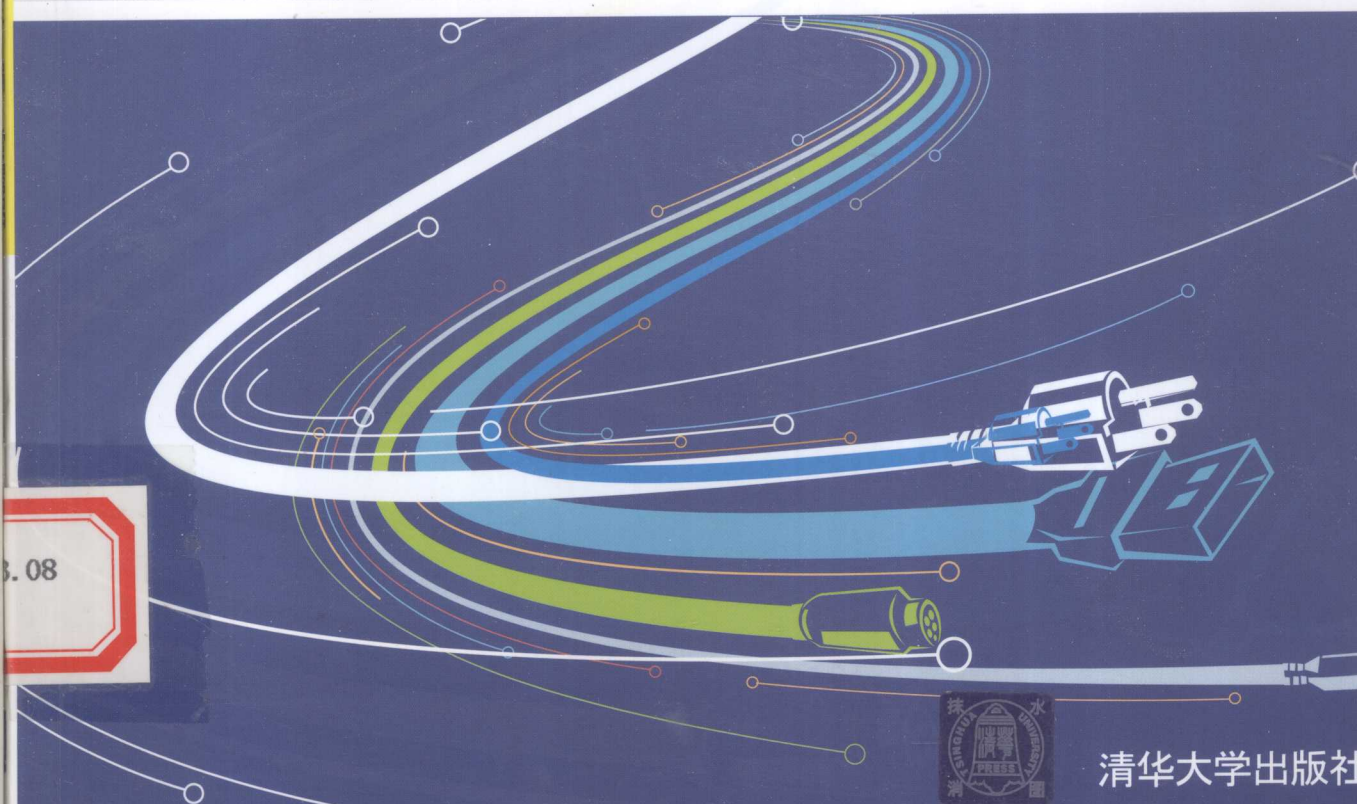
课件下载：www.tup.com.cn

- 数据加密技术
- 网络操作系统安全
- 数据库安全
- PKI技术、防火墙技术
- 网络扫描和网络监听
- Internet安全、VPN和IPSec

计算机网络安全技术与应用

主　编　雷渭侣
副主编　王兰波

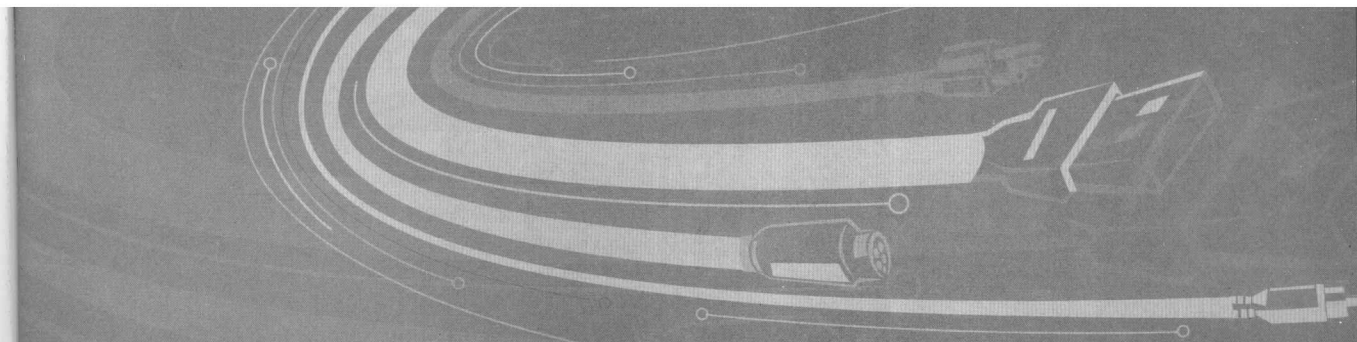


清华大学出版社

- 数据加密技术
- 网络操作系统安全
- 数据库安全
- PKI技术、防火墙技术
- 网络扫描和网络监听
- Internet安全、VPN和IPSec

计算机网络安全技术与应用

主　编　雷渭侣
副主编　王兰波
编　著　师　平　许丽娟　李　康



清华大学出版社
北　京

内 容 简 介

本书将计算机网络安全技术的基本理论与实际应用相结合，系统地介绍了计算机网络安全的基本概念以及网络安全体系结构、数据加密技术、网络操作系统安全、数据库与数据的安全、PKI 技术、防火墙工作原理及应用、计算机病毒防治、入侵检测系统、Internet 安全、VPN 和 IPSec 技术以及无线网络安全技术，各章均配有小结、练习与思考题，便于教学和自学。此外，附录部分还给出了网络安全实验的建议及题目。

本书内容安排合理，逻辑性强，语言表达通俗易懂，实例典型实用，可作为高等院校信息学科应用型本科学生计算机网络安全技术课程的教材，也可供从事计算机网络安全维护及管理的工程技术人员阅读参考。

图书在版编目（CIP）数据

计算机网络安全技术与应用/雷渭侣主编. —北京：清华大学出版社，2010.1

ISBN 978-7-302-21366-6

