新编计算机网络安全实用丛书

# 网络信息安全技术基础

北京启明星辰信息技术有限公司 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

新编计算机网络安全实用丛书

# 网络信息安全技术基础

北京启明星辰信息技术有限公司　编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

## 内 容 简 介

随着计算机网络越来越深入到人们的生活和工作之中，计算机的安全问题成了全世界关注的大问题，尤其是用于商业目的的计算机。本书基于此目的，重点向读者介绍计算机的安全知识，主要内容包括：计算机安全定义、安全等级、网络安全、计算机访问控制、操作系统安全、计算机病毒、密码技术和电子商务安全。书中涉及的内容通俗易懂，并附以大量图片，能够满足读者对计算机网络安全知识的需求。



**图书在版编目(CIP)数据**

网络信息安全技术基础/北京启明星辰信息技术有限公司编著 .—北京：电子工业出版社，2002.1
(新编计算机网络安全实用丛书)
ISBN 7-5053-6890-7

Ⅰ.网… Ⅱ.北… 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(2001)第 062125 号

丛 书 名：新编计算机网络安全实用丛书
书　　名：**网络信息安全技术基础**
编　　著：北京启明星辰信息技术有限公司
责任编辑：贾贺　张旭
排版制作：电子工业出版社计算机排版室监制
印 刷 者：北京天宇星印刷厂
装 订 者：河北省涿州桃园装订厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：12　字数：304 千字
版　　次：2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
书　　号：ISBN 7-5053-6890-7 / TP·3916
印　　数：5000 册　　定价：20.00 元

# 丛 书 序

全球信息高速公路的建设给整个社会的科学与技术、经济与文化带来了巨大的推动与冲击，同时也给我们带来了许多挑战。Internet/Intranet 的信息安全是一个综合的系统工程，需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大挑战。事实上，资源共享和信息安全历来是一对矛盾。随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的是信息安全问题日益突出。在人们对网络的优越性还没有完全接受的时候，黑客攻击开始肆虐全球的各大网站；而病毒制造者们也在各显其能，从 CIH 到爱虫，中毒者不计其数。一般认为，计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击三个方面。目前，人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的攻击手法包括：通过网络监听获取网上用户的账号和密码；监听密钥分配过程、攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程的缺省账户进行攻击，如 Telnet Daemon、FTP Daemon、RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 Send Mail，采用 Debug、Wizard、Pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等。目前，已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同，它们主要的区别是，“蠕虫”寄生于操作系统之上，而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多，极易传播，影响范围广。它动辄删除、修改文件，导致程序运行错误，甚至死机，已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件，从而影响正常业务的运行，严重时会使系统关机、网络瘫痪。

总而言之，对 Internet/Intranet 安全构成的威胁可以分为以下若干类型：黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等，这些都可以造成 Internet 的瘫痪等。可见我们面临的计算机网络系统的安全威胁日益严重。

那么，黑客攻击等威胁行为为什么经常能够得逞呢？主要原因在于 Internet/Intranet 系统内在的安全脆弱性；其次是人们思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性，没有采取有效的安全策略和安全机制；另外，缺乏先进的网络安全技术、工具、手段和产品等原因也导致网络的安全防范能力较弱。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生，该丛书系统全面地介绍了计算机网络安全各方面的问题，并且从一些新的角度进行探讨，例如，如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略；如何提出 Internet/Intranet 系统安全的整体解决方案；如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套新版的计算机网络安全实用丛书具有起点高、内容新、技术覆盖面广等特点，包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及防范黑客攻击手段等内容的详细分析和介绍。读者可以带着各种问题，从不同的角度来了解这些技术，一定会有所收获。

