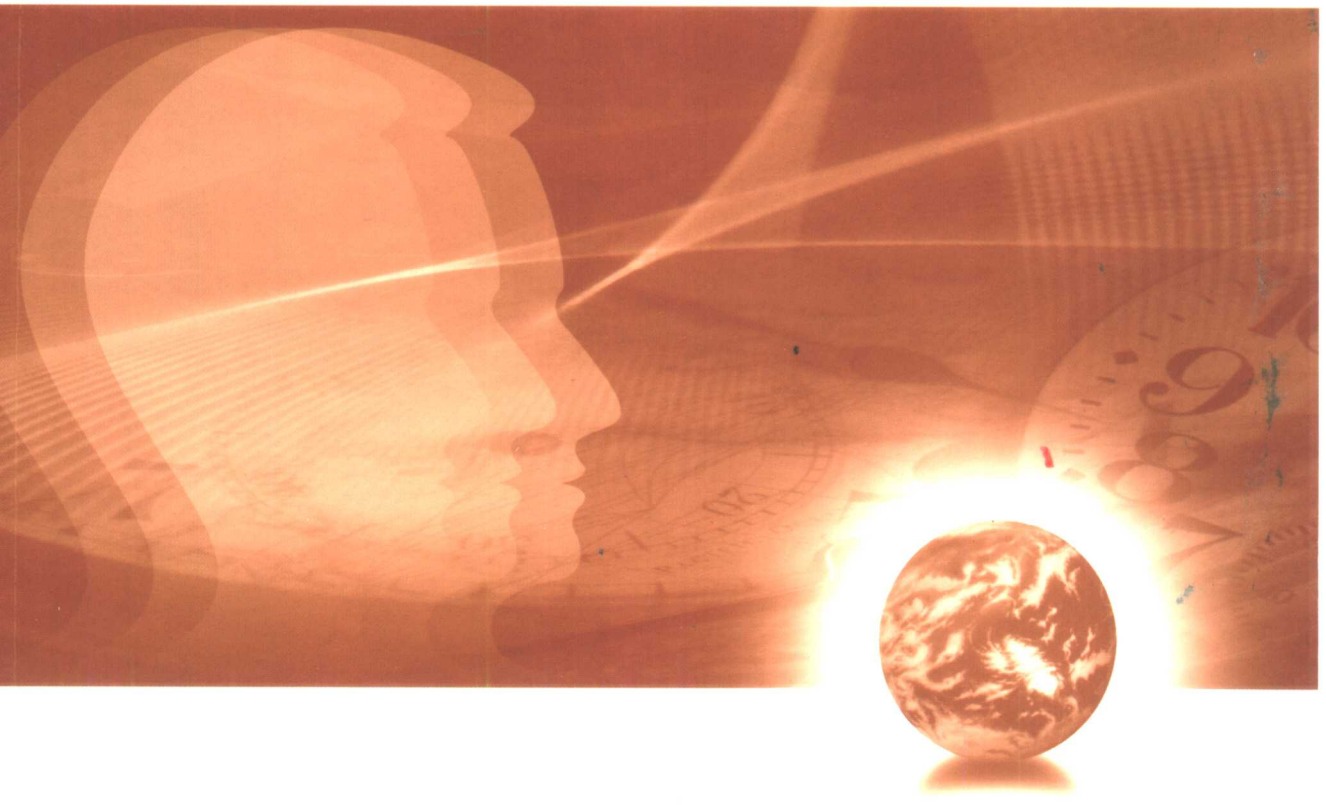
高等院校计算机科学与技术
“十五”规划教材

计算机网络安全技术教程



梁亚声　汪永益　刘京菊　汪　生　编著

机械工业出版社
CHINA MACHINE PRESS

高等院校计算机科学与技术“十五”规划教材

计算机网络安全技术教程

梁亚声　汪永益　刘京菊　汪　生　编著

机械工业出版社

本书系统介绍了计算机网络安全的体系结构、基础理论、技术原理和实现方法。主要内容包括：计算机网络的物理安全、信息加密与 PKI、防火墙技术、入侵检测技术、访问控制技术、网络安全检测与评估技术、计算机病毒防范技术、备份技术和网络安全解决方案。本书涵盖了计算机网络安全的技术和管理，在内容安排上将理论知识和工程技术应用有机结合，并介绍了许多计算机网络安全技术的典型应用方案。

本书可作为计算机、通信、信息安全等专业本科生的教科书，也可作为网络工程技术人员、网络管理人员、信息安全管理人员的技术参考书。

图书在版编目（CIP）数据

计算机网络安全技术教程/梁亚声等编著．—北京：机械工业出版社，2004.8
（高等院校计算机科学与技术“十五”规划教材）
ISBN 7-111-14871-1

Ⅰ.计… Ⅱ.梁… 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（2004）第 066653 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策　　划：胡毓坚
责任编辑：车　忱
责任印制：施　红

