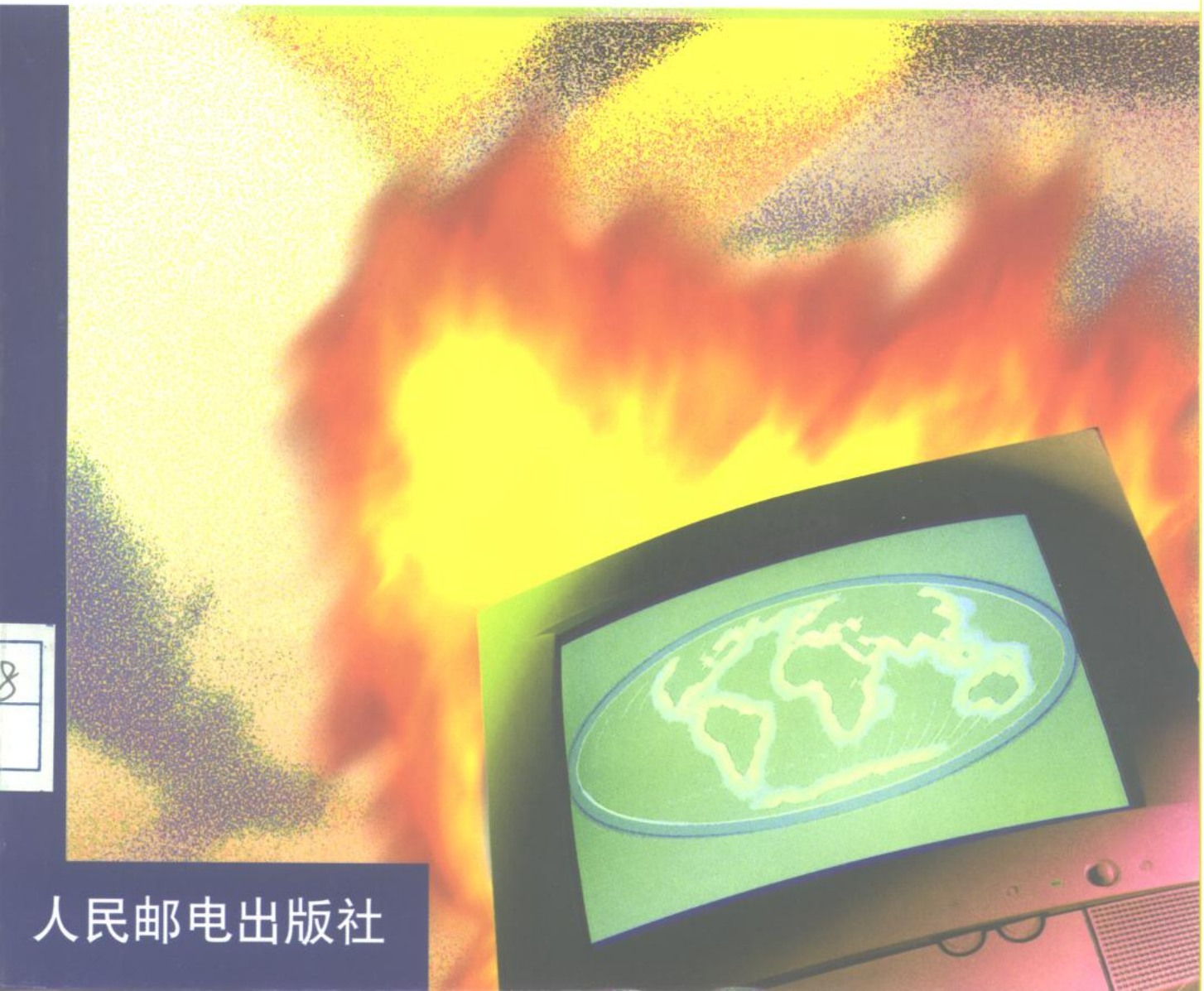
网络安全与防火墙技术

楚　狂　等编著



人民邮电出版社

网络安全与防火墙技术

楚 狂 等 编著

人民邮电出版社

内容提要

本书将网络安全理论融于实际的网络安全工程中，从网络安全工程的角度讲述了网络安全技术。主要内容包括：网络安全基础，网络安全威胁与防范，信息安全技术，防火墙技术和相关产品，企业网如何构筑防火墙，以及基于Windows NT网络的安全管理。

