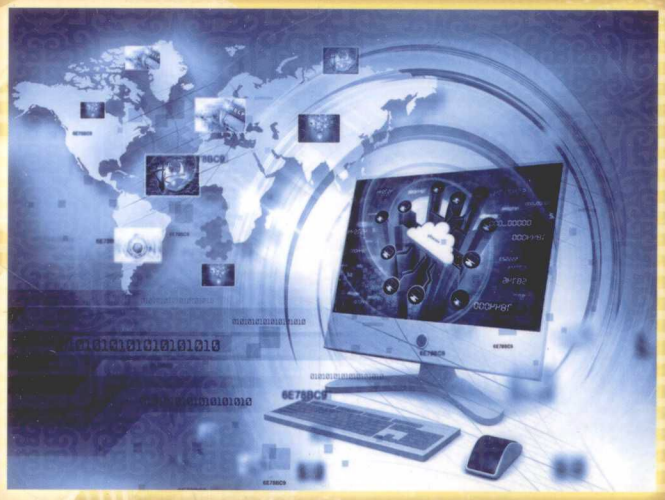
“十三五”国家重点出版物出版规划项目

高等教育规划教材

计算机网络安全教程

第3版

梁亚声　汪永益　刘京菊
汪　生　王永杰　编著



提供电子教案

http://www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

“十三五”国家重点出版物出版规划项目
高等教育规划教材

计算机网络安全教程

第3版

梁亚声　汪永益　刘京菊　汪 生　王永杰 编著

机械工业出版社

本书系统地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 技术、防火墙技术、入侵检测技术、操作系统与数据库安全技术、网络安全检测与评估技术、计算机病毒与恶意代码防范技术、数据备份技术、无线网络安全、云计算安全及网络安全解决方案。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、网络工程和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、网络管理人员和信息安全管理人员的技术参考书。

本书配有授课电子课件，需要的教师可登录 www.cmpedu.com 免费注册，审核通过后下载，或联系编辑索取（QQ：2850823885，电话：010-88379739）。

图书在版编目（CIP）数据

计算机网络安全教程 / 梁亚声等编著. —3 版. —北京：机械工业出版社，2016.4
高等教育规划教材
ISBN 978-7-111-53752-6

Ⅰ. ①计… Ⅱ. ①梁… Ⅲ. ①计算机网络－安全技术－高等学校－教材
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2016）第 103913 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：郝建伟 责任校对：张艳霞
责任印制：李 洋
北京宝昌彩色印刷有限公司印刷
2016 年 8 月第 3 版 • 第 1 次印刷
184mm×260mm • 22 印张 • 540 千字
0001－3000 册
标准书号：ISBN 978-7-111-53752-6
定价：49.90 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
服务咨询热线：（010）88379833
读者购书热线：（010）88379649

网络服务
机 工 官 网：www.cmpbook.com
机 工 官 博：weibo.com/cmp1952
教育服务网：www.cmpedu.com
金 书 网：www.golden-book.com

出 版 说 明

当前，我国正处在加快转变经济发展方式、推动产业转型升级的关键时期。为经济转型升级提供高层次人才，是高等院校最重要的历史使命和战略任务之一。高等教育要培养基础性、学术型人才，但更重要的是加大力度培养多规格、多样化的应用型、复合型人才。

为顺应高等教育迅猛发展的趋势，配合高等院校的教学改革，满足高质量高校教材的迫切需求，机械工业出版社邀请了全国多所高等院校的专家、一线教师及教务部门，通过充分的调研和讨论，针对相关课程的特点，总结教学中的实践经验，组织出版了这套“高等教育规划教材”。

本套教材具有以下特点：

1）符合高等院校各专业人才的培养目标及课程体系的设置，注重培养学生的应用能力，加大案例篇幅或实训内容，强调知识、能力与素质的综合训练。

2）针对多数学生的学习特点，采用通俗易懂的方法讲解知识，逻辑性强、层次分明、叙述准确而精炼、图文并茂，使学生可以快速掌握，学以致用。

3）凝结一线骨干教师的课程改革和教学研究成果，融合先进的教学理念，在教学内容和方法上做出创新。

4）为了体现建设“立体化”精品教材的宗旨，本套教材为主干课程配备了电子教案、学习与上机指导、习题解答、源代码或源程序、教学大纲、课程设计和毕业设计指导等资源。

5）注重教材的实用性、通用性，适合各类高等院校、高等职业学校及相关院校的教学，也可作为各类培训班的教材和自学用书。

欢迎教育界的专家和老师提出宝贵的意见和建议。衷心感谢广大教育工作者和读者的支持与帮助！

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。如何保证个人、企业及国家的机密信息不被黑客和间谍窃取，如何保证计算机网络不间断地工作，是国家和企业信息化建设必须考虑的重要问题。然而，计算机网络安全问题错综复杂，涉及面非常广，有技术因素，也有管理因素；有自然因素，也有人为因素；有外部的安全威胁，还有内部的安全隐患。

