宽带中国系列

信息网络安全与防护技术

Information Network Security And Defense Technology

兰巨龙 程东年 刘文芬 胡宇翔 于洪涛 李玉峰 陈越 编著

人民邮电出版社
POSTS & TELECOM PRESS

宽带中国系列

信息网络安全与防护技术

Information Network Security And Defense Technology

兰巨龙 程东年 刘文芬 胡宇翔 于洪涛 李玉峰 陈越 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

信息网络安全与防护技术 / 兰巨龙等编著. -- 北京：人民邮电出版社，2014.8
（宽带中国系列）
ISBN 978-7-115-35427-3

Ⅰ. ①信… Ⅱ. ①兰… Ⅲ. ①信息网络－安全技术
Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2014)第083806号

内 容 提 要

本书在介绍信息网络安全与防护概念和背景的基础上，对信息网络安全基础、网络故障防护、网络攻击防护以及网络信息内容审计的研究现状进行了全面系统的介绍。基于对信息网络安全与防护的理解和所从事工作的实践经验，作者在本书最后给出了信息网络安全与防护的系统实例。

本书取材新颖，内容翔实，实用性强，反映了国内外信息网络安全与防护研究的现状与未来，适合于从事信息网络安全与防护研究的广大工程技术人员阅读，也可作为高等院校通信、计算机等专业和相关培训机构的教材或教学参考书。

◆ 编　　著　兰巨龙　程东年　刘文芬　胡宇翔
于洪涛　李玉峰　陈　越
责任编辑　代晓丽
责任印制　杨林杰

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京天宇星印刷厂印刷

◆ 开本：787×1092　1/16
印张：17　　2014 年 8 月第 1 版
字数：400 千字　　2014 年 8 月北京第 1 次印刷

定价：88.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序　言

随着信息网络业务融合的不断演进，既有的网络体系面临着诸多问题和挑战，网络空间信息安全问题也日渐凸显。网络窃密技术的不断发展以及网络安全事件的持续增多，极大削弱了网络服务的公信力，肆无忌惮地侵犯了人们的隐私权，对人类社会发展构成了严重威胁。世界各国均已将网络空间安全上升到国家战略。加强信息网络安全与防护体系建设已成为抵御外来侵略、维护国家主权的神圣职责。

目前，关于信息网络安全与防护的专著很多，但很多读者阅读过后仍对信息网络安全与防护技术缺乏全面的理解和掌握。坦率地说，要想全面系统地论述信息网络安全与防护技术本身是件非常不容易的事情，这涉及非常广泛的领域，没有成体系高屋建瓴的统筹规划是难以完成的。兰巨龙教授等人编著的这本书从读者的角度出发，站在系统论的高度对信息网络安全与防护技术做了全面的呈现，涵盖了信息网络安全与防护技术的基本概念、基础理论、故障防护、攻击防护、内容审计和系统实例等6个方面，构成了本书的6个章节。全书内容丰富，条理清晰，深入浅出，循序渐进，能够帮助读者建立起对信息网络安全与防护全面、系统的认识，有助于读者逐步理解和掌握复杂的信息网络安全与防护技术。

网络安全问题的多样性使得现实系统并不存在解决难题的“万能钥匙”，尤其是目前主流的基于特征分析的被动防御技术，对于借助未知的可利用漏洞和刻意隐匿的后门实施的动态持续网络攻击来说，几乎没有任何有效的积极防御手段，网络空间安全黑洞问题尚未找到破解之道。可喜的是，学术界近些年来提出的基于动态化、多样化和随机化的主动防御思想正在取得富有前景的积极成果，诸如中国提出的拟态安全防御 MSD（Mimic Security Defense）和美国提出的移动目标防御 MTD(Moving Target Defense)等新体系。作为一种自然的延续，新体系能够方便地接纳现有的网络安全防护措施和手段并能通过组合应用放大或倍增安全功效。有兴趣的读者可以在系统掌握现有网络安全防护技术和体系的基础上，深入研究主被动融合的新体系和动态化、多样化、随机化新思想，为打造我国新一代更安全的“信息之盾”、在网络防护中实现“改变游戏规则”的变革中贡献新思路。

