

全国计算机技术与软件专业技术资格（水平）考试指定用书

信息安全工程师教程

（第2版）

蒋建春 主编 / 文伟平 焦健 副主编

清华大学出版社
北京

内 容 简 介

全国计算机技术与软件专业技术资格(水平)考试(以下简称“计算机软件考试”)是由人力资源和社会保障部、工业和信息化部领导的专业技术资格考试,纳入全国专业技术人员职业资格证书制度统一规划。根据人力资源和社会保障部办公厅《关于 2016 年度专业技术人员资格考试计划及有关问题的通知》(人社厅发〔2015〕182 号),在计算机技术与软件专业技术资格(水平)考试中开考信息安全工程师(中级)。信息安全工程师岗位的人才评价工作的实施,将成为科学评价我国信息安全专业技术人员的重要手段,也将为我国培养和选拔信息安全专业技术人才发挥重要作用。

本书依据信息安全工程师考试大纲编写,由 26 章组成,主要内容包括网络信息安全基础、网络信息安全体系、网络信息安全技术、网络信息安全工程等。本书针对常见的网络信息安全问题,给出了切合实际的网络信息安全方法、网络信息安全机制和常用的安全工具;汇聚了国家网络信息安全法律法规及政策与标准规范、工业界网络信息安全产品技术与服务、学术界网络信息安全前沿技术研究成果、用户网络信息安全最佳实践经验和案例。

本书是计算机软件考试中信息安全工程师岗位的考试用书,也可作为各类高校网络信息安全相关专业的教材,还可用作信息技术相关领域从业人员的技术参考书。

本书扉页为防伪页,封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

信息安全工程师教程/蒋建春主编. —2 版. —北京:清华大学出版社,2020.8

全国计算机技术与软件专业技术资格(水平)考试指定用书

ISBN 978-7-302-55934-4

I. ①信… II. ①蒋… III. ①信息安全—安全技术—资格考试—教材 IV. ①TP309

中国版本图书馆 CIP 数据核字(2020)第 115882 号

责任编辑:杨如林

封面设计:常雪影

责任校对:白 蕾

责任印制:宋 林

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座

邮 编:100084

社 总 机:010-62770175

邮 购:010-83470235

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:三河市龙大印装有限公司

经 销:全国新华书店

开 本:185mm×230mm

印 张:37.25

防伪页:1

字 数:886 千字

版 次:2016 年 7 月第 1 版

2020 年 9 月第 2 版

印 次:2020 年 9 月第 1 次印刷

定 价:118.00 元

产品编号:079223-01

前言

网络空间已成为国家继陆、海、空、天四个疆域之后的第五疆域，正如《国家网络空间安全战略》所指出，网络空间已成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域。与此同时，网络安全问题也逐渐凸显。目前，网络安全形势日益严峻，网络安全新型威胁不断出现，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临多种风险与挑战。国际上争夺和控制网络空间战略资源，抢占规则制定权和战略制高点，谋求战略主动权的竞争日趋激烈。2014年，习近平总书记在中央网络安全与信息化领导小组会议上指出，没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全为人民，网络安全靠人民。为此，全国计算机技术与软件专业技术资格（水平）考试办公室决定开展“信息安全工程师”岗位的人才评价工作，以加快推进国家网络信息安全人才队伍建设。

为配合“信息安全工程师”考试工作的开展，给准备参加考试的技术人员提供一本合适的教材，我们受全国计算机专业技术资格考试办公室的委托，编写了这本《信息安全工程师教程》（第2版）。全书共26章，主要内容包括网络信息安全基础知识、网络信息安全主流技术、网络信息安全风险评估和测评、网络信息安全工程、网络信息安全管理、网络信息安全应用案例。书中汇聚了国家网络安全法律法规及政策与标准规范、学术界网络安全前沿技术研究成果、工业界网络安全产品技术与服务、用户网络安全最佳实践经验和案例。

本书由蒋建春任主编，文伟平、焦健任副主编。参加编写的人员还有梅瑞、杨海、胡振宇、李经纬、刘洪毅、兰阳、方字形、贾云龙、蒋时雨、魏柳、张逸然、王林飞、杜笑宇、赵国梁、刘宇航、叶何、陈夏润、陈勇龙、王小育等。此外，本书还直接引用了网络信息安全标准成果，并参考了网络上与信息安全相关的文章，因受篇幅限制，不便一一列举，在此表示感谢。书中若有涉及知识产权不当之处，敬请联系作者加以修订。

本书的编写参考和引用了政府部门、学术界、工业界、用户以及行业机构等单位的网络信息安全资料，特此表示感谢。相关单位主要有：国家网络安全职能部门、国家互联网应急中心（CNCERT）、全国信息安全标准化技术委员会、中国科学院软件研究所、中国信息安全测评中心、北京大学软件安全研究小组、北京信息安全测评中心，以及华为技术有限公司、阿里巴巴网络技术有限公司、深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、北京安天网络安全技术有限公司、北京天融信网络安全技术有限公司、绿盟科技集团股份有限公司、启明星辰信息技术集团股份有限公司、杭州安恒信息技术股份有限公司、北京安华金和科技有限公司、成都科来软件有限公司、北京数字证书认证中心、广东南电智控系统有限公司等。

非常感谢工业和信息化部教育与考试中心领导的信任和指导，尽管本书在编写过程中受到诸多因素的影响，但他们一直保持足够的耐心支持本书撰写完稿。

在本书历经两年多的编写过程中，尽管做了不少努力，力图使本书完美无缺，将理论联系实际，做到通俗易懂，但受作者水平和经验所限，书中难免出现不妥和错误之处，敬请读者批评指正，并在此表示感谢。

编者
2020 年于北京

目 录

第 1 章 网络信息安全概述	1	1.6.4 网络信息安全管理要素	11
1.1 网络发展现状与重要性认识	1	1.6.5 网络信息安全管理流程	13
1.1.1 网络信息安全相关概念	1	1.6.6 网络信息安全管理工具	14
1.1.2 网络信息安全重要性认识	1	1.6.7 网络信息安全管理评估	14
1.2 网络信息安全现状与问题	2	1.7 网络信息安全法律与政策文件	15
1.2.1 网络信息安全状况	2	1.7.1 网络信息安全基本法律与国家 战略	15
1.2.2 网络信息安全问题	3	1.7.2 网络安全等级保护	15
1.3 网络信息安全基本属性	5	1.7.3 国家密码管理制度	16
1.3.1 机密性	5	1.7.4 网络产品和服务审查	16
1.3.2 完整性	6	1.7.5 网络安全产品管理	17
1.3.3 可用性	6	1.7.6 互联域名安全管理	17
1.3.4 抗抵赖性	6	1.7.7 工业控制信息安全制度	18
1.3.5 可控性	6	1.7.8 个人信息和重要数据保护制度	18
1.3.6 其他	6	1.7.9 网络安全标准规范与测评	19
1.4 网络信息安全目标与功能	7	1.7.10 网络安全事件与应急响应制度	19
1.4.1 网络信息安全基本目标	7	1.8 网络信息安全科技信息获取	19
1.4.2 网络信息安全基本功能	8	1.8.1 网络信息安全会议	19
1.5 网络信息安全基本技术需求	8	1.8.2 网络信息安全期刊	20
1.5.1 物理环境安全	8	1.8.3 网络信息安全网站	20
1.5.2 网络信息安全认证	9	1.8.4 网络信息安全术语	20
1.5.3 网络信息访问控制	9	1.9 本章小结	21
1.5.4 网络信息安全保密	9	第 2 章 网络攻击原理与常用方法	22
1.5.5 网络信息安全漏洞扫描	9	2.1 网络攻击概述	22
1.5.6 恶意代码防护	9	2.1.1 网络攻击概念	22
1.5.7 网络信息内容安全	10	2.1.2 网络攻击模型	23
1.5.8 网络信息安全监测与预警	10	2.1.3 网络攻击发展	25
1.5.9 网络信息安全应急响应	10	2.2 网络攻击一般过程	27
1.6 网络信息安全管理内容与方法	10	2.2.1 隐藏攻击源	27
1.6.1 网络信息安全管理概念	10	2.2.2 收集攻击目标信息	28
1.6.2 网络信息安全管理方法	10	2.2.3 挖掘漏洞信息	28
1.6.3 网络信息安全管理依据	11		