本书适用于网络工程师、网络管理人员，以及对网络安全技术感兴趣的广大网络爱好者，同时也可以作为一本网络安全技术的教学参考书。

网络安全与防火墙技术

◆ 编　　著　楚　狂　等
责任编辑　梁　凝
◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街14号
北京汉魂图文设计有限公司制作
北京朝阳隆昌印刷厂印刷
新华书店总店北京发行所经销
◆ 开本：787×1092　1/16
印张：19.5
字数：485　　2000年4月第1版
印数：1－5 000册　　2000年4月北京第1次印刷
ISBN 7-115-08412-2/TP·1542

定价：29.00元

前　言

随着 Internet 在世界范围内的逐渐普及，Internet 网络资源的安全问题变得越来越重要。1988 年 11 月发生的“蠕虫”事件，使人们第一次意识到计算机网络的安全问题同网络的其他技术一样应该作为今后计算机网络发展必须研究的课题。1996 年美国国防部宣布其计算机网络系统曾在该年内遭受到非法用户的 25 万次攻击，而且这些攻击中有 2/3 获得成功，尽管大多数攻击未造成损失，但毕竟是对计算机网络系统的潜在威胁。

为此，本书作者结合自己的研究成果，特意为广大的网络管理员和具有一定的网络管理基础并对网络安全感兴趣的读者提供一份及时的“网络安全快餐”，使读者在本书中获得如何制定网络安全策略和如何对网络进行安全管理的理论基础和有效的方法。

为便于读者更好地理解后续内容，本书首先介绍了网络管理的基本知识，然后结合实例分析网络本身及网络管理中的安全问题，提出制定安全策略的安全方案。最后结合具体的防火墙技术介绍如何制定具体的安全策略和如何进行实际的网络安全管理。

本书分为 10 章：

第一章为 Internet 基础，介绍 OSI 参考模型、TCP/IP 协议，以及常用的因特网服务及其安全性，并对 Unix、NT 网络的基本网络管理技术作了概述性的介绍，使得读者能掌握计算机网络的基本技术。

第二章为网络安全基础，概述了网络安全的基本知识及如何对网络进行危险性分析、危险识别和防止危险的对策。

第三章为网络安全威胁与防范，本章以 Unix 网络为基础介绍如何根据系统安全方法来制定合适的安全策略。

第四章为信息安全技术概论，介绍基本的信息安全技术和网络加密技术，及安全电子邮件 PGP 的使用。

第五章为防火墙基础，主要介绍防火墙的概念、特点及技术发展现状等。

第六章为防火墙体系结构，介绍包过滤器、双宿主主机、屏蔽子网等防火墙体系结构。

第七章为防火墙关键技术及发展，介绍防火墙的各种关键技术及未来发展趋势。

第八章为防火墙产品介绍及比较，介绍当前市场上流行的各种主要防火墙产品。

第九章为企业如何构筑防火墙，针对企业内部网的构筑介绍如何利用防火墙来保护企业内部网各项网络服务的安全。

第十章为 Windows NT 与网络安全，介绍 Windows NT 网络的安全基础及基于 Windows NT 网络的各项网络服务的安全。

本书由楚狂等人编写。全书由科苑 IT 技术研究小组策划。由于我们水平有限，时间短促，书中难免有所疏漏，敬请广大读者批评指正。来信地址：wuyongyi@163.net。

科苑 IT 技术研究小组

1999．12

目　录

第一章 Internet 基础

1.1 Internet 发展历史

Internet 的全称是 Internet Network，中文名称为因特网，它不是一个公司的名字，也不属于某个机构专有。从技术的角度来看，Internet 是一种计算机网络的集合。它以 TCP/IP 网络协议进行数据通信，将全世界众多的计算机网络和成千上万台计算机连接在一起，使原本分散在单台计算机上或限制在局部网络上的资源和信息，可以方便地互相共享。

从实际的角度来看，Internet 提供了一种机会，使用户利用普通的微机，就能与世界范围的计算机用户打交道，成为 Internet 大家庭中的一个成员。在这个大家庭里，人们可以进行科学方面的信息交流或实时的消息传递，也可以讨论普通问题、查找所需要的资料。在这里，时间和空间的差别不再重要，大家使用的是同一个 Internet，使人与人之间感觉不到不同计算机之间的差别，甚至注意不到国家和宗教之间的区别。

