网络工程师系列丛书

计算机网络安全管理

- 各种操作系统的安全管理
- 加密技术和安全工具
- 病毒和木马的防治和检测
- 防火墙和电子商务网站的安全管理

葛秀慧 田 浩 王凌云 盖俊飞 编著

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

网络工程师系列丛书

计算机网络安全管理

葛秀慧　田　浩
王凌云　盖俊飞　编著

清华大学出版社
北　京

内 容 简 介

本书完整地介绍了有关计算机网络安全的知识，内容丰富，讲解深入浅出。全书分为9章，第1章讲述了网络安全的基础知识；第2章详细讲述了加密技术的知识；第3、4、5章分别对当前流行的操作系统Windows NT、Windows 2000 Server和Linux网络操作系统的安全管理进行了详细的分析和阐述；第6章对电子邮件服务的安全以及客户端与邮件服务器的安全配置进行了详尽的分析；第7章对病毒的基本知识和病毒的查杀做了专门的讲解；第8章对防火墙进入了分析，并给出了配置实例；第9章对电子商务网站的安全SSL协议及其站点的配置做了详细的分析。通过本书的学习，读者可以对网络安全有一个全面而系统的认识，同时可以学会使用网络安全性工具。

本书适用于网络管理员和信息安全管理人员，既可以作为高等院校信息安全相关专业教学参考书，也可供从事相关专业的教学人员、科研和工程技术人员参考。

图书在版编目(CIP)数据

计算机网络安全管理/葛秀慧等编著. —北京：清华大学出版社，2003.8
(网络工程师系列丛书)
ISBN 7-302-06892-5

Ⅰ.计… Ⅱ.葛… 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(2003)第056797号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：丁　岭
文稿编辑：陶萃渊
封面设计：王　永
印 刷 者：北京密云胶印厂
发 行 者：新华书店总店北京发行所\清华大学出版社出版发行
开　　本：185×260　**印张**：19　**字数**：473千字
版　　次：2003年8月第1版　2003年8月第1次印刷
书　　号：ISBN 7-302-06892-5/TP·5104
印　　数：1～5000
定　　价：28.00元

丛 书 序

人类正进入信息时代，计算机与信息技术已成为推动社会全面进步的最活跃因素之一。新世纪对人们的知识结构、技能、素质的要求将更加全面和具体，计算机与信息技术的飞速发展正在改变着人们的思维、工作、生活和学习方式。掌握一定的网络管理知识，具备网络组建、管理与维护的实战操作技能，并将其作为工作、学习、生活的必备工具，无疑是新世纪网络组建、管理与维护从业人员的共同需求。

清华大学出版社组织多名有丰富实践经验的资深专业人士，倾情奉献、鼎力推出这套《网络工程师系列丛书》，其内容涉及校园网、局域网、网络安全、中小型网站等各方面。

本丛书具有如下特色：

专业性强 本丛书为专业读者度身定制，以丰富的专业选题满足不同专业人士的特殊需求。

覆盖面广 内容涉及校园网、局域网、网络安全、网吧、无盘工作站、中小型网站等与网络有关的各方面。广泛适用于专业人士、大专院校师生及网络发烧友。

定位准确 明确定位于初、中级用户。丛书坚持基础、技巧、经验并重，理论、操作、提高并举，尤其对初、中级学者容易出现的疏忽、困惑、难点进行重点突破。

精益求精 丛书作者均为有丰富教学和工作实践经验的资深专家。在广泛的读者调查基础上，博采国内外相关图书众家之长，以中国人的思维习惯和学习方式深入浅出地讲述相关的技巧。全套丛书可操作性强、语言凝练、重点突出、脉络清晰、浅显易懂。

经过紧张的组织、策划和创作，本丛书已陆续面市，尽管在写作过程中我们始终坚持严谨、求实的作风和追求高水平、高质量、高品位的目标，我们仍相信错误和不足之处在所难免，这里还敬请读者、专业人士和同行批评指正。