2.2.4 获取目标访问权限.....	29	3.2 密码体制分类.....	45
2.2.5 隐蔽攻击行为.....	29	3.2.1 私钥密码体制.....	45
2.2.6 实施攻击.....	29	3.2.2 公钥密码体制.....	46
2.2.7 开辟后门.....	30	3.2.3 混合密码体制.....	47
2.2.8 清除攻击痕迹.....	30	3.3 常见密码算法.....	47
2.3 网络攻击常见技术方法.....	30	3.3.1 DES.....	47
2.3.1 端口扫描.....	30	3.3.2 IDEA.....	48
2.3.2 口令破解.....	32	3.3.3 AES.....	48
2.3.3 缓冲区溢出.....	33	3.3.4 RSA.....	49
2.3.4 恶意代码.....	33	3.3.5 国产密码算法.....	49
2.3.5 拒绝服务.....	34	3.4 Hash 函数与数字签名.....	50
2.3.6 网络钓鱼.....	35	3.4.1 Hash 函数.....	51
2.3.7 网络窃听.....	36	3.4.2 Hash 算法.....	51
2.3.8 SQL 注入.....	36	3.4.3 数字签名.....	52
2.3.9 社交工程.....	36	3.5 密码管理与数字证书.....	53
2.3.10 电子监听.....	37	3.5.1 密码管理.....	53
2.3.11 会话劫持.....	37	3.5.2 数字证书.....	55
2.3.12 漏洞扫描.....	37	3.6 安全协议.....	57
2.3.13 代理技术.....	37	3.6.1 Diffie-Hellman 密钥交换协议.....	57
2.3.14 数据加密.....	37	3.6.2 SSH.....	58
2.4 黑客常用工具.....	38	3.7 密码学网络安全应用.....	60
2.4.1 扫描器.....	38	3.7.1 密码技术常见应用场景类型.....	60
2.4.2 远程监控.....	38	3.7.2 路由器安全应用参考.....	61
2.4.3 密码破解.....	38	3.7.3 Web 网站安全应用参考.....	62
2.4.4 网络嗅探器.....	39	3.7.4 电子邮件安全应用参考.....	62
2.4.5 安全渗透工具箱.....	39	3.8 本章小结.....	62
2.5 网络攻击案例分析.....	39	第4章 网络安全体系与网络安全模型	63
2.5.1 DDoS 攻击.....	39	4.1 网络安全体系概述.....	63
2.5.2 W32.Blaster.Worm.....	41	4.1.1 网络安全体系概念.....	63
2.5.3 网络安全导致停电事件.....	42	4.1.2 网络安全体系特征.....	63
2.6 本章小结.....	43	4.1.3 网络安全体系用途.....	64
第3章 密码学基本理论	44	4.2 网络安全体系相关安全模型.....	64
3.1 密码学概况.....	44	4.2.1 BLP 机密性模型.....	64
3.1.1 密码学发展简况.....	44	4.2.2 BiBa 完整性模型.....	65
3.1.2 密码学基本概念.....	45	4.2.3 信息流模型.....	65
3.1.3 密码安全性分析.....	45	4.2.4 信息保障模型.....	66

4.2.5 能力成熟度模型	66	5.1.3 物理安全保护	98
4.2.6 纵深防御模型	69	5.1.4 物理安全规范	99
4.2.7 分层防护模型	70	5.2 物理环境安全分析与防护	100
4.2.8 等级保护模型	70	5.2.1 防火	100
4.2.9 网络生存模型	71	5.2.2 防水	100
4.3 网络安全体系建设原则与安全策略	71	5.2.3 防震	101
4.3.1 网络安全原则	72	5.2.4 防盗	101
4.3.2 网络安全策略	73	5.2.5 防鼠虫害	101
4.4 网络安全体系框架主要组成和建设内容	73	5.2.6 防雷	101
4.4.1 网络安全体系组成框架	74	5.2.7 防电磁	102
4.4.2 网络安全策略建设内容	76	5.2.8 防静电	102
4.4.3 网络安全组织体系构建内容	76	5.2.9 安全供电	102
4.4.4 网络安全管理体系构建内容	77	5.3 机房安全分析与防护	102
4.4.5 网络安全基础设施及网络安全 服务构建内容	81	5.3.1 机房功能区域组成	102
4.4.6 网络安全技术体系构建内容	82	5.3.2 机房安全等级划分	103
4.4.7 网络信息科技与产业生态构建 内容	82	5.3.3 机房场地选择要求	104
4.4.8 网络安全教育与培训构建内容	82	5.3.4 数据中心建设与设计要求	105
4.4.9 网络安全标准与规范构建内容	83	5.3.5 互联网数据中心	106
4.4.10 网络安全运营与应急响应构建 内容	83	5.3.6 CA 机房物理安全控制	107
4.4.11 网络安全投入与建设构建内容	84	5.4 网络通信线路安全分析与防护	108
4.5 网络安全体系建设参考案例	84	5.4.1 网络通信线路安全分析	108
4.5.1 网络安全等级保护体系应用参考	85	5.4.2 网络通信线路安全防护	108
4.5.2 智慧城市安全体系应用参考	86	5.5 设备实体安全分析与防护	109
4.5.3 智能交通网络安全体系应用参考	87	5.5.1 设备实体安全分析	109
4.5.4 ISO 27000 信息安全管理体系 应用参考	91	5.5.2 设备实体安全防护	110
4.5.5 NIST 网络安全框架体系应用 参考	92	5.5.3 设备硬件攻击防护	111
4.6 本章小结	95	5.6 存储介质安全分析与防护	112
第 5 章 物理与环境安全技术	96	5.6.1 存储介质安全分析	112
5.1 物理安全概念与要求	96	5.6.2 存储介质安全防护	113
5.1.1 物理安全概念	96	5.7 本章小结	114
5.1.2 物理安全威胁	96	第 6 章 认证技术原理与应用	115
		6.1 认证概述	115
		6.1.1 认证概念	115
		6.1.2 认证依据	115
		6.1.3 认证原理	116
		6.1.4 认证发展	117

6.2 认证类型与认证过程	117
6.2.1 单向认证	118
6.2.2 双向认证	118
6.2.3 第三方认证	119
6.3 认证技术方法	120
6.3.1 口令认证技术	120
6.3.2 智能卡技术	121
6.3.3 基于生物特征认证技术	122
6.3.4 Kerberos 认证技术	125
6.3.5 公钥基础设施（PKI）技术	129
6.3.6 单点登录	130
6.3.7 基于人机识别认证技术	130
6.3.8 多因素认证技术	130
6.3.9 基于行为的身份鉴别技术	130
6.3.10 快速在线认证（FIDO）	131
6.4 认证主要产品与技术指标	133
6.4.1 认证主要产品	133
6.4.2 主要技术指标	134
6.5 认证技术应用	134
6.5.1 校园信任体系建设应用参考	134
6.5.2 网络路由认证应用参考	135
6.5.3 基于人脸识别机房门禁管理应 用参考	137
6.5.4 eID 身份验证应用参考	138
6.5.5 HTTP 认证应用参考	138
6.6 本章小结	139
第7章 访问控制技术原理与应用	140
7.1 访问控制概述	140
7.1.1 访问控制概念	140
7.1.2 访问控制目标	140
7.2 访问控制模型	141
7.2.1 访问控制参考模型	141
7.2.2 访问控制模型发展	142
7.3 访问控制类型	142
7.3.1 自主访问控制	143
7.3.2 强制访问控制	144

7.3.3 基于角色的访问控制	144
7.3.4 基于属性的访问控制	145
7.4 访问控制策略设计与实现	146
7.4.1 访问控制策略	146
7.4.2 访问控制规则	147
7.5 访问控制过程与安全管理	148
7.5.1 访问控制过程	148
7.5.2 最小特权管理	148
7.5.3 用户访问管理	148
7.5.4 口令安全管理	149
7.6 访问控制主要产品与技术指标	150
7.6.1 访问控制主要产品	150
7.6.2 访问控制主要技术指标	150
7.7 访问控制技术应用	151
7.7.1 访问控制技术应用场景类型	151
7.7.2 UNIX/Linux 系统访问控制应用 参考	151
7.7.3 Windows 访问控制应用参考	152
7.7.4 IIS FTP 访问控制应用参考	153
7.7.5 网络访问控制应用参考	154
7.7.6 Web 服务访问控制应用参考	155
7.7.7 基于角色管理的系统访问控制 应用参考	156
7.7.8 网络安全等级保护访问控制设 计应用参考	156
7.8 本章小结	158
第8章 防火墙技术原理与应用	159
8.1 防火墙概述	159
8.1.1 防火墙概念	159
8.1.2 防火墙工作原理	159
8.1.3 防火墙安全风险	161
8.1.4 防火墙发展	161
8.2 防火墙类型与实现技术	162
8.2.1 包过滤	162
8.2.2 状态检查技术	165
8.2.3 应用服务代理	165