Internet 的由来是在 60 年代末，当时美国国防部设想，在突然受到核武器攻击时，如果仅有一个集中的军事指挥中枢，一旦这个中枢被核武器摧毁，全国的军事指挥将处于瘫痪状态，其后果将不堪设想。因此，有必要设计这样一个分散的军事指挥系统：它由一个个分散的指挥点组成，当部分指挥点被摧毁后，其他点仍能正常工作，而这些分散的点又能通过某种形式的通信取得联系，而成为新的指挥系统。为对这一构思进行验证，由美国国防部资助，建造了一个名为 ARPANET 的网络，把美国的几个军事及研究机构用计算机连接起来，这种将不同计算机连接在一起的网络，成为了 Internet 的前身。

由于 ARPANET 是将不同的计算机网络连接在一起，这里的关键技术是用一种新的方法将广域网 WAN 和局域网 LAN 互相连接起来，结果是形成一个新的网际网的试验模型——Internetwork，我们通常称为 Internet。

70 年代末，Unix 开始在各个大学使用，当时的美国国家科学基金会(NSF)为鼓励大学与研究机构共享他们非常昂贵的 4 台计算机主机，希望通过计算机网络把全国的各个大学、研究所的计算机与这 4 台巨型计算机连接起来。开始的时候，他们想利用现成的 ARPANET，不过他们发现与美国军方打交道也不容易。于是，他们利用 ARPANET 的技术，自己出资建立了基于 TCP/IP 的 NSFNET 网络，NSF 从资金和技术上也资助了这个网络。由于 TCP/IP 可以将不同类型的计算机很好地连接在一起，众多的研究单位和科技公司也加入了采用 TCP/IP 协议的队伍。

全球两个最著名的广域网就是 ARPANET 和 NSFNET，现在的因特网就是在这两个广域网的基础上发展起来的，ARPANET 曾经是因特网的主干，现在 NSFNET 已经取代 ARPANET 成为了因特网的主干网。

ARPANET 建立于 1969 年，是最早出现的计算机网络之一，现代计算机网络的很多概

念都来自于 ARPANET。著名的 TCP/IP 协议也是在 ARPANET 上发展起来的。1980 年前后，ARPANET 所有机器使用的协议从以前的 ARPANET 协议转向了 TCP/IP 协议，这大大促进了 TCP/IP 协议的发展，TCP/IP 协议本身就是一个在实践上发展起来的协议。在那时，ARPANET 成为了因特网的主干网。ARPANET 作为网间网研究的平台，对网间的发展起了重大的作用，但其单一、集中式的主干思想使得因特网很难包容其它主干网，所以后来被 NSFNET 所取代，失去了因特网主干网的地位。

NSFNET 在 1986 年建成，并在 1990 年以前短短的五年间，就经历了三个发展阶段，并最终取代了 ARPANET 成为了因特网的主干。和 ARPANET 不同，它具有良好的扩展性，分为三个层次：第一层是横跨全美的主干；第二层是一组某区域内的“中级”或“地区”网，一个典型的中级网包含分布在同一地理区域内的 10 到 30 所大学和公司，中级网在财务管理和技术选择上均具有极大的自主权。中级网通过 NSFNET 主干进入因特网。第三层是一组“校园”网。校园网是 NSFNET 网络的第三层，通过中级网进入 NSFNET，它由大学或公司独立建立，技术无统一标准，可谓百花齐放，有局域网型的，有主干型的，有的速度快，有的速度慢。在美国，主要的大学和公司都有自己的校园网。这三层网络构成了树形层次结构，主干处于根的位置，这种结构为它良好的扩展性奠定了基础。

NSF 在全美设置了 6 个超级计算中心，为了使各地科学家方便地访问这些中心的资源，NSF 将此 6 个计算机中心互联起来，NSFNET 于 1986 年诞生，但当时的主干网还是 ARPANET，第一版 NSFNET 主干和 ARPANET 在卡尼基梅隆大学被连接了起来，形成了统一的网络。

第一版 NSFNET 主干投入运行后，收到了意想不到的效果，由于其容量小而用户需求太大，运行的头几个月就开始超负荷，于是 NSF 开始实施其第二版 NSFNET 主干的艰苦工作。第二版主干完全脱离了第一版的模式和结构，几乎是从头开始，其规模比第一版大得多，拓扑结构也复杂得多，其分组交换的速度也高于第一版的 NSFNET 主干。