中国工程院院士　沈昌祥

# 目　录


**第 1 章　计算机安全绪论** …… 1

1.1　Internet 上的传说 …… 2
1.2　网络安全概述 …… 4
1.2.1　计算机安全和网络安全的含义 …… 5
1.2.2　安全网络的特征 …… 6
1.2.3　网络化的安全威胁 …… 8
1.3　网络安全的主要领域和关键技术 …… 9
1.3.1　物理安全 …… 9
1.3.2　安全控制 …… 10
1.3.3　安全服务 …… 11
1.3.4　网络安全的关键技术 …… 11
1.3.5　实现网络安全的策略 …… 12
1.4　可信计算机评估标准 …… 12
1.4.1　D 级 …… 12
1.4.2　C1 级 …… 13
1.4.3　C2 级 …… 13
1.4.4　B1 级 …… 14
1.4.5　B2 级 …… 14
1.4.6　B3 级 …… 14
1.4.7　A 级 …… 14

**第 2 章　网络威胁与安全策略** …… 15

2.1　网络中常见的攻击手段 …… 16
2.1.1　信息收集 …… 16
2.1.2　口令攻击 …… 17
2.1.3　常见的对路由器的攻击手段 …… 17
2.1.4　利用 TCP/IP 协议的安全问题进行攻击 …… 18
2.1.5　利用系统接收 IP 数据包漏洞进行攻击 …… 21
2.1.6　网络窃听 …… 22

2.1.7 电子邮件攻击 …… 22
2.1.8 特洛伊木马（Trojan Horses）程序 …… 22
2.1.9 常见的其他攻击方法 …… 23
2.2 常用网络服务所面临的安全威胁 …… 23
2.2.1 FTP 文件传输的安全问题 …… 23
2.2.2 Telnet 的安全问题 …… 24
2.2.3 WWW 服务的安全问题 …… 24
2.2.4 电子邮件的安全问题 …… 24
2.2.5 Usenet 新闻 …… 25
2.2.6 DNS 服务 …… 25
2.2.7 网络管理服务 …… 25
2.2.8 网络文件系统 …… 25
2.3 网络安全防范策略 …… 26
2.3.1 安全策略的制定 …… 26
2.3.2 系统的日常维护 …… 27
2.3.3 网络服务器的安全控制 …… 30
2.3.4 常规安全防范建议 …… 31
2.3.5 网络的安全防范建议 …… 35

**第 3 章 网络体系结构与网络安全** …… 37

3.1 网络结构 …… 38
3.1.1 计算机网络的组成 …… 38
3.1.2 常见网拓扑结构 …… 38
3.1.3 局域网的安全性分析 …… 40
3.2 网络分层模型与安全 …… 41
3.2.1 OSI 分层模型 …… 41
3.2.2 TCP/IP 分层和 OSI 模型的比较 …… 43
3.2.3 TCP/IP 各层的安全性 …… 44
3.3 网络安全体系结构模型 …… 49
3.3.1 安全服务 …… 50
3.3.2 安全机制 …… 51
3.3.3 安全服务的层配置 …… 52
3.4 异种网的安全问题 …… 53

**第 4 章 UNIX 操作系统的安全** …… 55

4.1 UNIX 系统的访问控制 …… 56
4.1.1 登录到计算机上 …… 56
4.1.2 UNIX 系统的口令安全 …… 61

4.1.3 UNIX 系统文件访问控制 …… 63
4.2 UNIX 操作系统的安全管理 …… 65
4.2.1 UNIX 系统用户安全 …… 65
4.2.2 UNIX 系统管理员的安全 …… 66
4.3 UNIX 的一些服务的安全性 …… 69
4.3.1 远程过程调用和 NFS 的安全性 …… 69
4.3.2 X Windows 的安全性 …… 70
4.4 UNIX 的安全审计 …… 71
4.5 对 UNIX 操作系统安全的一些建议 …… 72

