高职高专21世纪计算机规划教材

信息安全技术基础

Information Technology Security

李俊宇 编著

冶金工业出版社

高职高专21世纪计算机规划教材

信息安全技术基础

李俊宇　编著

北　京

冶金工业出版社

2004

内 容 简 介

随着 Internet 的发展，网络安全问题越来越引起世界各国、各行各业的人们的关注，它所涉及的范围非常广泛。本书从网络安全的基本概念和安全标准开始，介绍了网络安全涉及的各个方面，主要包括信息安全概要、网络通信协议与安全、信息加密技术、防火墙技术、虚拟专用网、病毒和木马、灾难预防与恢复、Windows 系统安全以及网络攻击实例剖析。

本书针对性强、结构清晰，既可作为大、中专院校计算机应用基础类教程，也可供各类计算机基础教学的培训班和自学人士使用。

图书在版编目（CIP）数据

信息安全技术基础 / 李俊宇编著. —北京：冶金工业出版社，2004.12
ISBN 7-5024-3653-7

I. 信… II. 李… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2004）第 121838 号

出版人 曹胜利（北京沙滩嵩祝院北巷 39 号，邮编 100009）
责任编辑 程志宏
佛山市新粤中印刷有限公司印刷；冶金工业出版社发行；各地新华书店经销
2004 年 12 月第 1 版，2004 年 12 月第 1 次印刷
787mm × 1092mm 1/16； 24.5 印张； 569 千字； 384 页
35.00 元
冶金工业出版社发行部 电话：（010）64044283 传真：（010）64027893
冶金书店 地址：北京东四西大街 46 号（100711） 电话：（010）65289081
（本社图书如有印装质量问题，本社发行部负责退换）

前　言

一、关于本书

自从 Internet 诞生以来，有关网络安全的讨论就没有停止过。如今，随着网络的开放性、共享性、互联程度的扩大，安全问题已经被带入民用领域，并随时随地面临安全破坏与威胁。因而，如何保护自己的系统并且尽可能有效地打击系统入侵者，如何检测内部和外部的入侵，如何在被攻击之后恢复和重建，成为系统安全的主要问题。

本书全面、详细、系统地介绍了系统安全的策略和防护措施，分析了黑客常用的攻击手段，并讲述了与网络安全相关的各项技术，有助于系统管理人员和安全决策人员确定安全保护的方向和原则。

二、本书结构

本书共分为 9 章。前 7 章介绍网络信息安全方面的基本概念和相关的各项技术，第 8、9 章从实例出发，将理论应用到实际中，使读者进一步加深对前面内容的理解。

第 1 章：网络安全概要。主要介绍信息安全的相关知识、安全标准和安全威胁等。

第 2 章：网络通信协议与安全。主要介绍各种网络通信协议，讲述这些协议各自的安全问题和防御措施。

第 3 章：信息加密技术。主要介绍互联网中使用的传统加密技术和现代加密技术。

第 4 章：防火墙技术。主要介绍什么是防火墙、防火墙的体系结构和分类、防火墙的实现、防火墙的类型、防火墙的设置和 PIX 防火墙。

第 5 章：虚拟专用网。主要介绍 VPN 的相关知识，还介绍了基于数据链路层的 VPN 技术和网络层隧道技术以及 VPN 综合应用。

第 6 章：病毒和木马。主要介绍病毒的基础知识、蠕虫病毒、病毒的防范与检测、病毒与网络安全以及特洛伊木马的检测与防范。

第 7 章：灾难预防与恢复。主要介绍安全问题的起因、防范措施以及灾难发生之后的处理方法。

第 8 章：Windows 系统安全。主要介绍 Windows 操作系统的安全机制、采纳的安全标准和使用的安全组件以及 Windows 2003 安全的相关知识。

第 9 章：网络攻击实例剖析。通过实例讲述网络攻击的种类和黑客对系统攻击的步骤。

三、本书特点

本书针对性强、条理清晰、语言简洁明了，在准确地讲述各原理的同时结合大量图片和表格进一步讲解有关网络安全方面的知识，还利用实例加深读者对网络安全内涵的理解，使理论与实践结合起来。

