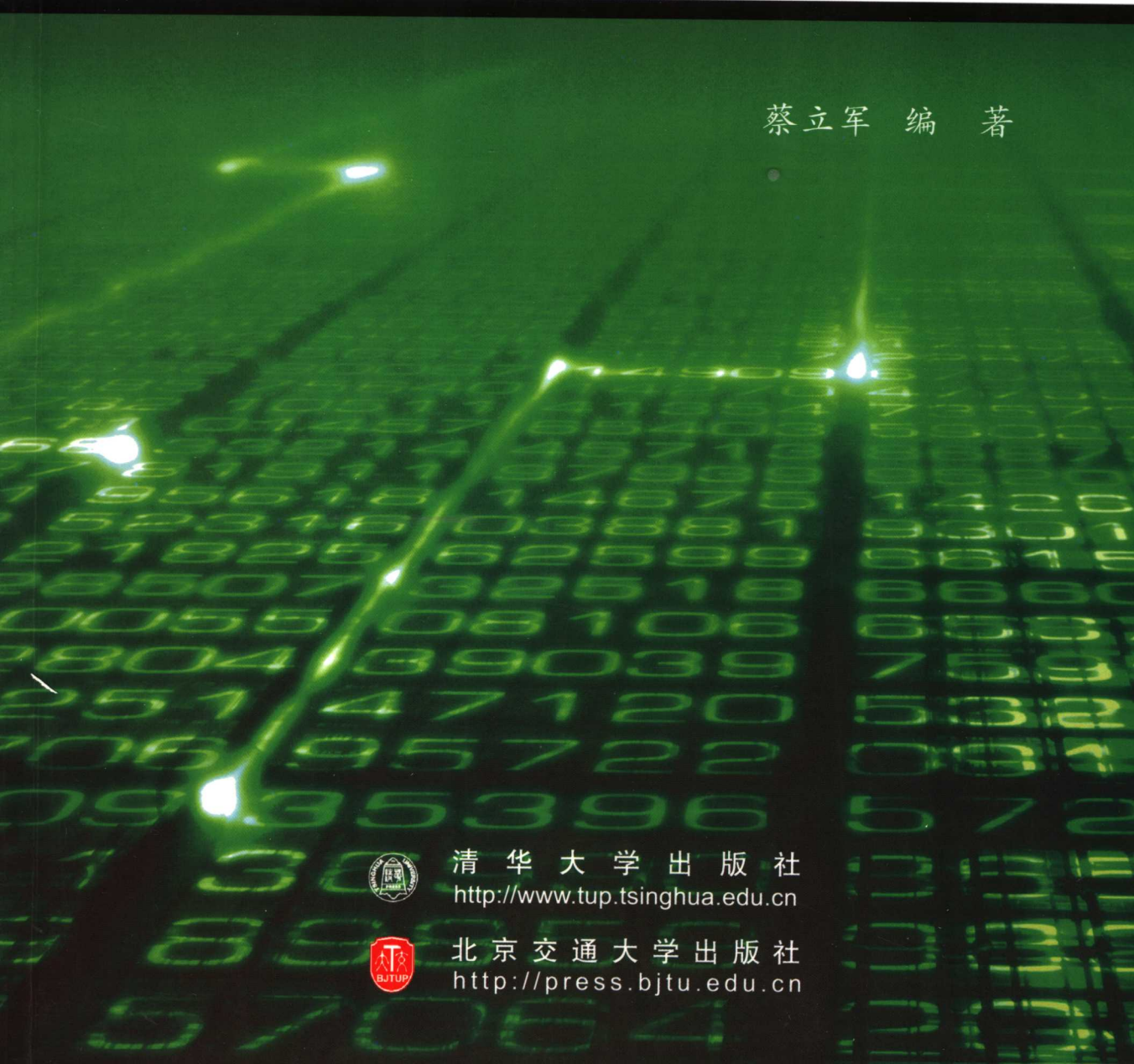
21世纪 高等学校电子信息类专业规划教材

网络安全技术

蔡立军 编 著



清华大学出版社
http://www.tup.tsinghua.edu.cn

北京交通大学出版社
http://press.bjtu.edu.cn

21 世纪高等学校电子信息类专业规划教材

网络安全技术

蔡立军　编著

清华大学出版社
北京交通大学出版社
· 北京 ·

内 容 简 介

本书全面系统地介绍了计算机网络安全技术的主要方面，基本概念、基础理论和实施技术并存。全书分为10章，涉及安全基础（安全模型、安全体系结构、安全服务和安全机制、安全的三个层次、评估标准）、物理安全（场地环境的安全要求、电磁干扰及电磁防护、物理隔离）、网络安全（攻击检测与系统恢复技术、访问控制技术、防火墙技术、病毒防治技术）、信息安全（数据库安全技术、密码体制与加密技术、认证技术）、安全管理（网络管理结构模型、SNMP/CMIP协议、RMON技术和基于Web的管理技术、安全管理的基本原则与工作规范）等内容。

本书具有教材和技术资料的双重特征，既可以作为高等院校计算机、网络安全、信息安全和通信等专业的教材使用，也可供从事网络安全、信息安全相关专业的教学、科研、管理和工程技术人员参考。

图书在版编目（CIP）数据

网络安全技术 / 蔡立军编著. —北京：清华大学出版社；北京交通大学出版社，2006.9
（21世纪高等学校电子信息类专业规划教材）
ISBN 7－81082－875－4

Ⅰ. 网… Ⅱ. 蔡… Ⅲ. 计算机网络－安全技术－高等学校－教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2006）第109009号

责任编辑：杨祎　　特邀编辑：曾小莉
出 版 者：清华大学出版社　　邮编：100084　　电话：010－62776969
　　北京交通大学出版社　　邮编：100044　　电话：010－51686414
印 刷 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　　印张：17.25　　字数：412千字