**第 5 章 Windows NT 操作系统的安全** …… 74

5.1 Windows NT 的访问控制 …… 75
5.1.1 Windows NT 的系统登录 …… 75
5.1.2 账户锁定 …… 76
5.1.3 Windows NT 安全性标识符（SID） …… 77
5.1.4 Windows NT 的账户口令管理 …… 77
5.2 文件和资源的访问控制 …… 78
5.2.1 Windows NT 的资源访问控制 …… 79
5.2.2 Windows NT 的 NTFS 文件系统 …… 82
5.3 Windows NT 的安全管理 …… 84
5.3.1 Windows NT 的用户安全管理 …… 84
5.3.2 Windows NT 的域管理 …… 85
5.3.3 Windows NT 的组管理 …… 86
5.3.4 Windows NT 系统的安全审计 …… 89
5.4 Windows NT 的 RAS 访问的安全性 …… 90

**第 6 章 数据库安全** …… 93

6.1 数据库的安全问题 …… 94
6.1.1 数据篡改 …… 94
6.1.2 数据损坏 …… 94
6.1.3 窃取 …… 95
6.2 数据库的安全需求 …… 95
6.2.1 数据库的组成 …… 95
6.2.2 数据库的安全需求 …… 96
6.2.3 数据库的保密性 …… 98
6.2.4 数据库的加密 …… 98
6.2.5 多层数据库系统的安全 …… 99
6.3 数据库的安全隐患 …… 100

6.4 SQL Server 数据库系统的安全性分析 …… 100
6.4.1 SQL Server 的运行安全模式 …… 100
6.4.2 使用和管理用户账号 …… 100
6.4.3 使用视图增强安全性 …… 102
6.4.4 SQL Server 的数据加密 …… 102

**第 7 章 密码技术** …… 104

7.1 数据加密技术 …… 105
7.1.1 数据加密的作用 …… 105
7.1.2 密码学基本概念 …… 106
7.1.3 密码通信模型 …… 107
7.1.4 公钥密码体制 …… 108
7.2 网络加密方式 …… 111
7.2.1 链路加密方式 …… 111
7.2.2 节点对节点加密方式 …… 112
7.2.3 端对端加密方式 …… 112
7.3 密码算法介绍 …… 112
7.3.1 数据加密标准（DES） …… 112
7.3.2 RSA 公钥密码算法 …… 114
7.3.3 消息摘要算法（Hash 算法） …… 116
7.4 密钥的管理和分发 …… 118
7.4.1 密钥管理 …… 118
7.4.2 保密密钥的分发 …… 119
7.5 密码技术的应用 …… 120
7.5.1 电子商务（E-business） …… 121
7.5.2 虚拟专用网（Virtual Private Network） …… 121
7.6 PGP（Pretty Good Privacy）——非常好的隐私性 …… 122

**第 8 章 计算机病毒** …… 126

8.1 计算机病毒的起源 …… 127
8.1.1 最早的计算机病毒：磁芯大战 …… 127
8.1.2 计算机病毒的历史 …… 128
8.1.3 计算机病毒的发展 …… 128
8.2 计算机病毒简介 …… 130
8.2.1 病毒的定义 …… 130
8.2.2 病毒的结构 …… 130
8.2.3 病毒的特点 …… 131
8.3 计算机病毒的种类 …… 132

8.3.1 按病毒存在的媒体分类 …… 133
8.3.2 按病毒传染的方法分类 …… 133
8.3.3 按病毒破坏的能力分类 …… 133
8.3.4 按病毒特有的算法分类 …… 134
8.3.5 按病毒的链接方式分类 …… 134
8.4 计算机病毒的工作机理 …… 134
8.4.1 引导扇区病毒 …… 135
8.4.2 文件型病毒 …… 135
8.4.3 混合型病毒 …… 136
8.5 计算机病毒与一般故障的区别 …… 137
8.5.1 计算机病毒的现象 …… 137
8.5.2 与病毒现象类似的硬件故障 …… 138
8.6 几种常见病毒 …… 139
8.6.1 CIH 病毒 …… 139
8.6.2 宏病毒 …… 141
8.6.3 Remote Explorer —— 一种 NT 病毒 …… 141
8.7 计算机病毒的预防 …… 142
8.8 计算机病毒的检测 …… 144
8.8.1 比较法 …… 144
8.8.2 搜索法 …… 145
8.8.3 特征字的识别法 …… 146
8.8.4 分析法 …… 146
8.9 病毒的清除 …… 147
8.9.1 文件型病毒的清除 …… 147
8.9.2 引导型病毒的清除 …… 147
8.9.3 内存杀毒 …… 148
8.9.4 未知病毒的检测 …… 148
8.9.5 压缩文件病毒的检测 …… 148
8.9.6 网络病毒防治 …… 148

