



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) 上册

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



信息安全保障人员认证培训教材

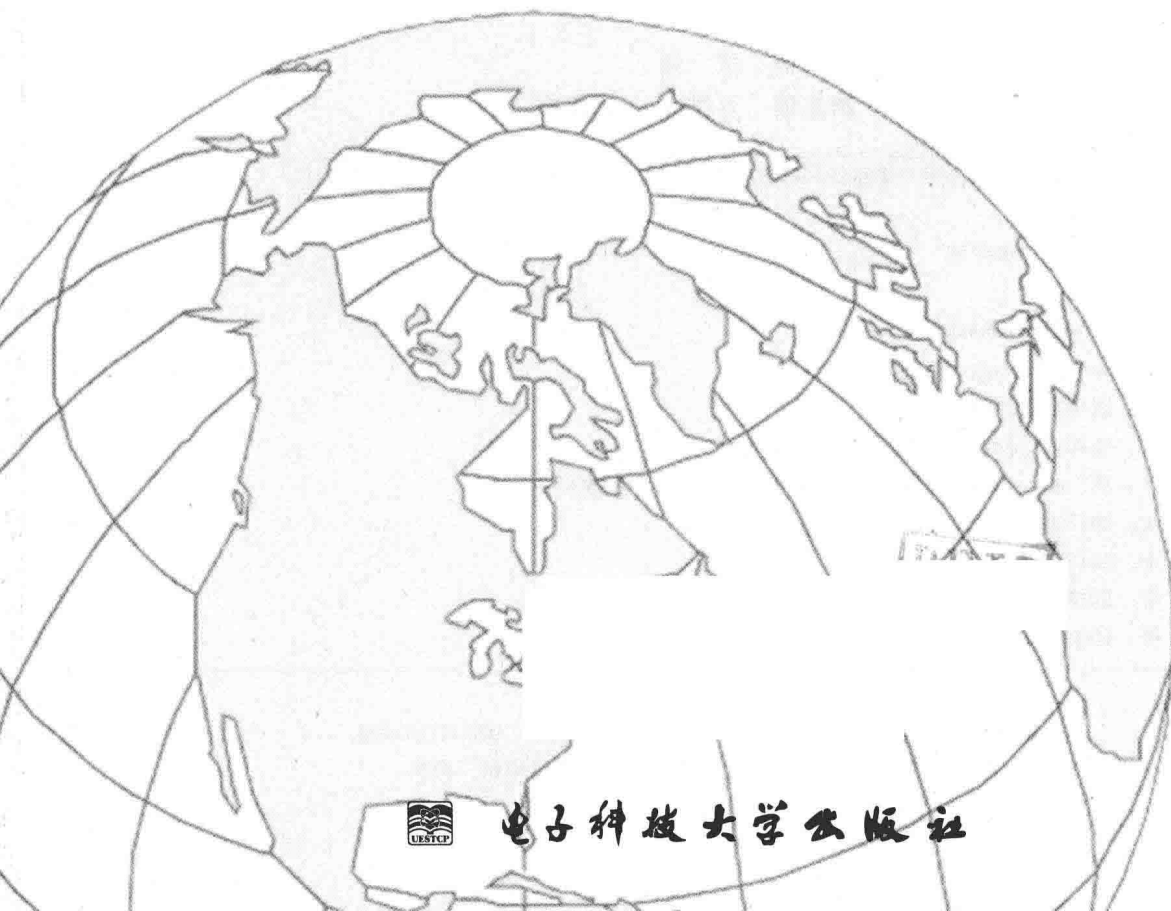
信息安全技术

XIN XI AN QUAN JI SHU (第二版) 上册

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 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1章 引言	1
1.1 基本概念	1
1.1.1 信息定义	1
1.1.2 安全定义	2
1.1.3 信息安全定义	2
1.1.4 可用性	2
1.1.5 完整性	3
1.1.6 真实性	3
1.1.7 机密性	4
1.1.8 不可否认性	4
1.1.9 其他属性	5
1.2 信息安全发展过程	5
1.2.1 数据通信安全	5
1.2.2 计算机安全	5
1.2.3 网络安全	6
1.2.4 信息安全保障	6
1.2.5 未来安全	6
1.3 CISAW 信息安全保障模型	7
1.3.1 模型的定义	7
1.3.2 信息安全保障对象	9
1.3.3 本质对象	10
1.3.4 实体对象	10