8.2.4	网络地址转换技术	167	9.3	VPN 主要产品与技术指标	189
8.2.5	Web 防火墙技术	168	9.3.1	VPN 主要产品	189
8.2.6	数据库防火墙技术	168	9.3.2	VPN 产品主要技术指标	189
8.2.7	工控防火墙技术	169	9.4	VPN 技术应用	191
8.2.8	下一代防火墙技术	169	9.4.1	VPN 应用场景	191
8.2.9	防火墙共性关键技术	170	9.4.2	远程安全访问	191
8.3	防火墙主要产品与技术指标	170	9.4.3	构建内部安全专网	191
8.3.1	防火墙主要产品	171	9.4.4	外部网络安全互联	192
8.3.2	防火墙主要技术指标	172	9.5	本章小结	192
8.4	防火墙防御体系结构类型	173	第 10 章 入侵检测技术原理与应用	193	
8.4.1	基于双宿主主机防火墙结构	173	10.1	入侵检测概述	193
8.4.2	基于代理型防火墙结构	174	10.1.1	入侵检测概念	193
8.4.3	基于屏蔽子网的防火墙结构	174	10.1.2	入侵检测模型	193
8.5	防火墙技术应用	175	10.1.3	入侵检测作用	194
8.5.1	防火墙应用场景类型	175	10.2	入侵检测技术	194
8.5.2	防火墙部署基本方法	176	10.2.1	基于误用的入侵检测技术	195
8.5.3	IPtables 防火墙应用参考	176	10.2.2	基于异常的入侵检测技术	196
8.5.4	Web 应用防火墙应用参考	180	10.2.3	其他	198
8.5.5	包过滤防火墙应用参考	180	10.3	入侵检测系统组成与分类	199
8.5.6	工控防火墙应用参考	181	10.3.1	入侵检测系统组成	200
8.6	本章小结	182	10.3.2	基于主机的入侵检测系统	200
第 9 章 VPN 技术原理与应用	183		10.3.3	基于网络的入侵检测系统	202
9.1	VPN 概述	183	10.3.4	分布式入侵检测系统	203
9.1.1	VPN 概念	183	10.4	入侵检测系统主要产品与技术指标	204
9.1.2	VPN 安全功能	183	10.4.1	入侵检测相关产品	205
9.1.3	VPN 发展	184	10.4.2	入侵检测相关指标	207
9.1.4	VPN 技术风险	184	10.5	入侵检测系统应用	208
9.2	VPN 类型和实现技术	184	10.5.1	入侵检测应用场景类型	208
9.2.1	VPN 类型	184	10.5.2	入侵检测系统部署方法	209
9.2.2	密码算法	184	10.5.3	基于 HIDS 的主机威胁检测	209
9.2.3	密钥管理	185	10.5.4	基于 NIDS 的内网威胁检测	210
9.2.4	认证访问控制	185	10.5.5	基于 NIDS 的网络边界威胁检测	210
9.2.5	IPSec	185	10.5.6	网络安全态势感知应用参考	210
9.2.6	SSL	186	10.5.7	开源网络入侵检测系统	211
9.2.7	PPTP	188	10.5.8	华为 CIS 网络安全智能系统应用	213
9.2.8	L2TP	188	10.6	本章小结	215

第11章 网络物理隔离技术原理与应用.....216

11.1 网络物理隔离概述.....216	
11.1.1 网络物理隔离概念.....216	
11.1.2 网络物理隔离安全风险.....216	
11.2 网络物理隔离系统与类型.....217	
11.2.1 网络物理隔离系统.....217	
11.2.2 网络物理隔离类型.....218	
11.3 网络物理隔离机制与实现技术.....218	
11.3.1 专用计算机上网.....218	
11.3.2 多PC.....218	
11.3.3 外网代理服务.....218	
11.3.4 内外网线路切换器.....219	
11.3.5 单硬盘内外分区.....219	
11.3.6 双硬盘.....220	
11.3.7 网闸.....220	
11.3.8 协议隔离技术.....221	
11.3.9 单向传输部件.....221	
11.3.10 信息摆渡技术.....221	
11.3.11 物理断开技术.....221	
11.4 网络物理隔离主要产品与技术指标.....221	
11.4.1 网络物理隔离主要产品.....222	
11.4.2 网络物理隔离技术指标.....223	
11.5 网络物理隔离应用.....224	
11.5.1 工作机安全上网实例.....224	
11.5.2 电子政务中国网闸应用实例.....225	
11.6 本章小结.....226	
第12章 网络安全审计技术原理与应用227	
12.1 网络安全审计概述.....227	
12.1.1 网络安全审计概念.....227	
12.1.2 网络安全审计相关标准.....227	
12.1.3 网络安全审计相关法规政策.....228	
12.2 网络安全审计系统组成与类型.....228	
12.2.1 网络安全审计系统组成.....228	
12.2.2 网络安全审计系统类型.....229	
12.3 网络安全审计机制与实现技术.....230	
12.3.1 系统日志数据采集技术.....230	

12.3.2 网络流量数据获取技术.....231	
12.3.3 网络审计数据安全技术.....234	
12.3.4 网络审计数据存储技术.....235	
12.3.5 网络审计数据保护技术.....235	
12.4 网络安全审计主要产品与技术指标.....236	
12.4.1 日志安全审计产品.....236	
12.4.2 主机监控与审计产品.....236	
12.4.3 数据库审计产品.....237	
12.4.4 网络安全审计产品.....238	
12.4.5 工业控制系统网络审计产品.....239	
12.4.6 运维安全审计产品.....239	
12.5 网络安全审计应用.....240	
12.5.1 安全运维保障.....241	
12.5.2 数据访问监测.....241	
12.5.3 网络入侵检测.....242	
12.5.4 网络电子取证.....242	
12.6 本章小结.....242	

第13章 网络安全漏洞防护技术原理

与应用243	
13.1 网络安全漏洞概述.....243	
13.1.1 网络安全漏洞概念.....243	
13.1.2 网络安全漏洞威胁.....243	
13.1.3 网络安全漏洞问题现状.....244	
13.2 网络安全漏洞分类与管理.....245	
13.2.1 网络安全漏洞来源.....245	
13.2.2 网络安全漏洞分类.....246	
13.2.3 网络安全漏洞发布.....249	
13.2.4 网络安全漏洞信息获取.....250	
13.2.5 网络安全漏洞管理过程.....252	
13.3 网络安全漏洞扫描技术与应用.....253	
13.3.1 网络安全漏洞扫描.....253	
13.3.2 网络安全漏洞扫描应用.....256	
13.4 网络安全漏洞处置技术与应用.....257	
13.4.1 网络安全漏洞发现技术.....257	
13.4.2 网络安全漏洞修补技术.....257	
13.4.3 网络安全漏洞利用防范技术.....258	

13.5 网络安全漏洞防护主要产品与技术指标	259	14.6 其他恶意代码分析与防护	290
13.5.1 网络安全漏洞扫描器	259	14.6.1 逻辑炸弹	291
13.5.2 网络安全漏洞服务平台	260	14.6.2 陷门.....	291
13.5.3 网络安全漏洞防护网关	260	14.6.3 细菌.....	291
13.6 本章小结.....	260	14.6.4 间谍软件	291
第 14 章 恶意代码防范技术原理	261	14.7 恶意代码防护主要产品与技术指标.....	292
14.1 恶意代码概述	261	14.7.1 恶意代码防护主要产品	292
14.1.1 恶意代码定义与分类	261	14.7.2 恶意代码防护主要技术指标.....	293
14.1.2 恶意代码攻击模型.....	262	14.8 恶意代码防护技术应用	293
14.1.3 恶意代码生存技术.....	263	14.8.1 终端防护	294
14.1.4 恶意代码攻击技术.....	266	14.8.2 APT 防护	294
14.1.5 恶意代码分析技术.....	267	14.9 本章小结	295
14.1.6 恶意代码防范策略.....	270	第 15 章 网络安全主动防御技术	
14.2 计算机病毒分析与防护	271	与应用	296
14.2.1 计算机病毒概念与特性	271	15.1 入侵阻断技术与应用.....	296
14.2.2 计算机病毒组成与运行机制	272	15.1.1 入侵阻断技术原理	296
14.2.3 计算机病毒常见类型与技术	272	15.1.2 入侵阻断技术应用	297
14.2.4 计算机病毒防范策略与技术	274	15.2 软件白名单技术与应用	297
14.2.5 计算机病毒防护方案	276	15.2.1 软件白名单技术原理	297
14.3 特洛伊木马分析与防护	278	15.2.2 软件白名单技术应用	298
14.3.1 特洛伊木马概念与特性	278	15.3 网络流量清洗技术与应用	301
14.3.2 特洛伊木马分类	278	15.3.1 网络流量清洗技术原理.....	301
14.3.3 特洛伊木马运行机制	278	15.3.2 网络流量清洗技术应用	301
14.3.4 特洛伊木马植入技术	279	15.4 可信计算技术与应用.....	302
14.3.5 特洛伊木马隐藏技术	279	15.4.1 可信计算技术原理	303
14.3.6 特洛伊木马存活技术	281	15.4.2 可信计算技术应用	305
14.3.7 特洛伊木马防范技术	281	15.5 数字水印技术与应用.....	308
14.4 网络蠕虫分析与防护	283	15.5.1 数字水印技术原理	308
14.4.1 网络蠕虫概念与特性	283	15.5.2 数字水印技术应用	309
14.4.2 网络蠕虫组成与运行机制	284	15.6 网络攻击陷阱技术与应用	310
14.4.3 网络蠕虫常用技术.....	285	15.6.1 网络攻击陷阱技术原理.....	310
14.4.4 网络蠕虫防范技术.....	287	15.6.2 网络攻击陷阱技术应用	313
14.5 僵尸网络分析与防护	289	15.7 入侵容忍及系统生存技术与应用	313
14.5.1 僵尸网络概念与特性	289	15.7.1 入侵容忍及系统生存技术原理 ...	314
14.5.2 僵尸网络运行机制与技术	290	15.7.2 入侵容忍及系统生存技术应用 ...	314
14.5.3 僵尸网络防范技术.....	290	15.8 隐私保护技术与应用.....	315