I. 计… II. 雷… 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（2009）第 190337 号

责任编辑：陈仕云　王　飞　纪文远
封面设计：张　岩
版式设计：杨　洋
责任校对：姜　彦
责任印制：李红英
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：23.25　**字　数**：537 千字
版　　次：2010 年 1 月第 1 版　　**印　　次**：2010 年 1 月第1 次印刷
印　　数：1～4000
定　　价：32.00 元

前言

随着 Internet 和 Intranet 技术的广泛应用，计算机网络资源共享进一步加强，但与此同时网络安全问题（既有来自外部的黑客攻击，也有来自内部的威胁）也变得日益突出，网络安全面临重大挑战。事实上，资源共享和信息安全历来就是一对矛盾，而计算机网络的开放性决定了网络安全问题是先天存在的，TCP/IP 框架基本上是不设防的。那么如何切实有效地保护计算机网络安全呢？您将从本书中找到答案。

本书根据作者多年从事本课程教学的讲稿，以及近几年来主编出版的 3 本计算机网络教材，并结合计算机网络安全技术的实际应用，综合计算机网络安全技术的发展现状编写而成。本书可作为普通高等院校计算机专业本科生计算机网络安全技术课程的教材，也可供信息学科非计算机专业本科生、成人教育学生、职业技术学院学生参考、学习。参考学时为 32～48 学时，其中含上机 6 学时。

本书最突出的特点是把计算机网络安全技术的基本理论、基本知识与实际应用技术和基本技能融为一体；紧密结合当前技术的新发展，在阐述理论知识的同时侧重实用性；力求在讲述概念和原理时做到严格、准确、精练。为便于教学，每章均附有小结、练习与思考题，画龙点睛地归纳该章精髓。

