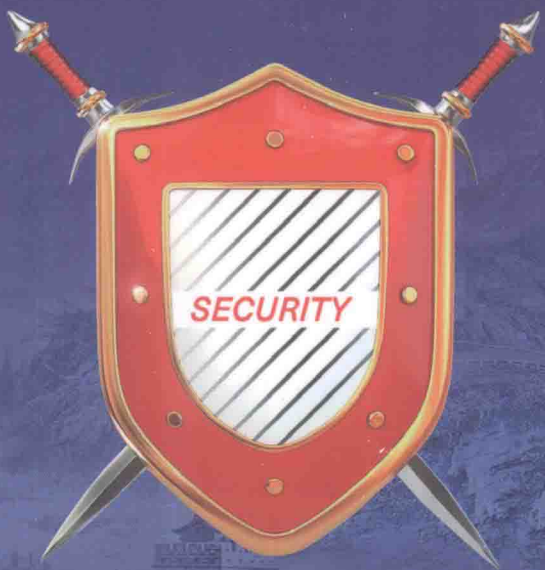
网信干部培训辅导丛书

网络安全技术基础
培训教程

中国网络空间研究院
中国网络空间安全协会 ◎ 编著



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

网信干部培训辅导丛书

网络安全技术基础
培训教程

中国网络空间研究院
中国网络空间安全协会 ◎ 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全技术基础培训教程 / 中国网络空间研究院，中国网络空间安全协会编著. -- 北京 : 人民邮电出版社，2016.10
（网信干部培训辅导丛书）
ISBN 978-7-115-42936-0

Ⅰ. ①网… Ⅱ. ①中… ②中… Ⅲ. ①网络安全－技术培训－教材 Ⅳ. ①TN915.08

中国版本图书馆CIP数据核字(2016)第207960号

内 容 提 要

本书系统介绍网络安全的基本理论和关键技术，共分三部分 14 章。其中，第一部分是基础技术，介绍网络安全现状、密码技术、身份认证、访问控制、网络攻击等；第二部分是中级防护，介绍系统安全、反恶意代码、网络边界安全、网络服务安全、网络信息内容安全等；第三部分是高级进阶，介绍云计算、大数据、物联网、工控网等网络安全。

本书旨在为全国网信干部提供理论指南、实践指导和趋势指引，也可以作为网络与信息安全技术学习、研究、实践和管理等专业人士的培训教材。

◆ 编　　著　中国网络空间研究院　中国网络空间安全协会
责任编辑　邢建春
执行编辑　肇　丽
责任印制　彭志环

◆ 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
固安县铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：27　　2016 年 10 月第 1 版
字数：657 千字　　2016 年 10 月河北第 1 次印刷

定价：98.00 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

2014 年 2 月，中央成立了由习近平总书记任组长的中央网络安全和信息化领导小组，统筹协调各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。习近平总书记明确指出：“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，没有网络安全就没有国家安全，没有信息化就没有现代化”“建设网络强国，要把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍”。

2015 年 6 月，“网络空间安全”成为一级学科，把网络安全人才培养提到了一个新的战略高度。2016 年 4 月，习近平总书记在网络安全和信息化工作座谈会上明确指出：“要聚天下英才而用之，为网信事业发展提供有力人才支撑。网络空间的竞争，归根结底是人才竞争”。2016 年 7 月，国家发布《国家信息化发展战略纲要》，指出：“优化人才队伍，提升信息技能。人才资源是第一资源，人才竞争是最终的竞争。要完善人才培养、选拔、使用、评价、激励机制”“全面开展国家工作人员信息化培训和考核”。

网信人才的培养受到党和国家的高度重视，网信干部不仅是网信人才的重要组成，更是推进网信事业发展的中坚力量。为了提高网信干部的业务和知识水平，加强网信干部培训工作，完善培训教材体系，中央网信办提出需要编写一系列与网络安全和信息化密切相关的培训教材，确保培训教材具备针对性、实用性、科学性、可读性，力争出精品、创特色。根据上述要求，开展了网络安全领域培训的调研工作，并组织专家编写本丛书，作为开展网信干部相关培训工作的辅导教材。

