其他素材或者是源代码、原始数据等文件，都可以在我们网站上下载。

3. 提供多媒体课件和教师培训

针对某些重点课程，我们配套有相应的多媒体课件。对大批量使用本套教材的学校，我们会免费提供多媒体课件，另外还将免费提供教师培训名额，组织使用本套教材的教师进行相应的培训。

北京大学出版社第六事业部(http://www.pup6.com)

七、职业本领

以计算机为核心、贴近职场需要的信息技术已经成为大多数人就业的关键本领。职业教育的目标之一就是培养学生过硬的 IT 从业本领，而且这个本领必须上升到职业化的高度。

职场需要的信息技术不仅是会使用键盘、录入汉字，而且还要提高效率、改善质量、降低成本。例如，两位学生都会用 Office 软件，但他们的工作效率、完成质量、消耗成本可能有天壤之别。领导喜欢谁？这是不言而喻的。因此，除了道德品质、工作态度外，必须通过严格的行业规范和个人行为规范，进行职业化训练才能养成正确的职业习惯。

我们肩负着艰巨的历史使命。我国人口众多，劳动力供大于求的矛盾将长期存在。发展和改革职业教育，是我国全面建设小康社会进程中一项艰巨而光荣的任务，关系到千家万户人民群众的切身利益。职业教育和高技能人才在社会主义现代化建设中有特殊的作用。我们一定要兢兢业业、不辱使命，把这套高职高专教材编写好，为我国职业教育的发展贡献一份力量。

刘瑞挺教授　曾任中国计算机学会教育培训委员会副主任、教育部理科计算机科学教学指导委员会委员、全国计算机等级考试委员会委员。目前担任的社会职务有：全国高等院校计算机基础教育研究会副会长、全国计算机应用技术证书考试委员会副主任、北京市计算机教育培训中心副理事长。

前　言

随着网络应用的广泛深入和电子商务技术的迅速发展，网络已成为现代社会生活与工作不可或缺的组成部分。但是，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，这就是网络安全问题。例如，电子邮件可能被截取，商业机密可能被窃听，网站可能被恶意破坏等，所有这些网络安全隐患都让我们在享用网络服务时变得忐忑不安。

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。全书共分 10 章：第 1 章阐述了网络安全的基础知识，对网络安全进行概要性描述；第 2 章主要介绍网络层和传输层各协议的报头结构；第 3 章介绍了一些密码算法的有关知识，包括基本概念和简单的实现方法；第 4 章详细介绍了 Windows 2000 操作系统的安全防护知识；第 5 章着重分析了病毒的特征和防御方法；第 6 章对 Web、FTP、E-mail、SQL Server 2000 等常用网络应用服务的安全进行了详细的讨论，并提供了一些可行的安全措施；第 7 章全面介绍了防火墙技术；第 8 章详细阐述了入侵检测技术；第 9 章介绍了典型的网络攻击和相应的防范技术；第 10 章深入剖析了 VPN 技术应用。

各章配有习题，大部分章节配有相应的实训，便于教学和自学。

扎扎实实学完本教材的学员将具备防病毒软件的应用与部署、防火墙的安装与使用、入侵检测系统的配置等一系列配置和使用安全设备及工具网络安全应用能力，能胜任初中级的网络安全管理工作。

本教材由常州信息职业技术学院的杨诚、太原电力高等专科学校的尹少平担任主编，辽东学院信息技术学院的刘华谱、石家庄职业技术学院的张恒杰担任副主编，石家庄计算机职业学院的李磊、石家庄职业技术学院的张军担任参编。其中杨诚负责撰写第 1 章，李磊负责撰写第 2 章，张恒杰负责编写第 3 章，张军负责撰写第 5 章，刘华谱负责撰写第 4、第 6 章，尹少平负责撰写第 7、第 8、第 9、第 10 章。全书由杨诚统一编排定稿。

由于编者水平有限，时间仓促，不妥之处在所难免，恳请广大读者批评指正。

编　者

2005 年 7 月

目　录

第 1 章　网络安全概论

教学提示：随着网络技术及其应用的深入和普及，电子商务、电子政务的开展、实施和应用，网络安全已经不再仅仅为科学研究人员和少数黑客所涉足，日益庞大的网络用户群同样需要掌握网络安全知识。只有这样，才有可能构筑属于全社会的信息安全体系。与早期网络技术的普及一样，对于数量庞大的普通用户群，网络安全问题始终是一个神秘而高深的话题。通过对本章的学习，希望大家从对网络安全的懵懂而又渴望的状态中获得解放，对网络安全问题有全面的了解。