15.8.1 隐私保护类型及技术原理	315	16.4.5 评估结果评审与认可	340
15.8.2 隐私保护技术应用	316	16.5 网络安全风险评估技术应用	340
15.9 网络安全前沿技术发展动向	317	16.5.1 网络安全风险评估应用场景	340
15.9.1 网络威胁情报服务	317	16.5.2 OWASP 风险评估方法参考	341
15.9.2 域名服务安全保障	318	16.5.3 ICT 供应链安全威胁识别参考	343
15.9.3 同态加密技术	319	16.5.4 工业控制系统平台脆弱性识别 参考	344
15.10 本章小结	320	16.5.5 网络安全风险处理措施参考	350
第 16 章 网络安全风险评估技术原理 与应用	321	16.5.6 人工智能安全风险参考	351
16.1 网络安全风险评估概述	321	16.6 本章小结	352
16.1.1 网络安全风险评估概念	321	第 17 章 网络安全应急响应技术原理 与应用	353
16.1.2 网络安全风险评估要素	322	17.1 网络安全应急响应概述	353
16.1.3 网络安全风险评估模式	322	17.1.1 网络安全应急响应概念	353
16.2 网络安全风险评估过程	323	17.1.2 网络安全应急响应发展	353
16.2.1 网络安全风险评估准备	323	17.1.3 网络安全应急响应相关要求	354
16.2.2 资产识别	324	17.2 网络安全应急响应组织建立与工作机制	354
16.2.3 威胁识别	326	17.2.1 网络安全应急响应组织建立	354
16.2.4 脆弱性识别	329	17.2.2 网络安全应急响应组织工作机制	355
16.2.5 已有安全措施确认	330	17.2.3 网络安全应急响应组织类型	355
16.2.6 网络安全风险分析	330	17.3 网络安全应急响应预案内容与类型	356
16.2.7 网络安全风险处置与管理	334	17.3.1 网络安全事件类型与分级	356
16.3 网络安全风险评估技术方法与工具	335	17.3.2 网络安全应急响应预案内容	357
16.3.1 资产信息收集	335	17.3.3 网络安全应急响应预案类型	357
16.3.2 网络拓扑发现	335	17.4 常见网络安全应急事件场景与处理流程	359
16.3.3 网络安全漏洞扫描	336	17.4.1 常见网络安全应急处理场景	359
16.3.4 人工检查	336	17.4.2 网络安全应急处理流程	360
16.3.5 网络安全渗透测试	337	17.4.3 网络安全事件应急演练	361
16.3.6 问卷调查	337	17.5 网络安全应急响应技术与常见工具	362
16.3.7 网络安全访谈	338	17.5.1 网络安全应急响应技术概况	362
16.3.8 审计数据分析	338	17.5.2 访问控制	363
16.3.9 入侵监测	338	17.5.3 网络安全评估	363
16.4 网络安全风险评估项目流程和工作内容	339	17.5.4 网络安全监测	365
16.4.1 评估工程前期准备	339	17.5.5 系统恢复	367
16.4.2 评估方案设计与论证	339	17.5.6 入侵取证	369
16.4.3 评估方案实施	339	17.6 网络安全应急响应参考案例	370
16.4.4 风险评估报告撰写	340		

17.6.1 公共互联网网络安全突发事件 应急预案	370	19.2 Windows 操作系统安全分析与防护	397
17.6.2 阿里云安全应急响应服务	370	19.2.1 Windows 系统架构	397
17.6.3 IBM 产品安全漏洞应急响应	373	19.2.2 Windows 安全机制	399
17.6.4 “永恒之蓝”攻击的紧急处置	374	19.2.3 Windows 系统安全分析	402
17.6.5 页面篡改事件处置规程	376	19.2.4 Windows 系统安全增强技术 方法与流程	403
17.7 本章小结	378	19.2.5 Windows 2000 系统安全增强 实例	406
第 18 章 网络安全测评技术与标准	379	19.2.6 Windows 系统典型安全工具 与参考规范	410
18.1 网络安全测评概况	379	19.3 UNIX/Linux 操作系统安全分析与防护	410
18.1.1 网络安全测评概念	379	19.3.1 UNIX/Linux 系统架构	410
18.1.2 网络安全测评发展	379	19.3.2 UNIX/Linux 安全机制	410
18.2 网络安全测评类型	380	19.3.3 UNIX/Linux 系统安全分析	412
18.2.1 基于测评目标分类	380	19.3.4 UNIX/Linux 系统安全增强方 法和流程	414
18.2.2 基于测评内容分类	381	19.3.5 UNIX/Linux 系统安全增强技术	416
18.2.3 基于实施方式分类	381	19.3.6 Linux 安全增强配置参考	419
18.2.4 基于测评对象保密性分类	382	19.3.7 UNIX/Linux 安全模块应用参考	422
18.3 网络安全测评流程与内容	383	19.3.8 UNIX/Linux 系统典型安全工 具与参考规范	424
18.3.1 网络安全等级保护测评流程与 内容	383	19.4 国产操作系统安全分析与防护	424
18.3.2 网络安全渗透测试流程与内容	383	19.4.1 国产操作系统概况	424
18.4 网络安全测评技术与工具	384	19.4.2 国产操作系统安全分析	425
18.4.1 漏洞扫描	384	19.4.3 国产操作系统安全增强措施	425
18.4.2 安全渗透测试	385	19.5 本章小结	427
18.4.3 代码安全审查	385	第 20 章 数据库系统安全	428
18.4.4 协议分析	385	20.1 数据库安全概况	428
18.4.5 性能测试	387	20.1.1 数据库安全概念	428
18.5 网络安全测评质量管理与标准	388	20.1.2 数据库安全威胁	428
18.5.1 网络安全测评质量管理	388	20.1.3 数据库安全隐患	429
18.5.2 网络安全测评标准	388	20.1.4 数据库安全需求	430
18.6 本章小结	394	20.2 数据库安全机制与实现技术	431
第 19 章 操作系统安全保护	395	20.2.1 数据库安全机制	431
19.1 操作系统安全概述	395	20.2.2 数据库加密	432
19.1.1 操作系统安全概念	395	20.2.3 数据库防火墙	433
19.1.2 操作系统安全需求	395		
19.1.3 操作系统安全机制	396		
19.1.4 操作系统安全技术	397		