本书每章后都配有丰富的习题，以供读者练习，同时读者可参考后面的答案检测自己的学习效果，以便进一步巩固提高。

四、本书适用对象

本书既可作为大、中专院校计算机应用基础类教程，也可供各类计算机基础教学的培训班和自学人士使用。

虽然经过严格的审核、精心的编辑，本书在质量上有了一定的保障，但我们的目标是力求尽善尽美，欢迎广大读者和专家对我们的工作提出宝贵意见和建议，联系方法如下：

电子邮件：service@cnbook.net

网址：www.cnbook.net

此外，**本书所附送的电子教案也可从该网站免费下载**，该网站还有一些其他相关书籍的介绍，可以方便读者选购参考。

编　者

2004 年 10 月

目　录

第 1 章　信息安全概要

在讨论有关信息安全的问题之前，首先要知道什么是 Internet，为什么会有那么多攻击 Internet 的事情发生。究其原因，主要是 Internet 最初是被设计为开放式网络（Open Network），它包含了互联网以及其他网络和服务。开放式网络是一个客户端和服务器端的群体，它们通过 TCP/IP 协议来进行相互之间的通信（访问）。

TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/互联网协议）是用于计算机通信的一组协议，通常称之为 TCP/IP 协议族。它是 20 世纪 70 年代中期美国国防部为其 ARPANNET 广域网开发的网络体系结构和协议标准。可以在 RFC 793 中找到 TCP 的参数。

但是由于 TCP/IP 本身的开放性，因而它们面临许多考验。

TCP/IP 本身没有内置保护信息的能力，Internet 用户可以相互发送信息而不必进行身份验证。即使服务器没有配置合理的安全措施也可以参与网络活动。这些随意访问网络的活动，可能会造成网络的滥用。现在，不需要懂得很高深的技术，只需要借助在网络上广为流传的脚本或者程序，就可以攻击其他连在网络上的机器。伴随着电子商务、电子现金、数字货币和网络银行等业务的兴起以及各种专用网（如金融网）的建设，网络与信息系统的安全与保密问题显得越来越重要。

国际标准化机构在安全方面从事了大量的工作。1985 年的 DOD 5200.28-STD 即可信计算机系统评测标准（TCSEC，美国国防部橙皮书）为计算机安全产品的评测提供了测试方法，指导信息安全的制造和应用。1987 年，美国国家计算机安全中心（NCSC）为 TCSEC 橙皮书提出了可依赖网络的解释，通常被称为红皮书。1991 年，美国国家计算机安全中心为 TCSEC 橙皮书提出可依赖数据库管理系统解释（TDI）。另外，世界上 IT 业界各大公司都在信息和信息系统安全方面推出了相应的技术产品，如：HP 公司的 ICF（国际密码架构）战略；DEC 公司推出安全级别为 C2 级的操作系统 Digital UNIX 和 OpenVMS，B1/CMW 级的操作系统 SEVMS 和 Digital MLS+；Sun 公司的 B1 级的操作系统 Solaris 等。

目前，系统保护技术已经有了很大的进步。通过加密技术可以更容易地混编网络传输数据，更容易地确认用户身份，更容易地划分网络和控制输入/输出，从而提高网络的安全性。不过，改变开放式的 Internet 还需要相当大的努力。

1.1　信息安全概述

1.1.1　信息安全涉及的问题

信息安全问题涉及到很多方面的问题。一提到网络传输的信息安全，人们总是会立即联想到加密、防黑客、反病毒等专业技术问题。实际上，网络环境下的信息安全不仅涉及到技术问题，而且涉及到法律政策问题和管理问题。技术问题虽然是最直接的保证信息安全的手段，但离开了法律政策和管理的基础，即使有最先进的技术，信息安全也得不到保障。