邬江兴

2014年3月

前　言

随着信息网络技术的不断发展，信息网络成为囊括电话网、广播电视网和互联网的总称。3 种网络有各自的形成过程、服务对象、发展模式，它们的功能有所交叉，又互为补充。近年来，3 种网络的发展方向是互相融通，取长补短，逐步实现三网融合。面向三网融合的信息网络不但是人们享受丰富的信息网络服务的平台，也成为国家政治、经济、军事、外交活动所依赖的重要信息基础设施，已经成为当今信息社会的基石。人类在享受其带来的方便和便捷的同时，信息网络及其采集、处理、传输、存储的信息也面临着各种安全威胁和风险。

在全球化、信息化、网络化的背景下，国与国之间的竞争在很大程度上取决于对信息的占有程度和对网络的控制程度。谁拥有制信息权和制网络权，谁就占领了政治、经济、军事、文化的制高点。美国著名未来学家托尔勒曾指出：“谁掌握了信息、控制了网络，谁将拥有整个世界。”信息网络安全与防护已成为关系到国家安全和主权、社会稳定、民族文化继承和发扬的重大关键问题。我国的信息网络安全问题如果得不到很好的解决，将全方位地危及我国的政治、军事、经济、文化和社会生活的各个方面。特别是随着网络终端移动化和智能化的趋势越来越明显，互联网作为基础信息网络的主要形式，其业务呈现井喷式的增长，而其开放性也给信息网络的安全带来了巨大的风险。因此，本书将以互联网为主要研究对象，介绍信息网络安全与防护的相关知识。

本书主要内容共 6 章。第 1 章介绍了信息网络安全与防护的背景，引入了信息网络安全与防护的相关概念，总结了信息网络安全与防护的目标和服务机制以及相应的防护技术；第 2 章主要介绍了信息网络安全基础，包括信息加密技术、hash 函数、安全认证协议和信任机制；第 3 章则介绍了当前网络故障防护技术，包括冗余设计技术、故障检测技术、故障切换技术和故障恢复技术；第 4 章介绍了当前的网络攻击防护技术，包括常见的网络攻击技术、防火墙技术、入侵检测技术、蜜罐技术和蜜网技术；第 5 章介绍了网络内容审计相关技术，包括流量分类、垃圾邮件检测、微博话题检测、不良图像内容审计、视频复制检测以及多层审计系统设计等技术；第 6 章则根据笔者所从事工作的实践经验和对信息网络安全与防护的理解，给出了信息网络安全与防护的系统实例。

本书在编著过程中得到了国家“973”计划项目“可重构信息通信基础网络体系研究”（项目编号：2012CB315900）、课题“网络组件模型与聚类机制”（课题编号：2013CB329104）、国家“863”计划课题“面向三网融合的统一安全管控网络”（课题编

号：2011AA01A103）等项目的资助。同时，笔者在编写第 6 章的过程中参考了国家“863”计划重大专项“新一代高可信网络”的大量技术资料。

兰巨龙教授负责本书的统筹规划并编写了第 1 章的 1.1 节、1.2 节和 1.3 节，陈越教授编写了第 1 章的 1.4 节和 1.5 节；刘文芬教授编写了第 2 章；程东年教授和王瑞民副教授编写了第 3 章；陈越教授和胡宇翔博士编写了第 4 章；于洪涛研究员编写了第 5 章；胡宇翔博士和李玉峰副教授编写了第 6 章。另外，项目组博士生王鹏、熊刚、程国振、王志明和叶茂，硕士生王文钊、孟飞、杜传震、刑池强、张岩和刘佳为本书的文字校阅、插图绘制等做了大量工作。