编 者

前　言

在信息时代，信息安全问题越来越重要，而现在大部分信息都是通过网络来传播，网络安全已成为21世纪世界十大热门课题之一。网络安全在IT业内可分为：网络安全硬件、网络安全软件、网络安全服务。网络硬件包括：防火墙和VPN、独立的VPN、入侵检测系统、认证令牌和卡、生物识别系统、加密机和芯片。网络安全软件包括：安全内容管理、防火墙/VPN、入侵检测系统、安全3A、加密；其中安全内容管理还包括防病毒、网络控制和邮件扫描；安全3A包括授权、认证和管理。网络安全服务包括顾问咨询、设计实施、支持维护、教育培训、安全管理。目前随着互联网的日益普及，网络安全正在成为人们关注的焦点。而要保证网络安全就必须对网络进行安全的管理。让我们先了解一下网络体系结构的相关知识以及在相应模型中的安全问题，再对网络安全进行详细的分析以及讨论，解决网络安全管理问题的关键技术。

本书完整地介绍了有关网络安全的知识，内容丰富，讲解深入浅出。全书分为9章，第1章讲述了加密技术的知识。加密技术作为一种主动的防卫手段，是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法。第3、4、5章分别对当前流行的操作系统Windows NT、Windows 200 Server和Linux网络操作系统的安全管理进行了详细的分析和阐述。对于今天的网络系统来说，信息安全是一个非常重要且又非常严重的问题，它涉及从硬件到软件、从单机到网络的各方面的安全性机制。而网络操作系统的安全性是整个网络系统安全体系中的基础环节，所以对网络操作系统的安全配置是极其重要的。第6章对电子邮件服务的安全和客户端以及邮件服务器的安全配置进行了详尽的解析。如今病毒的总数以每月递增上百个的速度发展，如蠕虫病毒、CIH病毒、BO黑客程序、宏病毒、求职信病毒以及以电子邮件传染的邮件病毒，都借助于网络这个世界性的传播途径而具备了更强的攻击力，所以第7章对病毒的基本知识和病毒的查杀进行了专门的讲解。防火墙是一种被动的防御技术，是一类防范措施的总称，是目前在网络安全技术中使用最多、最广泛的一种安全技术。第8章对防火墙进行了分析，并给出了配置实例。如何建立一个安全、快捷的电子商务应用环境，对信息提供足够的保护，已经成为商家和用户都十分关心的问题。所以要开展电子商务，就必须充分了解电子商务中应该注意的安全问题。第9章对电子商务网站的安全SSL协议及其站点的配置做了详细的分析。

通过本书的学习，读者可以对网络安全有一个全面而系统的认识，同时可以学会使用网络安全性工具的具体方法。本书适用于网络管理员和信息安全管理人员，既可以作为高

等院校与信息安全相关专业的本科生和专科生的参考书，也可供从事相关专业的教学、科研和工程技术人员参考。

本书由葛秀慧、田浩、王凌云、盖俊飞同志编著。在编写过程中，由于作者水平有限、经验不足，缺点和错误在所难免，希望读者多提宝贵意见，诚望专家和广大读者不吝赐教，批评指正。

编 者

目　　录

第 1 章　网络安全管理基础 …… 1
1.1　网络体系结构概述 …… 1
1.2　网络体系结构的参考模型 …… 2
1.2.1　OSI 参考模型 …… 2
1.2.2　TCP/IP 协议结构体系 …… 3
1.3　系统安全结构 …… 5
1.4　TCP/IP 层次安全 …… 6
1.4.1　网络层的安全性 …… 6
1.4.2　传输层的安全性 …… 6
1.4.3　应用层的安全性 …… 7
1.5　TCP/IP 的服务安全 …… 7
1.5.1　WWW 服务 …… 7
1.5.2　电子邮件服务 …… 8
1.5.3　FTP 服务和 TFTP 服务 …… 8
1.5.4　Finger 服务 …… 8
1.5.5　其他的服务 …… 8
1.6　个人网络安全 …… 9
1.7　局域网的安全 …… 9
1.7.1　网络分段 …… 9
1.7.2　以交换式集线器代替共享式集线器 …… 10
1.7.3　虚拟专网 …… 10
1.8　广域网的安全 …… 10
1.8.1　加密技术 …… 10
1.8.2　VPN 技术 …… 11
1.8.3　身份认证技术 …… 11
1.9　网络安全威胁 …… 11
1.10　网络系统安全应具备的功能 …… 12
1.11　网络安全的主要攻击形式 …… 13
1.11.1　信息收集 …… 13
1.11.2　利用技术漏洞型攻击 …… 15
1.12　网络安全的关键技术 …… 17
1.13　保证网络安全的措施 …… 19
1.14　网络的安全策略 …… 21