1. 法律政策问题

要使信息安全运行，信息安全传递，需要必要的法律建设，以法制来强化信息安全。这主要涉及网络规划与建设的法律，网络管理与经营的法律，信息安全的法律，用户（自然人或法人）数据的法律保护，电子资金划转的法律认证，计算机犯罪与刑事立法，计算机证据的法律效力等法律问题。同时，还要有法必依，有法必行。

法律是信息安全的第一道防线。如果没有这些法律的建设和法律的实施，网络将不成为网络。网络将没有规范、协调的运营管理，数据将得不到有效的保护，电子资金的划转将产生法律上的纠纷，网络将受到黑客的攻击而黑客受不到惩罚。仅仅这些问题的发生，就会使网络无法安全地传递信息，无法起到信息传递通道的作用。

有了相关法律的保障，没有相应的政策，也无法使保障信息安全具有可操作性。如美国联邦政府 1996 年发布了 A-130 通告。

2. 管理问题

管理问题包括三个层次的内容：组织建设、制度建设和人员意识。组织建设问题是指有关信息安全管理机构的建设。信息安全的管理包括安全规划、风险管理、应急计划、安全教育培训、安全系统的评估、安全认证等多方面的内容，因此只靠一个机构是没法解决这些问题的。在各信息安全管理机构之间，要有明确的分工，以避免“政出多门”和“政策擅车”现象的发生。

明确了各机构的职责之后，还需要建立切实可行的规章制度，以保证信息安全。如对人的管理，需要解决多人负责、责任到人的问题，任期有限的问题，职责隔离的问题，最小权限的问题等。

有了组织机构和相应的制度，还需要领导的高度重视和群防群治。这需要信息安全意识的教育和培训，以及对信息安全问题的高度重视。

3. 技术问题

影响计算机网络环境下信息安全的技术问题包括通信安全技术和计算机安全技术两个方面，二者共同维护着信息安全。

保证通信安全所涉及的技术有：

（1）信息加密技术。信息加密技术是保障信息安全的最基本、最核心的技术措施和理论基础。信息加密过程通过形形色色的加密算法来具体实施，它以较小的代价获得较大的安全保护。

（2）信息确认技术。信息确认技术通过严格限定信息的共享范围来达到防止信息被非法伪造、篡改和假冒。一个安全的信息确认方案应该能使：

① 合法的接收者能够验证他收到的消息是否真实。

② 发信者无法抵赖自己发出的消息。

③ 除合法发信者外，别人无法伪造消息。

④ 发生争执时可由第三人仲裁。按照其具体目的，信息确认系统可分为消息确认、身份确认和数字签名。

（3）网络控制技术。

① 防火墙技术。它是一种允许接入外部网络，但同时又能够识别和抵抗非授权访问

的信息安全技术。

② 审计技术。它使信息系统自动记录下网络中机器的使用时间、敏感操作和违纪操作等。

③ 访问控制技术。它允许用户对其常用的信息库进行适当权利的访问，限制用户随意删除、修改或拷贝信息文件。访问控制技术还可以使系统管理员跟踪用户在网络中的活动，及时发现并拒绝“黑客”的入侵。

④ 安全协议。整个网络系统的安全强度实际上取决于所使用的安全协议的安全性。

计算机安全涉及计算机硬件、软件和数据的安全。所涉及的技术问题主要有：

（1）容错计算机技术。容错计算机具有的基本特点是：稳定可靠的电源、预知故障、保证数据的完整性和数据恢复等。当任何一个可操作的子系统遭到破坏后，容错计算机能够继续正常运行。

（2）安全操作系统。操作系统是计算机工作的平台，一般的操作系统都在一定程度上具有访问控制、安全内核和系统设计等安全功能。但是微软视窗系统的“NSA 密钥”则在很大程度上危害着用户的信息安全。所谓 NSA 密钥，是指 1998 年有人发现视窗系统中存在用途等详情不清的第二把密钥。1999 年 8 月，加拿大 Cryotonym 公司首席科学家 Andrew Fernandes 宣布，他发现这第二把密钥叫做 NSAKey，而 NSA 就是美国国家安全局的简称，也就是说，微软在每一份视窗系统中都安装了一个“后门”，专供 NSA 在需要时侵入全世界用户的电脑。