第三版 NSFNET 主干即当前的 NSFNET 主干，是在第二版主干基础上改进而来的，增删了线路，并将线路速度提高到 DS-1，即 1.555Mbit/s。

Internet 是由众多子网所组成的，它的使用者不仅仅只限于计算机专业人员，还包括多种学术团体、企业研究机构，甚至个人。

新加入 Internet 的使用者发现：Internet 除了可共享 NSF 的巨型计算机资源外，还能进行相互间的通信，这对他们来说更具有吸引力。于是，他们将 Internet 当作了一种交流与通信的工具，而不仅仅是共享 NSF 巨型计算机的资源。

Internet 历史上的第二次飞跃应归功于 Internet 的商业化进程。

1992 年，由于 Internet 发展的太快，使美国政府不能担负起 NSFNET 的费用，NSF 要求私营公司分担一部分任务，于是由 IBM、MERIT 和 MCI 等 3 家公司新组建了一个非盈利的 ANS(Advanced Networks and Services)公司来运作 Internet。新公司扩充了 Internet 主干网的容量，超过了 NSFNET 通信容量的 30 倍。

与此同时，CERFnet、PSInet 及 Alternet 三个商用网络在一定程度上绕开由美国国家科学基金会出资建立的 Internet 主干网 NSFNET 而向客户提供 Internet 联网服务。他们在 1991 年组成了“商用 Internet 协会”，宣布用户可以把他们的 Internet 子网用于任何商业用途。

商业机构一进入 Internet 这个领域，很快就发现了它在通信、资料检索、客户服务等方面的巨大潜力。从此世界各地无数的企业和个人纷纷涌入 Internet，从而带来了 Internet 发展

史上一个新的飞跃。

由于对 Internet 商业化的迫切需要，1995 年 4 月 30 日，NSFNET 正式宣布停止管理运行 Internet 主干网，代替它的是由美国政府指定的 3 家私营公司：Pacific Bell、Ameritech Advanced Data Services and Bellcore 以及 Sprint。至此，Internet 完成了商业化的进程。

1993 年，美国提出了信息高速公路的设想，在全世界引起了很大的反响，各国都在对此进行研究。信息高速公路的目标是能够将有线电视、广播、电话、新闻出版、计算机和商业有机地融为一体，使用户方便地使用商业双向信息通道，并将其最终延伸到每个家庭。目前 Internet 还不能满足这种需要，但有一点可以肯定，今天的 Internet 正是实现信息高速公路的一个过渡，因此有人称 Internet 为准信息高速公路。

下面的表 1.1 显示了 Internet 上常用的服务。

表 1.1　　Internet 上的常用的服务

名　称	功　能	特　点	与其它功能的关系
FTP 文件传输协议	主机之间的文件拷贝，在不同的计算机之间互相拷贝文件	可以利用主机的 FTP 命令，也可以使用相应的软件实现	可用 Telnet 登录到主机后，运行 FTP 相关命令拷贝。用 Windows 界面工具，可以使用复杂命令，Gopher 和 WWW 里可以自动进行 FTP
Archie 文件查找	查找文件在哪个 FTP 服务器上	命令行方式，可根据文件名或某些通配符得到	可利用 telnet 登录到 Archie 主机上或用 mail 查找
Gopher 文本浏览	对 Internet 上文本文件进行浏览	采用菜单式界面，只能浏览文本	可通过 Gopher 实现 FTP、mail 等功能
Wais 广域信息查找	Wais 服务器上实现全文检索	根据文档内的某个单词来进行全文检索	一般是在 Gopher 里实现
Veronica	查找所需的 Gopher 服务器	根据所给的关键词去查找	是在 Gopher 内部实现的，实际上用户并不直接使用它
E-mail 电子邮件	收发电子邮件	最基本和最实用的，早期的 E-mail 只能实现文本传输，现在的 E-mail 已经能传输英文、中文、声音、图像等	在 WWW、Gopher、Usenet 里可以实现 E-mail 功能
Mailing List 电子邮件列表	众多的 Internet 用户参加的讨论组	参加某个或一些讨论组，用户会收到相应讨论的 E-mail，也可以退出讨论组	利用 E-mail 实现，实际上是通过 Mail 收发信件
Usenet 新闻组	发表、讨论信息的园地	阅读各个讨论组的文章，也可以发表自己的见解	利用 WWW，或专用的 Newsgroup 信件浏览器阅读或收发信件
IRC，Iphone 中继聊天，网上电话	利用键盘输入或麦克风进行实时谈话	参加一个讨论区，进行键盘讨论	可以和 Internet 上的一个或多个其他用户开会或个别谈话
WWW 环球网	文本或图形浏览	采用超文本连接，可以实现图像、声音，以及其他 Internet 功能。使用简单，是 Internet 发展的方向	提供多种方法，可以在全世界范围查找、检索各种信息
Telnet 远程登录	可以远程操作另一台功能强大的计算机，利用其资源	采用命令行方式，用户要记住相应的操作命令	利用登录到某个机器上后运行其程序，可以使用其他机器的 WWW、Gopher 等功能