**第 9 章 Web 与电子商务安全** …… 150

9.1 WWW 安全问题 …… 151
9.1.1 Web 服务器的安全 …… 152
9.1.2 一些脚本程序的安全性 …… 154
9.2 电子商务的安全问题 …… 155
9.2.1 电子商务概述 …… 155
9.2.2 电子商务的安全要求 …… 156
9.2.3 安全电子商务的体系结构 …… 159

9.2.4 电子商务安全模型 …… 160
9.2.5 电子商务中使用的核心安全技术 …… 162
9.2.6 电子商务中主要安全协议 …… 164

**附录 A Internet 上的安全信息资源** …… 167

A.1 Web 站点 …… 168
A.1.1 普度大学的 COAST 主页和计算机安全文档 …… 168
A.1.2 CIAC 的计算机安全 WWW 站点 …… 168
A.1.3 AUSCERT 信息主页 …… 168
A.1.4 8lgm: 安全咨询组织 …… 168
A.1.5 NIST Computer Security Resource Clearinghouse …… 168
A.1.6 University of California at Davis Computer Security Research Lab …… 169
A.1.7 WWW 的安全问题 …… 169
A.2 FTP 站点 …… 169

**附录 B Moris 关于安全的论述** …… 170

**附录 C 缩略语参考对照表** …… 175

第 1 章

# 计算机安全绪论

本章概要：

- 黑客攻击案例；
- 网络安全的特征与安全威胁；
- 网络安全的主要研究领域和关键技术；
- 可信计算机评估标准。

Internet 已遍及世界上 240 多个国家和地区，为用户提供多样化的网络与信息服务。在 Internet 上，除了原来的电子邮件、新闻论坛等文本信息的交流与传播之外，网上电话、网上传真、静态及视频等通信技术都在不断地发展与完善。

在信息化社会中，计算机通信网络在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大。社会对计算机网络的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施建设已经成为反映信息社会特征最重要的基础设施建设。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集中于计算机中。但是这些信息系统都是依靠计算机网络接受和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息社会的一个重要特征。网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。随着网络的开放性、共享性和互联程度扩大，特别是 Internet 的出现，网络的重要性和对社会的影响也越来越显著。随着网络上各种新业务的兴起，比如电子商务（Electronic Commerce）、电子现金（Electronic Cash）、数字货币（Digital Cash）、网络银行（Network Bank）等，以及各种专用网的建设，比如金融网等，使得安全问题显得越来越重要，成为关键之所在。

随着网络经济和网络社会的到来，网络将会进入一个无处不在，无所不有的境地。经济、文化、军事和社会生活将会强烈地依赖网络。网络的安全和可靠将成为世界各国共同关注的焦点。

现在世界上每年因利用计算机网络进行犯罪所造成的直接经济损失令人吃惊。据美国 ABA（American Bar Association）组织调查和专家估计，美国每年因计算机犯罪所造成的经济损失高达 150 亿美元。据报道，在 Internet 上，每天大约有 4 起计算机犯罪发生。计算机犯罪，作为一种更为隐蔽的犯罪手段，给社会带来了很大的危害，因此网络安全问题已经成为世界各国研究的热门课题。

