



信息安全保障人员认证培训教材

信息安全技术

XIN XI AN QUAN JI SHU (第二版) 下册

中国信息安全认证中心

◎ 主 编 张 剑 ◎ 副主编 万里冰 钱伟中

★★★ CISA ★★★★★



电子科技大学出版社



信息安全保障人员认证培训教材

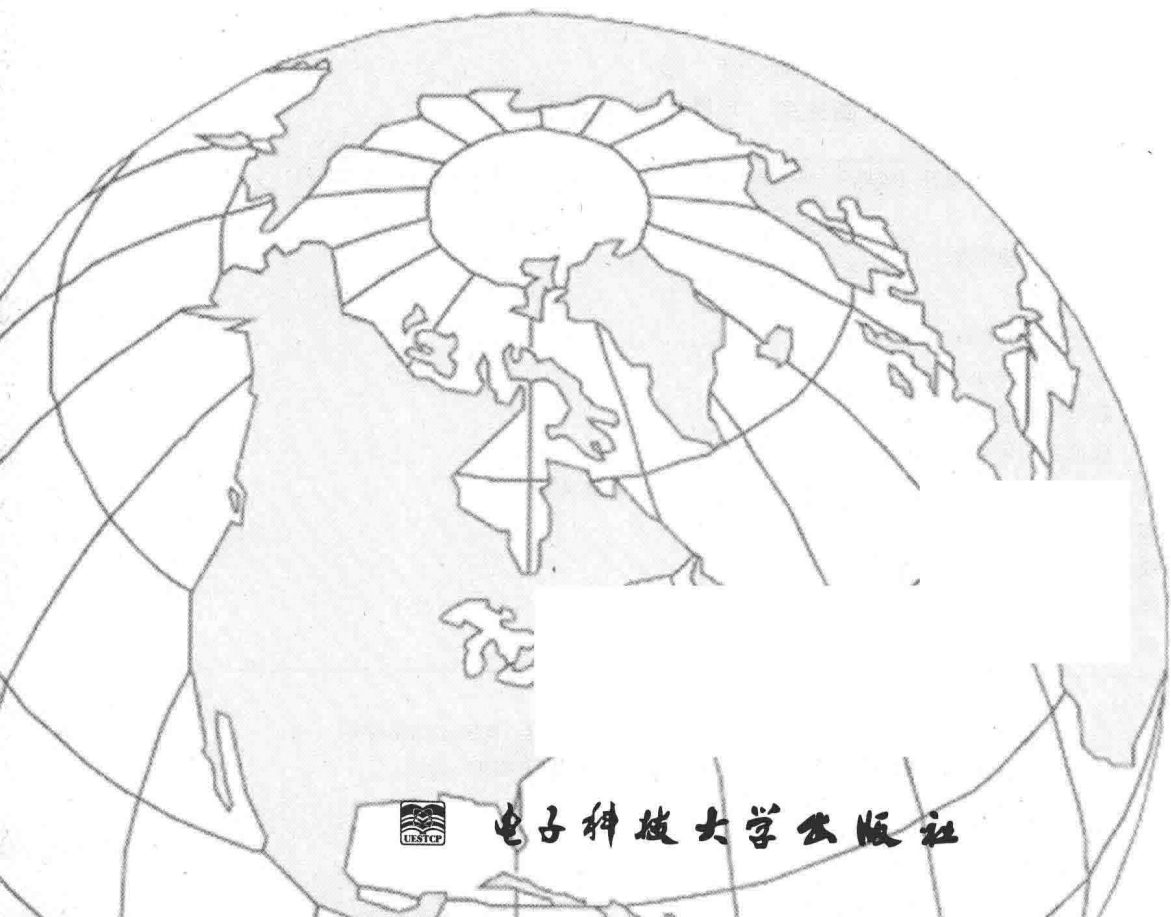
信息安全技术

XIN XI AN QUAN JI SHU (第二版) 下册

中国信息安全认证中心

◎ 主 编 张 剑 ◎ 副主编 万里冰 钱伟中

★★★ CISA ★★★★★



电子工业出版社

图书在版编目 (CIP) 数据

信息安全技术: 全 2 册 / 张剑主编. --2 版. -- 成

都: 电子科技大学出版社, 2015.5

ISBN 978-7-5647-2977-6

I. ①信… II. ①张… III. ①信息安全-安全技术

IV. ①TP309

中国版本图书馆 CIP 数据核字 (2015) 第 082242 号

内 容 提 要

本书以信息安全保障人员认证 (CISAW) 培训的需求为总纲, 结合 CISAW 信息安全保障模型, 根据信息安全保障实体对象的具体特征, 将信息安全主要技术构成分为数据安全、载体安全、环境安全、边界安全和应用安全五个部分。以理论联系实际为编著指导思想, 以业界成熟信息安全应用技术理论为基础, 以 CISAW 各专业方向认证培训所涉及的成熟信息安全技术为核心内容, 深入分析实际应用过程中的技术原理和构成, 突出各项信息安全技术的特色, 探讨各项信息安全技术的应用领域和方法, 展望各项信息安全技术的发展方向, 为各领域从事信息安全保障的设计、开发、实施、集成、运维、风险评估等工作的专业人员提供信息安全技术支撑。

信息安全技术 (第二版)

主 编 张 剑

副主编 万里冰 钱伟中

出 版: 电子科技大学出版社 (成都市一环路东一段 159 号电子信息产业大厦 邮编: 610051)

策划编辑: 徐守铭

责任编辑: 郭蜀燕 徐守铭

责任校对: 王 坤

主 页: www.uestcp.com.cn

电子邮箱: uestcp@uestcp.com.cn

发 行: 新华书店经销

印 刷: 成都市川侨印务有限公司

成品尺寸: 185 mm × 260 mm 印张 41.5 字数 835 千字