20.2.4 数据库脱敏	434	21.3.2 路由器安全增强技术方法	465
20.2.5 数据库漏洞扫描	434	21.4 网络设备常见漏洞与解决方法	469
20.3 Oracle 数据库安全分析与防护	434	21.4.1 网络设备常见漏洞	469
20.3.1 Oracle 概况	435	21.4.2 网络设备漏洞解决方法	470
20.3.2 Oracle 数据库安全分析	435	21.5 本章小结	472
20.3.3 Oracle 安全最佳实践	437	第 22 章 网站安全需求分析与安全保	
20.3.4 Oracle 漏洞修补	438	护工程	473
20.4 MS SQL 数据库安全分析与防护	439	22.1 网站安全威胁与需求分析	473
20.4.1 MS SQL Server 概况	439	22.1.1 网站安全概念	473
20.4.2 MS SQL 安全分析	439	22.1.2 网站安全分析	474
20.4.3 MS SQL Server 安全最佳实践	440	22.1.3 网站安全需求	475
20.4.4 MS SQL Server 漏洞修补	441	22.2 Apache Web 安全分析与增强	476
20.5 MySQL 数据库安全分析与防护	441	22.2.1 Apache Web 概述	476
20.5.1 MySQL 概况	441	22.2.2 Apache Web 安全分析	476
20.5.2 MySQL 安全分析	441	22.2.3 Apache Web 安全机制	477
20.5.3 MySQL 安全最佳实践	442	22.2.4 Apache Web 安全增强	480
20.5.4 MySQL 漏洞修补	443	22.3 IIS 安全分析与增强	483
20.6 国产数据库安全分析与防护	443	22.3.1 IIS 概述	483
20.6.1 国产数据库概况	443	22.3.2 IIS 安全分析	484
20.6.2 国产数据库安全分析	443	22.3.3 IIS 安全机制	485
20.6.3 国产数据库安全增强措施	444	22.3.4 IIS 安全增强	486
20.7 本章小结	446	22.4 Web 应用漏洞分析与防护	488
第 21 章 网络设备安全	447	22.4.1 Web 应用安全概述	488
21.1 网络设备安全概况	447	22.4.2 OWASP Top 10	488
21.1.1 交换机安全威胁	447	22.4.3 Web 应用漏洞防护	492
21.1.2 路由器安全威胁	448	22.5 网站安全保护机制与技术方案	495
21.2 网络设备安全机制与实现技术	449	22.5.1 网站安全保护机制	495
21.2.1 认证机制	449	22.5.2 网站构成组件安全加固	496
21.2.2 访问控制	452	22.5.3 网站攻击防护及安全监测	497
21.2.3 信息加密	456	22.6 网站安全综合应用案例分析	499
21.2.4 安全通信	457	22.6.1 政务网站安全保护	499
21.2.5 日志审计	458	22.6.2 网上银行安全保护	501
21.2.6 安全增强	459	22.7 本章小结	502
21.2.7 物理安全	461	第 23 章 云计算安全需求分析与安全	
21.3 网络设备安全增强技术方法	461	保护工程	503
21.3.1 交换机安全增强技术方法	461	23.1 云计算安全概念与威胁分析	503

23.1.1 云计算基本概念	503	24.2.10 工控安全管理	536
23.1.2 云计算安全分析	504	24.2.11 工控安全典型产品技术	537
23.1.3 云计算安全要求	508	24.3 工控系统安全综合应用案例分析	538
23.2 云计算服务安全需求	508	24.3.1 电力监控系统安全总体方案	538
23.2.1 云计算技术安全需求	509	24.3.2 水厂工控安全集中监控	540
23.2.2 云计算安全合规需求	509	24.3.3 工控安全防护厂商方案	541
23.2.3 云计算隐私保护需求	510	24.4 本章小结	542
23.3 云计算安全保护机制与技术方案	511	第 25 章 移动应用安全需求分析与安	
23.3.1 云计算安全等级保护框架	511	全保护工程	543
23.3.2 云计算安全防护	512	25.1 移动应用安全威胁与需求分析	543
23.3.3 云计算安全管理	513	25.1.1 移动应用系统组成	543
23.3.4 云计算安全运维	513	25.1.2 移动应用安全分析	543
23.4 云计算安全综合应用案例分析	514	25.2 Android 系统安全与保护机制	544
23.4.1 阿里云安全	514	25.2.1 Android 系统组成概要	544
23.4.2 腾讯云安全	516	25.2.2 Android 系统安全机制	545
23.4.3 华为云安全	520	25.3 iOS 系统安全与保护机制	547
23.4.4 微软 Azure 云安全	522	25.3.1 iOS 系统组成概要	547
23.4.5 云计算隐私保护	524	25.3.2 iOS 系统安全机制	548
23.5 本章小结	525	25.4 移动应用安全保护机制与技术方案	551
第 24 章 工控安全需求分析与安全保		25.4.1 移动应用 App 安全风险	551
护工程	526	25.4.2 移动应用 App 安全加固	551
24.1 工控系统安全威胁与需求分析	526	25.4.3 移动应用 App 安全检测	552
24.1.1 工业控制系统概念及组成	526	25.5 移动应用安全综合应用案例分析	553
24.1.2 工业控制系统安全威胁分析	529	25.5.1 金融移动安全	553
24.1.3 工业控制系统安全隐患类型	530	25.5.2 运营商移动安全	554
24.1.4 工业控制系统安全需求分析	531	25.5.3 移动办公安全	554
24.2 工控系统安全保护机制与技术	532	25.6 本章小结	555
24.2.1 物理及环境安全防护	532	第 26 章 大数据安全需求分析与安全	
24.2.2 安全边界保护	532	保护工程	556
24.2.3 身份认证与访问控制	533	26.1 大数据安全威胁与需求分析	556
24.2.4 远程访问安全	533	26.1.1 大数据相关概念发展	556
24.2.5 工控系统安全加固	534	26.1.2 大数据安全威胁分析	556
24.2.6 工控安全审计	534	26.1.3 大数据安全法规政策	558
24.2.7 恶意代码防范	534	26.1.4 大数据安全需求分析	560
24.2.8 工控数据安全	535	26.2 大数据安全保护机制与技术方案	560
24.2.9 工控安全监测与应急响应	535	26.2.1 大数据安全保护机制	561

26.2.2	大数据自身安全保护技术	561	26.3.3	上海数据交易中心安全保护	565
26.2.3	大数据平台安全保护技术	561	26.3.4	华为大数据安全实践	566
26.2.4	大数据业务安全保护技术	561	26.3.5	科学数据安全 管理	567
26.2.5	大数据隐私安全保护技术	561	26.3.6	支付卡行业数据安全规范	568
26.2.6	大数据运营安全保护技术	561	26.4	本章小结	568
26.2.7	大数据安全标准规范	562	附录 A	网络安全产品测评相关标准	569
26.3	大数据安全综合应用案例分析	562	附录 B	公共互联网网络安全突发事件	
26.3.1	阿里巴巴大数据安全实践	562	应急预案		571
26.3.2	京东大数据安全实践	564	参考文献		580

第 1 章 网络信息安全概述

1.1 网络发展现状与重要性认识

信息传递和安全的重要性自古以来都得到人们的认可。早在中国古代就建立了烽火台、驿站以快速传递军事信息，可见人们对信息重要价值的认同和重视。随着网络信息科技和应用的发展，数字化信息的传递日益快速和普及，全球变成了一个“地球村”，神话传说中的“顺风耳”和“千里眼”成为现实。数字化、网络化、智能化成为信息社会的主要特征，“万物互联”时代已经来临。基于 TCP/IP 协议的互联技术理念已广泛、深入地应用到工业生产、商业服务、社会生活等各个领域，形成各种各样的网络，如工业互联网、车联网、社交网、产业互联网等，这些网络不断推动各个领域的变革。计算机网络演变成人类活动的新空间，即网络空间，它是国家继陆、海、空、天四个疆域之后的第五疆域。与此同时，网络空间信息安全（通称为网络信息安全）问题也日益凸显，网络信息安全的影响越来越大。本节主要讲述网络空间的相关概念，简要给出了网络信息安全的演变过程，同时阐述了国内外对于网络信息安全重要性的认识和采取的战略措施。

1.1.1 网络信息安全相关概念

网络信息安全的发展历经了通信保密、计算机安全、信息保障、可信计算等阶段。狭义上的网络信息安全特指网络信息系统的各组成要素符合安全属性的要求，即机密性、完整性、可用性、抗抵赖性、可控性。广义上的网络信息安全是涉及国家安全、城市安全、经济安全、社会安全、生产安全、人身安全等在内的“大安全”。网络信息安全通常简称为网络安全。根据《中华人民共和国网络安全法》中的用语含义，网络安全是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

围绕网络安全问题，保障网络信息安全的对象内容、理念方法、持续时间都在不断演变，其新的变化表现为三个方面：一是保障内容从单维度向多维度转变，保障的维度包含网络空间域、物理空间域、社会空间域；二是网络信息安全保障措施从单一性（技术）向综合性（法律、政策、技术、管理、产业、教育）演变；三是保障时间维度要求涵盖网络系统的整个生命周期，保障响应速度要求不断缩短，网络信息安全没有战时、平时之分，而是时时刻刻。

1.1.2 网络信息安全重要性认识

正如《国家网络空间安全战略》所指出，网络空间已成为信息传播的新渠道、生产生活的

新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域。网络空间正在全面改变人们的生产生活方式，深刻影响人类社会历史的发展进程。