本书共包括 10 章和 1 个附录。第 1 章主要描述计算机网络安全的定义、目标、特征和安全策略，计算机网络安全的漏洞与威胁，网络安全体系结构，网络安全措施，网络安全评价标准等；第 2 章着重介绍数据加密技术，其中包括传统密码技术、对称和公开密钥密码体制、数字签名、密钥管理算法等；第 3 章重点介绍操作系统安全，其中包括 Windows NT 操作系统安全、UNIX/Linux 操作系统安全等；第 4 章介绍数据库与数据的安全，其中包括数据库安全的基本概念、数据库的安全特性、数据库的安全保护、Web 数据库的安全、SQL Server 数据库的安全；第 5 章介绍 PKI 技术，其中包括口令认证方法、身份识别与鉴别、PKI 的概念、证书权威 CA、PKI 应用举例；第 6 章介绍防火墙工作原理及应用，其中包括防火墙概述、防火墙技术、防火墙体系结构、防火墙的选型与产品简介、瑞星个人防火墙；第 7 章主要介绍计算机病毒防治，其中包括计算机病毒的特点与分类、恶意代码、计算机病毒的检测与清除、计算机病毒的现状和发展趋势；第 8 章主要介绍入侵检测系统，其中包括入侵检测原理与结构、网络扫描和网络监听、几种商用入侵检测系统；第 9 章重点介绍 Internet 安全、VPN 和 IPSec，其中包括 TCP/IP 协议及其安全、Web 站点安全、Web 电子商务安全、黑客与网络攻击、电子邮件系统的安全、虚拟专用网、IPSec 安全模式；第 10 章主要介绍无线网络的安全，其中包括无线网络标准、无线局域网有线等价保密安全机

制、无线局域网有线等价保密安全漏洞、无线局域网安全威胁、无线保护接入机制。在附录部分，分别给出了对网络安全实验的建议及题目、名词术语的英文缩写对照表、一些极具参考价值的网址。

本书撰写分工如下：第 1 章、第 2 章和第 10 章由雷渭侣教授执笔，并负责全书的统稿和主编工作；第 6 章和第 7 章由王兰波副教授执笔，并负责副主编工作；第 3 章由李康老师执笔；第 4 章和第 8 章由许丽娟讲师执笔；第 5 章和第 9 章由师平讲师执笔，并负责全书电子教案的制作。

在本书的立项、大纲编写和内容的确定以及全书的编写过程中得到了清华大学出版社各位老师的大力支持和帮助，在此表示衷心的感谢。同时，对曾参与制定本书大纲及为本书提供过宝贵意见和建议的老师和同学同样表示衷心的感谢。

由于作者水平有限，书中难免存在错误之处，恳请广大读者批评指正。

雷渭侣

2009 年 8 月于广州

目录

第1章

绪　论

本章学习要求：

（1）掌握网络安全定义及其特征。
（2）掌握网络安全漏洞。
（3）掌握网络安全威胁。
（4）掌握网络安全的体系结构。
（5）了解网络安全措施。
（6）了解其他国家信息安全评价标准。
（7）了解我国信息安全评价标准。

重点和难点：

（1）重点：掌握网络安全的定义、特征、漏洞和威胁。
（2）难点：掌握网络安全的体系结构概念。

随着 Internet 的迅速发展、广泛应用，网络的触角深入到政治、经济、文化、军事、意识形态和社会生活等各个方面，其影响与日俱增、无处不在，由此也宣告了网络社会化时代的到来。在我们尽情享受网络带来的快捷、便利服务的同时，全球范围内针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量也在持续不断增加，对国家安全、经济和社会生活造成了极大的威胁。因此，网络安全已成为当今世界各国共同关注的焦点。

事实上，资源共享和网络安全本身就是相互矛盾的，随着资源共享的加强，网络安全问题必然日益突出。因此，如何使计算机网络系统不受破坏，提高系统的安全性已成为人们关注且必须认真对待的问题。每个计算机用户都应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全、稳定地运行。

网络安全问题涉及到数据加密技术、网络操作系统、数据库与数据访问技术、PKI 技术、防火墙工作原理及应用、计算机病毒防治、入侵检测系统、Internet 安全等内容，我们将在以后各章中一一介绍。

1.1 计算机网络安全基本概念

1.1.1 什么是网络安全

所谓“安全”，字典中的定义是为防范间谍活动或蓄意破坏、犯罪、攻击而采取的措施。将安全的一般含义限定在计算机网络范畴，网络安全就是为防范计算机网络硬件、软件、数据偶然或蓄意被破坏、篡改、窃听、假冒、泄露、非法访问并保护网络系统持续有效工作的措施总和。