限于作者水平，并且各种信息网络安全与防护技术研究仍在快速发展和完善之中，本书难免存在缺点甚至错误之处，敬请广大读者批评指正。

作者

2014 年 3 月

目　录

第 1 章　信息网络安全与防护概述 ····· 1

1.1　信息网络安全与防护的背景 ····· 1

1.2　信息网络安全与防护的概念与目标 ····· 3

1.2.1　信息网络安全与防护的概念 ····· 3

1.2.2　信息网络安全与防护的目标 ····· 3

1.3　信息网络面临的主要威胁 ····· 7

1.4　网络安全服务与机制 ····· 8

1.4.1　网络安全服务 ····· 9

1.4.2　网络安全机制 ····· 10

1.5　信息网络安全防护技术 ····· 12

1.6　参考文献 ····· 14

第 2 章　信息网络安全基础 ····· 15

2.1　信息加密技术 ····· 15

2.1.1　对称密码体制 ····· 16

2.1.2　公钥密码体制 ····· 27

2.2　hash 函数 ····· 35

2.2.1　hash 函数的结构 ····· 36

2.2.2　SHA-3 标准 ····· 38

2.3　安全认证协议 ····· 39

2.3.1　数字签名 ····· 39

2.3.2　基于对称密码的实体认证协议 ····· 42

2.3.3　基于 hash 函数的实体认证协议 ····· 46

2.3.4　基于数字签名的实体认证协议 ····· 48

2.3.5　基于零知识技术的实体认证协议 ····· 51

2.3.6　其他安全认证技术及发展趋势 ····· 54

2.4　信任机制 ····· 59

2.4.1　信任管理技术概述 ····· 59

2.4.2　行为信任的评估算法 ····· 61

2.4.3 不同应用环境下的信任模型 …… 64
2.4.4 信任管理的发展趋势 …… 67
2.5 参考文献 …… 68
第 3 章 网络故障防护 …… 74
3.1 冗余与灾备技术 …… 74
3.1.1 冗余与灾备技术概述 …… 74
3.1.2 校验技术原理 …… 75
3.1.3 硬件容错系统 …… 76
3.1.4 软件容错系统 …… 77
3.1.5 数据容错 …… 78
3.2 故障检测技术 …… 80
3.2.1 网络拓扑及故障检测策略 …… 80
3.2.2 链路故障 …… 85
3.2.3 协议故障 …… 87
3.2.4 配置故障 …… 87
3.2.5 服务器故障 …… 88
3.3 故障切换技术 …… 90
3.3.1 连接迁移 …… 90
3.3.2 选举机制 …… 91
3.3.3 状态一致 …… 93
3.4 故障恢复技术 …… 95
3.4.1 网络故障原因 …… 95
3.4.2 网络故障类型 …… 97
3.4.3 底层故障恢复技术 …… 98
3.4.4 MPLS 故障恢复技术 …… 99
3.4.5 IP 层域内故障恢复技术 …… 102
3.5 参考文献 …… 107
第 4 章 网络攻击防护 …… 108
4.1 网络攻击 …… 108
4.1.1 黑客、骇客与网络攻击 …… 108
4.1.2 网络攻击分类 …… 108
4.1.3 常见的网络攻击原理、手段和工具 …… 109
4.1.4 网络攻击的防范策略 …… 123

4.2 防火墙技术 …… 132
4.2.1 防火墙概念、功能和分类 …… 132
4.2.2 常见的防火墙体系结构和技术原理 …… 135
4.2.3 防火墙的安全技术指标 …… 141
4.2.4 主要防火墙产品介绍 …… 145
4.3 入侵检测技术 …… 155
4.3.1 入侵检测的概念和原理 …… 155
4.3.2 入侵检测系统的组成 …… 156
4.3.3 入侵检测技术方法 …… 159
4.3.4 入侵检测的基本过程 …… 163
4.3.5 未来需求和入侵检测技术的发展趋势 …… 165
4.4 蜜罐技术 …… 167
4.4.1 蜜罐的概念 …… 168
4.4.2 蜜罐的分类和体现的安全价值 …… 168
4.4.3 蜜罐的配置模式 …… 171
4.4.4 蜜罐的信息收集 …… 172
4.4.5 蜜罐技术的应用 …… 172
4.5 蜜网技术 …… 174
4.5.1 蜜网技术的基本概念与核心需求 …… 174
4.5.2 蜜网技术的分类 …… 176
4.5.3 虚拟蜜网 …… 177
4.5.4 蜜网技术的应用 …… 177
4.5.5 蜜网技术的发展趋势 …… 178
4.6 参考文献 …… 179
第 5 章 网络信息内容审计 …… 180
5.1 流量分类技术 …… 180
5.1.1 流量分类研究现状 …… 181
5.1.2 流量分类技术发展趋势 …… 184
5.2 垃圾邮件检测技术 …… 185
5.2.1 垃圾邮件现状及发展趋势 …… 185
5.2.2 垃圾邮件审计技术 …… 186
5.3 微博话题检测 …… 189
5.3.1 微博文本特点及对话题检测的影响 …… 189