随着网络信息化应用的深入进展，网络空间已经成为支撑关键行业开展业务的基础平台，网络信息安全将直接影响业务的正常运转，关系国家安全、社会稳定和数字经济的发展。目前，网络信息安全形势日益严峻，网络信息安全新型威胁不断出现，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临多种风险与挑战。国际上争夺和控制网络空间战略资源，抢占规则制定权和战略制高点，谋求战略主动权的竞争日趋激烈。

网络空间是不同于陆、海、空、天的虚拟数字空间，人们常常难以直接感受到其存在。因而，网络空间信息安全与传统安全有着明显差异，其具有网络安全威胁高隐蔽性、网络安全技术高密集性、网络安全控制地理区域不可限制性、网络安全防护时间不可区分性、网络攻防严重非对称性等特点。2016年国家发布了《国家网络空间安全战略》，相关的网络安全法律法规政策也相继出台。《中华人民共和国网络安全法》已于2017年6月1日起实施。为加强网络安全教育，网络空间安全已被增设为一级学科。自2014年起，全国各地政府部门定期组织举办“国家网络安全宣传周”，以提升全民的网络安全意识。国家网络安全工作坚持网络安全为人民，网络安全靠人民，让“没有网络安全就没有国家安全”成为全社会的共识。

1.2 网络信息安全现状与问题

本节主要阐述网络信息安全的基本状况，分析网络信息安全存在的主要问题。

1.2.1 网络信息安全状况

目前，网络面临着不同动机的威胁，要承受不同类型的攻击。网络信息泄露、恶意代码、垃圾邮件、网络恐怖主义等都会影响网络安全。多协议、多系统、多应用、多用户组成的网络环境，复杂性高，存在难以避免的安全漏洞。网络安全事件时有发生，如震网病毒、乌克兰大停电事件、多国银行 SWIFT 系统被攻击事件、物联网恶意程序导致美国断网事件、域名劫持事件、永恒之蓝网络蠕虫事件等^①。2018年，CNCERT 协调处置网络安全事件约 10.6 万起，其中网页仿冒事件最多，其次是安全漏洞、恶意程序、网页篡改、网站后门、DDoS 攻击等事件。国内外研究表明，针对关键信息基础设施的高级持续威胁（简称 APT）日趋常态化。2018年，全球专业网络安全机构发布了各类高级威胁研究报告 478 份，同比增长了约 3.6 倍，这些报告涉及已被确认的 APT 攻击组织包括 APT28、Lazarus、Group 123、海莲花、MuddyWater 等 53 个^①。网络安全相关研究工作表明，国外 APT 组织已经针对国内的金融、政府、教育、科研等目标系统持续发动攻击。

^① 相关信息来源于 360 威胁情报中心《全球关键信息基础设施网络安全状况分析报告》、CNCERT《2018 年我国互联网网络安全态势综述》。

1.2.2 网络信息安全问题

网络信息安全是网络信息化不可避免的重要工作，主要有十二个方面的问题亟须解决，分别叙述如下。

1. 网络强依赖性及网络安全关联风险凸显

随着网络信息技术的发展，社会各个方面对网络信息系统的依赖性增强，且各种关键信息基础设施相互关联，因而对网络安全的影响范围日益扩大，产生级联反应、蝴蝶效应，建立可信的网络信息环境成为迫切的需求。

2. 网络信息产品供应链与安全质量风险

国内网信核心技术欠缺，许多关键产品和服务对国外的依赖度仍然较高，从硬件到软件都不同程度地受制于人，网络安全基础仍然不牢靠。同时，网络信息产品技术的安全质量问题具有普遍性，网络安全漏洞时有出现，即使知名 IT 厂商的产品也或多或少存在安全漏洞，网络安全漏洞的发现与管理任务仍然艰巨。根据国家信息安全漏洞共享平台统计（截至 2020 年 5 月），操作系统漏洞条目已达到上万条，网络设备漏洞条目有七千多条，数据库漏洞条目有两千多条。2018 年，CNCERT 使用工业互联网安全测试平台 Acheron，对主流工业控制设备、网络安全专用产品进行了安全入网抽检，并对电力二次设备进行了专项安全测试，在所涉及的产品中共发现两百多个高危漏洞，这些漏洞可能产生的风险有拒绝服务攻击、远程命令执行、信息泄露等。

3. 网络信息产品技术同质性与技术滥用风险

网络信息系统软硬件产品技术具有高度同质性，缺少技术多样性，极易构成大规模网络安全事件触发条件，特别是网络蠕虫安全事件。同时，网络信息技术滥用容易导致网络安全事件发生，如大规模隐私数据泄露，内部人员滥用网络信息技术特权构成网络安全威胁。网络安全威胁技术的工具化，让攻击操作易于实现，使网络攻击活动日益频繁和广泛流行。

4. 网络安全建设与管理发展不平衡、不充分风险

网络安全建设缺乏总体设计，常常采取“亡羊补牢”的方式构建网络安全机制，从而导致网络信息安全隐患。“重技术，轻管理；重建设，轻运营；重硬件，轻软件”的网络安全认识偏差，使得网络安全机制难以有效运行，导致网络安全建设不全面。例如，网络设备的口令直接用厂家默认配置，认证访问控制机制形同虚设。2018 年 CNCERT 开展的远程安全巡检工作发现，电力行业暴露相关监控管理系统 532 个，涉及政府监管、电企管理、用电管理和云平台 4 大类；城市公用工程行业暴露相关监控管理系统 1015 个，涉及供水、供暖和燃气 3 大类；石油天然气行业暴露相关监控管理系统 298 个，涉及油气开采、油气运输、油气存储、油品销售、

化工生产和政府监管 6 大类^①。

5. 网络数据安全风险

网络中大量数据不断地生成、传输、存储、加工、分发、共享，支撑着许多关系国计民生的关键信息系统运营。由于数据处理复杂，涉及多个要素，数据安全风险控制是一个难题。若关键系统的某些重要的数据失去安全控制，就会导致系统运行中断，引发社会信任危机，甚至危及人身安全。例如，电力控制系统指令的安全关系电网的正常运行，生产经营数据的失真影响企业决策，电子病历的安全影响个人健康和隐私。

6. 高级持续威胁风险

APT 攻击威胁活动日益频繁，包括对目标对象采用鱼叉邮件攻击、水坑攻击、网络流量劫持、中间人攻击等，综合利用多种技术以实现攻击意图，规避网络安全监测。APT 攻击目标总体呈现出与地缘政治紧密相关的特性，受攻击的领域主要包括国防、政府、金融、外交和能源等。此外，医疗、传媒、电信等国家服务性行业领域也正面临越来越多的 APT 攻击风险。

7. 恶意代码风险

网络时刻面临计算机病毒、网络蠕虫、特洛伊木马、僵尸网络、逻辑炸弹、Rootkit、勒索软件等恶意代码的威胁。2018 年，CNCERT 捕获勒索软件数量达到十万以上，全年总体呈现增长趋势。

8. 软件代码和安全漏洞风险

由于软件工程和管理等问题，新的软件代码安全漏洞仍然不断地输入网络信息环境中，这些安全漏洞都可能成为攻击切入点，攻击者利用安全漏洞入侵系统，窃取信息和破坏系统。2018 年，国家信息安全漏洞共享平台收集新增漏洞 14 201 个，其中，高危漏洞 4898 个。

9. 人员的网络安全意识风险

网络信息系统是人、机、物融合而成的复杂系统，而实际工作过程中容易忽略人的关键安全作用。研究表明，网络用户人员选择弱口令的比例仍然较大；利用网络用户 U 盘是实施网络物理隔离摆渡攻击的重要环节。

10. 网络信息技术复杂性和运营安全风险

随着云计算、大数据、人工智能、移动互联网、物联网等新一代信息技术的普及应用，网络信息系统的开放性、智能性等不断提升，网络安全运营的复杂性更高，其安全风险加大。云计算使得网络安全边界模糊化，网络安全防护难度增加，云平台的安全运维水平要求更高。业务连续性高的要求使得网络信息系统的安全补丁维护管理成本提升。物联网的开放性扩大了网

^① 相关数据来源于 CNCERT 《2018 年我国互联网网络安全态势综述》。

络信息系统的安全威胁途径。

11. 网络地下黑产经济风险

网络地下黑产组织利用攻击技术，建立“僵尸网络”，提供 DDoS 服务。根据 CNCERT 网络安全数据报告，2018 年以来利用“肉鸡”发起 DDoS 攻击的控制端有两千多个。随着“勒索软件即服务”的黑产兴起，活跃勒索软件的数量呈现快速增长势头，且更新频率加快。例如，某勒索软件一年出现了约 19 个版本，快速更新迭代以躲避安全查杀。受到加密货币利益驱动，挖矿团伙利用安全漏洞、僵尸网络、网盘等进行快速扩散传播挖矿木马。其中，WannaMine、Xmrig、CoinMiner 等是 2019 年流行的挖矿木马家族^①。