北京忠信诚胶印厂印刷·新华书店北京发行所发行

2004 年 9 月第 1 版·第 1 次印刷
787mm×1092mm 1/16·17.75 印张·440 千字
0 001—5000 册
定价：25.00 元

出版说明

适逢高等院校计算机专业教育改革的关键时期，为配合相关的教材建设，机械工业出版社会同全国在该领域内享誉盛名、具备雄厚师资和技术力量的高等院校，包括清华大学、上海交通大学、南京大学、电子科技大学、东南大学、西安电子科技大学、解放军理工大学、北京科技大学等重点名校，组织了多位长期从事教学工作的骨干教师，集思广益，对当前高等院校的教学现状开展了广泛而深入的研讨，继而紧密结合当前技术发展需要并针对教学改革所提出的问题，精心编写了这套面向普通高等院校计算机专业的系列教材，并陆续出版。

本套教材内容覆盖了普通高等院校计算机专业学生的必修课程，另外还恰如其分地添加了一些选修课程，总体上分为基础、软件、硬件、网络和多媒体五大类。在编写过程中，对教学改革力度比较大、内容新颖以及各院校急需的并且适应社会经济发展的新教材，优先选择出版。

本套教材注重系统性、普及性和实用性，力求达到专业基础课教材概念清晰、深度合理的标准，并且注意与专业课教学的衔接；专业课教材覆盖面广、深浅适中，在体现相关领域最新进展的同时注重理论联系实际。全套教材体现了教育改革的最新思想，可作为高等院校计算机科学与技术专业的教学用书，同时也是培训班和自学使用的最佳教材。

机械工业出版社

前　言

随着计算机网络的广泛应用，人类面临着信息安全的巨大挑战。如何保护个人、企业、国家的机密信息不受黑客和间谍的入侵；如何保证计算机网络安全并不间断地工作，是国家和单位信息化建设必须考虑的重要问题。然而，计算机网络的安全是一个错综复杂的问题，涉及面非常广，有技术因素，还有管理因素；有自然因素，还有人为因素；有外部的安全威胁，还有内部的安全隐患。

本书介绍了计算机网络安全的体系结构，从物理层、链路层、网络层、应用层到系统网络安全理论、技术原理和实现方法，使读者对计算机网络安全有一个系统、全面的了解。全书共10章。第1章主要介绍计算机网络安全的相关概念，计算机网络的安全体系结构。第2章主要介绍计算机网络的物理安全，从计算机机房、通信线路、设备和电源等方面介绍计算机网络物理层的安全。第3章主要介绍信息加密与PKI技术，包括：加密体系；单钥加密和双钥加密算法；链路、节点端到端加密；数字签名技术和身份认证技术；以及公开密钥基础设施(PKI)。第4章主要介绍防火墙技术，包括：防火墙体系结构、包过滤防火墙和应用代理防火墙，以及防火墙的应用。第5章主要介绍入侵检测系统，包括：入侵检测的技术实现、分布式入侵检测、入侵检测系统的标准和入侵检测系统的应用。第6章主要介绍访问控制技术，包括：操作系统的安全机制及安全级别、操作系统安全技术和数据库安全技术。第7章主要介绍网络安全检测与评估技术，包括：网络安全漏洞的分类、网络安全评估标准和方法、网络安全评估系统。第8章主要介绍计算机病毒防范技术，包括：计算机病毒的工作原理和分类、计算机病毒的检测和防范技术。第9章主要介绍备份技术，包括：硬盘备份、双机备份、网站镜像技术和数据备份，以及备份软件。第10章主要介绍网络安全解决方案，包括：网络安全解决方案、单机用户网络安全解决方案和内部网络安全管理制度。本书涉及的内容十分广泛，在学习时，可在内容、重点和深度等方面进行选择。

本书由梁亚声编写了第1章以及统稿，汪永益编写了第4、8、9章，刘京菊编写了第2、7、10章，汪生编写了第3、5、6章。由于作者水平有限，书中难免存在不妥之处，敬请读者批评指正。

第1章 绪 论

随着计算机技术的迅速发展，计算机上处理的业务由基于单机的数学运算、文件处理，基于简单连接的内部网络的业务处理、办公自动化，发展到基于企业内部网(Intranet)、企业外部网(Extranet)、全球互联网(Internet)的世界范围内的信息共享和业务处理。计算机网络(简称网络)的应用领域已从传统的小型业务逐渐向大型关键业务扩展。随着政府上网、企业上网、教育上网、家庭上网……，互联网在经济、军事、文教等诸多领域得到广泛应用。

计算机网络在为人们提供便利、带来效益的同时，也使信息安全面临着前所未有的巨大挑战。计算机网络存储、传输和处理着政府宏观调控决策、商业经济、银行资金转帐、股票证券、资源、国防和科研等大量关系国计民生的重要信息，许多信息直接关系到国家的安全。如何保护个人、企业、国家的机密信息不受黑客和间谍的入侵；如何保证网络安全不间断地工作，是国家和单位信息化建设必须考虑的重要问题。据统计，近年来，每年因网络安全造成的损失高达上百亿美元。