5.3.2 传统微博话题检测算法 …… 189
5.3.3 微博主题挖掘新算法 …… 192
5.4 不良图像内容审计 …… 193
5.4.1 肤色检测 …… 193
5.4.2 人脸检测 …… 194
5.4.3 总体研究现状 …… 195
5.5 视频副本检测 …… 196
5.5.1 视频副本检测的基本原理及视频数据的特点 …… 196
5.5.2 视频副本检测的关键技术 …… 198
5.5.3 视频副本检测的评测标准 …… 202
5.6 多层审计系统设计及性能评价 …… 203
5.6.1 单级审计系统的性能评估指标及评估模型 …… 203
5.6.2 多重审计系统的性能评估 …… 205
5.7 参考文献 …… 205
第 6 章 信息网络安全与防护系统实例 …… 207
6.1 信息网络安全需求 …… 207
6.1.1 信息网络脆弱性及风险 …… 207
6.1.2 信息网络安全等级 …… 209
6.1.3 信息网络安全功能 …… 213
6.2 信息网络安全防护系统的设计方案 …… 217
6.2.1 总体设计框架 …… 217
6.2.2 安全管理防护 …… 220
6.2.3 安全技术防护 …… 223
6.3 信息网络安全防护系统的具体实现 …… 230
6.3.1 安全管控系统的研发背景 …… 231
6.3.2 安全管控系统的结构模型 …… 232
6.3.3 安全管控系统的关键技术 …… 236
6.3.4 安全管控系统的部署 …… 252
6.4 本章小结 …… 255
6.5 参考文献 …… 255
名词索引 …… 257
作者简介 …… 261

第 1 章　信息网络安全与防护概述

随着信息化进程的逐步深入，网络化已成为信息化发展的大趋势。网络的开放性、互联性、共享性程度的扩大使得用户对信息与网络安全技术的依赖越来越强，随之而来的安全威胁也越来越多。本章从信息网络安全与防护的背景入手，介绍网络安全与防护的目标、网络面临的主要威胁、网络安全与服务等方面的知识。

1.1　信息网络安全与防护的背景

信息网络是指构成电子信息网络的线路、设备、协议的总称，是信息资源开发利用和信息技术应用的基础，是信息传输、交换和共享的必要手段。在 2001 年 3 月之前，人们通常将信息网络分为公用电话网、广播电视网和计算机网，这 3 种网络有各自的形成过程、服务对象、发展模式，它们的功能有所交叉，又互为补充。近年来，3 种网络的发展方向是互相融通，取长补短，逐步实现三网融合。目前，随着网络终端移动化和智能化的趋势越来越明显，互联网作为基础信息网络的主要形式，其业务呈现井喷式的增长，而其开放性也给信息网络的安全带来巨大的风险。因此，本书将以互联网为主要研究对象，介绍信息网络安全与防护的相关知识。

现代信息技术正在朝着网络化、智能化和普适化的方向迈进，人类社会、信息世界和物理世界正在实现全面连通并相互融合，一种全新的人—机—物和谐共生的发展模式正在孕育之中。信息网络不但是人们享受丰富的信息网络服务的平台，也成为国家政治、经济、军事、外交活动所依赖的重要信息基础设施，已经成为当今信息社会的基石。人类在享受其带来的方便和便捷的同时，信息网络及其采集、处理、传输、存储的信息也面临着各种安全威胁和风险。以下是近年来发生的典型案例[1]。

2009 年 5 月 19 日，我国十多个省市数以亿计的网民遭遇了罕见的“网络塞车”，这是继 2006 年台湾地震造成海底通信光缆发生中断之后，我国发生的又一起罕见的互联网网络大瘫痪，大多数网民的上网质量都受到了影响。

2010 年 7～9 月的震网病毒（Stuxnet）事件。震网病毒是世界上首个以直接破坏现实世界中工业基础设施为目标的蠕虫病毒，被称为网络“超级武器”。震网病毒于 2010 年 7 月开始爆发，截至 2010 年 9 月底，包括中国、伊朗、印度、俄罗斯在内的许多国家都发现了这个病毒。该病毒攻击了伊朗布什尔核电站，导致 1/5 的离心机报废。俄罗斯常驻北约代表罗戈津称：震网对伊朗核电站造成的危害不亚于切尔诺贝利核电站事故。据统计，全球有约 45 000 个网络被该病毒感染，其中我国有近 500 万网民以及多个行业的领军企业遭此病毒攻击。美国斯坦福大学教授罗兰·贝内迪克认为：“网络战的效果与