版　　次：2006年9月第1版　　2006年9月第1次印刷
书　　号：ISBN 7－81082－875－4/TP·306
印　　数：1～4 000册　　定价：24.00元

前　言

随着计算机及网络技术的发展和普及，人类对计算机、对网络的依赖程度越来越大，计算机网络安全的重要性也日益突出。国内外政府相关主管部门、研究机构、学术界、产业界的研究力度不断加大，陆续推出了相应的法规、标准、指南和产品，成立了专门的研究院（所）、测评认证机构。就连广大用户也纷纷加大投入，实施不同程度的安全建设。为了提高我国各级计算机网络主管部门的安全意识，普及计算机网络安全知识，提高国内的安全技术水平，有效地保护我国计算机网络的安全，将计算机网络安全技术纳入高等院校计算机专业及相近专业的主干课程是十分必要的，也是很迫切的。

本书是作者在多年从事计算机网络安全方面的研究、开发基础上，综合了一些学校、任课教师、学生及相关工程技术人员的反馈意见后完成的。本书内容全面、系统，涉及了计算机网络安全技术的主要方面，基本概念、基础理论和实施技术并存。全书共10章分为5部分。

第一部分是安全基础（第1章），包括安全模型、网络安全体系结构框架、安全服务和安全机制、计算机网络安全的三个层次、评估标准等内容。

第二部分是物理安全（第2章），包括计算机机房场地环境的安全要求、电磁干扰及电磁防护、物理隔离技术等内容。

第三部分是网络安全（由第3、4、5、6章共4章组成），重点介绍了攻击检测与系统恢复技术（第3章）、访问控制技术（第4章）、防火墙技术（第5章）和病毒防治技术（第6章）。

第四部分是信息安全（由第7、8、9章共3章组成），详细讲解了数据库安全技术（第7章）、密码体制与加密技术（第8章）和认证技术（第9章）等内容。

第五部分是安全管理（第10章），内容包括网络管理结构模型、SNMP/CMIP协议、RMON技术和基于Web的管理技术、安全管理的基本原则与工作规范。

本书具有教材和技术资料的双重特征，既可以作为高等院校计算机、网络安全、信息安全和通信等专业的教材使用，也可供从事网络安全、信息安全相关专业的教学、科研、管理和工程技术人员参考。