1. 网络安全保护范围

网络安全与信息安全、计算机系统安全和密码安全密切相关，但涉及的保护范围不同。信息安全所涉及的保护范围包括所有信息资源；计算机系统安全将保护范围限定在计算机系统硬件、软件、文件和数据范畴，安全措施通过限制使用计算机的物理场所和利用专用软件或操作系统来实现；密码安全是信息安全、网络安全和计算机系统安全的基础与核心，也是身份认证、访问控制、拒绝否认和防止信息窃取的有效手段。网络安全与信息安全、计算机系统安全和密码安全的关系如图 1-1 所示。

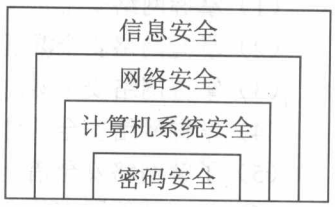


图 1-1 网络安全保护范围

2. 网络安全侧重点

事实上，网络安全也可以看成是计算机网络上的信息安全，凡涉及网络信息的可靠性、保密性、完整性、有效性、可控性和拒绝否认性的理论、技术与管理都属于网络安全的研究范畴，只是不同人员或部门对网络安全关注的侧重点有所不同。网络安全研究人员更关注从理论上采用数学方法精确描述安全属性，通过安全模型来解决网络安全问题。网络安全工程人员则从实际应用角度出发，对成熟的网络安全解决方案和新型网络安全产品更感兴趣，注重于各种安全防范工具、操作系统防护技术和安全应急处理措施。网络安全评估人员较多关注的是网络安全评价标准、安全等级划分、安全产品测评方法与工具、网络信息采集以及网络攻击技术。网络管理或网络安全管理人员通常更关心网络安全管理策略、身份认证、访问控制、入侵检测、网络安全审计、网络安全应急响应和计算机病毒防治等安全技术，因为他们的主要职责便是配置与维护网络，即在保护授权用户方便快捷地访问网络资源的同时，必须防范非法访问、病毒感染、黑客攻击、服务中断和垃圾邮件等各种威胁，一旦系统遭到破坏，造成数据或文件丢失，能够采取相应的网络安全应急响应措施予以补救。对国家安全保密部门来说，必须了解网络信息泄露、窃听和过滤的各种技术手段，避免涉及国家政治、军事、经济等重要机密信息的无意或有意泄露；抑制和过滤威胁国家安全的反动与邪教等意识形态信息传播，以免给国家的稳定带来不利的影响，甚至危

害到国家安全。对公共安全部门而言，应当熟悉国家和行业部门颁布的常用网络安全监察法律法规、网络安全取证、网络安全审计、知识产权保护、社会文化安全等技术，一旦发现窃取或破坏商业机密信息、软件盗版、电子出版物侵权、色情与暴力信息传播等各种网络违法犯罪行为，能够取得可信的、完整的、准确的、符合国家法律法规的诉讼证据。军事人员则更关心信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击和网络病毒传播等网络安全综合技术，以此夺取网络信息优势、扰乱敌方指挥系统、摧毁敌方网络基础设施，打赢未来信息战争。当然，并非只有这些专业部门、人员需要关注网络安全问题，我们每个人都无法置身度外。在网络为工作、生活和学习带来便捷的同时，我们更加关心如何保护个人隐私和商业信息不被窃取、篡改、破坏和非法存取，确保网络信息的保密性、完整性、有效性和拒绝否认性。

1.1.2　网络安全目标

网络安全的最终目标就是通过各种技术与管理手段实现网络信息系统的可靠性、保密性、完整性、有效性、可控性和拒绝否认性。可靠性（Reliability）是所有信息系统正常运行的基本前提，通常指信息系统能够在规定的条件与时间内完成规定功能的特性。可控性（Controllability）是指信息系统对信息内容和传输具有控制能力的特性。拒绝否认性（No-repudiation）也称为不可抵赖性或不可否认性，是指通信双方不能抵赖或否认已完成的操作和承诺（如利用数字签名防止通信双方否认曾经发送和接收信息的事实）。在多数情况下，网络安全更侧重强调网络信息的保密性、完整性和有效性。