为了保证质量，对丛书做了规划，丛书的目录和大纲征求了信息安全专业教学指导委员会专家的意见，由中国网络空间安全协会秘书处负责丛书编写的组织工作，由中国网络空间研究院与中国网络空间安全协会负责编写，并以自愿申领与定向邀请相结合的方式，委托国内知名科研院所和企事业单位的专家学者参与丛书的编写和统稿工作。

衷心希望本丛书能够提高网信干部的网络安全知识水平，促进网信干部的培训工作，为推进网信人才培养和网信事业发展做出应有的贡献。

中国工程院院士 方滨兴

2016 年 8 月 23 日

前　言

当前，网络空间已经成为继陆、海、空、天之后人类活动的第五大空间，其深度和广度覆盖政治、经济、文化、社会、军事、外交等各个领域并深入到社会生活的各个层面。网络空间安全在经济和社会发展的关键环节和基础保障方面发挥着日益重要的作用，已成为国家安全的核心组成部分。

随着人、机、物三元融合发展趋势在信息技术领域的不断演进，网络空间的安全形势日益严峻，各种各样的网络安全隐患急剧增多，渗透和反渗透、破坏和反破坏、黑客和反黑客的斗争愈演愈烈，不仅影响网络的稳定运行和用户的正常使用，造成重大经济损失，而且还严重威胁到国家安全。为了构建完备的网络安全管理与攻防体系，需要在完善网络安全法规标准的基础上，积极探索、努力发展更加有效的网络安全技术手段。因此，网络安全技术的意识提高、基本运用、体系建设、创新驱动等显得越来越重要，并得到各个国家的高度重视。

作为网信干部培训辅导丛书的重要教材，本书系统介绍了网络安全的基本理论和关键技术，共 14 章，分为三大部分。第一部分是基础技术（第 1 章～第 7 章），内容包括网络安全现状、网络安全体系、互联网协议安全、密码技术、身份认证、访问控制、网络攻击以及物理与人员安全等；第二部分是中级防护（第 8 章～第 13 章），内容包括系统安全、反恶意代码、网络边界安全、网络服务安全、移动网络安全以及网络信息内容安全等；第三部分是高级进阶（第 14 章），内容包括云计算、大数据、物联网、工控网等新技术与新应用的网络安全。同时，每章后面给出了典型的配置实例或应用案例，并针对重点、难点设计了适量的习题。

本书由中国网络空间研究院与中国网络空间安全协会负责编写，参与调研与编写的人员还有来自国内知名科研院所和企事业单位的专家学者。本书目录与大纲通过了信息安全专业教学指导委员会专家的咨询论证，并利用中国网络空间安全协会专家群的优势组织开展编写工作，向业界专家发出编写任务认领邀请，经遴选后委派编写工作。聘请专家对提交的稿件进行多次统稿，最终通过专家审稿会的评审。方滨兴院士对本书的整体筹划和布局给予了悉心指导，陈晓桦研究员负责本书的内容安排与组织，武传坤研究员负责本书的统稿，参与编写和组稿的还有（以下按姓氏笔画排序）丁滟、王海龙、王润合、王瑞兵、牛青、刘

建皓、李柏松、杨芸、肖新光、吴槟、何媛、陈驰、陈超、陈璐艺、林伟、郑骊、赵武、赵海波、胡怀亮、贾亚晨、徐克付、徐松泉、席斐、唐晓莉、黄辰林、黄振海、程叶霞、曾溪泉、蒲灿、路轶、蔡一兵、裴智勇、廖莎、翟健宏、翟海涛、薛锐，在此表示感谢！

由于水平有限，编写过程中难免有错误之处，欢迎大家批评指正！

目　录

第一部分　基础技术

第 1 章　网络安全概述 …… 3

1.1　网络安全现状 …… 3

1.1.1　网络安全现状及影响 …… 3

1.1.2　网络的安全性分析 …… 5

1.2　网络安全挑战 …… 6

1.2.1　传统的网络威胁 …… 6

1.2.2　网络安全的新挑战 …… 8

1.3　网络安全体系 …… 10

1.3.1　网络安全防护体系 …… 10

1.3.2　网络安全信任体系 …… 12

1.3.3　网络安全保障体系 …… 13

1.4　网络安全标准法规 …… 14

1.4.1　网络安全标准 …… 15

1.4.2　网络安全法律法规 …… 19

练习题 …… 22

第 2 章　互联网协议安全 …… 23

2.1　引言 …… 23

2.2　TCP/IP …… 24

2.2.1　TCP/IP 的起源 …… 24

2.2.2　TCP/IP 的特点 …… 25

2.2.3　OSI 网络分层参考模型 …… 25

2.2.4 TCP/IP 参考模型 …… 28
2.3 TCP/IP 安全性分析 …… 29
2.3.1 TCP/IP 攻击的分类 …… 29
2.3.2 TCP/IP 攻击利用的常见协议漏洞 …… 30
2.4 网络安全协议 …… 32
2.5 网络安全协议的安全问题 …… 35
练习题 …… 36