在我国 Internet 的发展虽然较晚，但发展还是比较迅速，1987 年北京计算机应用研究所

率先开通到德国的 X.25 线路，此后中科院、清华大学、北京大学纷纷建立起自己的校园网并实现与 Internet 的连接，以此为基础我国的 Internet 初具雏形。随着我国科学技术的飞速发展，这几个规模有限的网络无法满足我国科技教育的需要，在国家的大量投入下，到 1995 年我国初步建成四大骨干网络，为 Internet 在我国的进一步发展奠定了基础。这四大骨干网为：

(1) 国家计算机与网络设施 NCFC：NCFC 是由中科院主持建立的，目前已经连接了全国 24 个城市的上百个研究所。

(2) 中国教育科研网 CERNET：CERNET 是在国家教委主持下建立的，主要由清华大学、北京大学、上海交通大学、西安交通大学、华中理工大学、电子科技大学、华南理工大学、东南大学等 10 所大学承建的，目前已经连接了全国三百多所大学，拥有 2Mbit/s 的国际专线，CERNET 计划连接全国绝大部分大学和有条件的中学、小学。

(3) 中国公用计算机互联网 CHINANET：CHINANET 是由原邮电部主持建设的，主要面向个人和商业用户，CHINANET 目前已经覆盖了全国 31 个省市，拥有 86Mbit/s 的国际专线。

(4) 中国金桥信息网 CHINAGBN：中国金桥信息网是我国第二个可以用于商业的计算机互联网，由原电子工业部组建，覆盖了全国大部份省市和自治区。

以上四大骨干网的建立为 Internet 在我国的使用、发展奠定了良好的基础，相信 Internet 在我国会有一个美好的明天。

1.2 Internet 安全现状

最初面向研究的 Internet 和它的通信协议族是为在用户和主机之间互相信任，旨在进行自由开放的信息交换的环境而设计的。而如今 Internet 上的安全问题成了关注的焦点。尽管众说纷纭，但有一点是大家差不多都同意的，那就是 Internet 需要更多更好的安全机制。早在 1994 年，在 IAB(Internet 体系结构理事会)的一次研讨会上，扩充与安全就被当作关系到 Internet 全局的两个最重要的问题。

本质上，Internet 的安全性只能通过提供下面两方面的安全服务来达到：

- 访问控制服务：用来保护计算机和联网资源不被非授权者使用。
- 通信安全服务：用来提供认证、数据保密性与完整性和各通信端的不可否认性服务。例如，基于 Internet 或 WWW 的电子商务就必须依赖于通信安全服务的广泛采用。

计算机的安全是一个越来越引起世界各国关注的重要问题，也是一个十分复杂的课题。随着计算机在人类生活各个领域中的广泛应用，计算机病毒也在不断产生和传播，计算机网络被不断非法入侵，重要资料被窃密，甚至由此造成网络系统的瘫痪等。因此计算机系统的安全问题已给各个国家以及众多公司造成巨大的经济损失，甚至危及到国家和地区的安全。必须给予充分的重视并设法解决。

计算机安全包括物理安全和逻辑安全，对于前者只要加强计算机机房的管理，如门卫、出入者身份检查、下班锁门以及各种硬件安全手段等预防措施，而对于后者需要用口令密码、文件许可和查帐等方法来实现。

计算机安全的目标是：在安全和通信方便之间建立平衡。毫无疑问，要求计算机系统越安全，则对通信的限制和使用的难度就越大，而现代信息技术的发展又使通信成为不可缺少的组成部分，它包括跨组织、跨学科、跨地区的以及全球的通信。在这里计算机安全的重要性显然是毫无疑问的，但是计算机的安全程度应与所涉及的信息的价值相符合，即应当有一个从低、中级到高级的多层次的安全系统，分别对不同重要性的信息资料给予必要的不同等级的保护。例如，在贝尔实验室，高度机密的个人信息(如付税数据)是完全与其它各种数据相隔离的，对所有高度机密数据的存取都被严格地控制着。