1.14.1 数据防御 …… 22
1.14.2 应用程序防御 …… 22
1.14.3 主机防御 …… 22
1.14.4 网络防御 …… 22
1.14.5 周边防御 …… 22
1.14.6 物理安全 …… 23

第2章 加密技术 …… 24
2.1 密码算法 …… 24
2.2 对称加密技术 …… 25
2.2.1 DES 算法 …… 25
2.2.2 三重 DES 算法 …… 26
2.3 不对称加密技术 …… 26
2.4 RSA 算法简介 …… 28
2.4.1 RSA 算法 …… 28
2.4.2 密钥对的产生 …… 29
2.4.3 RSA 的安全性 …… 29
2.4.4 RSA 的速度 …… 30
2.4.5 RSA 的选择密文攻击 …… 30
2.4.6 RSA 的数字签名 …… 31
2.4.7 RSA 的缺点 …… 31
2.4.8 关于 RSA 算法的保密强度安全评估 …… 31
2.4.9 RSA 的实用性 …… 32
2.5 RSA 算法和 DES 算法的比较 …… 33
2.6 DSS/DSA 算法 …… 34
2.7 椭圆曲线密码算法 …… 34
2.8 量子加密技术 …… 36
2.9 PKI 管理机制 …… 37
2.9.1 认证机构 …… 37
2.9.2 加密标准 …… 38
2.9.3 证书标准 …… 38
2.9.4 数字证书 …… 38
2.10 智能卡 …… 41

第3章 Windows NT 网络操作系统的安全管理 …… 43
3.1 Windows NT 的安全环境 …… 43
3.2 Windows NT 的安全服务 …… 44
3.2.1 验证 …… 44
3.2.2 访问控制 …… 45

3.2.3 责任 …… 45
3.2.4 审核 …… 46
3.2.5 安全分区 …… 46
3.2.6 完整性 …… 47
3.2.7 机密性 …… 48
3.2.8 可管理性 …… 48
3.3 Windows NT 的安全模式 …… 49
3.3.1 Windows NT 的安全策略 …… 50
3.3.2 在网络中 Windows NT 的安全性 …… 51
3.4 Windows NT Server 的安全管理 …… 57
3.5 基于 Windows NT 建立安全 Web 站点 …… 59
3.5.1 安装 …… 59
3.5.2 Windows NT 设置 …… 60
3.5.3 IIS 设置 …… 63
3.6 安全工具 …… 66
3.6.1 nbtstat 实用命令 …… 66
3.6.2 net view …… 69
3.6.3 net use …… 70

第 4 章 Windows 2000 操作系统的安全管理 …… 73
4.1 Windows 2000 的安全性设计 …… 73
4.2 Windows 2000 中的验证服务架构 …… 73
4.3 Windows 2000 安全特性 …… 74
4.4 Windows 2000 组策略的管理安全 …… 76
4.4.1 Windows 2000 中的组策略 …… 76
4.4.2 加强内置账户的安全 …… 82
4.4.3 组策略的安全模板 …… 83
4.4.4 组策略的实现 …… 84
4.5 审计与入侵检测 …… 87
4.5.1 审计 …… 87
4.5.2 入侵检测 …… 96
4.6 修补程序 …… 98

第 5 章 Linux 网络操作系统的安全管理 …… 100
5.1 系统安全 …… 100
5.1.1 C1/C2 安全级设计框架 …… 100
5.1.2 身份认证 …… 101
5.1.3 用户权限和超级用户 …… 106
5.1.4 存储空间安全 …… 108

