



普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

信息安全管 理

Xinxi
Anquan Guanli

徐国爱 彭俊好 张 淼 编著



北京邮电大学出版社
www.buptpress.com



普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

信息安全管理

徐国爱 彭俊好 张森 编著

北京邮电大学出版社
·北京·

内 容 简 介

本书作为信息安全系列教材之一,在汇总作者及所在团队多年来信息安全管理相关工作的基础上,还提炼了国内和国际上信息安全管理方面的最新成果。本书在保证知识点讲解精炼的基础上,全面吸纳了最新国内外信息安全管理相关标准和指南的内容,能够反映出信息安全管理及与方法的研究和应用现状。

本书内容共9章。第1章是绪论。第2章是信息安全控制规范。第3章是信息系统安全审计。第4章是信息安全事件管理。第5章是信息安全风险评估。第6章是信息安全管理体系实施。第7章是信息安全测评认证。第8章是信息安全工程管理。第9章是信息安全法规标准。

本书适用于高等院校通信专业本科教材,也可作为相关专业技术人员的参考书日。

图书在版编目(CIP)数据

信息安全管理/徐国爱,彭俊好,张森编著. —北京:北京邮电大学出版社,2008

ISBN 978-7-5635-1671-1

I. 信… II. ①徐…②彭…③张… III. 信息系统—安全管理—教材 IV. TP309

中国版本图书馆CIP数据核字(2008)第033918号

书 名: 信息安全管理

作 者: 徐国爱 彭俊好 张 森

责任编辑: 满志文

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路10号(邮编:100876)

发 行 部: 电话: 010-62282185 传真: 010-62283578

E-mail: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京市梦宇印务有限公司

开 本: 787 mm×960 mm 1/16

印 张: 20.25

字 数: 441千字

印 数: 1—5 000册

版 次: 2008年6月第1版 2008年6月第1次印刷

ISBN 978-7-5635-1671-1

定 价: 36.00元

· 如有印装质量问题,请与北京邮电大学出版社发行部联系 ·

信息安全专业系列教材(第2版)

编委会

主 编 杨义先

编 委 (排名不分先后)

章照止 钮心忻 牛少彰 徐国爱

卓新建 崔宝江 张 茹 谷利泽

郑康锋 辛 阳 李 剑 李 晖

裘晓峰 马春光

第 2 版总序

发展 21 世纪中国信息安全要靠教育,而搞好信息安全教育就需要好的教材。2004 年,灵创团队北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材,该套教材被教育部列入了“普通高等教育‘十五’国家级规划教材”。至今,三年多的时间过去了,这套教材在信息安全专业的教学中发挥了重要的作用,起到了较好的教学效果,受到教师和学生的好评。

在这三年中,我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设和校企就业(创业)平台建设等在内的信息安全本科专业的全面建设。2005 年,作为组长单位我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题;召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”。我们完成的国内第一次制定的信息安全专业规范,从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系;由通识教育内容、专业教育内容和综合教育内容三大部分,构建课程参考体系;采用顶层设计的方法构建了带有实践性环节的教学体系。我们在国内第一次较全面地提出信息安全学科专业教学改革与创新的研究以及发展思路和政策建议;这些成果已提交教育部相关教学指导委员会,对于引导高等学校信息安全学科专业教学改革与建设,指导信息安全学科专业评估,促进信息安全学科专业教学规范建设与管理,提高专业教育质量和水平起到了重要的作用。多所举办信息安全专业的高校都参照该课题成果调整了自己的教学计划、课程体系和实验方案。

我们积极搭建信息安全专业校际交流平台,组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”和“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地 40 亩的全国信息安全专业本科生实习实训基地,接受了来自全国近 30 所高校的本科生进入该基地参加丰富多彩的实训。

我们努力建设精品课程,主办了“全国高校信息安全专业精品课程建设经验交流会议”,来自全国各地高校的专家齐聚北京邮电大学,介绍了精品课程建设的经验。我们组织了全国第一批信息安全实验室,并且编写出版了实验教材《信息安全实验指导》,我们的《现代密码学》课程已经被评为北京市精品课程,并在 2007 年度被评为“国家精品课程”。

经过灵创团队全体人员的共同努力,北京邮电大学信息安全本科专业被教育部评为

第二类优势特色专业。

三年多的时间过去了,无论信息安全的教育和产业都取得了丰硕的成果,随着信息安全向更高层次的发展,其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要,积极探索培养创新型高素质人才,我们按照制定的学科发展战略和专业规范的精神,结合近几年的教学实践,我们对这套信息安全专业本科系列教材进行了全面修订,并及时成立了灵创团队北京邮电大学数字内容研究中心。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善,还补充了信息安全最新的研究成果,使教材的内容更加翔实和新颖。同时,在原有的教材上又增加了一些新的课程教材,在新修订的系列教材中,目前有《信息安全概论》(第2版)、《现代密码学及其应用》、《网络安全》(第2版)、《信息安全管理》、《计算机病毒原理及防治》(第2版)、《数字版权管理》、《计算机系统安全》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》、《数字图像取证技术》等13本教材,今后随着信息安全专业教学的需要,还将不断地有新的教材补充到这个系列中来,使之更加完善和系统。目前,计划列入的相关教材还有:《入侵检测》(第2版)、《信息内容安全》、《信息安全工程》、《软件安全》及《信息安全标准与法律法规》等。