本书由蔡立军编著。参加本书编写大纲讨论及技术工作的有李立明、凌民、池鹏、陈浩文、肖强、岳文焕、张涛、沈小乔、章灏、曾彰龙、汤腊梅和王民武。刘红飞、杨丹、刘涛、凌红武和陈知等做了本书的文字录入和图表制作工作。在此一一表示感谢。

由于编者水平有限，书中难免有错误和不足之处，敬请读者和同行专家批评指正。

编　者

2006年9月于岳麓山

目　录

第1章 概 述

本章重点：

（1）计算机网络安全系统的脆弱性；
（2）P^2DR 安全模型和 PDRR 网络安全模型；
（3）Internet 网络体系层次结构、网络安全体系结构框架；
（4）5 种安全服务和 8 种安全机制；
（5）计算机网络安全的三个层次；
（6）可信计算机系统评估标准。

跨入21世纪，人类社会步入了信息时代。计算机网络改变了人们工作、生活的方式，但同时其安全问题也日渐突出，已威胁到国家的政治、经济、军事、文化、意识形态等领域。因此，认清计算机网络的脆弱性和潜在威胁，采取强有力的安全技术措施，对于保障计算机网络的安全性变得十分重要。计算机网络安全技术涉及到物理环境、硬件、软件、数据、传输、体系结构等各个方面，包括计算机安全、通信安全、操作安全、访问控制、实体安全、电磁安全、系统平台与网络站点的安全，以及安全管理和法律制裁等诸多内容，并逐渐形成独立的学科体系。

从狭义的保护角度来看，计算机网络安全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，即指计算机、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到破坏、更改、泄露，确保系统能连续可靠正常地运行，使网络服务不中断。计算机网络安全从其本质上来讲就是系统上的信息安全。计算机网络安全是一门涉及计算机科学、网络技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科的综合性科学。

从广义来说，凡是涉及计算机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计算机网络安全的研究领域。所以，广义的计算机网络安全还包括信息设备的物理安全性，诸如场地环境保护、防火措施、防水措施、静电防护、电源保护、空调设备、计算机辐射和计算机病毒等。

1.1 计算机网络安全系统的脆弱性

计算机网络面临着黑客、病毒、特洛伊木马程序、系统后门和窥探等多个方面安全威胁。尽管近年来计算机网络安全技术取得了巨大的进展，但计算机网络系统的安全性比以往任何时候都更加脆弱。主要表现在它极易受到攻击和侵害，它的抗打击力和防护力很弱。其脆弱性主要表现在如下几个方面。

1. 操作系统的安全脆弱性

操作系统不安全，是计算机不安全的根本原因。

2. 网络系统的安全脆弱性

（1）网络安全的脆弱性

由于 Internet/Intranet 的出现，网络的安全问题更加严重。可以说，使用 TCP/IP 协议的网络所提供的 FTP、E-mail、RPC 和 NFS 都包含许多不安全的因素，存在着许多漏洞。

（2）计算机硬件系统的故障

由于生产工艺或制造商的原因，计算机硬件系统本身有故障，如电路短路、断线、接触不良引起系统的不稳定、电压波动的干扰等。

（3）软件本身的“后门”

软件本身的“后门”是软件公司的程序设计人员为了方便自己进入而在开发时预留设置的，一方面为软件调试、进一步开发或远程维护提供了方便，但同时也为非法入侵提供了通道。这些“后门”一般不为外人所知，但一旦“后门”洞开，入侵者就可以利用“后门”多次进入系统，或采取其他措施绕过安全控制路径进入系统，即使系统管理员已经弥补了系统漏洞，入侵者也可以取得对系统的访问权限，造成的后果将不堪设想。