有关计算机的安全技术研究始于20世纪60年代。当时，计算机系统的脆弱性已日益为美国政府和一些私营机构所认识。但是，由于当时计算机的速度和性能还比较落后，使用的范围也不广，再加上美国政府把它当作敏感问题而施加控制。因此，有关计算机安全的研究一直局限在比较小的范围内。

进入20世纪80年代后，计算机的性能得到了成百上千倍的提高，应用的范围不断扩大，计算机几乎遍及世界各个角落。并且，人们利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。随之而来的计算机网络的安全问题就日益严峻，成为信息技术中最重要的问题之一。

1.1 计算机网络面临的主要威胁

计算机网络是颇具诱惑力的攻击目标，无论是个人、企业、还是政府机构，只要使用计算机网络，都会感受到网络安全问题带来的威胁；无论是局域网还是广域网，都存在着自然和人为等诸多脆弱性和潜在威胁。

1.1.1 计算机网络实体面临的威胁

实体是指网络中的关键设备，包括各类计算机(服务器、工作站等)、网络通信设备(路由器、交换机、集线器、调制解调器、加密机等)、存放数据的媒体(磁带、磁盘、光盘等)、传输线路、供配电系统，以及防雷系统和抗电磁干扰系统等。这些设备不管哪一个环节出现问题，都会影响网络的正常运行，甚至给整个网络带来灾难性的后果。

1.1.2 计算机网络系统面临的威胁

1986～1989年，原西德黑客团伙“汉诺威集团”试图进入美国军事计算机网络刺探机密，

这一事件于1989年3月2日在德国电视上曝光后，引起媒体连锁反应。1990年1月15日又发生了AT&T"一·一五"大瘫痪事件，从而使美国意识到黑客对计算机网络的严重威胁，1990年在全国范围内掀起了一场"扫黑大行动"。

网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公共网传送的信息可能被他人窃听或篡改等等。表1-1所列为典型的网络安全威胁。

表1-1 典型的网络安全威胁

威　胁	描　述
窃听	网络中传输的敏感信息被窃听
重传	攻击者事先获得部分或全部信息，以后将此信息发送给接收者
伪造	攻击者将伪造的信息发送给接收者
篡改	攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者
非授权访问	通过假冒、身份攻击、系统漏洞等手段，获取系统访问权，从而非法用户进入网络系统读取、删除、修改、插入信息等
拒绝服务攻击	攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁/射频截获	攻击者从电子或机电设备所发出的无线射频或其他电磁辐射中提取信息
人员疏忽	授权的人为了利益或由于粗心将信息泄漏给未授权人

1.1.3 计算机病毒的威胁

1988年11月发生了互联网络蠕虫(worm)事件，也称莫里斯蠕虫案。22岁的罗伯特·泰潘·莫里斯是美国康奈尔大学计算机系研究生，其父鲍勃·莫里斯是美国安全局的首席安全专家。罗伯特从小喜爱计算机，非常熟悉UNIX系统。罗伯特利用UNIX系统中Sendmail、Finger、FTP的安全漏洞，编写了一个蠕虫病毒程序。11月2日晚，罗伯特将病毒程序安放在与ARPANET(国际互联网的前身)联网的麻省理工学院的网络上。由于病毒程序中一个参数设置错误，该病毒迅速在与ARPANET联网的几乎所有计算机中扩散，并被疯狂复制，大量侵蚀计算机资源，使得美国成千上万台计算机一夜之间陷入瘫痪。

1999年4月26日，CIH病毒爆发，俄罗斯十多万台电脑瘫痪，韩国二十四万多台电脑受影响，马来西亚十二个股票交易所受侵害。

计算机病毒严重破坏程序和数据，使网络的效率和作用大大降低，使许多功能无法正常使用，导致计算机系统的瘫痪。目前，全球已发现6万余种计算机病毒，并且，还在以每天10余种的速度增长。据统计，计算机病毒所造成的损失，占网络经济损失的76%，仅"爱虫"病毒在全球所造成的损失就达96亿美元。虽然，至今尚未出现灾难性的后果，但各种各样的计算机病毒层出不穷，并活跃在各个角落。

1.1.4 网络威胁的潜在对手和动机

对网络进行攻击的潜在对手有恶意攻击的，也有非恶意的。网络威胁的潜在对手举例见

表 1-2。

表 1-2 潜在的对手举例

对手		描述
恶意攻击	国家	国家经营，组织精良并得到很好的财政资助，收集别国的机密或关键信息
	黑客	探求网络系统的脆弱性及其缺陷，进行网络攻击
	恐怖分子/计算机恐怖分子	各种恐怖分子或极端势力的个人或团体，强迫或恐吓政府或社会，以满足其需要为目的
	有组织计算机犯罪	有组织和财政资助的协同犯罪
	其他犯罪成员	犯罪群体的其他部分，通常是由少量成员构成，或是单独行动的个人
	国际新闻社	收集和发布消息（有时是非法的），并将其服务出售给出版社和娱乐媒体的组织。其行为包括在任何指定时间收集关于任何人和事的情报
	工业竞争	在竞争市场中营运的国内或外国公司，它们经常以商业间谍的形式，从竞争对手或外国政府那里非法收集情报
	不满的雇员	具有访问系统条件，能够对系统实施内部威胁
非恶意	粗心或未受良好训练的工作人员	缺乏训练，或者粗心大意导致信息系统损坏