5.1.5 数据的加密 …… 111
5.1.6 B1 安全级强化 …… 115
5.1.7 日志 …… 117
5.2 网络安全 …… 122
5.2.1 网络接口层 …… 122
5.2.2 网络层 …… 126
5.2.3 传输层 …… 128
5.2.4 应用层 …… 130
5.3 安全工具 …… 139
5.3.1 tcpserver …… 139
5.3.2 xinetd …… 141
5.3.3 Sudo …… 151
5.3.4 安全检查工具 nessus …… 154
5.3.5 监听工具 sniffit …… 159
5.3.6 扫描工具 nmap …… 160
5.3.7 其他安全工具 …… 165
5.4 配置安全可靠的系统 …… 166
5.4.1 SSH 实践 …… 166
5.4.2 SSL 实践 …… 173
5.4.3 构造 chroot 的 DNS …… 177
5.4.4 代理服务器 socks …… 179
5.4.5 邮件服务器 …… 181

第 6 章 电子邮件的安全管理 …… 185
6.1 电子邮件概述 …… 185
6.2 电子邮件使用的协议 …… 185
6.2.1 POP 邮局协议 …… 185
6.2.2 IMAP 交互式电子邮件访问协议 …… 186
6.2.3 SMTP 简单电子邮件传输协议 …… 186
6.3 电子邮件发送方式的安全 …… 186
6.3.1 Web 页方式 …… 186
6.3.2 客户端收发电子邮件的安全 …… 188
6.4 电子邮件加密工具 …… 190
6.4.1 A-Lock 邮件加密软件 …… 190
6.4.2 Puffer 邮件加密工具 …… 191
6.5 Exchange 邮件服务器的安全配置与管理 …… 199
6.5.1 收件人的创建与配置 …… 202
6.5.2 Exchange Server 的监控 …… 208

第7章 计算机病毒 …… 210
7.1 计算机病毒概述 …… 210
7.1.1 计算机病毒的定义 …… 210
7.1.2 病毒的产生 …… 210
7.1.3 计算机病毒的特征 …… 211
7.1.4 病毒的分类 …… 211
7.1.5 计算机病毒的发展 …… 212
7.1.6 计算机病毒的破坏现象 …… 213
7.2 常见的几种病毒 …… 213
7.2.1 CIH 病毒 …… 213
7.2.2 木马病毒 …… 214
7.2.3 宏病毒 …… 216
7.2.4 BO 黑洞病毒 …… 216
7.2.5 邮件病毒 …… 216
7.2.6 CodeRed 病毒 …… 219
7.2.7 常见病毒发作日期表 …… 220
7.3 计算机病毒的检测 …… 222
7.4 计算机病毒的防治策略 …… 222
7.5 病毒的检测方法 …… 224
7.5.1 特征代码法 …… 224
7.5.2 校验和法 …… 224
7.5.3 行为监测法 …… 225
7.5.4 软件模拟法 …… 225
7.6 常用杀毒软件 …… 225
7.6.1 金山毒霸杀毒软件 …… 225
7.6.2 KV3000 杀病毒软件 …… 229

第8章 防火墙安全管理 …… 232
8.1 防火墙概述 …… 232
8.1.1 防火墙的特点 …… 233
8.1.2 实现防火墙的技术 …… 233
8.2 防火墙的类型 …… 235
8.2.1 网络级防火墙 …… 236
8.2.2 应用级网关防火墙 …… 237
8.2.3 电路级网关防火墙 …… 237
8.2.4 规则检查防火墙 …… 238
8.2.5 状态监视器 …… 238
8.3 防火墙体系结构 …… 239
8.3.1 双重宿主主机体系结构 …… 239

8.3.2 屏蔽主机体系结构 …… 239
8.3.3 屏蔽子网体系结构 …… 239
8.3.4 防火墙体系结构的组合形式 …… 241
8.4 防火墙的选择 …… 242
8.5 常用防火墙的配置与管理 …… 243
8.5.1 配置防火墙 …… 244
8.5.2 防火墙的管理 …… 248