核弹相似”。

2011 年诺顿网络犯罪调查报告称：网络犯罪让全球每年损失 3 880 亿美元，远超全球毒品交易总额（2 880 亿美元）。2010 年，全球 4.31 亿人遭受过网络侵害，其中近一半（1.96 亿人）在中国。继 CSDN、天涯社区用户数据泄露后，互联网行业人心惶惶，而在用户数据最为重要的电商领域，也不断传出存在漏洞、用户信息泄露的消息。2011 年 12 月 29 日，漏洞报告平台乌云发布漏洞报告称，支付宝用户信息大量泄露，被用于网络营销，其总量达 1 500 万～2 500 万账号之多，泄露时间不明，里面只有支付用户的账号，没有密码。已经被卷入的企业有京东商城、支付宝和当当网，其中京东商城及支付宝否认信息泄露，而当当网则表示已经向当地公安局报案。

2012 年 2 月 13 日，据称一系列政府网站均遭到了匿名组织的攻击，而其中美国中央情报局官网被黑长达 9 个小时，黑客盗走政府网中数万份私人信息。这一组织之前也曾拦截伦敦警察与美国联邦调查局之间的一次机密电话会谈，并随后上传于网络。

2012 年 11 月 21 日，我国互联网实验室总裁张笑容指出，包括广州联通、辽宁联通、厦门电信等重要地区在内的信息网络近期因外国企业设备故障而不能正常工作。国外企业对中国电信和中国联通骨干网等的垄断，使得其可以通过控制路由器，而破坏通信网络。

2013 年 6 月 6 日，英国《卫报》和美国《华盛顿邮报》报道[2]，美国国家安全局和联邦调查局于 2007 年启动了一个代号为“棱镜”的秘密监控项目，直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等在内的 9 家网际网络巨头皆参与其中。据美国中情局前职员爱德华·斯诺登爆料：美国情报机构一直在 9 家美国互联网公司中进行数据挖掘工作，从音视频、图片、邮件、文档以及连接信息中分析个人的联系方式与行动。监控的类型有 10 类：电子邮件、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间、社交网络资料的细节，其中包括两个秘密监视项目，一是监视、监听用户电话的通话记录，二是监视用户的网络活动。

2013 年 6 月 23 日，中国外交部指出：有媒体披露，美方曾对中国电信运营公司和清华大学进行网络攻击。中国外交部发言人华春莹表示，对最近所披露的美政府有关机构对中国进行网络攻击等情况表示严重关切。

从上述典型案例可以看到，在全球化、信息化、网络化的背景下，国与国之间的竞争在很大程度上取决于对信息的占有程度和对网络的控制程度。谁拥有制信息权和制网络权，谁就占领了政治、经济、军事、文化的制高点。美国著名未来学家托尔勒曾指出：“谁掌握了信息，控制了网络，谁将拥有整个世界”。信息网络安全与防护已成为关系到国家安全和主权、社会稳定、民族文化继承和发扬的重大关键问题。信息网络安全和防护能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分。我国的网络信息安全问题如果解决不好，将全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面。

1.2 信息网络安全与防护的概念与目标

1.2.1 信息网络安全与防护的概念

对于信息网络安全与防护的概念并无严格定义，随着信息网络技术的发展以及人们侧重点的不同，其概念略有差异。信息网络安全是指保护信息网络系统的硬件、软件及其系统中的数据，使其在遭受到偶然的或者恶意的攻击时而不被破坏、更改、泄露，系统能连续可靠正常地运行，网络服务不中断。即防止信息网络本身及其采集、加工、存储、传输的信息数据被故意或偶然地非授权泄露、更改、破坏或使信息被非法辨认、控制，保障网络信息的保密性、完整性、可用性、认证性、可控性、不可抵赖性等安全属性。

信息网络安全从其本质上来讲就是网络上的信息安全[3]。从广义来说，凡是涉及网络上信息安全属性的相关技术和理论都是信息网络安全的研究领域。信息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。其内涵包括以下几个方面。

网络运行系统安全：指信息所依附的处理、存储、传输等系统的安全，如网络系统、网络操作系统、网络数据库系统、网络存储系统等软硬件的安全性，主要涉及可用性、可控性、保密性等安全属性，侧重于保证系统正常运行，避免由于系统崩溃和损坏而使系统存储、处理和传输的信息遭受破坏和损失，避免由于电磁泄露所引起的信息泄露、电磁攻击而导致系统失效等情况发生。

网络上系统信息的安全：指为保证信息网络上的信息安全，在网络运行系统中采取的控制与防护本身的安全性，主要涉及保密性、认证性、可控性、不可抵赖性等安全属性，包括用户口令鉴别、用户存取权限控制、数据存取权限与方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