本书旨在介绍一些计算机安全的基础知识，本章主要介绍黑客的攻击范例，网络安全的概念及内涵，可信计算机的评价标准等。通过本章的学习，可以对网络安全有一个较全面的印象。本书的一些内容将涉及到 TCP/IP 协议，如果读者对 TCP/IP 协议有一定的了解，那么对本书内容的理解会有很大帮助。

## 1.1 Internet 上的传说

生活在今天的人们，常常听到关于“黑客”的故事，这些都是一些有着传奇色彩的故事：1996 年 8 月 17 日，美国司法部的网络服务器遭到黑客入侵，并将“美国司法部”的主页改为“美国不公正部”，将司法部部长的照片换成了阿道夫·希特勒，将司法部徽章换成了纳粹党徽，并加上一幅色情女郎的图片作为所谓司法部部长的助手。此外还留下了很多攻击美国司法政策的文字。

1988 年 11 月 2 日，美国 6000 多台计算机被病毒感染，致使 Internet 不能正常运行。这是一次非常典型的计算机病毒入侵计算机网络的事件，迫使美国政府立即作出反应，国防部成立了计算机应急行动小组。这次事件中遭受攻击的有 5 个计算机中心和 12 个

地区节点，链接着政府、大学、研究所和拥有政府合同的约25万台计算机。这次病毒事件，计算机系统直接经济损失达 9600 万美元。这个病毒程序设计者是罗伯特·莫里斯（Robert T.Morris），当年他仅23岁，是在康奈尔（Cornell）大学攻读学位的研究生，罗伯特·莫里斯设计的病毒程序利用了系统存在的弱点。由于罗伯特·莫里斯成了入侵 ARPANET 的最大的电子入侵者，而获准参加康奈尔大学的毕业设计，并获得哈佛大学 Aiken 中心超级用户的特权。他也因此被判 3 年缓刑并罚款 1 万美元，还被命令进行 400 小时的社区服务。

1994 年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，向美国 CITYBANK 银行发动了一连串攻击，通过电子转账方式，从 CITYBANK 银行在纽约的计算机主机里窃取了 1100 万美元。

1991 年 5 月，在 Biscay 海湾发生了一起由于网络系统被攻破造成的沉船事故。由于欧洲气象预报中心的计算机系统被网络黑客侵入并进行破坏，导致气象预报卫星不能正常工作，致使一场暴风雨的预报失误，酿成了这起不该发生的沉船事故。

1993 年 6 月，美国一家医院链接到网络上的一些测试数据结果被黑客侵入后，许多被测者误认为自己患上了癌症。

1996 年 9 月 18 日，黑客又光顾美国中央情报局的网络服务器，将其主页由“中央情报局”改为“中央愚蠢局”，并且也同样把主页给弄了个面目全非。

1996 年 12 月 29 日，黑客侵入美国空军的全球网网址并将其主页肆意改动，迫使美国国防部一度关闭了其他 80 多个军方网址。据《华尔街日报》报道：国防部国防技术信息中心的官员于 1996 年 12 月 29 日发现，美国空军的全球网页完全变了样，其中空军介绍、新闻发布等内容被替换成一段简短的黄色录像，且声称美国政府所说的一切都是谎言。

在国内仅 1998 年报道的黑客事件就层出不穷。1998 年 8 月 22 日，江西省中国公用多媒体信息网（169 台）被电脑“黑客”攻击，整个系统瘫痪。同年 4 月 25 日下午 5 时 30 分左右，一神秘的电脑“黑客”非法侵入中国公众多媒体信息网（CHINANET）贵州站点的 WWW 主机，该“黑客”将“贵州省情”的 Web 页面改换成一幅不堪入目的淫秽画面。1998 年 6 月 16 日，黑客入侵了上海某信息网的 8 台服务器，破译了网络大部分工作人员的口令和 500 多个合法用户的账号和密码，其中包括两台服务器上超级用户的账号和密码。1998 年 10 月 27 日，刚刚开通的由中国人权研究会与中国国际互联网新闻中心联合创办的“中国人权研究会”网页，被“黑客”严重篡改。