计算机安全的另一个重要问题是：当有人窃走某人所有信息时，他并不需要将信息从计算机文件中移走。这一特点使得难于确认信息事实上已被窃走了，这也使在道义上、道德和法律上的问题复杂化了。

要强调的是，必须要求各级机构的高层管理人员要经常关注和强化计算机安全技术和保密措施，否则，将会造成无可挽救的危险和损失。

对于计算机安全，最重要的起点显然是从涉及计算机的人员开始，即用户、系统管理员和超级管理员。影响安全的一个主要问题是人们的粗心大意，例如：登录和使用计算机后，不退出系统就离开终端不管了；与他人共用计算机存取口令；将重要的机密资料存入不适当的计算机文件中等。

超级管理员可按下列各项来评定自己单位的计算机系统的安全程度如何。

- 别人知道用户计算机的存取权限吗？不要与他人(即使是你的助理工作人员)共用口令，如果用户的同组人员需要存取其他人员的文件，他们也应当有自己的口令。
- 用户的计算机能拒绝未授权的远程计算机的请求吗？如果不拒绝，则应重新修改计算机的许可设置以改变这一情况。
- 用户有系统管理员吗？管理和修改安全设计与设置是他(她)的工作职责吗？最安全的系统是那些具有责任心和能力都很强的系统管理员管理的计算机系统。
- 用户将一些私人信息如公司计划或个人审查资料存入了计算机文件吗？假若出现糟糕的情况(如一个偶然浏览文件的人能读到用户所写入计算机的信息)，那么必须尽快将重要资料保存到其他地方。
- 同组用户严肃对待计算机的安全问题吗？必须确保同组用户懂得计算机安全的必要性以及他们应当怎样做才能保证计算机的安全。

这里值得强调的另一点是责任者的重要性，责任者是指用户管理员和超级管理员。例如：计算机的任何使用都需要有超级用户给予的许可，以便能控制谁使用机器和机器被用于其他目的。

在计算机安全检查中，最后要强调的一点是，通过使用特殊的软件包来限制对各个用户文件的普通存取，以提高安全程度。用户可以使用软件来保护存于计算机文件中的信息，该软件限制了其他人存取非自己所有的文件，直到该文件的所有者明确准许其他人可以存取该文件时为止。限制存取的另一种方式是通过硬件来完成，在接收到存取要求后，先询问并确认口令，然后访问列于目录中的授权用户标志号。

有一些安全软件包也可跟踪可疑的未授权的存取企图，例如，多次试登录或请求别人的文件。显然，用户可以限制试登录的次数，或对试探操作加上时间限制，在此之后，系统就自动地退出。

现有的各种技术提供了高水平的计算机安全措施，特别是计算机上的军事安全保密。

想要破坏含有保密信息的计算机的安全控制，其代价是非常昂贵的。当然维护这样高级的安全的代价通常是将各计算机隔离以及使进入计算机的手续操作麻烦，但随着安全技术的进一步提高，将会大大降低这种代价——即使整个安全控制对合法用户更透明一些。随着新一代计算机的研制也发展了“用户友好”的界面，在发展和加强计算机的安全系统时，也充分注意到了用户的需要。

防止和检测计算机通信线被侵入的技术，就像识别拨号系统一样简单。这种能力允许根据授权电话号码表来进行安全检查，也可提供追踪未授权存取企图的记录。这种识别已存在于今天的一些计算机化的业务通信系统中。

此外，还可使用“信用卡终端”它可提供便宜而又防窜改的方式，对于识别用户比通常用的口令具有更高程度的可靠性。采用这种方式也有助于提高识别用户的能力，这种简单的硬件可产生软件不能伪造的信号，这将能提高网络地址的安全程度。

然而，计算机安全的最基本方法也许还是人的因素第一，正如前面多次指出的，需要尽更大的努力去提高人们对于计算机安全的认识。各级教育部门和单位应在这方面做大量的教育工作，人们也需要经常考核计算机以及偷窃管理人员，他们是首先要提高安全意识的人，因为他们更易于进行电子偷阅、非法进入系统。同时有必要澄清涉及计算机安全的复杂问题，避免有人声称不知道如何防备而对危害计算机安全的错误行为与作法推卸责任。