1.3.5 资源	12
1.3.6 管理	13
1.4 相关标准及法律法规	13
1.4.1 相关标准	13
1.4.2 法律法规	14
1.5 本书结构	16
1.6 小结	16
第2章 密码技术	17
2.1 概述	17
2.1.1 发展历程	17
2.1.2 发展趋势	18
2.2 密码学基础	20
2.2.1 基础概念	20
2.2.2 对称密码体制	21
2.2.3 非对称密码体制	37
2.3 公钥基础设施	40
2.3.1 PKI 概述	41
2.3.2 PKI 组成	41
2.4 数字摘要技术	43
2.4.1 基本原理	43
2.4.2 Hash 函数	43
2.5 数字签名技术	50
2.5.1 RSA 数字签名算法	52
2.5.2 DSA 数字签名算法	52
2.5.3 ECDSA 数字签名算法	53
2.5.4 双重签名	53
2.5.5 其他签名方案	54
2.6 密钥管理技术	54
2.6.1 密钥管理相关标准	54
2.6.2 密钥的生命周期	55
2.7 典型开发环境介绍	59
2.7.1 Crypto++ 开发环境	59

2.7.2	OpenSSL	62
2.8	小结	66
	思考题	67
第3章	身份认证	68
3.1	概述	68
3.1.1	基本概念	68
3.1.2	认证基础	69
3.2	基于口令的身份认证技术	70
3.3	基于生物特征的身份认证技术	74
3.3.1	人脸识别技术	74
3.3.2	指纹识别技术	76
3.3.3	虹膜识别技术	77
3.4	基于密码学的身份认证技术	78
3.4.1	基于对称密钥的认证协议	78
3.4.2	基于公开密钥的认证协议	79
3.5	身份认证技术应用与实现	80
3.6	小结	84
	思考题	84
第4章	访问控制	85
4.1	概述	85
4.1.1	基本概念	85
4.1.2	访问控制的通用模型	86
4.2	访问控制模型	88
4.2.1	自主访问控制模型	88
4.2.2	强制访问控制模型	88
4.2.3	基于角色的访问控制	91
4.2.4	其他访问控制模型	94
4.3	访问控制技术实现与应用	95
4.3.1	访问控制技术实现	95
4.3.2	访问控制技术应用实例	97
4.4	小结	101
	思考题	102

第5章 信息隐藏	103
5.1 概述	103
5.1.1 信息隐藏的定义	103
5.1.2 信息隐藏的分类	104
5.1.3 信息隐藏技术特点	105
5.1.4 信息隐藏算法	106
5.1.5 信息隐藏技术的发展	106
5.2 信息隐藏模型	107
5.2.1 隐写模型	107
5.2.2 数字水印模型	109
5.3 信息隐藏算法与实现	110
5.3.1 位平面算法与实现	110
5.3.2 空域信息隐藏算法与实现	114
5.3.3 变换域信息隐藏算法与实现	116
5.4 信息隐藏应用方案	118
5.4.1 版权保护	118
5.4.2 数字签名	119
5.4.3 数字指纹	119
5.4.4 广播监视	120
5.4.5 安全通信	120
5.5 小结	121
思考题	122
第6章 容错容灾	123
6.1 概述	123
6.1.1 相关概念	123
6.1.2 容错容灾概述	124
6.2 存储技术	125
6.2.1 存储设备	125
6.2.2 网络存储技术	126
6.2.3 分级存储技术	129
6.3 备份技术	132
6.3.1 备份策略和方式	132

6.3.2 备份技术	133
6.4 独立磁盘冗余阵列技术	134
6.4.1 RAID 关键技术	134
6.4.2 RAID 的级别	135
6.5 复制技术	140
6.5.1 基于服务器逻辑卷的数据复制技术	141
6.5.2 基于存储设备的磁盘数据复制技术	143
6.5.3 基于数据库的数据复制技术	144
6.5.4 基于应用的数据复制技术	146
6.6 迁移技术	146
6.7 数据快照技术	147
6.7.1 快照概念	147
6.7.2 快照的实现方式	148
6.7.3 快照的实现层次	151
6.8 失效检测技术	151
6.8.1 失效检测评价标准	152
6.8.2 失效检测方法	153
6.9 双机热备	154
6.9.1 双机热备模式	154
6.9.2 双机互备模式	156
6.9.3 双机热备的实现方式	157
6.10 集群技术	157
6.10.1 集群的分类	157
6.10.2 集群的软件体系结构	160
6.10.3 集群的实现	161
6.11 小结	161
思考题	162
第7章 反垃圾邮件技术	163
7.1 概述	163
7.1.1 相关概念	163
7.1.2 电子邮件系统工作原理	163
7.1.3 反垃圾邮件技术的现状	166