网络上信息传播的安全：指信息传播后果的安全，主要涉及可控性等安全属性，包括信息过滤、信息传播控制、信息引导等。它侧重于防止和控制非法、有害的信息进行传播，避免公用网络上大量自由传输的信息失控。

网络上信息内容的安全：指保证信息内容本身的安全性，侧重于保护信息的保密性、完整性、认证性、可控性和不可抵赖性，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。

信息网络防护是指为保证信息网络安全所采取的策略、技术和方法的总称，致力于如何保证网络信息安全性的技术手段，主要包括物理安全分析技术、网络结构安全分析技术、系统安全分析技术、管理安全分析技术、安全服务和安全机制策略等，所采用的具体技术与信息网络安全与防护的目标相关，详见下一节的说明。

1.2.2 信息网络安全与防护的目标

从技术角度来说，信息网络安全与防护的目标主要表现在网络信息或者网络信息系统的保密性、完整性、可用性、认证性、可控性、不可抵赖性等安全属性方面[4]。

（1）保密性

保密性是信息不被泄露给非授权的用户和实体，或供其利用的特性。也就是说，防止信息泄露给非授权的个人或实体，信息只为授权用户使用。保密性是网络信息系统面向数据内容的安全属性，是保障网络信息安全的重要手段。

常用的保密防护技术包括以下几点。

- 防侦收：使对手侦收不到有用的信息；
- 防辐射：防止有用信息以各种途径辐射出去；
- 信息加密：在密钥的控制下，用加密算法对信息进行加密处理，即使对手得到了加密后的信息，也会因为没有密钥而无法读懂有效信息；
- 物理保密：利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露；
- 身份认证与访问控制：通过认证访问信息系统的主体身份，并对其访问的信息资源实施访问控制，以阻止非授权用户或实体获得保密信息；
- 安全通信协议：通过通信双方或多方进行安全协商，在认证、加密等技术的配合下完成保密通信。

（2）完整性

完整性是信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入的特性。完整性是网络信息系统面向用户的安全性能，要求保持信息的原样，即信息的正确生成、存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人或实体，而完整性则要求信息不致受到各种原因的破坏或篡改。影响网络信息完整性的主要因素有设备故障、误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码）、人为攻击、计算机病毒等。

信息完整性的主要防护方法包括以下几点。

- 安全协议：又称密码协议，是以密码学为基础的消息交换协议，其目的是在网络环境中提供各种安全服务。安全协议是建立在密码体制基础上的一种交互通信协议，运用密码算法和协议逻辑来实现认证和密钥分配等目的。网络中有了安全协议，就能进行实体之间的认证，在实体之间安全地分配密钥或其他各种秘密，确认发送和接收的消息的完整性、保密性和不可否认性等。
- 纠错码：是信息在传输过程中发生错误后能在接收端自行发现或纠正的编码技术。一般用于纠正设备故障和误码导致的数据错误，最简单的纠错编码方法是奇偶校验法。
- 密码校验和：密码校验和（Cryptographic Checksum）是分配给一个文件的数学值（称作校验和），它用来检查和校验包含在文件中的数据没有被恶意更改。密码校验和由一系列复杂的数学操作创建，它将文件的数据转换为固定的数字字串，这个字串叫做散列值，也就是随后用的密码校验和。在不知道用何种算法创建了散列值的情况下，一个未经授权的用户不太可能修改数据并使计算结果表现出正确的校验和。密码校验和用于数据传输和存储。
- 数字签名：数字签名是给电子文档进行签名的一种方法，可在网络通信中鉴别签名人的身份和通信内容的完整性。数字签名方案通常包括密钥生成算法、签名算法和验证算法 3 部分。

- 公证：请求网络管理或中介机构证明信息的完整性和真实性。

（3）可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性是所有网络信息系统的建设和运行目标。网络信息系统的可用性测度主要有3种：抗毁性、生存性和有效性。

信息网络抗毁性是指当网络中出现确定性或随机性故障时，网络能维持或恢复其性能到一个可接受程度的能力。网络抗毁性注重的是当系统的关键部分遭受到攻击或摧毁时系统的恢复性和适应性，并在此情况下仍能完成关键服务的能力。增强抗毁性可以有效地避免因各种灾害造成的网络大面积瘫痪事件。