（3）计算机反病毒技术。计算机病毒其实是一种在计算机系统运行过程中能够实现传染和侵害的功能程序，是影响计算机安全不容忽视的重要因素。

4. 其他因素

影响网络环境下的信息安全还有一个很重要的因素，即信息安全产业的发展问题。保证网络环境下的信息安全，涉及很多信息安全产品和服务，如：防火墙、安全操作系统、相应的信息安全软件等。如果一个国家的信息安全产品都是依靠国外进口，那么就很难保证一些涉及国家经济安全的信息的安全应用。如果出口国完全掌握着信息安全产品的核心技术，就很容易侵入进口国的网络系统得到进口国的机密信息。例如，目前我们大面积使用国外的 CPU 和操作系统，类似 Intel 芯片奔腾 III 的序列号问题、微软公司视窗系统的“NSA 密钥”就可能威胁我国的信息安全。

另一个问题是信息安全产品和技术的标准及其标准化。制定行业标准是保证行业发展的重要基础，在信息安全产品和技术方面，如果没有统一的标准，那么将无法度量和测评各种信息安全产品和技术。

1.1.2 威胁信息安全的因素

计算机信息安全受到的威胁包括：

（1）“黑客”的攻击。

（2）计算机病毒。

（3）拒绝服务攻击（Denial of Service Attack）。

目前黑客的行为正在不断地走向系统化和组织化。黑客严重影响到系统的正常业务展开，系统功能的丧失，甚至使网络系统瘫痪。

信息安全存在的威胁主要表现在以下几个方面：

（1）非授权访问。这主要的是指对网络设备以及信息资源进行非正常使用或超越权限使用。

（2）假冒合法用户，主要指利用各种假冒或欺骗的手段非法获得合法用户的使用权，以达到使用合法用户资源的目的。

（3）数据完整性受到破坏。

（4）干扰系统的正常运行，改变系统正常运行的方向，延缓系统的响应时间。

（5）病毒。

（6）通信线路被窃听等。

1.1.3 信息安全分类

根据我国的国家计算机安全规范，计算机的安全大致可分为三类：

（1）实体安全，包括机房、线路、主机等。

（2）网络与信息安全，包括网络的畅通、准确以及网上信息的安全。

（3）应用安全，包括程序开发运行。

网络信息安全可分为以下几类：

1. 基本安全类

基本安全类包括访问控制、授权、认证、加密以及内容安全。

访问控制是一种基本的隔离机制，它把企业内部与外界以及企业内部的不同信息源隔离。但是，采用隔离的方法不是最终的目的。网络用户利用网络技术，特别是利用 Internet 技术的最终目的是在保证安全的前提下提供方便的信息访问，这就是对授权的需求。在对授权需求的同时，有必要对授权人的身份进行有效的识别与确认，这就是认证的需求。此外，为了保证信息不被篡改、窃听，必须对信息，包括存储的信息和传输中的信息给予加密，同时，为了实施对进出企业网流量的控制，就需要解决内容安全的问题。

2. 管理与记账类

管理与记账类安全包括安全策略的管理、实时监控、报警以及企业范围内的集中管理与记账。

3. 网络互联设备安全类

网络互联设备包括路由器、远程访问服务器、通信服务器、交换机等。网络互联设备安全正是针对这些互联设备而言的，它包括路由器安全管理、远程访问服务器安全管理、通信服务器安全管理以及交换机安全管理等。

4. 连接控制类

连接控制类包括负载均衡、可靠性以及流量管理等。

1.1.4 信息安全解决方案

信息安全系统实际上是一组用于控制网络之间通信流的部件。这种信息安全系统根据本单位规定的安全策略，准许或拒绝网络通信。

由于信息安全范围的不断扩大，如今的信息安全不再是仅仅保护内部资源的安全，还必须提供附加的服务，例如：用户确认、通过保密、甚至安全管理传统的商务交易机制，

如订货和记账等。

1. 网络信息安全模型

网络信息安全系统并非局限于通信保密和信息加密功能要求等技术问题，它是涉及到方方面面的一项极其复杂的系统工程。一个完整的网络信息安全系统至少包括三类措施，并且三者缺一不可。