第9章 电子商务网站的安全 …… 250
9.1 电子商务的安全概述 …… 250
9.1.1 电子商务站点的安全准则 …… 250
9.1.2 电子商务安全体系 …… 251
9.2 电子商务中所使用的安全技术 …… 251
9.2.1 密码技术 …… 252
9.2.2 数字签名 …… 253
9.3 电子商务中的认证 …… 253
9.3.1 认证机构 …… 254
9.3.2 数字证书 …… 256
9.4 SSL 协议 …… 259
9.4.1 协议概述 …… 260
9.4.2 SSL 协议连接安全的特征 …… 261
9.4.3 协议规范 …… 262
9.5 建立安全的 Web 站点 …… 263
9.5.1 建立安全的 Web 站点应具备的条件 …… 264
9.5.2 建立并安装一个站点证书 …… 268

第1章　网络安全管理基础

在信息时代，信息安全问题越来越重要。现在，大部分信息都是通过网络来传播，网络安全成为21世纪世界十大热门课题之一。网络安全在IT业内可分为网络安全硬件、网络安全软件和网络安全服务。其中，网络硬件包括：防火墙和VPN、独立的VPN、入侵检测系统、认证令牌环卡、生物识别系统、加密机和芯片；网络安全软件包括：安全内容管理、防火墙和VPN、入侵检测系统、安全3A、加密等。其中安全内容管理还包括防病毒、网络控制和邮件扫描，安全3A包括授权、认证和管理；网络安全服务包括：顾问咨询、设计实施、支持维护、教育培训、安全管理。随着互联网的日益普及，网络安全正在成为一个受人关注的焦点。而要保证网络安全就必须对网络进行安全管理。让我们先了解一下网络体系结构的相关知识，以及在相应模型中的安全问题，再对网络安全进行详细的分析以及讨论解决网络安全管理问题的关键技术。

1.1　网络体系结构概述

大家知道，一个计算机网络有许多互相连接的节点，在这些节点之间要不断地进行数据交换。要做到有序的交换数据，每个节点就必须遵守一些事先约定好的规则，这些规则明确规定了所交换数据的格式以及相关的同步问题。这些为进行网络数据交换而建立的规则、标准或约定就称为网络协议。一个网络协议主要由以下三个要素组成：

- 语法，即数据与控制信息的结构或格式；
- 语义，即需要发出何种控制信息、完成何种协议以及做出何种应答；
- 同步，即事件实现顺序的详细说明。

由此可见，网络协议是计算机网络不可缺少的部分。很多经验和实践表明，对于非常复杂的计算机网络协议，为了减少网络设计的复杂性，大多数网络都按层(layer)或级(level)的方式来进行组织。不同的网络，其层的数量、名字、内容和功能都不尽相同。这样分层的好处在于：每一层都实现相对的独立功能，因此就能将一个难以处理的复杂问题分解为若干个较容易处理的问题。

计算机网络的各层及协议的集合，称为网络的体系结构(Network architecture)。换言之，计算机网络的体系结构是使这个计算机网络及其部件所应该完成的功能的精确定义。需要强调的是，这些功能究竟由何种硬件或软件完成，则是一个遵循这种体系结构的实现的问题。可见体系结构是抽象的，是存在于纸上的，而对它的实现是具体的，是运行在计算机软件和硬件之上的。常见的网络层次结构如图1-1所示。