生存性是指信息网络及其信息服务系统在攻击、故障和意外事故已发生的情况下，在限定时间内完成使命的能力。传统的网络安全性研究的重点是如何防止入侵，而生存性的研究重点是在网络受到攻击之后如何进行入侵容忍。

有效性则是一种基于业务性能的可靠性，是指在信息网络部件失效的情况下，满足业务性能要求的程度，比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均时延增加、线路阻塞等现象。

对网络可用性的损害主要来自于人为操作错误、系统软件或应用软件缺陷、硬件损毁、电脑病毒、黑客攻击、突然断电、意外宕机、自然灾害等诸多因素，这些需要不同的安全防护技术来应对。针对信息网络可用性的主要防护技术有以下3种。

① 可自愈的自适应路由协议（如 Internet 路由协议）：通过路由节点的不断交互，感知相邻节点链路和节点失效情况的变化，通过维护路由表来改变信息传输的路径，从而实现在部分节点和链路失效的情况下，仍然能够完成信息传输服务。为了缩小网络从失效中恢复的时间，网络应具有快速自愈的能力。

② 数据备份与灾难恢复技术：数据备份是指将重要数据保存到指定的介质上，在原数据因人为或其他原因被破坏时能够快速地恢复数据，比较常见的备份方式有定期磁带备份、远程磁带库/光盘库备份、远程关键数据＋磁带备份、远程数据库备份、网络数据镜像等。灾难恢复是指当灾难发生时，网络信息系统被破坏，造成业务中断，通过预先制定的预案，从管理流程、技术方案等方面执行一系列活动，恢复网络信息系统，保证业务持续进行。

③ 入侵容忍技术：隶属于信息网络生存性技术范畴，它假设不能完全正确地检测对系统的入侵行为，当入侵和故障突然发生时，能够利用“容忍”技术来解决系统的“生存”问题。其主要的技术途径是攻击响应和攻击屏蔽技术。其中，攻击响应技术通过检测到局部系统的失效或估计到系统被攻击，而加快反应时间，调整系统结构，重新分配资源，使系统上升到一种在攻击发生的情况下能够继续工作的状态；攻击屏蔽技术借用了容错技术的思想，在设计时就考虑足够的冗余，保证当部分系统失效时，整个系统仍旧能够正常工作。

（4）认证性

认证性是指确保一个消息的来源或消息本身被正确地标识，同时确保该标识没有被伪造。认证性分为数据源认证和实体认证。数据源认证是指能向接收方保证该消息确实

来自于它所宣称的源。实体认证是指在连接发起时能确保这两个实体是可信的，即每个实体的确是它们宣称的那个实体，使得第三方不能假冒这两个通信方中的任何一方。

信息的认证性一般应用密码技术实现，其中数字签名技术除了可以完成数据完整性验证外，还是完成数据源认证的重要机制之一。数字签名技术采用密码技术，可在电子通信中鉴别签名人的身份（数据的来源）以及该通信中的数据完整性。

（5）不可否认性

不可否认性也称作不可抵赖性，在网络信息系统的信息交互过程中，确信参与者的真实同一性，并且所有参与者都不可能否认或抵赖曾经完成的操作和承诺。当发送一个信息时，接收方不但能证实该消息的确是由所宣称的发送方发来的，且发送方客观上不能否认曾经发出此消息的事实及此消息的内容（源不可否认性）。当接收方收到一个消息时，发送方能够证实该消息的确送到了指定的接收方，且接收方客观上不能否认曾经接收到此消息的事实及此消息的内容，也不能否认其接收到消息后对消息进行篡改（如果发生过）的事实（宿不可否认性）。

一般通过数字签名来提供抗否认服务。利用信息源证据可以防止发送方不真实地否认已发送信息；利用递交接收证据能够防止接收方事后否认已经接收的信息。

（6）可控性

可控性是指对网络信息的传播及内容具有控制能力的特性。保障系统依据授权提供服务，使系统在任何时候都不被非授权人使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取防范措施。

可控性还应该满足以下要求：身份识别与验证、访问控制（对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。包括自主访问控制和强制访问控制）、业务流控制（利用均分负荷方法，防止业务流量过度集中而引起网络阻塞）、路由选择控制（选择那些稳定可靠的子网、中继线或链路等）、审计跟踪（把网络信息系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。审计跟踪的信息主要包括事件类型、被管客体等级、事件时间、事件信息、事件回答以及事件统计等方面的信息）。