对计算机网络进行恶意破坏的目的多种多样，主要是为了获取商业、军事或个人情报，通常，从事这些行为的人被称为黑客。黑客的范围很广，从没有经验的职员、大学生或新手到具有高技术能力的人员。大多数黑客以他们的技术为荣，寻求各种获得对系统的访问权（而非破坏）。

黑客刺探特定目标的通常动机是：

- 获取机密或敏感数据的访问权；
- 跟踪或监视目标系统的运行（跟踪分析）；
- 扰乱目标系统的正常运行；
- 窃取钱物或服务；
- 免费使用资源（例如，计算机资源或网络）；
- 向安全机制进行技术挑战。

从信息系统方面看，这些动机具有三个基本目标：

- 访问信息；
- 修改或破坏信息或系统；
- 使系统拒绝服务。

在攻击信息处理系统时，也面临着一定风险，这些风险包括：

- 暴露其攻击能力；
- 打草惊蛇，使对手有所防范，从而增加了在未来进一步成功攻击的难度；
- 遭受惩罚（如罚款或入狱等）；
- 危及生命安全。

1.2 计算机网络的不安全因素

一般来说，计算机网络本身的脆弱性和通信设施脆弱性共同构成了计算机网络的潜在威胁。一方面，计算机系统硬件和通信设施极易遭受到自然环境的影响（如：温度、湿度、灰尘度和电磁场等），以及自然灾害（如：洪水、地震等）和人为（故意破坏和非故意破坏）的物理破坏；另一方面，计算机网络的软件资源和数据信息易受到非法的窃取、复制、篡改和毁坏；再有，计算机网络硬件的自然损耗和自然失效，软件的逻辑错误，同样会影响系统的正常工作，造成计算机网络系统内信息的损坏、丢失和安全事故。

1.2.1 不安全的主要因素

对计算机网络安全构成威胁的因素很多，综合起来包括：

偶发性因素：如电源故障、设备的机能失常、软件开发过程中留下的某种漏洞或逻辑错误等。

自然灾害：各种自然灾害（如地震、风暴、泥石流、建筑物破坏等）对计算机网络构成威胁。此外，火灾、水灾、空气污染也对计算机网络构成严重威胁。

人为因素：一些不法之徒，利用计算机网络或潜入计算机房，篡改系统数据、窃用系统资源、非法获取机密数据和信息、破坏硬件设备、编制计算机病毒等。此外，管理不好、规章制度不健全、有章不循、安全管理水平低、人员素质差、操作失误、渎职行为等都会对计算机网络造成威胁。

对计算机网络安全威胁最大的是人为因素，也称作人对计算机网络的攻击，可分为几个方面。

1. 被动攻击

这类攻击主要是监视公共媒体（如无线电、卫星、微波和公共交换网）上的信息传送，典型的被动攻击如表 1-3。抵抗这类攻击的对策包括使用虚拟专用网 VPN，加密被保护网络，以及使用加保护的分布式网络。

表 1-3 典型被动攻击举例

攻　击	描　述
监视明文	监视网络，获取未加密的信息
解密通信数据	通过密码分析，破解网络中传输的加密数据
口令嗅探	使用协议分析工具，捕获用于各类系统访问的口令
通信量分析	不对加密数据进行解密，而是通过对外部通信模式的观察，获取关键信息。例如，通信模式的改变可以暗示紧急行动

2. 主动攻击

主动攻击是指避开或打破安全防护、引入恶意代码（如计算机病毒），破坏数据和系统的完整性，典型的主动攻击如表 1-4。典型对策是增强内部网络的保护（如防火墙和边界护卫），采用基于身份认证的访问控制、远程访问保护、质量安全管理、自动病毒检测、审计和入侵检测等