常见的后门有修改配置文件、建立系统木马程序和修改系统内核等。入侵者利用“后门”可以从非特权用户变为能够使用 root 权限的特权用户。

（4）软件的漏洞

软件不可能是百分之百的无缺陷和无漏洞的，因此，这些漏洞和缺陷就成了黑客进行攻击的首选目标。典型的缺陷和漏洞如操作系统中的 BUGS 等。

3. 数据库管理系统的安全脆弱性

当前，大量的信息存储在各种各样的数据库中，然而，对这些数据库系统在安全方面的考虑却很少。而且，数据库管理系统安全必须与操作系统的安全相配套。例如，DBMS 的安全级别是 B2 级，那么操作系统的安全级别也应该是 B2 级，但实践中往往不是这样的。

4. 防火墙的局限性

防火墙仍然存在着一些不能防范的安全威胁，例如不能防范不经过防火墙的攻击，也就是说很难防范来自于网络内部的攻击以及病毒的威胁等。

5. 天灾人祸

天灾指不可控制的自然灾害，如地震、雷击等。天灾轻则造成业务工作混乱，重则造成系统中断或造成无法估量的损失。

人祸是指人为因素对计算机网络系统构成的威胁。人祸可分为有意的和无意的。

有意的是指人为的恶意攻击、违纪、违法和计算机犯罪。这是目前计算机网络系统所面临的最大威胁。

人为的无意失误和各种各样的误操作都可能造成严重的不良后果，典型的错误有文件的误删除，输入错误的数据等。又如操作员安全配置不当；用户口令选择不慎；用户将自己的账号随意转借他人或与别人共享等无意行为都可能会对计算机网络安全带来威胁。

6. 其他方面的原因

如环境和灾害的影响，计算机领域中任何重大的技术进步都对安全性构成新的威胁等。

总之，系统自身的脆弱和不足，是造成计算机网络安全问题的内部根源。但系统本身

的脆弱性、社会对系统应用的依赖性这一对矛盾又将促进计算机网络安全技术的不断发展和进步。

1.2 安全模型

计算机网络系统安全是一个系统工程，必须保证网络设备和各个组件的整体安全性。安全的概念是相对的，任何一个系统都具有潜在的危险，没有绝对的安全。在一个特定的时期内，在一定的安全策略下，系统可能是安全的。但是，随着攻击技术的进步、新漏洞的暴露，系统可能会变得不安全了。因此，安全具有动态性，需要适应变化的环境并能做出相应的调整以确保计算机网络系统的安全。

1.2.1 P^2DR 安全模型

美国国际互联网安全系统公司（ISS）提出的 P^2DR 安全模型包括策略（Policy）、防护（Protection）、检测（Detection）和响应（Response），如图 1-1 所示。

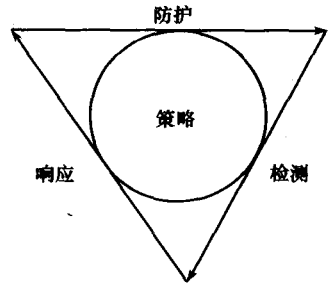


图 1-1 P^2DR 安全模型

P^2DR 安全模型可以描述为：

安全 = 风险分析 + 执行策略 + 系统实施 + 漏洞监测 + 实时响应

P^2DR 安全模型认为没有一种技术可完全消除网络中的安全漏洞，必须在整体安全策略的控制指导下，在综合运用防护工具的同时，利用检测工具了解和评估系统的安全状态，通过适当的反馈将系统调整到相对最安全和风险最低的状态，才能达到所需的安全要求。也就是说，系统的安全实际上是理想中的安全策略和实际的执行之间的一个平衡，强调在防护、监控检测、响应等环节的循环过程，通过这种循环达到保持安全水平的目的。所以，P^2DR 安全模型是整体的、动态的安全模型，应该依据不同等级的系统安全要求来完善系统的安全功能、安全机制。P^2DR 安全模型也称为可适应安全模型 ANSM（Adaptive Network Security Model）。