教学要求：本章主要学习网络安全概念、网络安全威胁、网络安全标准、网络安全组件、安全策略的制定与实施。学完本章将对网络安全从宏观上有较好的把握。

1.1　网络安全概念

以 Internet 为代表的全球性信息化浪潮所带来的影响日益深刻，信息网络技术的应用正日益普及，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型的、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要因素，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在以下两个方面。

(1) 开放性的网络，导致网络的技术是全开放的，任何组织和个人都可能获得，因而网络所面临的破坏和攻击可能是多方面的。例如：任何具有不良企图的黑客可以对物理传输线路实施攻击，也可以对网络通信协议实施攻击；可以对软件实施攻击，也可以对硬件实施攻击。网络的国际化还意味着网络的攻击不仅仅来自本地网络用户，它可以来自 Internet 上的任何一台主机，也就是说，网络安全所面临的是一个国际化的挑战。

(2) 自由意味着网络最初对用户的使用并没有提供任何的技术约束，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。用户只对自己的行为负责，而不受任何的法律限制。

开放的、自由的、国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得人们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力，同时人们又要面对网络开放带来的数据安全的新挑战和新危险。如何保护内部机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所必须考虑的重要事情之一。

1.1.1　网络安全的概念

网络安全包括 5 个要素：机密性、完整性、可用性、可控性和可审查性。机密性指确保信息不暴露给未授权的实体或进程。完整性则意味着只有得到授权的实体才能修改数据，

并且能够判别出数据是否已被篡改。可用性说明得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。可控性表示可以控制授权范围内的信息流向及行为方式。可审查性指对出现的网络安全问题提供调查的依据和手段。

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，从广义来说，凡是涉及到计算机网络上信息的机密性、完整性、可用性、可控性、可审查性的相关技术和理论都是计算机网络安全的研究领域。

1.1.2 网络安全的现状

现在全球普遍存在缺乏网络安全意识的状况。人们在组建一个网络的时候，并没有意识到网络安全的重要性。这导致大多数网络存在着先天性的安全漏洞和安全威胁。

国际上也存在着信息安全管理规范和标准不统一的问题。美国是西方国家中对信息安全着力较多的国家之一，同样存在着规范和标准跟不上技术进步发展的问题。西欧国家则另有一套信息安全标准，虽然在原理和结构上同美国有相同的部分，但是不同的部分也相当多。

在信息安全的发展过程中，企业和政府的要求有一致的地方，也有不一致的地方。企业更注重于信息和网络安全的可靠性，政府更注重信息和网络安全的可管性和可控性。由美国政府组织的 KRS 系统，就是由于企业不欢迎而无法推广。在发展中国家，对信息安全的投入还满足不了信息安全的需求，同时投入也常常被挪用和借用。

但不可忽视的现象是信息和安全的技术仍然在发展过程中。

同样在国内，网络安全产品的“假、大、空”现象在一定程度上普遍存在，防火墙变成了网络安全的全部。产生这种情况的原因是重技术、轻管理，以及网络安全知识的普及程度不够。

1.2 网络安全所产生的威胁

使用 TCP/IP 协议的网络所提供的网络服务都包含许多不安全的因素，存在着许多漏洞。同时，网络的普及使信息共享达到了一个新的层次，信息被暴露的机会大大增多。特别是 Internet 网络就是一个不设防的开放大系统。另外，数据处理的可访问性和资源共享的目的性之间是一对矛盾，这些都给网络带来了威胁。

1.2.1 网络中存在的威胁

目前网络中存在的威胁主要表现在以下几个方面。

1. 非授权访问

没有预先经过同意就使用网络或计算机资源被看作是非授权访问，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，或擅自扩大权限，越权访问信息。非授权访问主要包括以下几种形式：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. 泄漏或丢失信息

泄漏或丢失信息指敏感数据被有意泄漏出去或丢失，通常包括，信息在传输中丢失或泄漏(如“黑客”们利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，得到用户密码、账号等重要信息)，信息在存储介质中丢失或泄漏，敏感信息被隐蔽隧道窃取等。

3. 破坏数据完整性

指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等。

4. 拒绝服务攻击

通过不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序响应来减慢甚至使网络服务瘫痪，影响正常用户的使用，导致合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务等。