12. 网络间谍与网络战风险

根据公开信息，某国大批量的网络武器被曝光。网络空间并非天下太平，一些国家建立起网军，网络战威胁时隐时现。2019 年 6 月，《纽约时报》称俄罗斯电网被植入后门程序。北约举行全球网络安全演习——“锁盾 2019”，来应对网络战，如图 1-1 所示^②。



图 1-1 北约“锁盾 2019”示意图

1.3 网络信息安全基本属性

常见的网络信息安全基本属性主要有机密性、完整性、可用性、抗抵赖性和可控性等，此外还有真实性、时效性、合规性、隐私性等。

1.3.1 机密性

机密性（Confidentiality）是指网络信息不泄露给非授权的用户、实体或程序，能够防止非授权者获取信息。例如，网络信息系统上传递口令敏感信息，若一旦攻击者通过监听手段获取

^① 相关信息来源于 CNCERT《2018 年我国互联网网络安全态势综述》《2019 年我国互联网网络安全态势综述》。

^② 摘编自第七届互联网安全大会（简称“ISC 2019”）演讲 PPT。

到,就有可能危及网络系统的整体安全,如网络管理账号口令信息泄露将会导致网络设备失控。机密性通常被称为网络信息系统 CIA 三性之一,其中 C 代表机密性(Confidentiality)。机密性是军事信息系统、电子政务信息系统、商业信息系统等的重点要求,一旦信息泄密,所造成的影响难以计算。

1.3.2 完整性

完整性(Integrity)是指网络信息或系统未经授权不能进行更改的特性。例如,电子邮件在存储或传输过程中保持不被删除、修改、伪造、插入等。完整性也被称为网络信息系统 CIA 三性之一,其中 I 代表 Integrity。完整性对于金融信息系统、工业控制系统非常重要,可谓“失之毫厘,差之千里”。

1.3.3 可用性

可用性(Availability)是指合法许可的用户能够及时获取网络信息或服务的特性。例如,网站能够给用户提供正常的网页访问服务,防止拒绝服务攻击。可用性是常受关注的网络信息系统 CIA 三性之一,其中 A 代表可用性(Availability)。对于国家关键信息基础设施而言,可用性至关重要,如电力信息系统、电信信息系统等,要求保持业务连续性运行,尽可能避免中断服务。

1.3.4 抗抵赖性

抗抵赖性是指防止网络信息系统相关用户否认其活动行为的特性。例如,通过网络审计和数字签名,可以记录和追溯访问者在网络系统中的活动。抗抵赖性也称为非否认性(Non-Repudiation),不可否认的目的是防止参与方对其行为的否认。该安全特性常用于电子合同、数字签名、电子取证等应用中。

1.3.5 可控性

可控性是指网络信息系统责任主体对其具有管理、支配能力的属性,能够根据授权规则对系统进行有效掌握和控制,使得管理者有效地控制系统的行为和信息的使用,符合系统运行目标。

1.3.6 其他

除了常见的网络信息系统安全特性,还有真实性、时效性、合规性、公平性、可靠性、可生存性和隐私性等,这些安全特性适用于不同类型的网络信息系统,其要求程度有所差异。

1. 真实性

真实性是指网络空间信息与实际物理空间、社会空间的客观事实保持一致性。例如,网络谣言信息不符合真实情况,违背了客观事实。

第 2 章 网络攻击原理与常用方法

2.1 网络攻击概述

《孙子兵法》曰：“知己知彼，百战不殆。”网络攻击活动日益频繁，要掌握网络信息安全主动权，应先了解网络威胁者的策略方法。本节主要阐述网络攻击概念，分析网络攻击发展趋势。

2.1.1 网络攻击概念

网络攻击是指损害网络系统安全属性的危害行为。危害行为导致网络系统的机密性、完整性、可用性、可控性、真实性、抗抵赖性等受到不同程度的破坏。常见的危害行为有四个基本类型：

- (1) 信息泄露攻击；
- (2) 完整性破坏攻击；
- (3) 拒绝服务攻击；
- (4) 非法使用攻击。

网络攻击由攻击者发起，攻击者应用一定的攻击工具（包括攻击策略与方法），对目标网络系统进行（合法与非法的）攻击操作，达到一定的攻击效果，实现攻击者预定的攻击意图，如表 2-1 所示。

表 2-1 网络攻击原理表

攻击者	攻击工具	攻击访问	攻击效果	攻击意图
黑客	用户命令 脚本或程序 自治主体 电磁泄露	本地访问 远程访问	破坏信息	挑战
间谍			信息泄密	好奇
恐怖主义者			窃取服务	获取情报
公司职员			拒绝服务	经济利益
职业犯罪分子				恐怖事件
破坏者				报复

1. 攻击者

根据网络攻击来源，攻击者可分成两大类：内部人员和外部人员。根据网络攻击的动机与目的，常见的攻击者可以分为六种：间谍、恐怖主义者、黑客、职业犯罪分子、公司职员和破坏者。

2. 攻击工具

攻击者通过一系列攻击工具，对目标网络实施攻击，具体包括：

- 用户命令：攻击者在命令行状态下或者以图形用户接口方式输入攻击命令；
- 脚本或程序：利用脚本和程序挖掘弱点；
- 自治主体：攻击者初始化一个程序或者程序片断，独立执行漏洞挖掘；
- 电磁泄漏：通过电子信号分析方法，实施电磁泄漏攻击。

3. 攻击访问

攻击者为了达到攻击目的，一定要访问目标网络系统，包括合法和非法的访问。但是，攻击过程主要依赖于非法访问和目标网络资源的使用，即未授权访问或未授权使用目标系统的资源。攻击者能够进行未授权访问和系统资源使用的前提是，目标网络和系统存在安全弱点，包括设计弱点、实现弱点和配置弱点。进入目标系统之后，攻击者就开始执行相关命令，如修改文件、传送数据等，实施各类不同的攻击。

4. 攻击效果

攻击效果包括以下几种：

- 破坏信息：删除或修改系统中存储的信息或者网络中传送的信息；
- 信息泄密：窃取或公布敏感信息；
- 窃取服务：未授权使用计算机或网络服务；
- 拒绝服务：干扰系统和网络的正常服务，降低系统和网络性能，甚至使系统和网络崩溃。

5. 攻击意图

攻击者的意图可分为以下六类：

- 黑客：攻击的动机与目的是表现自己或技术挑战；
- 间谍：攻击的动机与目的是获取情报信息；
- 恐怖主义者：攻击的动机与目的是获取恐怖主义集团的利益；
- 公司职员：攻击的动机与目的是好奇，显示才干；
- 职业犯罪分子：攻击的动机与目的是获取经济利益；
- 破坏者：攻击的动机与目的是报复或发泄不满情绪。

2.1.2 网络攻击模型

掌握网络攻击模型有助于更好地理解分析网络攻击活动，以便对目标系统的抗攻击能力进行测评。目前，常见的网络攻击模型主要如下。

第二步，攻击有安全漏洞的主机，并设法获取控制权；

第三步，在已攻击成功的主机中安装客户端攻击程序；

第四步，利用已攻击成功的主机继续进行扫描和攻击；

第五步，当攻击客户端达到一定的数目后，攻击者在主控端给客户端攻击程序发布向特定目标进行攻击的命令。

从分布式拒绝服务攻击的案例来看，攻击者进行大型或复杂的攻击之前，需要利用已攻击成功的主机，时机成熟后再向最终的目标发起攻击。从这一点上来说，大型或复杂的攻击并不能一步到位，而是经过若干个攻击操作步骤后，才能实现最终的攻击意图。DDoS 常用的攻击技术手段有 HTTP Flood 攻击、SYN Flood 攻击、DNS 放大攻击等。其中，HTTP Flood 攻击是利用僵尸主机向特定目标网站发送大量的 HTTP GET 请求，以导致网站瘫痪，如图 2-4 所示。