技术。

表 1-4 典型主动攻击举例

攻　击	描　述
修改传输中的数据	截获并修改网络中传输的数据，例如修改电子交易数据，从而改变交易的数量或者将交易转移到别的帐户
重放	将旧的消息重新反复发送，造成网络效率降低
会话拦截	未授权使用一个已经建立的会话
伪装成授权的用户或服务器	这类攻击者将自己伪装成他人，从而未授权访问资源和信息。一般过程是，先利用嗅探或其他手段获得用户/管理员信息，然后作为一个授权用户登陆。这类攻击也包括获取敏感数据的欺骗服务器，通过与未产生怀疑的用户建立信任服务关系来实施攻击
利用系统软件漏洞	攻击者探求以系统权限运行的软件中存在的脆弱性。例如针对 sendmail 和 X-Windows 服务器缺陷的攻击。几乎每天都能发现软件和硬件平台中新的脆弱性
利用主机或网络信任	攻击者通过操纵文件，使虚拟/远方主机提供服务，从而获得信任。典型的攻击有 rhost 和 rlogin
利用恶意代码	攻击者通过系统的脆弱性进入用户系统，并向系统内植入恶意代码；或者是，将恶意代码植入看起来无害的供下载的软件或电子邮件中，从而使用户去执行恶意代码
利用协议或基础设施的系统缺陷	攻击者利用协议中的缺陷来欺骗用户或重定向通信量。这类攻击包括：哄骗域名服务器进行未授权远程登陆；使用 ICMP 炸弹使某个机器离线；源路由伪装成信任主机源；TCP 序列号猜测获得访问权；为截获合法连接而进行 TCP 组合等
拒绝服务	攻击者有很多实施拒绝服务的攻击方法，包括有效地将一个路由器从网络中脱离的 ICMP 炸弹；在网络中扩散垃圾包；向邮件中心发送垃圾邮件等

3. 邻近攻击

邻近攻击是指未授权者可物理上接近网络、系统或设备，从而可以修改、收集信息，或使系统拒绝访问，典型的临近攻击如表 1-5。接近网络可以是秘密进入或公开，也可以是两者都有。

表 1-5 临近攻击举例

攻　击	描　述
修改数据或收集信息	攻击者获取系统管理权，从而修改或窃取信息，如：IP 地址、登录的用户名和口令等
系统干涉	攻击者获取系统访问权，从而干涉系统的正常运行
物理破坏	该攻击获取系统物理设备访问权，从而对设备进行物理破坏

4. 内部人员攻击

内部工作人员具有对系统的直接访问权，可轻易地对系统实施攻击。内部人员攻击分为恶意和非恶意(不小心或无知行为)两种。因为非恶意行为也会导致安全事件，故非恶意破坏也被认为是一种攻击，典型的内部人员攻击如表 1-6。

表 1-6 内部人员攻击举例

攻击		描述
恶意	修改数据或安全机制	内部人员直接使用网络，具有系统的访问权。因此，内部人员攻击者比较容易实施未授权操作或破坏数据
	擅自连接网络	对涉密网络具有物理访问能力的人员，擅自将机密网络与密级较低的网络或公共网络连接，违背涉密网络的安全策略和保密规定
	隐通道	隐通道是未授权的通信路径，用于从本地网向远程站点传输盗取的信息
	物理损坏或破坏	对系统具有物理访问权限的工作人员，对系统故意破坏或损坏
非恶意	修改数据	由于缺乏知识或粗心大意，修改或破坏数据或系统信息
	物理损坏或破坏	由于渎职或违反操作规程，对系统的物理设备造成意外损坏或破坏

恶意内部人员攻击：根据美国联邦调查局的评估，80%的攻击和入侵来自内部。内部人员知道系统的布局、有价值的数据在何处以及系统所采用的安全防范措施。而且，内部人员的攻击常常是最难于检测和防范的。

非恶意内部人员攻击：这类攻击，并非故意破坏信息或信息处理系统，而是由于无意的行为对系统产生了破坏。这些破坏一般是由于缺乏知识或不小心所致。

典型对策包括：加强安全意识和技术培训；对系统的关键数据、服务采取特殊的访问控制机制；采用审计、入侵检测等技术。

5. 分发攻击

分发攻击是指在软件和硬件开发出来后和安装之前，当它从一个地方送到另一个地方时，攻击者恶意地修改软硬件，典型的分发攻击如表 1-7。可以通过受控分发，以及由最终用户检验软件签名和访问控制来消除分发威胁。

表 1-7 分发攻击举例

攻击	描述
在设备商的设备上修改软硬件	当软件和硬件在生产线上流通时，通过修改软硬件配置来实施这类攻击
在产品分发时修改软硬件	在产品分发期内修改软硬件配置(如安装窃听设备)

1.2.2 不安全的主要原因

计算机网络安全的脆弱性是伴随计算机网络一同产生的，换句话说，安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中，网络特性决定了不可能无条件、无限制地提高其安全性能。要使网络方便快捷，又要保证网络安全，这是一个非常棘手的“两难选择”，而网络安全只能在“两难选择”所允许的范围中寻找支撑点。因此，可以说任何一个计算机网络都不是绝对安全的。

1. 互联网具有的不安全性

最初，互联网用于科研和学术目的，它的技术基础存在不安全性。互联网是对全世界所有国家开放的网络，任何团体或个人都可以在网上方便地传送和获取各种各样的信息，具有开放性、国际性和自由性，这就对网络安全提出了挑战。互联网的不安全性主要表现在如下

方面：

- 网络的开放性，导致网络的技术是全开放的，使得网络所面临的破坏和攻击来自多方面。可能来自物理传输线路的攻击，也可能来自对网络通信协议的攻击，以及对软件和硬件实施的攻击。
- 网络的国际性，意味着网络的攻击不仅来自本地网络的用户，而且可以来自互联网上的任何一个机器，也就是说，网络安全面临的是国际化的挑战。
- 网络的自由性，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。