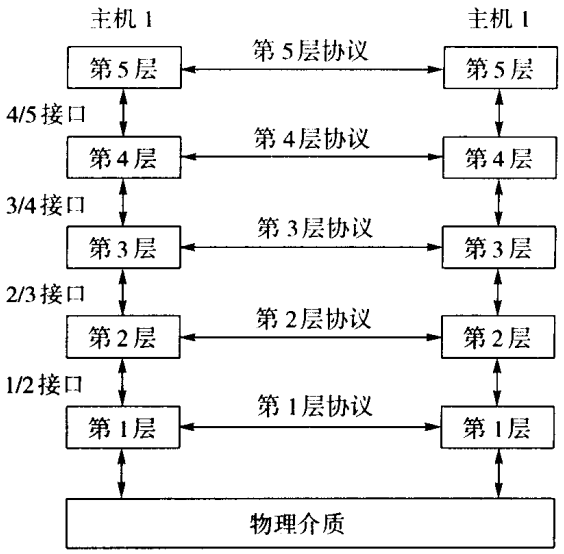

图　1-1

1.2　网络体系结构的参考模型

网络体系结构的参考模型主要有两种，即 OSI 模型和 TCP/IP 模型。

1.2.1　OSI 参考模型

现代计算机网络的设计，是按高度结构化方式进行的。为减少协议设计的复杂性，大多数网络都按层或级的方式来组织，每一层都建立在它的下层之上。不同的网络，其层的数量，各层的名字、内容和功能都不尽相同。然而，在所有的网络中，每一层的目的，都是向它的上一层提供服务的，而把这种服务是如何实现的细节对上层加以屏蔽。

最著名的网络体系结构是国际标准化组织 ISO 的开放系统互联 OSI(Open System Interconnection)参考模型，即通常所提的 OSI 模型。OSI 模型有七层，其分层原则如下：

- 根据功能的需要分层；
- 每一层应当实现一个定义明确的功能；
- 每一层功能的选择应当有利于制定国际标准化协议；
- 各层界面的选择应当尽量减少通过接口的信息量；
- 层数应足够多，以避免不同的功能混杂在同一层中；但也不能过多，否则体系结构会过于庞大。

OSI 参考模型由低到高依次是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，其体系结构如图 1-2 所示。

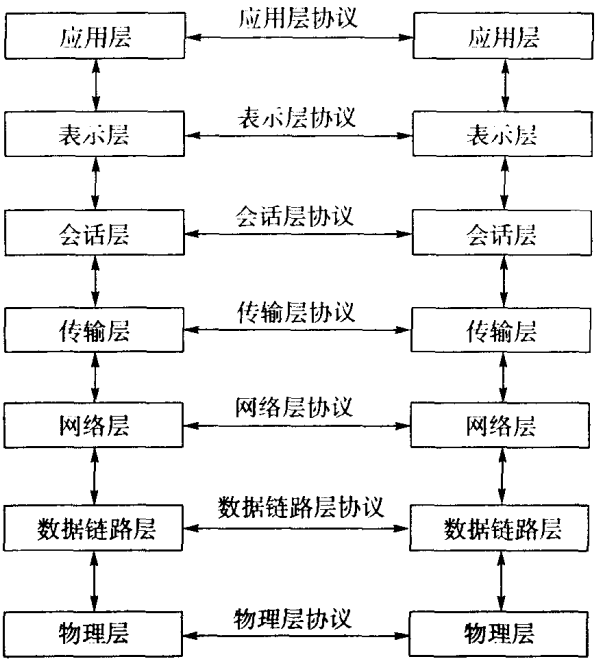

图　1-2

1.2.2　TCP/IP 协议结构体系

OSI 参考模型的建立是计算机网络技术发展的一个里程碑，它为网络的标准化提供了一致的框架和前景。但由于 OSI 参考模型的庞大，所以在建立网络时，并没有完全依赖 OSI 参考模型。事实上，基于 TCP/IP 协议的 Internet 网络有着自己的网络体系结构——TCP/IP 网络体系结构。这种体系结构，目前已经成为事实上的网络标准。

TCP/IP 协议体系结构与 OSI 参考模型类似，也为分层体系结构，但比 OSI 参考模型的层数要少，一般指的四层结构，从低到高，依次为网络接口层、网络层、传输层和应用层，如图 1-3 所示。

1. 网络接口层

网络接口层在 TCP/IP 协议结构的最底层。该层中的协议提供了一种数据传送的方法，使得系统可以通过直接的物理连接的网络，将数据传送到其他设备，并定义了如何利用网络来传送 IP 数据报。TCP/IP 网络接口层一般包括 OSI 参考模型的物理层和数据链路层的全部功能，因此这一层的协议很多，包括各种局域网、广域网的各种物理网络的标准。