版 次: 2015 年 5 月第二版

印 次: 2015 年 5 月第二次印刷

书 号: ISBN 978-7-5647-2977-6

定 价: 100.00 元 (上、下册)

■ 版权所有 侵权必究 ■

◆ 本社发行部电话: 028-83202463; 本社邮购电话: 028-83201495。

◆ 本书如有缺页、破损、装订错误, 请寄回印刷厂调换。

丛书编委会

主 任 魏 昊

副主任 史小卫 陈晓桦 吴晓龙 亓明和

委 员 (按姓氏笔画排序)

丁元汉	丁 锋	于春刚	万里冰	马卫东	王 刚	王怀宾
王 莉	王夏莲	王 强	王 静	亓明和	尹远飞	尹朝万
邓 刚	甘杰夫	史小卫	冯 丽	冯 峰	成林芳	朱灿庭
朱 强	华颜涛	刘春旺	刘春波	刘 洋 (广东)	刘 洋 (辽宁)	
刘润乾	汤志伟	孙 爽	杜孝伟	李 倩	李 源	杨惟泓
肖鸿江	吴永东	吴芳琼	吴晓龙	何一丁	宋 杨	宋明秋
张会平	张良龙	张 剑	张徐亮	张 雪	张维石	张 斌
陈 宇	陈晓桦	武 刚	林 利	林海峰	罗小兵	罗俊海
岳笑含	周佩雯	周福才	郑 莹	赵国庆	赵 洋	赵 辉
胡 松	钟 毅	段先斐	段静辉	秦潇潇	钱伟中	徐全生
徐 俊	徐 剑	徐 然	高天鹏	郭心平	郭剑锋	蒋 军
蒋宏伟	韩 征	傅 翀	谢 兄	蓝 天	雷 冰	蔡运娟
廖国平	翟亚红	熊万安	潘 伟	魏 昊		



编 写 组

主 编 张 剑

副主编 万里冰 钱伟中

编 委 秦潇潇 罗俊海 张徐亮 蓝 天

王 静 赵 洋 傅 翀 熊万安



序

2014 年，我国提出了建设网络强国战略与目标。实现网络强国，培养和造就网络与信息安全人才队伍是关键。据调查，截至 2014 年年底，国内网络与信息安全人才缺口高达 50 万人，并呈现持续增长的趋势。加快人才培养是我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。

作为我国专业信息安全认证机构和培训机构，中国信息安全认证中心以保障国家网络与信息安全为己任，于 2011 年推出了信息安全保障人员认证（CISAW）。CISAW 认证是面向 IT 从业人员、在校学生，特别是与网络与信息安全密切相关的高级管理人员、专业技术人员推出的人员资格认证和专业水平认证。CISAW 认证的推出和实施，为培养和造就我国网络与信息安全人才探索了一条有效途径，得到了业内专家和社会各界的好评。