1. 策略

安全策略具有一般性和普遍性，一个恰当的安全策略总会把关注的核心集中到最高决策层认为必须值得注意的那些方面。概括地说，一种安全策略实质上表明：当设计所涉及的那个系统在进行操作时，必须明确在安全领域的范围内，什么操作是明确允许的，什么操作是一般默认允许的，什么操作是明确不允许的，什么操作是默认不允许的。安全策略

一般不作出具体的措施规定，也不确切说明通过何种方式才能够达到预期的结果，但是应该向系统安全实施者们指出在当前的前提下，什么因素和风险才是最重要的。就这个意义而言，建立安全策略是实现安全的最首要的工作，也是实现安全技术管理与规范的第一步。目前，如何能使安全策略与用户的具体应用紧密结合是计算机网络安全系统面临的最关键问题。所以，安全策略的制定实际上是一个按照安全需求、依照应用实例不断精确细化的求解过程。

安全策略是 P^2DR 安全模型的核心，所有的防护、检测、响应都是依据安全策略实施的，安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制订、评估、执行等。只有对计算机网络系统进行了充分的了解，才能制订出可行的安全策略。

2. 防护

防护就是采用一切手段保护计算机网络系统的保密性、完整性、可用性、可控性和不可否认性，预先阻止攻击可以发生的条件产生，让攻击者无法顺利地入侵。所以说，防护是网络安全策略中最重要的环节。

防护可以分为三大类：系统安全防护、网络安全防护和信息安全防护。

（1）系统安全防护是指操作系统的安全防护，即各个操作系统的安全配置、使用和打补丁等。不同操作系统有不同的防护措施和相应的安全工具。

（2）网络安全防护是指网络管理的安全，以及网络传输的安全。

（3）信息安全防护是指数据本身的保密性、完整性和可用性。数据加密就是信息安全防护的重要技术。

3. 检测

安全政策的第二个安全屏障就是检测。检测是动态响应和加强防护的依据，是强制落实安全策略的工具，通过不断地检测和监控网络及系统，来发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。

网络的安全风险是实时存在的，检测的对象主要针对系统自身的脆弱性及外部威胁。主要检查系统存在的脆弱性，即在计算机系统运行过程中，检查、测试信息是否发生泄漏、系统是否遭到入侵，并找出泄漏的原因和攻击的来源。如计算机网络入侵检测、信息传输检查、电子邮件监视、电磁泄漏辐射检测、屏蔽效果测试和磁介质消磁效果验证等。

检测和防护有根本性的区别。如果防护和黑客的关系是："防护在明，黑客在暗"，那么检测和黑客的关系是："黑客在明，检测在暗"。防护主要修补系统和网络的缺陷，增加系统的安全性能，从而消除攻击和入侵的条件。检测并不是根据网络和系统的缺陷，而是根据入侵事件的特征去检测。但是，黑客攻击系统的时候往往是利用网络和系统的缺陷进行的，所以入侵事件的特征一般与系统缺陷的特征有关。

在安全模型中，防护和检测之间有互补关系。如果防护部分做得很好，绝大多数攻击事件都被阻止，那么检测部分的任务就很少。反过来，如果防护部分做得不好，检测部分的任务就很多。

4. 响应

响应就是在检测到安全漏洞或一个攻击（入侵）事件之后，及时采取有效的处理措施，避免危害进一步扩大，目的是把系统调整到安全状态，或使系统能提供正常的服务。

通过建立响应机制和紧急响应方案，能够提高快速响应的能力。

在一个大规模的网络中，响应这个工作都是有一个特殊部门负责，那就是计算机紧急响应小组。我国第一个计算机紧急响应小组 CCERT 于 1999 年建立，主要服务于中国教育和科研网。

1.2.2 PDRR 网络安全模型

网络安全的整个环节可以用一个最常用的安全模型——PDRR 模型来描述，如图 1-2 所示。PDRR 就是防护（Protection）、检测（Detection）、响应（Response）和恢复（Recovery）4 个英文单词的头一个字符。