2. 网络层

网络层在网络接口的上一层。网络层协议 IP 是 TCP/IP 的核心协议，也是网络层中最重要的协议。IP 可提供基本的分组传输服务，这是构造 TCP/IP 的基础。网络层上、下层

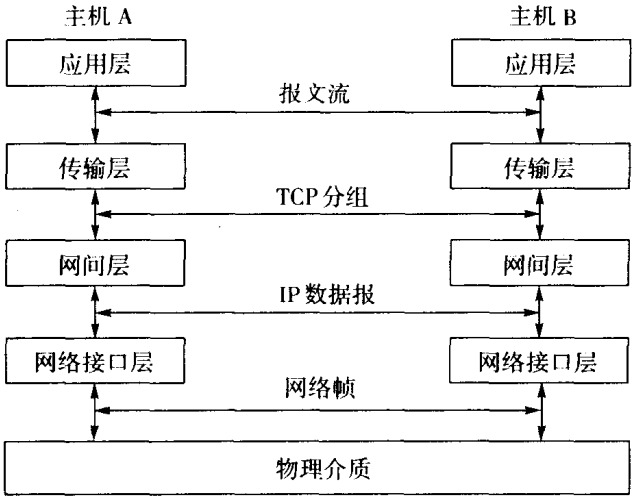

图　1-3

中的所有协议都使用 IP 协议传送数据；所有的 TCP/IP 数据，无论是进来的还是出去的，都流经 IP，并与它的最终目的地无关。另外，网络层还有两个协议，地址转换协议(ARP)和网间控制报文协议(ICMP)，其中 ICMP 协议具有测试网络链路和检测网络故障的功能，是 IP 协议不可分割的一部分。

3. 传输层

传输层在网络层的上一层，又称主机到主机传输层。传输层有两个重要的协议是传输控制协议 TCP 和用户数据报协议 UDP，用以提供端到端的数据传输服务，即从一个应用程序到另一个应用程序之间的信息传递。TCP 利用端到端的错误检测与纠正功能，提供可靠的数据传输服务。而 UDP 则提供低开销、无链接的数据报传输服务。

4. 应用层

TCP/IP 协议体系结构的顶层是协议最多的一层。应用层的协议大多数都为用户提供直接的服务，而且还在不断地增加新的服务。

常见的应用层协议有：

- Telnet 网络终端协议；
- FTP 文件传输协议；
- SMTP 简单邮件传输协议；
- POP 邮件接收协议；
- HTTP 超文本传输协议；
- DNS 域名服务等。

1.3 系统安全结构

网络系统的安全涉及平台的各个方面。按照网络 OSI 的七层模型，网络安全贯穿于整个七层模型。针对网络系统实际运行的 TCP/IP 协议，网络安全贯穿于信息系统的四个层次。网络的安全体系层次模型如表 1-1 所示。

表 1-1 网络的安全体系层次模型

应用系统	应用系统安全
应用平台	应用平台安全
会话层	会话安全
网络层	安全路由/访问机制
链路层	链路安全
物理层	物理层安全

1. 物理层

物理层信息安全，主要防止物理通路的损坏、物理通路的窃听、对物理通路的攻击(干扰等)。

2. 数据链路层

数据链路层的网络安全需要保证通过网络链路传送的数据不被窃听。主要采用划分 VLAN(局域网)、加密通信(远程网)等手段。

3. 网络层

网络层的安全需要保证网络只给授权的客户使用授权的服务，保证网络路由正确，避免被拦截或监听。

4. 操作系统

操作系统安全要求保证客户资料、操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

5. 应用平台

应用平台指建立在网络系统之上的应用软件服务，如数据库服务器、电子邮件服务器、Web 服务器等。由于应用平台的系统非常复杂，通常采用多种技术(如 SSL 等)来增强应用平台的安全性。

6. 应用系统

应用系统完成网络系统的最终目的——为用户服务。应用系统的安全与系统设计和实