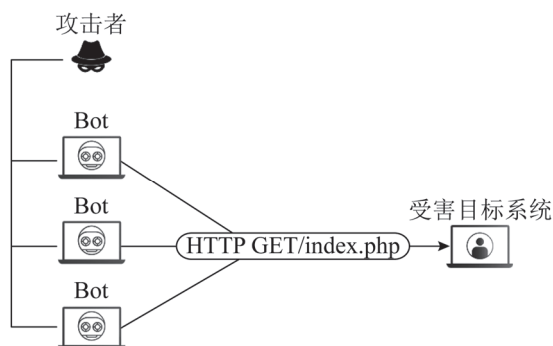


图 2-4 HTTP Flood 攻击示意图

SYN Flood 攻击利用 TCP/IP 协议的安全缺陷，伪造主机发送大量的 SYN 包到目标系统，导致目标系统的计算机网络瘫痪，如图 2-5 所示。

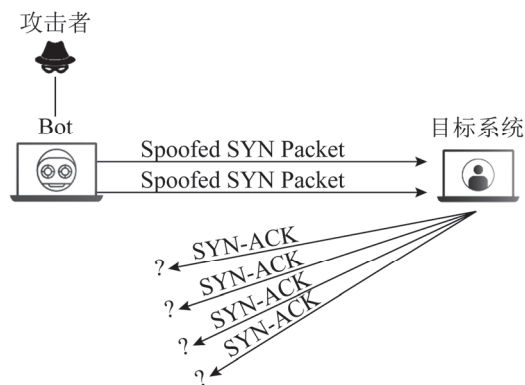


图 2-5 SYN Flood 攻击示意图

DNS 放大攻击是攻击者假冒目标系统向多个 DNS 解析服务器发送大量请求，而导致 DNS 解析服务器同时应答目标系统，产生大量网络流量，形成拒绝服务，如图 2-6 所示。

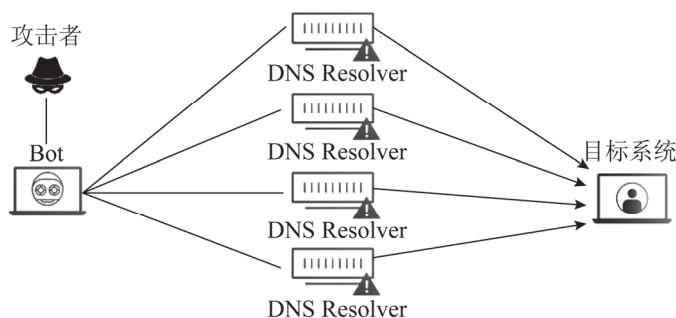


图 2-6 DNS 放大攻击示意图

2.5.2 W32.Blaster.Worm

W32.Blaster.Worm 是一种利用 DCOM RPC 漏洞进行传播的网络蠕虫，其传播能力很强。感染蠕虫的计算机系统运行不稳定，系统会不断重启。并且该蠕虫还将对 windowsupdate.com 进行拒绝服务攻击，使得受害用户不能及时地得到这个漏洞的补丁。如图 2-7 所示，当 W32.Blaster.Worm 运行时，会进行以下操作。

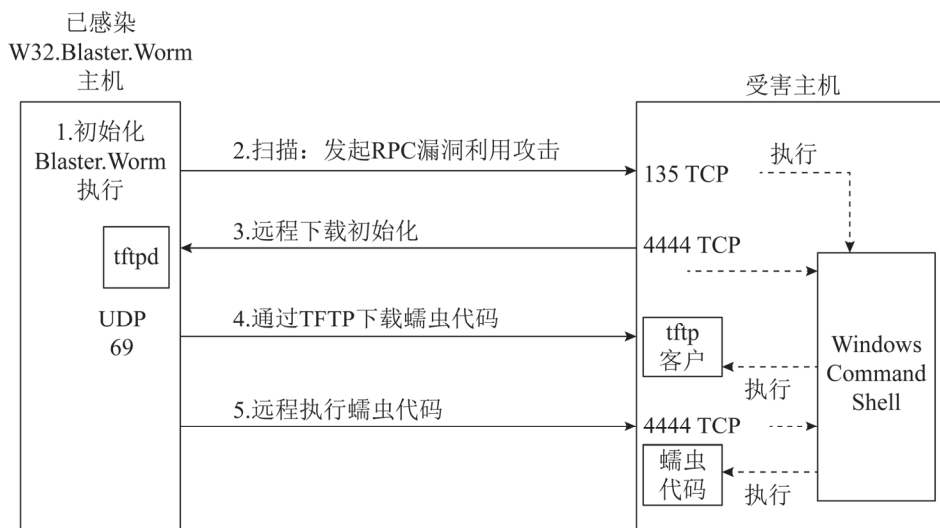


图 2-7 W32.Blaster.Worm 网络攻击示意图

- (1) 创建一个名为 BILLY 的互斥体。如果这个互斥体存在，蠕虫将放弃感染并退出。
- (2) 在注册表中添加下列键值：

"windows auto update"="msblast.exe"

并且将其添加至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

这样就可以使蠕虫在系统被重起的时候能够自动运行。

(3) 蠕虫生成攻击 IP 地址列表, 尝试去感染列表中的计算机, 蠕虫对有 DCOM RPC 漏洞的机器发起 TCP 135 端口的连接, 进行感染。

(4) 在 TCP 4444 端口绑定一个 cmd.exe 的后门。

(5) 在 UDP port 69 口上进行监听。如果收到了一个请求, 将把 Msblast.exe 发送给目标机器。

(6) 发送命令给远端的机器使它回联已经受到感染的机器并下载 Msblast.exe。

(7) 检查当前日期及月份, 若当前日期为 16 日或以后, 或当前月份处在 9 月到 12 月之间, 则 W32.Blaster.Worm 蠕虫将对 windowsupdate.com 发动 TCP 同步风暴拒绝服务攻击。

2.5.3 网络安全导致停电事件

本网络安全事件材料来源于北京安天网络安全技术有限公司 (以下简称安天公司) 发布的《乌克兰电力系统遭受攻击事件综合分析报告》及相关网络信息。2015 年 12 月 23 日, 乌克兰多地区发生同时停电的事件。调查显示, 乌克兰电厂停电是因网络攻击导致电力基础设施被破坏。如图 2-8 所示, 根据安天公司的分析报告, 黑客首先利用钓鱼邮件, 欺骗电力公司员工下载了带有 BlackEnergy 的恶意代码文件, 然后诱导用户打开这个文件, 激活木马, 安装 SSH 后门和系统自毁工具 Killdisk, 致使黑客最终获得了主控电脑的控制权。最后, 黑客远程操作恶意代码将电力公司的主控计算机与变电站断连并切断电源; 同时, 黑客发动 DDoS 攻击电力客服中心, 致使电厂工作人员无法立即进行电力维修工作。

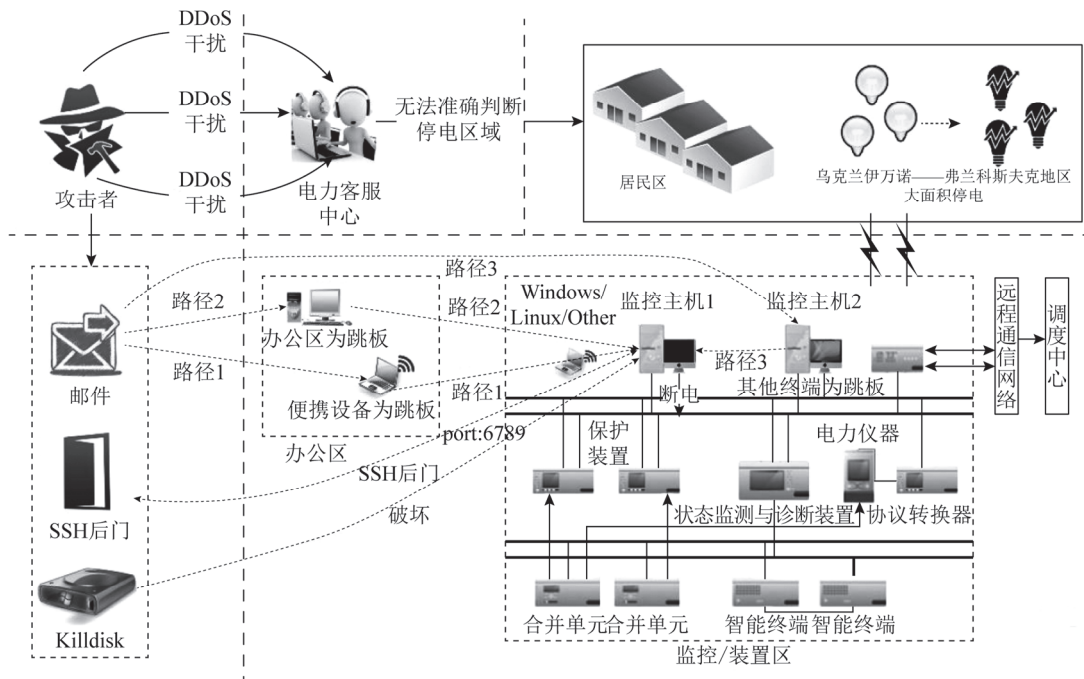


图 2-8 乌克兰停电事件攻击全程示意图