1．保密性

保密性（Confidentiality）是指信息系统防止信息非法泄露的特性，信息只限于授权用户使用。保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现。信息加密是防止信息非法泄露的最基本手段。口令加密可以防止密码被盗，保护密码是防止信息泄露的关键。如果密码以明文形式传输，在网络上窃取密码非常简便，轻而易举就可以办到。事实上，大多数网络安全防护系统都采用了基于密码的技术，密码一旦泄露，就意味着整个安全防护系统的全面崩溃。机密文件和重要电子邮件在 Internet 上传输也需要加密，加密后的文件和邮件即使被劫持，尽管多数加密算法是公开的，但由于没有正确密钥进行解密，劫持的密文仍然是不可读的。此外，机密文件即使不在网络上传输，也应该进行加密，否则窃取密码就可以获得机密文件。对机密文件加密，可以提供双重保护。

2．完整性

完整性（Integrity）是指信息未经授权不能改变的特性。完整性与保密性强调的侧重点不同，保密性强调信息不能非法泄露，而完整性强调信息在存储和传输过程中不能被偶然或蓄意修改、删除、伪造、添加、破坏或丢失，信息在存储和传输过程中必须保持原样。信息完整性表明了信息的可靠性、正确性、有效性和一致性，只有完整的信息才是可信任的信息。影响信息完整性的因素主要有硬件故障、软件故障、网络故障、灾害事件、入侵

攻击和计算机病毒等。保障信息完整性的技术主要有安全通信协议、密码校验和数字签名等。实际上，数据备份是防范信息完整性受到破坏的最有效恢复手段。

3. 有效性

有效性（Availability）是指信息资源容许授权用户按需访问的特性（信息系统面向用户服务的安全特性）。信息系统只有持续有效，授权用户才能随时、随地根据自己的需要访问信息系统提供的服务。有效性在强调面向用户服务的同时，还必须进行身份认证与访问控制，只有合法用户才能访问限定权限的信息资源。一般而言，如果网络信息系统能够满足保密性、完整性和有效性 3 个安全目标，在通常意义下就可认为信息系统是安全的。

1.1.3 网络安全的特征

网络安全主要涉及系统的可靠性，软件及数据的完整性、可用性和保密性等几方面。

（1）网络系统的可靠性（Reliability）

网络系统的可靠性是指保证网络系统不因各种因素的影响而中断正常工作。

（2）软件及数据的完整性（Integrity）

软件及数据的完整性是指保护网络系统中存储和传输的软件（程序）及数据不被非法操作，即保证数据不被插入、替换和删除，数据分组不丢失、乱序以及数据库中的数据或系统中的程序不被破坏等。

（3）软件及数据的可用性（Availability）

软件及数据的可用性是指在保证软件和数据完整性的同时，还要使其可被正常利用和操作。

（4）软件及数据的保密性（Confidentiality）

软件及数据的保密主要是指利用密码技术对软件和数据进行加密处理，保证在系统中存储和在网络上传输的软件和数据不被无关人员识破。

1.1.4 网络安全策略

网络安全策略是保障机构网络安全的指导文件。一般而言，网络安全策略包括总体安全策略和具体安全管理实施细则。总体安全策略用于构建机构网络安全框架和战略指导方针，包括分析安全需求、分析安全威胁、定义安全目标、确定安全保护范围、分配部门责任、配备人力物力、确认违反策略的行为和相应的制裁措施。总体安全策略只是一个安全指导思想，还不能具体实施，在总体安全策略框架下针对特定应用制定的安全管理细则才规定了具体的实施方法和内容。

1. 安全策略总则

无论是制定总体安全策略，还是制定安全管理实施细则，都应当根据网络安全特点遵守均衡性、时效性和最小限度原则。

（1）均衡性原则

由于软件漏洞、协议漏洞、管理漏洞和网络威胁永远不可能消除，网络安全必定是计算机网络的永恒主题。无论制定多么完善的网络安全策略，还是使用多么先进的网络安全技术，网络安全也只是一个相对概念，因为世上没有绝对的安全系统。此外，网络易用性、网络效能与安全强度是一对天生的矛盾。夸大网络安全漏洞和威胁不仅会浪费大量投资，而且会降低网络易用性和网络效能，甚至有可能引入新的不稳定因素和安全隐患。忽视网络安全比夸大网络安全更加严重，有可能造成机构或国家重大经济损失，甚至威胁到国家安全。因此，网络安全策略需要在安全需求、易用性、效能和安全成本之间保持相对平衡，科学制定均衡的网络安全策略是提高投资回报和充分发挥网络效能的关键。