第 3 章 密码技术 …… 38

3.1 密码学概述 …… 38
3.1.1 起源与发展 …… 38
3.1.2 加密体制简介 …… 39
3.1.3 加密体制的分类 …… 40
3.1.4 现代密码学中的其他重要分支 …… 41
3.2 数据加密技术 …… 41
3.2.1 私钥加密体制——流密码 …… 41
3.2.2 私钥加密体制——分组密码 …… 44
3.2.3 公钥加密体制 …… 51
3.3 加密技术应用 …… 54
3.3.1 TLS/SSL …… 54
3.3.2 VPN …… 54
3.3.3 PKI …… 55
3.3.4 PGP …… 55
3.3.5 SSH …… 55
3.3.6 数字版权保护技术——DRM …… 56
3.3.7 文件加密技术 …… 56
3.3.8 软件加密技术 …… 57
3.3.9 隐蔽通信技术 …… 58
3.3.10 数字签名技术 …… 59
3.4 技术标准化 …… 60
3.4.1 国内密码标准 …… 60
3.4.2 国际密码标准 …… 62
练习题 …… 63

第 4 章 身份认证 …… 64

4.1 身份认证概述 …… 64
4.2 身份认证机制 …… 65
4.3 对“人”的认证 …… 65
4.3.1 基于口令的认证 …… 66
4.3.2 双因子身份认证技术 …… 68
4.3.3 生物特征识别认证技术 …… 69
4.4 对“机”的认证 …… 71
4.5 对“物”的认证 …… 72
4.6 其他身份认证技术 …… 73
4.6.1 数字签名技术 …… 73
4.6.2 数字证书 …… 74
4.6.3 匿名认证技术 …… 75
4.6.4 群组认证技术 …… 75
4.7 身份认证系统 …… 76
4.7.1 Kerberos …… 76
4.7.2 公钥基础设施（PKI） …… 81
4.8 身份认证应用案例 …… 85
4.8.1 统一身份认证管理与单点登录技术 …… 85
4.8.2 UNIT 认证系统的基本结构 …… 87
4.8.3 UNIT 认证系统的身份认证 …… 89
4.8.4 UNIT 系统的单点登录 …… 90
4.9 数字证书应用案例 …… 91
练习题 …… 93

第 5 章 访问控制 …… 94

5.1 访问控制概述 …… 94
5.1.1 访问控制技术背景 …… 94
5.1.2 访问控制的主要内容 …… 95
5.2 访问控制模型与管理 …… 96
5.2.1 访问控制基本概念 …… 96
5.2.2 访问矩阵（Access Matrix） …… 97
5.2.3 自主访问控制 …… 98

5.2.4 强制访问控制 100
5.2.5 基于角色的访问控制 103
5.2.6 基于任务的访问控制 106
5.2.7 授权管理模型介绍 108
5.3 安全策略 111
5.3.1 访问控制策略简介 111
5.3.2 授权描述语言 113
5.3.3 可扩展访问控制标记语言 114
5.4 访问控制实现技术 115
5.4.1 访问控制列表与能力列表 115
5.4.2 访问控制决策中间件 116
5.4.3 信任管理技术 117
练习题 119
第 6 章 网络攻击 120
6.1 网络攻击概述 120
6.1.1 网络攻击的定义 120
6.1.2 网络攻击原因解析 121
6.1.3 网络攻击防护措施 123
6.2 攻击的一般流程 123
6.2.1 准备阶段 123
6.2.2 实施阶段 124
6.2.3 善后阶段 124
6.3 攻击的技术方法 125
6.3.1 端口扫描 125
6.3.2 口令破解 131
6.3.3 缓冲区溢出 133
6.3.4 拒绝服务攻击 137
6.3.5 社会工程学 143
6.3.6 信息窃密 145
6.4 网络攻击软件 150
6.4.1 远程控制软件 150
6.4.2 系统攻击实例 152