7.2 传统过滤技术	167
7.2.1 关键词过滤	167
7.2.2 黑白名单技术	167
7.2.3 基于规则的过滤	168
7.2.4 Hash 技术	169
7.2.5 传统过滤技术特点分析	169
7.3 智能和概率系统	169
7.3.1 基于贝叶斯分类器的过滤	169
7.3.2 基于规则评分系统的过滤	171
7.3.3 基于行为模式识别的过滤	171
7.3.4 智能和概率系统技术特点分析	172
7.4 前端验证技术	172
7.4.1 反向查询技术	172
7.4.2 DKIM 技术	173
7.4.3 SenderID 技术	174
7.5 挑战-响应技术	175
7.6 小结	176
思考题	176
第8章 存储介质安全技术	177
8.1 概述	177
8.1.1 相关概念	177
8.1.2 存储介质种类和特点	178
8.1.3 存储介质逻辑结构	179
8.1.4 存储介质数据存储结构	180
8.1.5 介质安全技术综述	182
8.2 介质物理安全技术	183
8.2.1 防震技术	183
8.2.2 故障检测技术	184
8.3 介质加密技术	184
8.3.1 硬盘加密技术	185
8.3.2 存储介质级加密技术的应用特点	187
8.4 硬盘防拷贝技术	188

8.4.1 主引导扇区设置密码	188
8.4.2 利用文件首簇号	188
8.5 介质数据恢复技术	189
8.5.1 磁盘恢复原理	189
8.5.2 主引导记录恢复	189
8.5.3 分区恢复	190
8.5.4 DBR 恢复	190
8.5.5 FAT 表恢复	191
8.5.6 RAID 恢复	192
8.6 介质数据安全销毁技术	193
8.6.1 磁介质的安全销毁技术	193
8.6.2 光存储介质的安全销毁	194
8.6.3 半导体存储介质的安全销毁	195
8.7 小结	195
思考题	196
第9章 恶意代码及防护	197
9.1 恶意代码概述	197
9.1.1 恶意代码发展简介	197
9.1.2 恶意代码的特征	198
9.1.3 典型恶意代码	198
9.1.4 恶意代码的分析方法	202
9.1.5 恶意代码传播手法	203
9.1.6 恶意代码传播趋势	203
9.2 病毒	204
9.2.1 病毒原理	204
9.2.2 病毒编制技术	205
9.3 蠕虫	206
9.3.1 蠕虫简介	206
9.3.2 蠕虫关键模块	207
9.3.3 蠕虫工作机制	208
9.4 木马	208
9.4.1 木马概述	208

9.4.2 木马的关键技术	209
9.5 其他	213
9.5.1 流氓软件	213
9.5.2 基于邮件漏洞的恶意代码	214
9.5.3 移动终端恶意代码	214
9.5.4 网络僵尸	216
9.5.5 Rookit 恶意代码	217
9.6 网络恶意代码防护	220
9.6.1 恶意代码的检测	220
9.6.2 恶意代码的防治手段	221
9.7 小结	222
思考题	222
第10章 传输安全	223
10.1 概述	223
10.1.1 基本概念	223
10.1.2 传输安全的发展历程	224
10.2 传输载体安全技术	225
10.2.1 传输介质的安全	225
10.2.2 传输设备的安全	227
10.3 传输协议安全技术	232
10.3.1 常见的传输协议	232
10.3.2 典型的协议安全问题	234
10.3.3 协议安全技术	235
10.4 安全协议	241
10.4.1 基本知识	241
10.4.2 IPSec	243
10.4.3 SSL	249
10.4.4 HTTPS	255
10.5 小结	256
思考题	257
第11章 机房环境	258
11.1 概述	258