另外，互联网使用的 TCP/IP(传输控制协议/网际协议)，以及 FTP(文件传输协议)、E-mail(电子邮件)、RPC(远程程序通信规则)、NFS(网络文件系统)等都含有许多不安全的因素，存在着许多安全漏洞。

2. 操作系统存在的安全问题

操作系统软件自身的不安全性，以及系统设计时的疏忽或考虑不周而留下的“破绽”，都给网络安全留下了许多“后门”。

操作系统的体系结构造成的不安全性是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的，例如：I/O 的驱动程序和系统服务，这些程序和服务可以通过打“补丁”的方式进行动态连接，许多 UNIX 操作系统的版本升级也都是采用打补丁的方式进行的。这种动态连接的方法容易被黑客所利用，并且也是计算机病毒产生的环境。另外，操作系统的一些功能也带来不安全因素，例如支持在网络上传输可以执行的文件映像，网络加载程序等。

操作系统不安全的另一原因在于它可以创建进程，支持进程的远程创建与激活，支持被创建的进程继承创建进程的权利，这些机制提供了在远端服务器上安装“间谍”软件的条件。若将间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，黑客或间谍软件就可以使系统进程与作业的监视程序都监测不到它的存在。

操作系统的无口令入口，以及隐蔽通道(原是为系统开发人员提供的便捷入口)，也是黑客入侵的通道。

3. 数据的安全问题

在网络中，数据是存放在数据库中的，供不同的用户共享。然而，数据库存在许多不安全因素，例如：授权用户超出了访问权限进行数据的更改活动；非法用户绕过安全内核，窃取信息资源等。对于数据库的安全而言，就是要保证数据的安全可靠和正确有效，即确保数据的安全性、完整性和并发控制。数据的安全性就是防止数据库被故意的破坏和非法的存取；数据的完整性是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入、输出而造成无效操作和错误结果；并发控制就是在多个用户程序并行存取数据时，保证数据库的一致性。

4. 传输线路的安全问题

尽管在光缆、同轴电缆、微波、卫星通信中窃听其中指定一路的信息是很困难的，但是从安全的角度来说，没有绝对安全的通信线路。

5. 网络安全管理问题

网络系统缺少安全管理人员，缺少安全管理的技术规范，缺少定期的安全测试与检查，缺少安全监控，是网络最大的安全问题之一。

1.3 计算机网络安全的概念

计算机网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

1.3.1 计算机网络安全的定义

计算机网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，信息数据的机密性、完整性及可使用性受到保护。要做到这一点，必须保证网络系统软件、应用软件、数据库系统具有一定的安全保护功能，并保证网络部件如终端、调制解调器、数据链路的功能仅仅能被那些被授权的人访问。网络的安全问题实际上包括两方面的内容，一是网络的系统安全，二是网络的信息安全，而保护网络的信息安全是最终目的。

从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、不可否认性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义随着角度的变化而变化。从用户（个人、企业等）的角度来说，希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和不可否认性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯，即用户的利益和隐私不被非法窃取和破坏。从网络运行和管理者角度说，希望其网络的访问、读写等操作受到保护和控制，避免出现“后门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御黑客的攻击。对安全保密部门来说，希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，避免给国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容、会对社会的稳定和人类的发展造成威胁，必须对其进行控制。

1.3.2 计算机网络安全的目标

从计算机网络安全定义中可以看出，计算机网络安全应达到以下目标：

1. **保密性**

是指网络中的保密信息只供经过允许的人员，以经过允许的方式使用，信息不泄露给非授权用户、实体或过程，或供其利用。从技术上说，任何传输线路，包括电缆（双绞或同轴）、光缆、微波和卫星，都可能被窃听。提供保密性安全服务取决于若干因素：

- 需保护数据的位置：数据可能存放于个人机器中（如硬盘或服务器中）、局域网的线路上或其他流通机制（如软盘）上，也可能流经一个完全公开的媒体（如穿过互联网或通信卫星）；
- 需保护数据的类型：数据元素可以是本地文件（如口令或密钥）、网络协议所携带的数据、网络协议的信息交换（如一个协议数据单元）；
- 需保护数据的数量或部分：保护整个数据元素、部分数据单元、还是协议数据单元；
- 需保护数据的价值：被保护数据的敏感性，以及数据对用户的价值。