6.4.3 口令破解软件 …… 154
6.4.4 网络监听软件 …… 156
6.5 高级持续性威胁 …… 158
6.5.1 高级持续性威胁概述 …… 158
6.5.2 APT 与传统恶意代码攻击的对比 …… 159
6.5.3 APT 攻击手段 …… 160
6.5.4 APT 检测和防御 …… 161
6.5.5 APT 分析实例 …… 162
练习题 …… 165
第 7 章 物理与人员安全 …… 166
7.1 物理安全 …… 166
7.1.1 物理安全概述 …… 166
7.1.2 机房环境安全 …… 167
7.1.3 电磁安全 …… 169
7.1.4 物理隔离 …… 173
7.1.5 物理设备安全 …… 174
7.2 人员安全 …… 176
7.2.1 人员安全管理概述 …… 176
7.2.2 教育与培训 …… 177
7.2.3 安全审查管理 …… 183
练习题 …… 184

第二部分 防护技术

第 8 章 系统安全 …… 189
8.1 操作系统安全 …… 189
8.1.1 操作系统安全概述 …… 189
8.1.2 操作系统面临安全问题 …… 192
8.1.3 操作系统的安全机制 …… 194
8.1.4 操作系统的安全配置 …… 197
8.2 可信计算 …… 208
8.2.1 可信计算概述 …… 208

8.2.2 可信计算技术 …… 210
8.2.3 可信计算应用 …… 216
8.3 数据库安全 …… 218
8.3.1 数据库安全概述 …… 218
8.3.2 数据库安全问题 …… 219
8.3.3 数据库安全技术 …… 221
8.3.4 数据库安全防护策略 …… 225
8.3.5 数据库安全典型配置实例 …… 228
8.4 个人数据安全 …… 229
8.4.1 个人数据安全概述 …… 229
8.4.2 个人数据安全面临的问题 …… 230
8.4.3 个人数据安全保护技术 …… 231
8.4.4 个人数据安全防护策略 …… 233
8.4.5 个人数据安全典型配置实例 …… 234
8.5 备份与恢复 …… 236
8.5.1 备份与恢复概述 …… 236
8.5.2 灾难备份 …… 236
8.5.3 桌面操作系统备份与恢复典型操作实例 …… 239
练习题 …… 244
第 9 章 反恶意代码 …… 245
9.1 恶意代码查杀 …… 245
9.1.1 分类与特征 …… 245
9.1.2 结构与原理 …… 247
9.1.3 反病毒引擎 …… 249
9.1.4 清除防范技术 …… 249
9.1.5 不同平台下的恶意代码查杀 …… 251
9.1.6 案例 …… 258
9.2 流氓软件清理 …… 262
9.2.1 流氓软件清理概述 …… 262
9.2.2 技术原理 …… 264
9.2.3 流氓软件主要危害 …… 266
9.2.4 清除与防范 …… 267

9.2.5 流氓软件清除实例 …… 267
9.3 蜜 罐 …… 269
9.3.1 蜜罐简介 …… 269
9.3.2 蜜罐技术 …… 270
9.3.3 蜜罐类型 …… 271
9.3.4 蜜罐风险 …… 273
9.3.5 虚拟机与沙箱 …… 273
练习题 …… 274

第 10 章 网络边界安全 …… 275

10.1 防火墙 …… 275
10.1.1 防火墙概述 …… 275
10.1.2 防火墙典型配置实例 …… 276
10.2 入侵检测与防御 …… 282
10.2.1 什么是入侵检测系统 …… 282
10.2.2 为什么需要入侵检测系统 …… 282
10.2.3 入侵检测系统的基本组成 …… 282
10.2.4 入侵检测系统的常规分类 …… 283
10.2.5 入侵检测的技术手段 …… 283
10.2.6 入侵检测实例——Snort …… 284
10.2.7 入侵检测的前景 …… 285
10.2.8 入侵防御系统 …… 285
10.3 虚拟专用网络（VPN） …… 286
练习题 …… 291