推行 CISAW 认证，编写高质量的教材尤为重要。鉴于此，中国信息安全认证中心组织国内信息安全保障的专业技术和应用领域的专家，依据《信息安全保障人员认证考试大纲》要求，结合信息安全保障工作的各岗位知识和应用能力要求，共同编著了信息安全保障人员认证系列教材。本系列教材包括《信息安全技术》《信息安全技术应用》和《信息安全实验》3 种基础教材；《软件安全开发》《信息系统安全集成》《信息安全管理》《信息安全咨询手册》《信息系统安全运维》《信息系统安全审计》《信息安全风险管理》《网络攻防技术》《业务连续性管理》《云计算安全》《物联网安全》《电子认证技术》和《工业控制安全》13 种专业技术应用教材；《电子政务安全》《电子商务安全》《CA 服务安全》《交通服务信息安全》《能源

服务信息安全》《医疗卫生信息安全》《教育服务信息安全》《金融服务信息安全》《通信服务信息安全》《宾馆服务信息安全》和《物流服务信息安全》11种应用领域教材。

本系列教材以实用为首要原则,从统一的信息安全保障模型出发,构建了包括信息安全技术基础知识、信息安全专业技术知识和应用领域安全保障管理知识的完整信息安全保障知识体系。既是广大 CISA W 认证申请者的考试指导用书,同时也是广大信息安全保障工作者的工作指南和参考用书。

希望本系列教材的出版,能为广大信息安全保障从业者学习、工作和申请认证提供指导和帮助。

是为序。

中国信息安全认证中心主任 魏 昊

2014年12月28日

前 言

2013 年 12 月,《信息安全技术》第 1 版出版。由于时间仓促,在第 1 版中出现了结构不合理、内容较混乱等不理想现象。本书在第 1 版的基础上进行了大幅度的调整,引入并详细解析了信息安全保障参考模型(CISAW 统一模型),进而以模型为主线展开,根据模型中的实体对象将本书的具体内容分为了数据安全、载体安全、环境安全、边界安全和应用安全五个部分。各章针对一项具体技术,在介绍基本知识的基础上,详细讲解和深入分析技术原理,并适当地给出应用实例。通过上述努力和组织,本书最终达到了结构合理、思路清晰、内容翔实、用词严谨、体系完整、点面兼顾的目标和效果。

需要说明的是,本书将某项技术划归为书中一个特定部分,并不暗示这项技术只能用于该部分中实体对象的安全保障。例如,本书将密码技术归为数据安全部分,并不代表密码技术只能用于数据对象的安全保障,它仅代表本书的一个关注点。众所周知,密码技术的应用是非常广泛的。

本书按照信息安全保障人员认证考试大纲的要求进行编写,既可作为各专业方向的信息安全保障人员认证考试的辅导用书,也可以作为信息安全相关从业人员和对信息安全技术感兴趣的人员学习用书。

本书内容共分 23 章,由张剑、万里冰、钱伟中、秦潇潇、罗俊海、张徐亮、蓝天、王静、赵洋、傅翀、熊万安等共同编写。

本书在成书过程中得到了《信息安全保障人员认证考试用书》编委会的指导,得到了中国信息安全认证中心、四川省中认信安技术服务有限公司

司、四川亚和企业咨询服务有限公司的大力支持，在此表示衷心感谢。

本书在编写过程中，参考或引用了国内外同行的文献资料，在此向这些文献资料的作者表示衷心感谢。

尽管本书进行了多次研讨和反复审核修订，仍难免存在疏漏和错误。在此，恳请广大读者和同行批评指正，以便我们再版修订时加以改正和完善。

张 剑

2014 年 12 月 28 日

目 录

第 12 章 漏洞管理	315
12.1 概述	315
12.1.1 漏洞的定义	315
12.1.2 漏洞的分类	316
12.1.3 漏洞产生的原因	317
12.1.4 漏洞的发现、发布和修复	318
12.1.5 漏洞管理机制和管理组织	322
12.2 漏洞测试规范和标准协议	324
12.2.1 漏洞危害程度评价标准介绍	324
12.2.2 典型国家漏洞库	328
12.2.3 安全内容自动化协议	329
12.3 漏洞分析技术	333
12.3.1 软件漏洞的静态分析	335
12.3.2 软件漏洞的动态分析	339
12.4 小结	342
思考题	343
第 13 章 主机安全	344
13.1 概述	344
13.2 主机防火墙技术	345
13.2.1 Winsock 2 SPI	345
13.2.2 NDIS - HOOK	346
13.3 主机入侵检测技术	347
13.3.1 基于操作系统的检测	348
13.3.2 基于网络的检测	349