保密性的要素如下：

- 数据保护：防止信息内容的泄露（如网络中的数据流）；
- 数据隔离：提供隔离路径或采用过程隔离（COMPUSEC 技术等）；

- 通信流保护：数据的特征包括频率、数量、通信流的目的地等，通信流保护是指对通信的特征信息，以及推断信息（如命令结构等）进行保护。

2. **完整性**

是指网络中的信息安全、精确与有效，不因种种不安全因素而改变信息原有的内容、形式与流向。确保信息在存储或传输过程中不被修改、不被破坏和丢失。

破坏信息的完整性既有人为因素，也有非人为因素。非人为因素是指通信传输中的干扰噪声、系统硬件或软件的差错等。人为因素包括有意和无意两种，前者是非法分子对计算机的侵入、合法用户越权对数据进行处理，以及隐藏的破坏性程序（计算机病毒、时间炸弹、逻辑陷阱等）等；无意危害是指操作失误或使用不当。完整性被破坏是计算机网络安全的主要威胁。另外，信息完整性是一个很广泛的问题，例如分布式数据库中并发性操作或者对多个数据副本的更新所引起数据的一致性问题；又如，由于系统的设计不完善造成使用不当或操作失误所引起的数据完整性问题等。

提供完整性服务的要求与保密性服务的要求相似。包括需要保护的数据的位置、类型、数量及内容。

3. **可用性**

指网络资源在需要时即可使用，不因系统故障或误操作等使资源丢失或妨碍对资源的使用，是被授权实体按需求访问的特性。在网络环境下，拒绝服务、破坏网络和系统的正常运行等都属于对可用性的攻击。

网络可用性还包括在某些不正常条件下继续运行的能力。对网络可用性的破坏包括合法用户不能正常访问网络资源和有严格时间要求的服务不能得到及时响应。影响网络可用性的因素包括人为与非人为两种。前者是指非法占用网络资源、切断或阻塞网络通信、降低网络性能、甚至使网络瘫痪等。后者是指灾害事故（火、水、雷击等）和系统死锁、系统故障等。

保证可用性的最有效的方法是提供一个具有普适安全服务的安全网络环境。通过使用访问控制阻止对未授权资源访问，利用完整性和保密性服务来防止可用性攻击。访问控制、完整性和保密性成为协助支持可用性安全服务的机制。

- 避免受到攻击：一些基于网络的攻击旨在破坏、降级或摧毁网络资源。解决办法是加强这些资源的安全防护，使其不受攻击。免受攻击的方法包括：关闭操作系统和网络配置中的安全漏洞；控制授权实体对资源的访问；防止路由表等敏感网络数据的泄露；
- 避免未授权使用：当资源被使用、占用、过载时，其可用性就会受到限制。如果未授权用户占用了有限的资源（如处理能力、网络带宽、调制解调器连接等），则这些资源对授权用户就是不可用的，通过访问控制可以限制未授权使用；
- 防止进程失败：操作失误和设备故障也会导致系统可用性降低。解决方法是使用高可靠性设备、提供设备冗余和提供多路径的网络连接等。

4. **不可否认性**

“否认”指参与通信的实体拒绝承认它参加了那次通信，不可否认是保证信息行为人不能否认其信息行为。不可否认性安全服务提供了向第三方证明该实体确实参与了那次通信的能力。

- 数据的接收者提供数据发送者身份及原始发送时间的证据；
- 数据的发送者提供数据已交付接收者（某些情况下，包括接收时间）的证据；
- 审计服务提供了信息交换中各参与方的可审计性，这种可审计性记录了可用来跟踪某

些人的相关事件，这些人应对其行为负责。

不可否认性服务主要由应用层提供。通常用户最关心的是应用程序数据（如电子邮件和文件）的不可否认性。在底层提供不可否认性功能，仅能证明产生过的连接，而无法将流经该连接的数据同特定的实体相绑定。

5. **可控性**

是指对信息的传播及内容具有控制能力、保证信息和信息系统的授权认证和监控管理，确保某个实体（人或系统）身份的真实性，也可以确保执法者对社会的执法管理行为。

1.3.3 计算机网络安全所涉及的内容

网络安全所研究的主要内容包括：

- 网络安全体系结构；
- 网络的攻击手段与防范措施；
- 网络安全设计；
- 网络安全标准制定、安全评测及认证；
- 网络安全检测技术；
- 网络安全设备；
- 安全管理，安全审计；
- 网络犯罪侦查；
- 网络安全理论与政策；
- 网络安全教育；
- 网络安全法律。

概括起来，网络安全包括三个重要部分，即：

- 先进的技术：先进的安全技术是网络安全的根本保障，用户通过风险评估，决定所需的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。
- 严格的管理：即使用网络的机构、企业和单位建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。
- 威严的法律：安全的基石是社会法律、法规与手段，通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

1.4 计算机网络安全体系结构

研究计算机网络安全的体系结构，就是研究如何从管理和技术上保证网络的安全得以完整准确地实现，网络安全需求得以全面准确的满足。

1.4.1 OSI 安全体系结构

OSI 安全体系结构的研究始于 1982 年，当时 OSI 基本参考模型刚刚确立。这项工作由 ISO/IEC JTC1/SC21 完成，结束于 1988 年，其成果标志是 ISO 发布了 ISO 7498-2 标准，作为 OSI 基本参考模型的新补充。1990 年，ITU 决定采用 ISO7498-2 作为它的 X.800 推荐标准，我国的国标 GB/T 9387.2-1995《信息处理系统 开放系统互连 基本参考模型 第 2 部分：安全