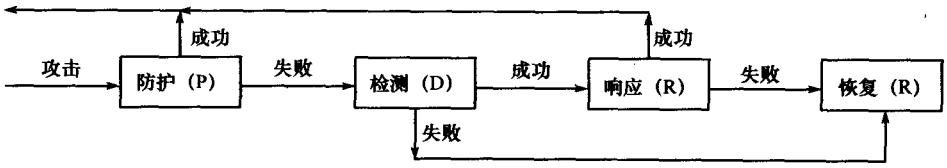


图 1-2 PDRR 网络安全模型

PDRR 安全模型中安全策略的前三个环节与 P^2DR 安全模型中后三个环节的内涵基本相同，不再赘述。最后一个环节，“恢复”是指在系统被入侵之后，把系统恢复到原来的状态，或者比原来更安全的状态。系统的恢复过程通常需要解决两个问题：一是对入侵所造成的影响进行评估和系统的重建，二是采取恰当的技术措施。系统的恢复主要有重建系统、通过软件和程序恢复系统等方法。详见本书 3.3 节。

安全策略的每一部分包括一组安全单元来实施一定的安全功能。安全策略的第一部分就是防护。根据系统已知的所有的安全问题做出防护的措施，如打补丁、访问控制、数据加密等。防护是安全策略的第一个战线。安全策略的第二个战线就是检测。攻击者如果穿过了防护系统，检测系统就会检测出来。这个安全战线的功能就是检测出入侵者的身份，包括攻击源、系统损失等。一旦检测出入侵，响应系统开始响应包括事件处理和其他业务。安全策略的最后一个战线就是系统恢复。在入侵事件发生后，把系统恢复到原来的状态。每次发生了入侵事件，防护系统都要更新，保证相同类型的入侵事件不能再发生。所以整个安全策略包括防护、检测、响应和恢复 4 个部分，组成了一个动态的网络安全周期。系统遭受攻击时，如果防护成功，系统是安全的；如果防护失败且检测失败，就意味着攻击成功了，那就只能恢复系统了；如果防护失败但检测成功且响应成功，那系统仍是安全的；如果防护失败、虽检测成功但响应失败，攻击仍然实施了，系统仍需恢复。

PDRR 安全模型阐述了下面一个结论：安全的目标实际上就是尽可能地增大保护时间，尽量减少检测时间和响应时间，在系统遭受到破坏后，应尽快恢复，以减少系统暴露时间。也就是说，及时的检测和响应就是安全。

1.3 网络安全体系结构

计算机网络安全体系结构是网络安全最高层的抽象描述，在大规模的网络工程建设和管

理，以及基于网络的安全系统的设计与开发过程中，需要从全局的体系结构角度考虑安全问题的整体解决方案，才能保证网络安全功能的完备性与一致性，降低安全的代价和管理的开销。这样一个安全体系结构对于网络安全的理解、设计、实现与管理都有重要的意义。

1.3.1　开放式系统互连参考模型（OSI/RM）

国际标准化组织 ISO 于 1983 年提出了开放式系统互连参考模型 OSI/RM（Open System Interconnection Reference Model）。它采用了分层的结构化技术（共分 7 层），从逻辑上定义了一组功能分层，并定义了每层所完成的服务。任何系统只要遵循 OSI 标准即可进行相互通信，它是 Internet 的 TCP/IP 协议的基础。