第 11 章 网络服务安全 …… 292

11.1 WWW 安全 …… 292
11.1.1 Web 与脚本程序安全概述 …… 292
11.1.2 WWW 安全增强手段 …… 297
11.1.3 Web 欺骗技术与典型实例 …… 299
11.1.4 电子交易安全 …… 303
11.2 域名服务安全 …… 305
11.2.1 域名服务安全概述与增强手段 …… 305

11.2.2 域名欺骗技术与典型实例 …… 308
11.3 电子邮件安全 …… 310
11.3.1 电子邮件安全概述 …… 310
11.3.2 电子邮件欺骗技术与典型实例 …… 312
11.3.3 配置 Microsoft Outlook …… 313
11.4 网络文件服务安全 …… 314
11.4.1 网络文件服务安全概述与增强手段 …… 314
11.4.2 网络文件系统典型配置实例 …… 317
11.5 其他常用互联网典型应用服务安全 …… 319
11.5.1 搜索引擎服务安全 …… 319
11.5.2 即时通信工具安全 …… 320
练习题 …… 323
第 12 章 移动网络安全 …… 324
12.1 无线广域网安全 …… 324
12.1.1 无线广域网安全发展趋势 …… 324
12.1.2 无线广域网安全要求概述 …… 325
12.1.3 2G 安全机制 …… 325
12.1.4 3G 安全机制 …… 327
12.1.5 4G 安全机制 …… 330
12.1.6 5G 安全机制 …… 336
12.2 无线局域网（WLAN）安全 …… 336
12.2.1 无线局域网 …… 336
12.2.2 无线局域网国家标准发展情况 …… 338
12.2.3 无线局域网安全概述 …… 340
12.2.4 无线局域网面临的安全问题 …… 341
12.2.5 无线局域网安全性 …… 342
12.2.6 WAPI 技术介绍 …… 343
12.2.7 无线局域网（WAPI）安全配置实例 …… 345
12.3 移动终端安全 …… 346
12.3.1 移动终端安全概述 …… 346
12.3.2 终端安全风险 …… 347
12.3.3 Android 平台安全 …… 347

12.3.4 iOS 平台安全 …… 352
12.3.5 Windows Phone 平台安全 …… 356
12.3.6 终端安全防护建议 …… 358
12.4 近距离无线通信网络安全 …… 359
12.4.1 射频识别（RFID）安全 …… 360
12.4.2 近场通信（NFC）安全 …… 361
12.4.3 无线传感器网络安全 …… 362
12.4.4 无线个域网安全 …… 363
12.4.5 超宽带无线通信安全 …… 364
12.4.6 磁域网安全 …… 366
12.4.7 非接触式卡安全 …… 367
练习题 …… 368
第 13 章 网络信息内容安全 …… 369
13.1 网络信息内容安全技术 …… 369
13.1.1 内容安全技术概述 …… 369
13.1.2 内容采集、过滤、审计技术 …… 369
13.2 网络舆情分析 …… 372
13.2.1 网络舆情定义 …… 372
13.2.2 网络舆情分析概述 …… 372
13.2.3 网络舆情分析关键技术 …… 375
13.2.4 话题跟踪与热点识别 …… 379
13.3 社交网络安全 …… 381
13.3.1 社交网络安全现状 …… 381
13.3.2 社交网络安全存在问题 …… 382
13.3.3 社交网络安全的技术解决方案 …… 383
13.3.4 提供社交网络安全的管理措施 …… 385
练习题 …… 386

第三部分 新技术与新应用

第 14 章 新技术与新应用的网络安全 …… 389
14.1 云安全 …… 389

14.1.1 云安全概述 389
14.1.2 云安全面临的挑战 389
14.1.3 云安全技术现状 392
14.1.4 云安全服务体系 395
14.2 大数据安全 396
14.2.1 大数据安全概述 396
14.2.2 大数据安全面临的问题及挑战 397
14.2.3 大数据安全技术现状 399
14.3 物联网安全 402
14.3.1 物联网安全概述 402
14.3.2 物联网安全面临的挑战 404
14.3.3 物联网安全特征 405
14.3.4 物联网安全技术现状 406
14.4 工控网络安全 408
14.4.1 工控网络安全概述 408
14.4.2 工控网络安全面临的挑战 409
14.4.3 工控网络安全的特征 410
14.4.4 工控网络安全技术现状 411
练习题 415