13.3.3 基于应用程序的检测	349
13.3.4 基于文件完整性的检测	350
13.3.5 主机入侵检测技术的优点	350
13.4 操作系统安全机制	351
13.4.1 硬件安全机制	351
13.4.2 访问控制机制	353
13.4.3 标识与鉴别机制	354
13.4.4 其他安全机制	355
13.5 操作系统安全实例	357
13.5.1 Windows 系统安全基本概念	357
13.5.2 Windows 的安全模型	358
13.5.3 Windows 的账号与群组管理	362
13.5.4 Windows 的口令保护	362
13.5.5 Windows 认证	363
13.6 主机加固	363
13.6.1 基本概念	364
13.6.2 主要技术	365
13.6.3 主机加固实例	366
13.7 小结	367
思考题	368
第14章 安全审计	369
14.1 概述	369
14.1.1 安全审计相关概念	369
14.1.2 安全审计的发展历程	371
14.1.3 安全审计的四要素	372
14.1.4 安全审计的分类	372
14.2 日志采集技术	373
14.2.1 文本方式采集	374
14.2.2 SNMP Trap 方式采集	374
14.2.3 Syslog 方式采集	375
14.3 日志分析技术	378
14.3.1 日志数据预处理	381
14.3.2 模式匹配技术	385
14.4 审计跟踪技术	387

14.4.1 审计跟踪的目的	387
14.4.2 审计跟踪的技术架构	389
14.4.3 审计跟踪技术分类	389
14.4.4 审计跟踪工具	391
14.5 小结	392
思考题	392
第15章 取证技术	393
15.1 概述	393
15.1.1 定义	393
15.1.2 发展	394
15.1.3 电子证据及其特点	395
15.1.4 计算机取证的基本原则	396
15.1.5 计算机取证的基本步骤	397
15.2 证据获取技术	398
15.2.1 存储介质证据获取	398
15.2.2 网络数据证据获取	401
15.3 证据分析技术	403
15.3.1 内容分析技术	403
15.3.2 证据鉴定技术	404
15.3.3 数据解密技术	405
15.4 反取证技术	406
15.4.1 反取证技术的原理	406
15.4.2 反取证技术的实现	406
15.5 小结	407
思考题	408
第16章 安全测试	409
16.1 概述	409
16.2 安全审查技术	410
16.2.1 文档审查	410
16.2.2 日志审查	413
16.2.3 规则集审查	419
16.2.4 系统配置审查	419
16.2.5 文件完整性检查	420
16.3 渗透测试	422

16.3.1	渗透测试概述	422
16.3.2	渗透测试策略	422
16.3.3	渗透测试方法	423
16.3.4	目标识别与分析技术	425
16.3.5	口令破解	438
16.3.6	物理安全测试	444
16.4	应用程序安全测试	446
16.4.1	基本概念	446
16.4.2	安全测试过程	446
16.4.3	安全测试组织	448
16.4.4	常见安全性缺陷和漏洞	449
16.4.5	常用安全测试工具	450
16.4.6	应用服务器的安全性测试技术	451
16.5	小结	453
	思考题	453
第17章	安全编码	454
17.1	概述	454
17.2	内存安全	455
17.2.1	缓冲区溢出	455
17.2.2	整数溢出	458
17.2.3	数组和字符串问题	459
17.3	线程/进程安全	460
17.3.1	线程同步安全	460
17.3.2	协作安全	461
17.3.3	死锁安全	463
17.3.4	线程控制安全	465
17.3.5	进程安全	465
17.3.6	并发测试工具	465
17.4	异常/错误处理中的安全	468
17.4.1	异常/错误的基本机制	468
17.4.2	异常捕获中的安全	469
17.5	输入安全	470
17.5.1	输入安全概述	471
17.5.2	典型输入安全问题	471



17.5.3 数据库输入安全问题	474
17.6 国际化安全	476
17.6.1 国际化中的安全问题	477
17.6.2 面向对象中的编程安全	482
17.6.3 内存分配与释放	482
17.7 Web 编程安全	483
17.7.1 Web 概述	484
17.7.2 避免 URL 操作攻击	484
17.7.3 页面状态值安全	484
17.7.4 Web 跨站脚本攻击	486
17.8 源代码混淆技术	487
17.9 小结	487
思考题	488
第 18 章 物理边界控制	489
18.1 概述	489
18.2 门禁系统	490
18.2.1 门禁系统的原理	490
18.2.2 门禁系统的实现	491
18.3 巡更系统	492
18.3.1 巡更系统的原理	492
18.3.2 巡更系统的实现	493
18.4 红外防护系统	494
18.4.1 红外防护系统的原理	494
18.4.2 红外防护系统的实现	495
18.5 视频监控系统	496
18.5.1 视频监控系统的原理	496
18.5.2 视频监控系统的实现	498
18.6 小结	500
思考题	501
第 19 章 防火墙技术	502
19.1 概述	502
19.1.1 相关概念	503
19.1.2 防火墙的功能和策略	503
19.1.3 防火墙的适用范围	504