OSI/RM 各层的含义及主要功能见表 1-1。

表 1-1　OSI/RM 各层的主要功能

层　次	名　称	主要功能	功能概述	应用样例
7	应用层	做什么	提供（OSI）用户服务，如文件传输、电子邮件、网络管理等	Telnet、HTTP
6	表示层	对方看起来像什么	实现不同格式和编码之间的交换	ASCII、JPEG、EBCDIC
5	会话层	对方是谁	在两个应用进程之间建立和管理不同形式的通信对话。其数据流方向控制模式有三种，即单工、半双工和双工	操作系统/应用访问规划
4	传输层	对方在何处	提供传送方式，进行多路利用，实现端点到端点间的数据交换，为会话层实体提供透明的、可靠的数据传输服务	TCP、UDP、SPX
3	网络层	走哪条路可以到达	通过分组交换和路由选择为传输层实体提供端到端的交换网络数据，传送功能使得传输层摆脱路由选择、交换方式、拥挤控制等网络传输细节，实现数据传输	IP、IPX
2	数据链路层	每一步应该怎样走	进行二进制数据块传送，并进行差错检测和数据流控制。它分为两个子层，即介质访问控制协议（MAC）和逻辑链路控制协议（LLC）	802.3/802.2、HDLC
1	物理层	对上一层的每一步怎样利用物理传输介质	通过机械和电气的互联方式把实体连接起来，让数据流通过	EIS/TIA-232　V.35 10BASE5、10BASE2 和 10BASET

1.3.2　Internet 网络体系层次结构

现在 Internet 使用的协议是 TCP/IP 协议。TCP/IP 协议是一个 4 层结构的网络通信协议组，这 4 层协议分别是：物理网络接口层协议、网际层协议、传输层协议和应用层协议。TCP/IP 模型及所包含的协议、基于 TCP/IP 协议的 Internet 与 OSI 参考模型的体系结构对比如图 1-3 所示。

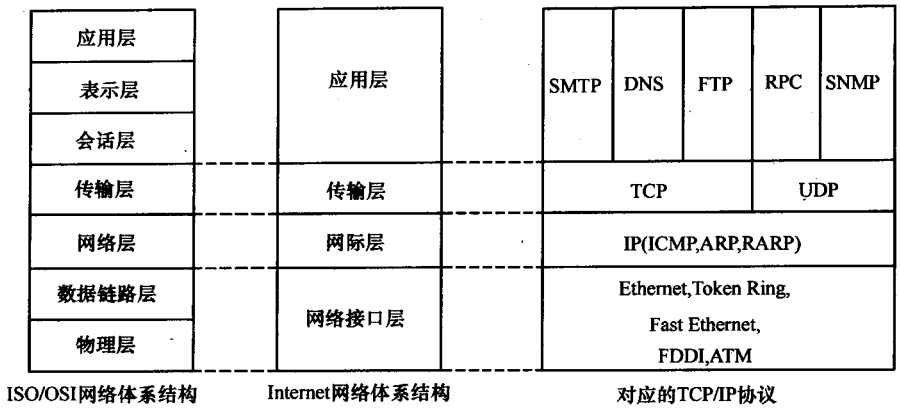


图 1-3 Internet 协议与 OSI 参考模型的体系结构对比图

1. 网络接口层

网络接口层定义了 Internet 与各种物理网络之间的网络接口。该协议层接收上层（IP 层）的数据并把它封装成对应的、特定的帧，或者从下层物理网接收数据帧并从帧中提取数据报文，然后提交给 IP 层。

2. 网际层

网际层是网络互联层，负责相邻计算机之间的通信，提供端到端的分组传送、数据分段与组装、路由选择等功能。该层使用的协议有 IP、ICMP 等。其功能包括如下 3 个方面。

（1）该层处理来自传输层的分组发送请求。IP 把来自传输层的数据封装成一个个数据报文（Data gram），并依据数据要发往的 IP 地址进行路由选择和处理，最后把这些数据报文送至目的地址的主机上。

（2）该层处理输入数据报文。首先检查其合法性，然后进行路由选择；或去掉报头，将剩下的传输层报文交给适当的传输协议或转发该数据报文。

（3）该层处理 ICMP 报文、路由、流控，以及阻塞等问题。

3. 传输层

传输层为应用层的应用进程或应用程序提供端到端的有效、可靠的连接以及通信和事务处理，该层使用的协议有 TCP 和 UDP。TCP 利用下层不可靠的 IP 数据报文服务为应用层提供面向连接的、可靠的端到端通信，包括数据报文的顺序控制与流量控制；而 UDP 则直接为应用层提供低可靠的、无连接的通信服务。传输层的功能包括如下 3 个方面。