三类措施如下：

（1）社会的法律政策，企业的规章制度及信息安全教育。

（2）技术方面的措施，如防火墙技术、防病毒、信息加密、身份确认以及授权等。

（3）审计与管理措施，包括技术与社会措施。主要有实时监控、提供安全策略改变的能力以及对安全系统实施漏洞检查等。

如图 1-1 所示为网络信息安全模型图。

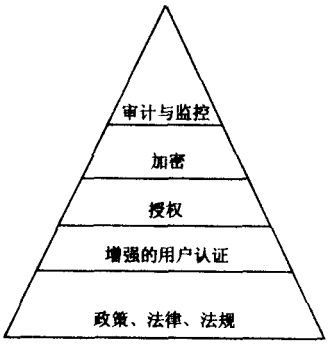

图 1-1 网络信息安全模型

该网络信息安全模型中的政策、法律、法规是安全的基石，是建立安全管理的标准和方法。

第二部分为增强的用户认证，它是安全系统中居于技术措施的首道防线。用户认证的主要目的是提供访问控制。

用户认证方法按其层次的不同，可以根据以下三种情况提供认证：

（1）用户持有的证件，如大门钥匙、门卡等。

（2）用户知道的信息，如密码。

（3）用户特有的特征，如指纹、声音、视网膜扫描等。

授权，主要是为特许用户提供合适的访问权限，并监控用户的活动。

加密，主要满足如下的需求：

（1）认证。识别用户身份，提供访问许可。

（2）一致性。保证数据不被非法篡改。

（3）隐密性。保证数据不被非法用户查看。

（4）不可抵赖。使信息接收者无法否认曾经收到的信息。

加密是信息安全应用中最早使用的一种行之有效的手段，数据经过加密来保证在存取与传送的过程中不被非法查看、篡改、窃取等。在实际使用中，利用加密技术至少需解决如下问题：

（1）钥匙的管理，包括数据加密钥匙和证书的分发措施。

（2）建立权威的钥匙分发机制。

（3）数据加密传输。

（4）数据存储加密等。

在网络信息模型的顶部是审计与监控，这是系统安全的最后一道防线，它包括数据的备份。系统一旦出现了问题，审计与监控可以提供问题的再现、责任追查、重要数据恢复等保障。

2. 安全策略设计依据

设计一个信息安全系统的首要任务是确认该单位的需要和目标，制定安全策略。安全策略需要反映出该单位同公用网络连接的理由，分别规定对内部用户和公众用户提供的服务。制定安全策略时，首先需要确定的最重要的原则是：准许访问除明确拒绝以外的全部服务程序，还是拒绝访问除明确准许以外的全部服务程序。在建立安全策略时，这是关键性的，但往往又是容易被忽视的一步。准许的访问除明确拒绝以外的全部服务程序，对大部分服务程序都很少干预。危及安全的服务程序可能被提供使用并已引发一系列问题，直到管理人员明确加以禁止，其安全问题颇为突出。在另一方面，当安全策略是拒绝访问除明确准许以外的全部服务程序时，可能有新的有用的服务程序可供使用，但用户却无法得到，此时，用户需要将该新服务程序通知管理人员，对该程序进行鉴定后决定是否允许被使用。

在作出基本的决策之后，就可以决定哪些服务程序向内部用户提供，哪些服务程序向外部网络用户提供使用。

安全策略设计还需要有监视安全的方式和实施策略的方式。

在设计安全策略和选择信息安全系统时，还需要考虑成本与方便之间的平衡。这取决于所期望的安全程度和所选用的安全系统。它可能需要额外的硬件，如路由器和专用主计算机，也可能需要特殊的软件，还可能需要安全专家进行系统编程和维护工作。另外需要考虑的因素是安全系统对生产率和服务利用率的影响。有的信息安全系统工具会降低网络速度；有的会限制或拒绝网络上的一些有用的服务程序，如邮件和文件传输；有的则需要新软件分配给内部网络中每一台主机，给用户带来了诸多不便。因此，信息安全系统应该被设计成一个透明的安全系统。这样才能为网络提供安全保护而不会对网络性能有重大的影响，也不会迫使用户放弃一些服务程序或迫使用户去学习某些新的服务程序。