19.1.4	防火墙的发展	505
19.1.5	防火墙技术的分类	505
19.2	包过滤技术	505
19.2.1	静态包过滤技术	505
19.2.2	动态包过滤技术	511
19.2.3	包过滤规则	514
19.3	代理防火墙技术	517
19.3.1	应用级网关防火墙	518
19.3.2	链路中继网关防火墙	520
19.3.3	透明代理网关防火墙	520
19.4	防火墙的实现技术	521
19.4.1	Netfilter 概述	521
19.4.2	Netfilter 框架介绍	522
19.5	小结	523
	思考题	523
第 20 章	入侵检测	524
20.1	概述	524
20.1.1	基本概念	524
20.1.2	功能	524
20.1.3	模型	525
20.1.4	分类	526
20.1.5	发展	527
20.1.6	主要技术	528
20.2	误用检测	528
20.2.1	专家系统	529
20.2.2	模型推理	529
20.2.3	状态转换分析	530
20.3	异常检测	531
20.3.1	统计分析	532
20.3.2	神经网络	533
20.4	入侵检测预处理技术	534
20.4.1	协议分析技术	535
20.4.2	HTTP 解码技术	536
20.5	IDS 的实现技术	538

20.5.1 Snort 入侵检测系统概述	538
20.5.2 Snort 规则	538
20.5.3 Snort 的总体流程	541
20.6 小结	543
思考题	543
第 21 章 网闸	544
21.1 概述	544
21.1.1 相关概念	544
21.1.2 网闸的功能	547
21.1.3 网络隔离的发展	547
21.2 网络隔离原理	549
21.2.1 网络协议断开原理	549
21.2.2 网络隔离数据交换原理	551
21.3 网闸的关键技术	553
21.3.1 网闸的技术原理	553
21.3.2 网闸的技术实现	554
21.4 小结	560
思考题	560
第 22 章 云计算安全	561
22.1 概述	561
22.2 云用户端安全	563
22.2.1 云用户端设备安全	563
22.2.2 云用户端身份管理	563
22.3 云服务端安全	566
22.3.1 云接入安全	566
22.3.2 IaaS 安全	568
22.3.3 PaaS 安全	573
22.3.4 SaaS 安全	575
22.3.5 云数据安全	577
22.4 云运营安全	586
22.4.1 访问控制	586
22.4.2 事件管理	587
22.4.3 补丁管理	587
22.4.4 灾难恢复	587
22.4.5 云安全监控	587

22.4.6 云安全评估	588
22.4.7 云安全审计	588
22.5 云安全相关标准与工作	589
22.5.1 ITU 云计算安全标准	589
22.5.2 CSA 云计算安全标准	590
22.5.3 GSMA 云计算安全标准	591
22.5.4 OASIS 云计算安全标准	592
22.5.5 NIST 云计算安全标准	592
22.5.6 CCSA 云计算安全标准	593
22.6 小结	594
思考题	595
第23章 物联网安全	596
23.1 概述	596
23.1.1 基本概念	596
23.1.2 物联网安全框架	602
23.1.3 物联网及其安全的发展	602
23.2 物联网面临的安全问题	607
23.2.1 感知层安全问题	607
23.2.2 网络层安全问题	609
23.2.3 应用层安全问题	611
23.3 物联网相关安全技术	612
23.3.1 无线传感器网络密钥管理技术	612
23.3.2 无线传感器网络安全路由技术	613
23.3.3 无线传感器网络认证与访问控制技术	614
23.3.4 无线传感器网络恶意行为检测技术	616
23.3.5 无线传感器网络容错容侵技术	617
23.3.6 RFID 物理安全技术	618
23.3.7 RFID 安全协议机制	619
23.3.8 物联网隐私保护技术	622
23.4 相关法律法规标准	624
23.4.1 法律法规	624
23.4.2 相关标准	625
23.5 小结	626
思考题	626
参考文献	627