（1）该层格式化信息流。

（2）该层提供可靠传输。传输层协议规定接收端必须发回确认，假如分组丢失，必须重新发送。

（3）该层解决不同应用程序的识别问题。因为因特网常常同时被多个应用程序访问，为区别它们，传输层在每一分组中增加识别的信息。

4. 应用层

应用层位于 TCP/IP 协议的最上层，向用户提供一组应用程序和各种网络服务，如文件传输、电子邮件等。该层使用的协议很多，主要包括：Telnet、FTP、SMTP、DNS、NFS

（实现主机间文件系统的共享）、BOOTP（用于无盘主机的启动）、RPC（实现远程主机的程序运行）、SNMP（实现网络管理的协议）等。

1.3.3　网络安全体系结构框架

网络安全是一个覆盖范围很广的领域。为了更深刻地理解网络安全问题，必须对这个领域进行系统、全面的了解。对于整个网络安全体系，从不同的层面来看，包含的内容和安全要求不尽相同。

（1）从消息的层次来看，主要包括：完整性、保密性和不可否认性。

（2）从网络层次来看，主要包括：可靠性、可控性和可操作性；保证协议和系统能够互相连接、可计算。

（3）从技术层次上讲，主要包括：数据加密技术、防火墙技术、攻击检测技术和数据恢复技术等。

（4）从设备层次来看，主要包括：质量保证、设备冗余备份和物理安全等。

由此可见，计算机网络安全的研究涉及多个学科领域，其边界几乎是无法限定的。同时随着网络技术的发展，也还会有新的安全问题不断出现。

一般把计算机网络安全看成一个由多个安全单元组成的集合。其中，每一个安全单元都是一个整体，包含了多个特性。可以从安全特性的安全问题、系统单元的安全问题以及开放系统互连（ISO/OSI）参考模型结构层次的安全问题等三个主要特性去理解一个安全单元。所以安全单元集合可以用一个三维的安全空间去描述，如图1-4所示。图中描述了一个三维的计算机网络安全空间，反映了计算机网络安全的需求和体系结构的共性。

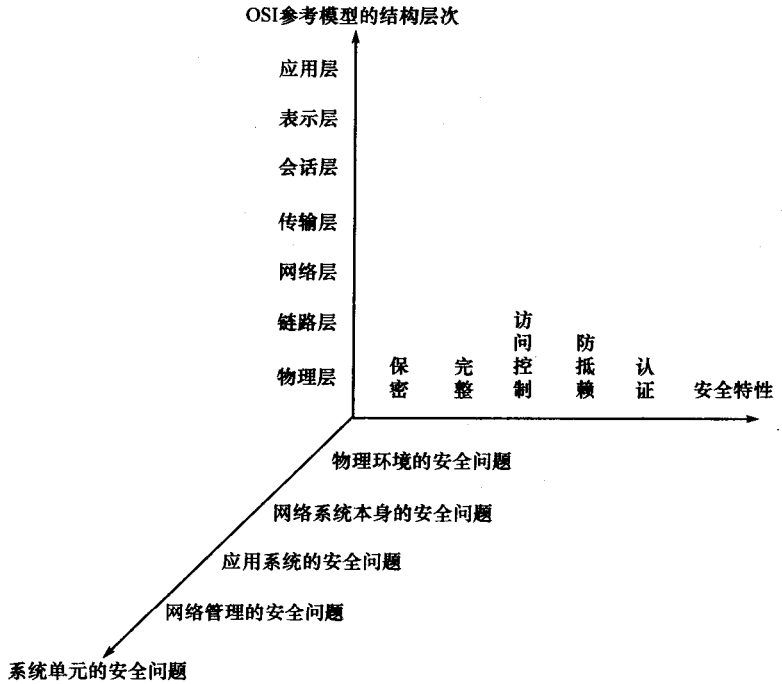


图1-4　计算机网络安全空间