体系结构》等同于 ISO/IEC 7498-2。

OSI 安全体系结构不是能实现的标准，而是如何设计标准的标准。因此，具体产品不应声称自己遵从这一标准。OSI 安全体系结构定义了许多术语和概念，还建立了一些重要的结构性准则。它们中有一部分已经过时，仍然有用的部分主要是术语、安全服务和安全机制的定义。

1. 术语

OSI 安全体系结构给出了标准族中的部分术语的正式定义，其所定义的术语只限于 OSI 体系结构，在其他标准中对某些术语采用了更广的定义。

2. 安全服务

OSI 安全体系结构中定义了五大类安全服务，也称为安全防护措施。

鉴别服务：提供对通信中对等实体和数据来源的鉴别。对等实体鉴别提供对实体本身的身份进行鉴别；数据源鉴别提供对某个数据项是否来自某个特定实体进行鉴别。

访问控制服务：对资源提供保护，以对抗非授权使用和操纵。

数据机密性服务：保护信息不被泄漏或暴露给未授权的实体。机密性服务又分为数据机密性服务和业务流机密性服务，数据机密性服务包括：连接机密性服务，对某个连接上传输的所有数据进行加密；无连接机密性服务，对构成一个无连接数据单元的所有数据进行加密；选择字段机密性服务，仅对某个数据单元中所指定的字段进行加密。业务流机密性服务使攻击者很难通过网络的业务流来获得敏感信息。

数据完整性服务：对数据提供保护，以对抗未授权的改变、删除或替代。完整性服务有三种类型：连接完整性服务，对某个连接上传输的所有数据进行完整性保护，确保收到的数据没有被插入、篡改、重排序或延迟；无连接完整性服务，对无连接数据单元的数据进行完整性保护；选择字段完整性服务，对某个数据单元中所指定的字段进行完整性保护。

完整性服务还分为具有恢复功能和不具有恢复功能两种类型。如果仅能检测和报告信息完整性被破坏，而不采取进一步措施的服务为不具有恢复功能的完整性服务；如果能检测到信息完整性被破坏，并能将信息正确恢复的服务为具有恢复功能的完整性服务。

抗抵赖性服务：防止参与某次通信交换的任何一方事后否认本次通信或通信内容。抗抵赖服务可分为两种不同的形式：数据原发证明的抗抵赖，使发送者不承认曾经发送过这些数据或否认其内容的企图不能得逞；交付证明的抗抵赖，使接收者不承认曾收到这些数据或否认其内容的企图不能得逞。

表 1-8 给出了对付典型网络威胁的安全服务，表 1-9 给出了网络各层提供的安全服务。

表 1-8 对付典型网络威胁的安全服务

安全威胁	安全服务
假冒攻击	鉴别服务
非授权侵犯	访问控制服务
窃听攻击	数据机密性服务
完整性破坏	数据完整性服务
服务否认	抗抵赖服务
拒绝服务	鉴别服务、访问控制服务、数据完整性服务等

表 1-9　网络各层提供的安全服务

安全服务 \ 协议层		物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
鉴别	对等实体鉴别			√	√			√
	数据原发鉴别			√	√			√
访问控制				√	√			√
数据机密性	连接机密性	√	√	√	√		√	√
	无连接机密性		√	√	√		√	√
	选择字段机密性						√	√
	业务机密性	√		√				√
数据完整性	可恢复的连接完整性				√			√
	不可恢复的连接完整性			√	√			√
	选择字段的连接完整性							√
	无连接完整性			√	√			√
	选择字段的无连接完整性							√
抗抵赖性	数据原发证明的抗抵赖							√
	交付证明的抗抵赖							√

3. 安全机制

OSI 安全体系结构没有详细说明安全服务应该如何来实现。作为指南，它给出了一系列可用来实现这些安全服务的安全机制，基本的机制有：

加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务流填充机制、路由控制、公证机制(把数据向可信第三方注册，以便在将来可使人相信数据的内容、来源、时间和传递过程)。计算机网络安全体系，安全服务与安全机制的关系见图 1-1 和表 1-10。

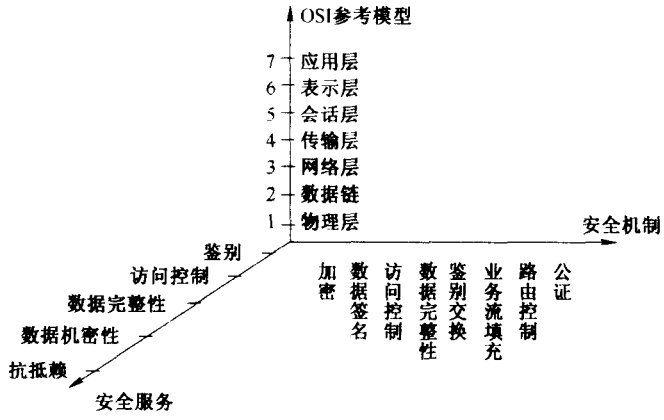


图 1-1　计算机网络安全体系结构三维图