从控制的对象来说，可控性可以分为如下几个方面。

- 实体可信：实体指构成信息网络的基本要素，主要有网络基础设备、软件系统、用户和数据，即保证构建网络的基础设备和软件系统安全可信，没有预留后门或逻辑炸弹。保证接入网络的用户是可信的，防止恶意用户对系统的攻击破坏；保证在网络上传输、处理、存储的数据是可信的，防止搭线窃听、非授权访问或恶意篡改。
- 行为可控：保证用户行为可控，即保证本地计算机的各种软硬件资源（如内存、中断、I/O 端口、硬盘等硬件设备，文件、目录、进程、系统调用等软件资源）不被非授权使用或不被用于危害本系统或其他系统的安全；保证网络接入可控，即保证用户接入网络应严格受控，用户上网必须申请登记并得到许可；保证网络行为可控，即保证网络上的通信行为受到监视和控制，防止滥用资源、非法外联、网络攻击、非法访问和传播有害信息等恶意事件发生。
- 资源可管：保证对路由器、交换机、服务器、邮件系统、目录系统、数据库、域名系统、安全设备、密码设备、密钥参数、交换机端口、IP 地址、用户账号、服务端口

等网络资源进行统一管理。

- 事件可查：保证对网络上的各类违规事件进行监控记录，确保日志记录的完整性，为安全事件稽查、取证提供依据。
- 运行可靠：保持对信息网络运行的可用性的控制，即保证网络节点在发生自然灾难或遭到硬摧毁时仍能不间断运行，具有容灾抗毁和备份恢复能力；保证能够有效防范病毒和黑客的攻击所引起的网络拥塞、系统崩溃和数据丢失，并具有较强的应急响应和灾难恢复能力。

1.3 信息网络面临的主要威胁

目前，随着信息网络应用的普及和技术的不断升级，非法访问、恶意攻击等安全威胁也不断出新，各种潜在的不安全因素时时刻刻威胁着信息网络的安全。因此，了解网络面临的各种威胁的根源，制定适宜的安全措施，做到事前主动防御、事发灵活控制、事后分析跟踪，具有极其重要的现实意义。网络威胁主要来自以下 7 个方面[5]。

（1）人为因素

人为因素分两种情况。第一种是由于用户自己无意操作失误而引发的网络安全事故，如管理员安全配置不当造成安全漏洞；用户安全意识淡薄，将自己的账户随意转借他人或与别人共享等。第二种是用户恶意破坏，如对网络硬件设备的破坏以及利用黑客技术对网络系统的破坏。这种恶意破坏可有选择地破坏信息的安全属性，如通过截取、破译等方式破坏信息的保密性，通过截取、篡改、重放来破坏信息的完整性，通过假冒他人破坏信息的认证性等。随着黑客技术逐渐被越来越多的人掌握、利用，甚至有些黑客站点在介绍一些攻击方法和攻击软件的使用，公布系统的一些漏洞，使得系统、站点遭受攻击的可能性变大，加之现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，黑客攻击的隐蔽性深，导致攻击的破坏力极强。

（2）网络协议的局限性

指网络和信息系统自身的缺陷。互联网的显著特点就是开放性，这种开放性在某种程度上意味着不安全，容易遭受攻击。互联网本身依赖的 TCP/IP，在设计过程中没有对具体的安全问题给予详细分析，导致现行 IP 网络存在明显的安全缺陷，成为网络安全隐患中最核心的问题，如在信息输入、处理、传输、存储、输出过程中存在着信息容易被篡改、伪造、破坏、窃取、泄露等不安全因素。最常见的隐患有 SYN-Flood 攻击、ICMP 攻击、IP 地址盗用、源路由攻击、截取连接攻击等。信息网络自身在网络操作系统、网络数据库及其通信协议等方面也存在安全漏洞和隐蔽信道等不安全因素。

（3）硬件和设备的局限性

指硬件和设备自身的安全缺陷。比如，当磁盘高密度存储受到损坏时，易造成大量信息丢失；存储介质中的残留信息泄密；计算机设备工作时产生的辐射电磁波会造成信息泄密等。

（4）软件漏洞

随着软件系统规模的不断扩大，系统中的安全漏洞或“后门”也不可避免地存在。比如常用的操作系统，无论是 Windows 还是 UNIX 都或多或少地存在安全漏洞。很多服务器、浏览器以及其他一些桌面软件也都被发现存在一些安全隐患。