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。

1.2.2 主机网络安全

由于主机安全和网络安全的技术手段难以有机地结合，因此容易被入侵者各个击破。并且由于它们在保护计算机和信息的安全上各自为政，因此很难解决系统安全性和使用方便性之间的矛盾。举一个简单的例子，从严密保护主机安全来说应该禁止用户的远程登录，但是这给用户的使用将带来极大的不便，对 Internet 上绝大多数 UNIX 主机来说是不可以接受的。而一旦允许用户远程登录，却无法区分用户的远程登录是合法的还是非法的，也就控制不了非法用户的入侵，并且系统一旦被入侵，入侵者就拥有合法用户的全部权力，危害极大。对于防火墙系统来说也有同样的问题，防火墙可以禁止外部主机对于内部主机的访问(安全但不方便)，但是一旦允许用户经防火墙授权认证后进入内部主机，就无法控制其在内部主机上的行为(方便但不安全)。

为了解决这些问题，一种结合主机安全和网络安全的边缘安全技术开始兴起，这就是主机网络安全技术。主机网络安全技术是一种主动防御的安全技术，它结合网络访问的网络特性和操作系统特性来设置安全策略，用户可以根据网络访问的访问者及访问发生的时间、地点和行为来决定是否允许访问继续进行，以使同一用户在不同场所拥有不同的权限，从而保证合法用户的权限不被非法侵占。主机网络安全技术考虑的元素有 IP 地址、端口号、协议、MAC 地址等网络特性和用户、资源权限以及访问时间等操作系统特性，并通过对这些特性的综合考虑，来达到用户网络访问的细粒度控制。

与网络安全采用安全防火墙、安全路由器等在被保护主机之外的技术手段不同，主机网络安全所采用的技术手段通常在被保护的主机内实现，并且一般为软件形式。因为只有在被保护主机之上运行的软件，才能同时获得外部访问的网络特性以及所访问资源的操作

系统特性。在当前广泛使用的计算机安全产品中，已经有一些软件在主机网络安全技术方面做了一些探索。

这类产品中，应用最为广泛的当属 Wietse Venema 开发的共享软件 TCP Wrapper。TCP Wrapper 是一种对进入的网络服务请求进行监视与过滤的工具，它可以截获 systat、finger、ftp、telnet、rlogin、rsh、exec、tftp、talk 等网络服务请求，并根据系统管理员设置的服务访问策略来禁止或允许服务请求。一般情况下，其策略主要考虑的是外部主机的域名(或 IP 地址)和请求的服务类型。通过扩充，还可以将请求访问的用户名和访问时间包括进来，即可以制定“在某时间允许/禁止某用户从外部某主机对某服务的访问”这样的策略。

另外，现在一些操作系统厂商已经或即将在操作系统中提供主机网络安全产品，如 IBM 公司在 AIX4.3.1 中引入了强制访问控制、控制访问的多级目录管理，并可内置 Check Point 公司的 Firewall-1/VPN-14.0；SUN 公司即将发布的 Solaris 中也将引入公共密钥结构(PKI)、基于 IP Security 的虚拟私有网络(VPN)和内置的防火墙。这些措施都将极大地改善主机的网络安全状况。不过它们都是侧重于从访问的网络特性方面考虑，对于访问的操作系统特性考虑不够，因此对于冒充合法用户之类的攻击缺乏有效的办法。

1.2.3 主机网络安全系统体系结构

主机网络安全系统是为了解决主机安全性与访问方便性之间的矛盾，将用户访问时表现的网络特性和操作系统特性综合起来考虑，因此，这样的系统必须建立在被保护的主机上，并且贯穿于网络体系结构中的应用层、传输层、网络层之中。在不同的层次中，可以实现不同的安全策略，具体内容如下。

(1) 应用层：是网络访问的网络特性和操作系统特性的最佳结合点。通过对主机所提供服务的应用协议的分析，可以知道网络访问的行为，并根据用户设置的策略判断在当前环境下是否允许该行为；另外，还要附加更严格的身份论证。

(2) 传输层：是实现加密传输的首选层。对于使用了相同安全系统的主机之间的通信，可以实现透明的加密传输，而对于没有加密措施的通用客户软件之间的通信，仍可以使用不加密方式，并且加密与否对于用户来说是透明的。

(3) 网络层：是实现访问控制的首选层。通过对 IP 地址、协议、端口号的识别，能方便地实现包过滤功能。

当然，更复杂的设计可以在更多的层实现更多的安全功能，下面就前面的设想提出一个可行的主机网络安全系统的结构模型，如图 1.1 所示。

在图 1.1 的结构模型中，安全检查承担了防火墙的任务，它对进出的数据包按照系统设置的安全规则进行过滤，另外，在该模块中还可以实现加密/解密。对用户的访问进行细粒度控制是主机网络安全系统最为重要的特点，它包括两个方面：内部资源访问控制和外部资源访问控制。