在设计信息安全系统时，还需要考虑安全程度和复杂程度之间的平衡。在信息安全设计中，一个总的原则是：安全系统越复杂，就越容易遭到破坏，维护起来也越困难。而信息安全系统的复杂程度会由于下述因素而增加：增添和管理较多的网络，追加额外的硬件，增加筛选规则的数量。复杂的系统不容易进行正确的配置，因而可能出现问题。

总之，在制定信息安全策略时应当考虑以下因素：

（1）对于内部用户和外部用户分别提供哪些服务程序。

（2）初始投资额和后续投资额（新的硬件、软件及工作人员）。

（3）方便程度和服务效率。

（4）复杂程度和安全等级的平衡。

3. 信息安全解决方案

实施一个信息安全策略，可以使用多种方法，包括信息包筛、应用网关（或中继器）

以及非军事区（DMZ）的各种配置。这几个方法通常是组合使用的，如果是更先进的系统就需另外采用加密手段来提高安全等级。

1）TCP/IP 概述

TCP/IP 是 Internet 的基本网络协议，所有的网络计算机都以协议为标准来定义一些公用的或私用的服务，如文件存取、Web 服务、打印控制等。

协议和操作系统一起完成文件存取过滤，管理网络内的用户、执行文件传输和远距离登录以及实现和 Internet 的连接。

TCP/IP 协议由 TCP 协议和 IP 协议组成。它们是用在 Internet 上的两个网络协议，也可称之为数据传输方法，分别表示传输控制协议和互联网协议。这两个协议属于众多 TCP/IP 协议族的一部分。

TCP/IP 协议族中的协议保证 Internet 上各种类型的计算机之间的数据传输，提供了几乎现在上网所用到的所有服务，这些服务包括电子邮件的传输、文件的传输、BBS、新闻组的发布以及 WWW 的访问等。

2）信息包筛选

信息包筛选，是常驻于路由器或专用主计算机系统（通常在两个网络之间）的数据库规则，它审查网络通信并决定是否允许该信息通过（通常是从一个网络到另一个网络）。信息包筛选允许某些数据信息包通过而阻止另一些信息包的通行，这取决于信息包中的信息是否符合给定的准则。所给定的准则是一组（称作筛选规则）加到每一信息包上的逻辑规则。筛选规则通过信息包筛选，哪一些服务程序是允许使用的，例如，可能有一条规则是这样的：从上午 9 时到下午 5 时之间，允许主机 A 和 B 之间的全部 Telnet 信息通过。在传统的方式中，信息包筛选获得每一信息包上的信息，局限于源 IP 地址和目的 IP 地址、信息包类型（TCP 或 UDP）和目的端口。

由于它不能检查源端口，因而导致许多信息包筛选效率不高而且也不完整。新型的更加有效的信息包筛选引擎能够从数据信息包提取更多的信息，因此，可以将一套更加完整的规则附加到进入和发出的信息包上。然而，这种筛选能力的提高是以系统的成本和复杂程度的增加为代价的。

传统的信息包筛选工具具有一定的优点：对于用户和应用程序来说，它们是快速的、透明的，相对地独立于协议之外；网络的全部信息都必须通过一个通信点（扼流点）。扼流点对于安全管理人员非常有用，因为它可以提供一个惟一界限分明的位置来监视和记录通信，并且实施安全策略。