（2）时效性原则

由于影响网络安全的因素随时间有所变化，导致网络安全问题具有显著的时效性。例如，网络用户增加、信任关系发生变化、网络规模扩大、新安全漏洞和攻击方法不断暴露都是影响网络安全的重要因素。因此，网络安全策略必须考虑环境随时间的变化。

（3）最小限度原则

网络系统提供的服务越多，安全漏洞和威胁也就越多。因此，应当关闭网络安全策略中没有规定的网络服务；以最小限度原则配置满足安全策略定义的用户权限；及时删除无用账号和主机信任关系，将威胁网络安全的风险降至最低。

2. 安全策略内容

一般而言，大多数网络都是由网络硬件、网络连接、操作系统、网络服务和数据组成，网络管理员或安全管理员负责安全策略的实施，网络用户则应当严格按照安全策略的规定使用网络提供的服务。因此，在考虑网络整体安全问题时应主要从网络硬件、网络连接、操作系统、网络服务、数据、安全管理责任和网络用户几方面着手。

（1）网络硬件物理安全

核心网络设备和服务器应当设置防盗、防火、防水、防毁等物理安全设施以及温度、湿度、洁净、供电等环境安全设施。例如，每年因雷电击毁网络设施的事例层出不穷，这就要求位于雷电活动频繁地区的网络基础设施必须配备良好的防雷与接地装置。在规划物理安全设施时可参考《电子计算机机房设计规范》（GB 50174—1993）、《计算站场地安全要求》（GB 9361—1988）、《建筑物电子信息系统防雷技术规范》（GB 50343—2004）、《计算站场地技术条件》（GB 2887—1989）、《计算机机房用活动地板技术条件》（GB 6650—1986）等国家技术标准。

核心网络设备和服务器最好集中放置在中心机房，其优点是便于管理与维护，也容易保障设备的物理安全，更重要的是能够防止直接通过端口窃取重要资料。防止信息空间扩散也是规划物理安全的重要内容，除光纤之外的各种通信介质、显示器以及设备电缆接口都不同程度地存在电磁辐射现象，利用高性能电磁监测和协议分析仪有可能在几百米范围内将信息复原，对于涉及国家机密的信息必须考虑电磁泄露防护技术。例如，铺设电缆采用金属导管屏蔽，计算机和显示器最好使用符合美国瞬态电磁脉冲辐射标准 TEMPEST

（Transient Electromagnetic Pulse Emanation Standard，美国国家安全部制定的计算机信息泄漏安全防护标准）的产品，尽可能减小因电磁辐射导致失密的危险。我国也先后颁布了国家公共安全保密标准《计算机信息系统设备电磁泄漏发射限值》（GGBBl—1999）、《计算机信息系统设备电磁泄漏发射测试方法》（GGBB2—1999）和国家保密标准《涉密信息设备使用现场的电磁泄漏发射防护要求》（BMB5—2000）。

（2）网络连接安全

网络连接安全主要考虑网络边界的安全，例如，内部网（Intranet）与外部网（Extranet）、Internet 有连接需求，可使用防火墙和入侵检测技术双层安全机制来保障网络边界的安全。内部网安全主要通过操作系统安全和数据安全策略来保障；由于网络地址转换（Network Address Translator，NAT）技术能够对 Internet 屏蔽内部网地址，必要时也可以考虑使用 NAT 保护内部网私有 IP 地址。

对网络安全有特殊要求的内部网最好使用物理隔离技术保障网络边界的安全。根据安全需求，可以采用固定公用主机、双主机或一机两用等不同物理隔离方案。固定公用主机与内部网无连接，专用于访问 Internet，虽然使用不够方便，但能够确保内部主机信息的保密性。双主机指在一个机箱中配备两块主板、两块网卡和两个硬盘，在启动时由用户选择内部网或 Internet 连接，较好地解决了安全性与方便性的矛盾。一机两用隔离方案由用户选择接入内部网或 Internet，但不能同时接入两个网络，虽然成本低廉、使用方便，但仍然存在泄密的可能性。