事实上，我们听到的关于通过网络的入侵只是实际所发生的事例中非常微小的一部分，相当多的网络入侵或攻击并没有被发现，即使被发现了，由于这样或那样的原因，人们并不愿意公开它，以免公众作出强烈的惊慌失措的反应。绝大多数涉及数据安全的事件从来就没有被公开报道过。据统计，商业信息被窃取的事件以每月 260% 的速率在增加。然而，据专家估计，每公开报道一次网络入侵，就有近 500 例是不被公众所知晓的。

可以说，在现在的 Internet 上，没有任何事情是可以绝对相信的，从远方的一个 IP 地址，到收到的一份电子邮件，我们都不能完全相信它是真实的。

今天，网络和主机是否是易受攻击的（Vulnerable），成了网络世界最受关注的事

情和最时髦的话题。网络的安全不止是研究者的论文研讨的课题，它已变成全球 Internet 使用者和建设者最关注的话题。

过去的十几年中，网络黑客们一直在通过计算机的漏洞来对计算机系统进行攻击，而且这种攻击的方法变得越来越复杂。

1988 年，大部分入侵者的方法仅仅是猜口令、利用系统的配置不当，以及系统上软件本身的漏洞。到了 1994 年，这些方法仍被使用，但又增加了新的方法。有些入侵者甚至通过读操作系统源代码的方法来获取系统的漏洞，并以此展开对系统的攻击。一些网络黑客编写的攻击站点的工具软件，在 Internet 上也可以很容易地得到，这就给网络安全带来了更严峻的挑战。

面对如此严重危害计算机网络的种种威胁和计算机网络安全，必须采取有力的措施来保证计算机网络的安全。但是现有的计算机网络大多数在建设之初都忽略了安全问题，即使考虑了安全，也只是把安全机制建立在物理安全机制上，因此，随着网络的互联程度的扩大，这种安全机制对于网络环境来讲形同虚设。另外，目前网络上使用的协议，比如 TCP/IP 协议，在制订之初也没有把安全考虑在内，所以就没有安全可言。TCP/IP 协议中存在很多的安全问题，不能满足网络安全要求。开放性和资源共享是计算机网络安全问题的主要根源，它的安全性主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。

网络的安全措施一般分为三类：逻辑上的、物理上的和政策上的。面对越来越严重危害计算机网络安全的种种威胁，仅仅利用物理上和政策（法律）上的手段来有效地防范计算机犯罪显得十分有限和困难，因此也应采用逻辑上的措施，即研究开发有效的网络安全技术，例如安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等，以防止网络上传输的信息被非法窃取、篡改、伪造，保证其保密性（Secrecy）和完整性（Integrity）；防止非法用户（或程序）的侵入，限制网络上用户（或程序）的访问权限，保证信息存放的私有性（Privacy）。除了私有性和完整性之外，一个安全的计算机网络还必须考虑通信双方的身份真实性（Authenticity）和信息的可用性（Available）。

网络安全就是要保证网络上存储和传输信息的安全性。但是由于网络设计之初，只考虑方便性、开放性，使得网络非常脆弱，极易受到黑客的攻击或有组织的群体的入侵，也会由于系统内部人员的不规范使用和恶意破坏，使得网络信息系统遭到破坏，信息泄露。为了解决这个问题，国内外很多研究机构在这方面做了很多工作，主要从事数据加密技术、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、IC 卡（存储卡、加密存储卡、CPU 卡）、拒绝服务、网络安全性分析、网络信息安全监测和信息安全标准化等方面的研究。

## 1.2 网络安全概述

网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题，也是一个涉及计算机科学、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边缘学科。网络安全的重要性已有目共睹。特别是