本书紧密结合计算机网络安全技术的最新发展，不断更新内容，在操作系统、无线网络和云计算等方面，对《计算机网络安全教程》（第2版）进行了调整、补充和完善。

本书共12章，第1章主要介绍计算机网络的相关概念和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技术。第3章主要介绍信息加密与PKI技术，包括密码学基础、加密体制、古典密码/单钥加密/双钥加密/同态加密等加密算法、信息加密技术应用、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、应用代理、状态检测、NAT等防火墙技术，以及防火墙的应用和个人防火墙。第5章主要介绍入侵检测技术，包括入侵检测的基本原理、系统结构、系统分类、技术实现、分布式入侵检测、入侵检测系统的标准、入侵防护系统和入侵检测系统的应用。第6章主要介绍操作系统和数据库安全技术，包括访问控制技术、操作系统的安全技术、UNIX/Linux/Windows 7系统安全技术、数据库安全机制及安全技术。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和检测技术、网络安全评估标准和方法，以及网络安全评估系统。第8章主要介绍计算机病毒与恶意代码防范技术，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，以及恶意代码的防范技术。第9章主要介绍数据备份技术，包括磁盘备份、双机备份、网络备份技术、数据备份方案、数据备份与恢复策略，以及备份软件。第10章主要介绍无线网络的安全技术，包括Wi-Fi和无线局域网安全、移动终端安全、无线安全技术及应用。第11章主要介绍云计算安全，包括云安全威胁和安全需求、云计算安全架构和云计算安全技术。第12章主要介绍网络安全解决方案，包括网络安全体系结构，以及企业和单机用户网络安全解决方案。

本书具有以下主要特点。

1）在内容安排上具有全面性和系统性，本书从计算机网络安全的体系结构、软硬件安全、安全设计和管理等方面，系统地介绍了计算机网络完全的基础理论、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。

2）在介绍技术时注重理论性和实用性，对于每种网络安全技术，首先介绍技术的理论基础和原理，再通过具体的实例介绍安全技术的应用和操作方法。

3）在章节编排上具有独立性和完整性，虽然本书涉及的内容十分广泛，但通过合理安排章节，使各章节内容相对独立，在实施教学时可结合教学对象和实际情况，进行适当的选取和编排。

本书由梁亚声编写第1章并统稿，汪永益编写第4、8、9章，刘京菊编写第2、7、12章，汪生编写第3、5、6章，王永杰编写第10、11章。

由于作者水平有限，书中难免存在不妥之处，敬请广大读者批评指正。

编　者

目　录

第1章 绪 论

在信息化时代，互联网在全球范围掀起一场影响人类所有层面的深刻变革，实现了基于企业内部网（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。随着政府上网、企业上网、教育上网、家庭上网等的普及，计算机网络在经济、军事和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，也使人类面临着信息安全的巨大挑战。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、银行资金转账、股票证券、能源资源、国防和科研等大量关系国计民生的重要信息，许多重要信息直接关系到国家的安全。如何保护个人、企业和国家的机密信息不受黑客和间谍的入侵，如何保证网络系统安全地、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。

有关计算机安全技术的研究始于 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，应用的范围也在不断扩大，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

实体是指计算机网络中的关键设备，包括各类计算机（服务器、工作站等）、网络和通信设备（路由器、交换机、集线器、调制解调器和加密机等）、存放数据的媒体（磁带、磁盘和光盘等）、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。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系统的严重威胁，1990 年在

美国全国范围内掀起了一场“扫黑大行动”。2014 年 4 月爆出了 Heartbleed（心脏出血）漏洞，涉及各大网银、门户网站等，该漏洞可被用于窃取服务器敏感信息，实时抓取用户的账号密码。在漏洞被公开后到系统被修复前这段时间内，该漏洞已经被利用，有些网站用户信息或许已经被黑客非法获取。2014 年 12 月，索尼影业公司被黑客攻击，摄制计划、明星隐私及未发表的剧本等敏感数据都被黑客窃取，并逐步公布在网络上，预计索尼影业损失高达 1 亿美元。

计算机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。表 1-1 所示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、删除或插入后，再发送给接收者
非授权访问	通过假冒、身份攻击或系统漏洞等手段，获取系统访问权，从而使非法用户进入网络系统读取、删除、修改或插入信息等
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
APT（Advanced Persistent Threat，高级持续性威胁）攻击	利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。 APT 在发动攻击之前对攻击对象的业务流程和目标系统进行精确的收集，挖掘被攻击对象受信系统和应用程序的漏洞，利用 0day 漏洞进行攻击
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　恶意程序的威胁

以计算机病毒、网络蠕虫、间谍软件和木马程序等为代表的恶意程序时刻都威胁着计算机网络的安全。

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。在恶作剧心态的操纵下，罗伯特利用 UNIX 系统中 Sendmail、Finger 和 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 Internet 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 10 多万台计算机瘫痪，韩国 24 万多台计算机受影响，马来西亚 12 个股票交易所受到侵害。