传统的信息包筛选工具也存在着天生的缺点：实施和维护都比较复杂。有时过滤的准则不足以产生有效的筛选决定;往往没有关于以前通过筛选的信息包的上下文或状态信息。

大部分路由器都允许对进入的信息包或者发出的信息包进行筛选，也可以对两种信息包都进行筛选。另外，筛选可以在进入路由器的路上或离开路由器的路上进行，也可以在进入和离开路由器的路上都进行，这与数据来自何处无关。在进入路由器的路上对进入的信息包进行筛选的最重要的目的是防止地址欺骗（为了进行破坏，而在信息包上伪造一个虚构的地址），因为关键性的信息（例如：该信息包是由哪条线路进入的）会在发出信息包筛选上丢失。

如图 1-2 所示为在路由器中可以设置信息包筛选的位置。

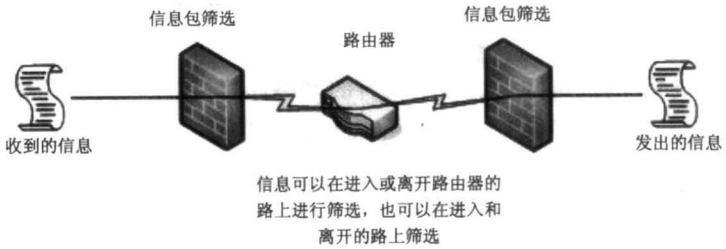

图 1-2 信息包筛选在路由器上的位置

信息包筛选既可以设置于连接两个网络（可靠网络和不可靠网络）的硬件路由器内，也可以设置于通用计算机系统或主计算机系统上，通常是嵌入操作系统。采用主计算机的危险是，主机可能被断开且危及系统的安全。这种危险是主计算机系统信息包筛选特有的，因为主计算机通常存储有可能被窃取的重要信息，还具有进入该系统的方便条件（注册、Telnet 等），而且，一旦有一个入侵者闯入系统，那么整个网络就可能会受到损害。然而，一个主计算机系统信息包筛选，通常比作为路由器一部分的信息包筛选更为有力，因为它没有路由器的局限性。

目前的路由器不能保存状态，不能执行记录功能，而且，在路由器内的编程规则通常非常复杂。另外，在路由器中进行信息包筛选会大大降低路由器的速度。

然而，由于路由器是连接网络的标准手段，而且往往配有基本的信息包筛选工具，所以，路由器是设置信息包筛的最常用的位置。

无论是设置在路由器上，还是设置在主计算机上，当安全管理人员制定安全策略时（确定在什么时候准许或者拒绝通信，哪些主计算机和服务程序是准许使用的，哪些主计算机和服务程序是不准使用的），复杂程度会成为关键性的问题。描述安全策略的规则，必须以正确的语法，使用正确的逻辑表达式和过滤准则，并且按照正确的次序书写。定义规则时的任何差错，都可能导致出现安全上的漏洞。组成一个筛选的规则的数量越多越复杂，则筛选有可能以不可预料的方式工作或者出现安全漏洞。

许多信息包筛选的一个重大缺点是，不能保留有关业已通过的信息包的详细信息（叫做上下文或状态信息）。如果对有关信息包的信息能够加以记录和保存，例如：信息包来自何处，发往哪里，做了什么事等等，就可以进行更加有效的、安全的筛选。这一点对于处理无连接协议特别有效。例如，当一个筛选看到 UDP 信息包（无连接协议）时，它无法区别原始请求（来自内部）和响应。允许无连接协议通过筛的惟一安全方式是保留状态信息，记录下请求发生的实际情况，并且检查进入的 UDP 信息包是不是所预期的信息包。如果不是列在清单上的预期信息包，就予以废弃。利用有效的状态信息，可以建立虚拟的连接。

3）应用中继器

信息包筛选利用一种普通的独立于协议和服务程序之外的机制进行全部通信的筛选作业，而应用中继器可以使未用的协议或服务专用软件提供每一项服务。通常，每一项服务程序和应用程序，例如 FTP、Mail 或者 Telnet，需要安装在最终主机和堡垒主机（网关主机）上，这种主机起着可靠网络和不可靠网络之间的中继器作用。如图 1-3 所示为一种应用中继器的配置实例。当最终主机要求服务时，服务程序连接到堡垒主机上，由堡垒主