随着全球信息基础设施和各个国家的信息基础逐渐形成，国与国之间变得“近在咫尺”，信息电子化已成为现代社会的一个重要特征。信息本身就是时间，就是财富，就是生命，就是生产力。因此，各国开始利用电子空间的无国界性和信息战来实现其以前军事、文化、经济侵略所达不到的战略目的。另外，由于网络的快速、普及、客户端软件多媒体化、协同计算、资源共享、开放、远程管理化，电子商务、金融电子化（即在 Internet 上开展金融服务）成为网络时代必不可少的一个产物。但是科技进步在造福人类的同时，也带来了新的危害。事物总是辩证统一的，福兮祸焉，祸兮福焉。从某种意义上讲，计算机网络的产生就像一个打开了的潘多拉魔盒，使得新的邪恶与罪孽（比如，计算机网络犯罪）相伴而来。计算机网络中的各种犯罪活动已经严重地危害着社会的发展和国家的安全，也给人们带来了许多新的课题。比如：如何解决网络安全问题？如何解决由于信息网络化、商务电子化后给社会带来的不稳定因素？实际上，由于信息密集的金融业电子化后，使得国际上资金流动、清算的速度加快，巨额资金操纵、洗钱等非法金融行为变得非常便利，这样极有可能爆发国家甚至世界级的金融危机。1998 年发生的亚洲金融危机很大程度上是由于金融电子化。大量事实表明，确保网络安全已经是一件刻不容缓的大事，否则悔之晚矣！有人预计，未来计算机网络安全问题比核威胁还要严重，因此，解决网络安全课题具有十分重要的理论意义和现实背景。

### 1.2.1　计算机安全和网络安全的含义

计算机安全的主要目标是保护计算机资源免受毁坏、替换、盗窃和丢失。这些计算机资源包括计算机设备、存储介质、软件、计算机数据等等。计算机安全就是一个组织机构本身的安全。

网络安全从其本质上来讲就是网络上的信息安全，它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。从广义来说，凡是涉及到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网络安全所要研究的领域。下面给出网络安全的一个通用定义。

网络安全是指网络系统的硬件、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，系统连续可靠正常地运行，网络服务不中断。

从用户（个人、企业等）的角度来说，他们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、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、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，制止和防御网络“黑客”的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，对国家造成巨大的经济损失。

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。

网络安全在不同的环境和应用会得到不同的解释。

运行系统安全，即保证信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏，产生信息泄露，干扰他人，受他人干扰，本质上是保护系统的合法操作和正常运行。

网络上系统信息的安全，包括用户口令鉴别，用户存取权限控制，数据存取权限，方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密等。

网络上信息传播安全，即信息传播后果的安全。包括信息过滤，不良信息的过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果。避免公用通信网络上大量自由传输的信息失控。本质上是维护道德、法则或国家利益。

网络上信息内容的安全，即我们讨论的狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。下面给出本文所研究和讨论的网络安全的含义。

网络安全的含义是通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。网络安全的结构层次包括：物理安全、安全控制和安全服务。

### 1.2.2 安全网络的特征

**1．保密性**

信息不泄露给非授权的用户、实体或过程，或供其利用的特性；数据保密性就是保证只有授权用户可以访问数据，而限制其他人对数据的访问。数据保密性分为网络传输保密性和数据存储保密性。就像电话可以被窃听一样，网络传输也可以被窃听，解决这个问题的办法就是对传输数据进行加密处理，在本书后面将详细地讲到数据加密及其应用。数据存储保密性主要通过访问控制来实现的，管理员把数据分类，分成敏感型、机密型、私有型和公用型，对这些数据的访问加以不同的访问控制，如经理可以访问所有数据，一些技术人员除了敏感型数据以外都能进行访问，一般职员只能访问私有型数据和公司型数据。这种访问控制是不难实现的，许多安全型操作系统都能做到，如 UNIX、Windows NT 等操作系统，人们常使用的 Windows 95 和 DOS 操作系统并不具有这种功能。