计算机病毒可以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。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”发作在全球所造成的损失就高达 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 计算机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怀有恶意的，也有非恶意的。网络威胁的潜在对手举例如表 1-2 所示。

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	寻找网络系统的脆弱性及其缺陷，进而攻击网络
	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，以强迫、恐吓政府或社会以满足其需要为目的
	有组织的计算机犯罪	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	具有访问系统的条件，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，影响计算机系统正常运行。

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，寻求简单方法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如下。

- 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（如计算机资源或用网络）。
- 向安全机制进行技术挑战。

从信息系统方面看，这些动机具有以下 3 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，面临着一定风险，这些风险包括以下几个。

- 暴露其攻击能力。
- 打草惊蛇，使对手有所防范，从而增加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，计算机网络的硬件和通信设施极易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，以及软件的逻辑错误，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，综合起来包括以下三个方面。

- **偶发因素**：如电源故障、设备的机能失常、软件开发过程中留下的漏洞或逻辑错误等。
- **自然灾害**：各种自然灾害（如地震、风暴、泥石流和建筑物破坏等）对计算机系统构成严重的威胁。此外，火灾、水灾和空气污染也对计算机网络构成严重威胁。
- **人为因素**：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、破坏硬件设备或编制计算机病毒等。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，以及渎职行为等都会对计算机网络造成威胁。

人为因素对计算机网络的破坏也称为人对计算机网络的攻击，可分为下列几个方面。

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）上传送的信息，典型的被动攻击如表 1-3 所示。抵抗这类攻击的对策主要包括：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

主动攻击主要是避开或突破安全防护、引入恶意代码（如计算机病毒），以及破坏数据和

系统的完整性，典型的主动攻击如表 1-4 所示。抵抗这类攻击的对策主要包括：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账户
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录。这类攻击也包括用于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
利用系统软件的漏洞	攻击者探求以系统权限运行的软件中存在的脆弱性。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：哄骗域名服务器以进行未授权远程登录，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，以及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 所示。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　邻近攻击举例

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。非恶意行为也会导致安全事件，因此，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 所示。

1）内部人员的恶意攻击：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，内部人员的攻击通常是最难以检测和防范的。

2）内部人员的非恶意攻击：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，对系统的关键数据和服务采取特殊的访问控

制机制，采用审计、入侵检测等技术。

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

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件或硬件，典型的分发攻击如表 1-7 所示。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攻击威胁。

表 1-7　分发攻击举例

攻　击	描　述
在设备生产时修改软、硬件	当软件和硬件在生产线上时，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

计算机网络系统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。既要使网络方便快捷，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”所允许的范围内寻找平衡点。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，这就对安全提出了更高的要求，主要表现在以下三个方面。

- **开放性的网络**：导致网络的技术全开放，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。
- **国际性的网络**：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台计算机，也就是说，网络安全面临的是国际化的挑战。
- **自由性的网络**：意味着网络最初对用户的使用并没有提供任何技术约束，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）和 NFS（网络文件系统）等都包含许多不安全的因素，存在许多安全漏洞。

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”，都给危害网络安全的人留下了许多“后门”。

操作系统体系结构造成的不安全隐患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，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和开发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利用，而且还是计算机病毒产生的好环境。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，以及网络加载程序的功能等。

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及隐蔽通道（原是为系统开发人员提供的便捷入口），也都成为黑客入侵的通道。

3．数据的安全问题

在网络中，数据存放在数据库中，供不同的用户共享。然而，数据库存在着许多不安全性，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，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破坏和非法存取；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地存取数据库时，保证数据库的一致性。

4．传输线路安全问题

尽管在光缆、同轴电缆、微波和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．网络应用存在的安全问题

伴随着互联网更加开放，用户开展的业务也更加丰富多彩，终端智能普遍使用，数据中心和各种云的建设应用，网络的安全问题也出现了新的形式及特点，应用安全问题已经成为移动互联网网络推广的主要问题。

6．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、数论和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，必须保证网络的系统软件、应用软件和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、调制解调器和数据链路等）的功能只能被授权的人们访问。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会随着“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、篡改和抵赖等手段侵犯，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来说，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，以及网络资源被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，避免对社会造成危害，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阻碍，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几个目标。

1．保密性

保密性是指网络中的保密信息只能供经过允许的人员，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，都是可能被窃听的。提供保密性安全服务取决以下若干因素。

- **需保护数据的位置**：数据可能存放在 PC 或服务器、局域网的线路上，或其他流通机制（如磁带、U 盘和光盘等）上，也可能流经一个完全公开的媒体（如经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和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、部分数据单元或协议数据单元。
- **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。
- **数据隔离**：提供隔离路径或采用过程隔离。
- **通信流保护**：数据的特征，包括：频率、数量和通信流的目的地等，通信流保护是指对通信的特征信息及推断信息（如命令结构等）进行保护。

2．完整性

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、不被破坏和不丢失。