计算机安全与保密问题是现代信息社会中一个十分重要并具有普遍意义的问题，必须认真对待，并且掌握有关安全的技术和方法。

1.3 OSI 模型

ISO(国际标准化组织)将主机间的通信过程划分为七个层次（如图 1.1 所示），通过不同层次间的分工与合作，来完成任意两台机器间的通信。在 OSI 参考模型中，每一层只与相邻的上下两层交换信息。

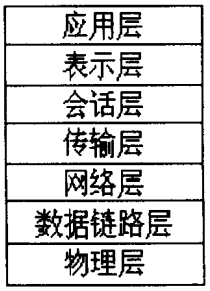


图 1.1 OSI 参考模型

物理层关注的是位流在信道上的传输。这一层用来确保发送出一个“1”，在接收端收到的是一个“1”，而不是“0”。这一层详细规定了数据传输过程中的各种电气、机械特性，以及使用的物理传输媒介。

数据链路层将网络层送来的连续的数据流装配成一个个数据帧，然后按序发送这些数据帧，以及处理由接收端发送来的确认帧。物理层仅仅是传送连续的位流，而在数据链路层

在信道上由于噪音而引起的传送错误，发送方要重新发送那些数据帧。当接受方速度较慢时，发送方数据链路层还要进行流量控制，降低数据发送的速率。

网络层最重要的作用是将数据包从源主机发送到目的主机。数据链路层仅仅是在相邻的两台主机间传送数据，而网络层所说的两台主机不一定是相邻的，很可能不在一个局域网内，甚至要跨越几个网络。数据包在网上传送的过程中，网络层根据数据包中携带的目的主机地址的不同，为它们选择合适的路径，直到数据包到达目的主机。

当数据包在穿越不兼容的网络时，可能会产生许多问题。比如，地址格式不同，包要求的大小不同，甚至使用的协议也不同。这些问题都需要网络层来解决。当包要进入不兼容的网络时，对那些不兼容的信息，将进行必要的转换。

传输层的基本功能为从会话层接收数据，如果需要，将这些数据分成更小的数据单元，并将这些数据单元传送给网络层，确保数据能正确地到达接收信息的主机。

会话层，英文是“session”。用来实现不同主机上用户间的一次会话。或者是一个用户远程登录进另一个分时系统，或者在两台主机间传送一个文件。会话层允许信息以双向或是单向的方式进行传送。

表示层关注着要传送信息的拼写和信息的内涵。一个典型的例子是将要传送的数据用一种标准的格式编码。不同的主机对字串实行不同的编码方式，如有 ASCII 和 Unicode 编码之分。为了方便不同编码的主机间的信息交流，必须将要传送的信息转换成双方主机都能理解的信息表示形式。

应用层包括了许多常用的协议。应用层解决了两个典型的问题，一是解决不兼容的终端类型问题，另一个是文件传输问题，在不同文件系统上传输文件，必须解决文件名的转换，文本行的表示等问题。

值得注意的是，实际应用中往往并不采用 OSI 七层协议模型，Internet 上使用的是 TCP/IP 协议，它负责网际之间的互联，对应着网络层（包含）以上的层次，而 OSI 七层模型下两层的实现在不同的局域网上是不同的。OSI 七层模型仅仅是两台主机间通信行为的一个抽象。与其说它是一种模型，不如说是一种分层的思想。虽然现实中的模型不是 OSI 模型，但是它们都可以和 OSI 模型中的某几层相对应。因此，理解七层协议模型有着重要的意义。

1.4 TCP/IP 协议基础

TCP/IP 是 Internet 能够实现网络互联的基础，理解它的原理对于网络安全管理具有重要作用。有很多直接利用 TCP/IP 实现攻击的例子，目前正流行的有 OOB，LAND 等，难度较大的攻击技术有 IP 欺骗等，它们对网络安全造成巨大的威胁。

这些攻击之所以能够成功，既有协议的不完备，也有协议实现软件的漏洞，给黑客和入侵者以可乘之机。

1.4.1 TCP/IP 与 OSI 模型

TCP/IP 协议簇包含了许多的协议，在本书中我们并不详细讨论这些协议。其实了解所有的协议是网络专家的事情，对于一般网络管理员只要知道存在哪些协议以及如何使用它们