（3）操作系统安全

操作系统安全应重点考虑计算机病毒、特洛伊木马（Trojan Horse）和入侵攻击威胁。计算机病毒是隐藏在计算机系统中的程序；具有自我繁殖、相互感染、激活再生、隐藏寄生、迅速传播等特点；以降低计算机系统性能、破坏系统内部信息或破坏计算机系统运行为目的。截至目前，已发现有两万多种不同类型的病毒。病毒传播途径已经从移动存储介质转向 Internet，在网络中以指数增长规律迅速扩散，诸如邮件病毒、Java 病毒和 ActiveX 病毒都给网络病毒防治带来了新的挑战。而“特洛伊木马”与计算机病毒不同，它是一种未经用户同意私自驻留在正常程序内部、以窃取用户资料为目的的间谍程序。

目前并没有特别有效的计算机病毒和“特洛伊木马”程序防治手段，主要还是通过提高病毒防范意识、严格安全管理、安装性能优异的防、杀病毒软件及“特洛伊木马”专杀软件来尽可能减少病毒与木马入侵的机会。操作系统漏洞为入侵攻击提供了条件，因此经常升级操作系统、防病毒软件和木马专杀软件是提高操作系统安全性的最有效、最简便方法。

（4）网络服务安全

目前，网络提供的电子邮件、文件传输、Usenet 新闻组、远程登录、域名查询（虽然用户并不直接使用域名查询服务，但域名查询通过将主机名转换成主机 IP 地址为其他网络服务奠定了基础）、网络打印和 WWW（World Wide Web）服务都存在大量的安全隐患。由于不同网络服务的安全隐患和安全措施不同，应当在分析网络服务风险的基础上，为每一种网络服务分别制定相应的安全策略细则。

（5）数据安全

根据数据机密性和重要性的不同，一般将数据分为关键数据、重要数据、有用数据和非重要数据，以便对不同类型数据采取不同的保护措施。关键数据是指直接影响网络系统正常运行或无法再次得到的数据，例如操作系统和关键应用程序等；重要数据是指具有很高机密性或高使用价值的数据，例如国防或国家安全部门涉及国家机密的数据、金融部门涉及用户的账目数据等；有用数据一般是指网络系统经常使用但可以从其他地方复制的数据；非重要数据则是很少使用而且很容易得到的数据。由于任何安全措施都不可能保证网络绝对安全或不发生故障，在网络安全策略中除考虑重要数据加密之外，还必须考虑关键数据和重要数据的备份。

目前数据备份使用的介质主要是磁带、硬盘和光盘。因磁带具有容量大、技术成熟、成本低廉等优点，大容量数据备份多选用磁带存储介质。随着硬盘价格不断下降，网络服务器转而采用硬盘作为存储介质。目前流行的硬盘数据备份技术主要有磁盘镜像和冗余磁盘阵列（Redundant Arrays of Inexpensive Disks，RAID）。磁盘镜像技术能够将数据同时写入型号与格式相同的主磁盘和辅助磁盘，而 RAID 是专用服务器广泛使用的磁盘容错技术。大型网络常采用光盘库、光盘阵列和光盘塔作为存储设备，但光盘特别容易划伤，导致数据读出错误，因此数据备份使用更多的还是磁带和硬盘存储介质。

（6）安全管理责任

由于人是制定和执行网络安全策略的主体，所以必须明确网络安全管理责任人。小型网络可由网络管理员兼任网络安全管理职责，但大型网络、电子政务、电子商务、电子银行或其他要害部门的网络应配备专职网络安全管理责任人。网络安全管理采用技术与行政相结合的手段，主要对授权、用户和资源进行管理，其中授权是网络安全管理的重点。安全管理责任包括行政职责、网络设备、网络监控、系统软件、应用软件、系统维护、数据备份、操作规程、安全审计、病毒防治、入侵跟踪、恢复措施、内部人员和网络用户等与网络安全相关的各种功能。

（7）网络用户安全责任

网络安全不只是网络安全管理员的事，网络用户对网络安全也负有不可推卸的责任。网络用户应特别注意不能私自将调制解调器（Modem）接入 Internet；不要下载未经安全认证的软件和插件；确保本机没有安装文件和打印机共享服务；不要使用脆弱性口令；经常更换口令等。

1.1.5　下一代网络安全

网络安全威胁多种多样，随着环境的变化和技术的发展，其形式和手段也在不断变化。经典网络安全技术以威胁为出发点而设计，对于威胁的多样性和不断变化的特性有着明显的局限性。从网络系统业务出发、以管理和监控为核心手段、以经典网络安全技术为重要补充的网络安全技术和方案成为近几年网络安全技术发展的主流。