我们组织了强大的师资队伍,广泛吸收了有着丰富教学科研经验并多次讲授该系列教材的教师充实到这次修订工作中。作者队伍中不但包括北京邮电大学的教师,还包括哈尔滨工程大学、北京交通大学等重点院校的教师。经过反复研讨,本着理论与实际相结合的原则,对原来的系列教材进行了较大的修改和扩充,我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向专业的不同需求。

这次修订我们对内容进行了精心的组织和安排,希望能促进信息安全课程的建设,涌现出更多的信息安全精品课程。虽然我们在这次修订中投入了很大精力,但是由于水平有限,时间仓促,且信息安全专业的发展速度非常快,书中的不足之处和错误在所难免,我们衷心期望使用和关心该系列教材的师生,继续对新的系列教材提出宝贵的意见和建议。

本套系列教材也是国家重点基础研究发展计划(973)(课题编号:2007CB310704和2007CB311203)资助的成果,并被教育部增补为“普通高等教育‘十一五’国家级规划教材”的选题。

在本系列教材的修订过程中,得到了北京邮电大学出版社的大力支持,同时也得到了灵创团队的骨干机构(北京邮电大学信息安全中心和北京邮电大学数字内容研究中心)三百余位成员的支持与配合,在此一并表示感谢。

教授、博导、长江学者特聘教授

杨义先

2007年7月

前 言

随着人们对信息技术依赖程度的不断加深,信息安全受到了社会的普遍关注。通过技术手段针对性地解决信息安全问题是信息安全防范的基本思路,然而,由于信息安全的多层次、多因素和动态性等特点,管理手段的应用在一个完整的信息安全防范方案中必不可少。信息安全管理模型、流程和方法最近几年有了长足的发展,信息安全管理的相关标准、法规也如雨后春笋般相继被推出。三分技术、七分管理的理念正在为社会各界广泛接受。

北京邮电大学信息安全中心从1984年以来,一直专注于信息安全领域的理论和应用研究,中心先后承担过数项国家级信息安全相关课题的研究,并成功的将其中的大部分成果实现商业转化,为国家信息化建设做出了不错的贡献。信息安全系列教材是我们专为信息安全教学和科研推出的一款系列书籍,内容涵盖信息安全领域的方方面面。系列教材既可作为高等院校信息安全及相关专业研究生和高年级本科生的教材使用,也可作为相关专业人员全面参考的系列手册。

作为信息安全系列教材之一,本书在汇总作者及所在团队多年来信息安全管理相关工作的基础上,还提炼了国内和国际上信息安全管理方面的最新成果。本书在保证知识点讲解精炼的基础上,全面吸纳了最新国内外信息安全管理相关标准和指南的内容,能够反映出信息安全管理理论与方法的研究和应用现状。本书通过第1章梳理了各种信息安全管理理论、方法和流程的内涵及它们之间的关系,并以此展开全书的主体内容。本书主体内容分为三个部分,第一部分在介绍信息安全管理控制规范的基础上,没有全面展开对信息安全技术的介绍,而突出介绍了偏于管理的信息安全技术内容——信息系统安全审计,这包括第2~3章;第二部分包括第4~8章,依次介绍了信息安全事件管理、信息安全风险评估、信息安全管理体系实施、信息安全测评认证和信息安全工程管理等信息安全管理的主流方法;最后,在第三部分集中介绍了作为信息安全保障体系关键内容的信息安全法规标准,这就是第9章。

本书由北京邮电大学信息安全中心组织编写。徐国爱参与了第1、3章的编写,彭俊好参与了第4~6章的编写,刘凡凡参与了第6章的编写,陈晓光参与了第2、8章的编写,汤永利参与了第6、9章的编写,李娜参与了第7章的编写,朱伽参与了第9章的编写;朱强、吴正华、牛婷芝、刘嘉、姜磊、李娜、姚志东、肖靖、郜小亮、张建武、郭承青和高洋等共同参与了资料收集、整理工作;全书由徐国爱、彭俊好统稿,张森协助。此外,本书得到了胡

正明教授、杨义先教授、钮心忻教授和罗群副教授的大力支持和指导,他们对书中的内容提出了宝贵的意见,在此一并表示衷心的感谢。

本书在编写过程中,除引用了作者自身的研究内容和成果之外,还大量参考了众多国内外优秀论文、书籍以及互联网上公布的相关资料,我们尽量在书后面的参考文献中列出,但由于互联网上资料数量众多、出处杂乱,可能无法将所有文献一一注明出处。我们对这些资料的作者表示由衷的感谢,同时声明,原文版权属于原作者。

本书作为教材,教师在讲授时可以根据学时安排做出一些取舍。本书全部讲授建议34学时;如果有更多学时安排,建议酌情增加信息安全技术方面的内容,以深化对全书内容的理解。

信息安全管理是信息安全领域中新的分支,代表了信息安全发展的一种趋势,本书尝试对此领域的理论和方法做一些归纳,以期有益于读者。由于作者的水平有限,书中难免有一些缺点和错误,真诚希望读者不吝赐教,以期再版修订。

编者

目 录

第 1 章 绪论

1.1 信息安全管理	1
1.1.1 什么是信息安全管理	1
1.1.2 信息安全管理模型	3
1.1.3 信息安全管理体系	4
1.1.4 信息安全管理意义	5
1.2 信息安全技术体系	6
1.2.1 信息安全技术体系的概念	6
1.2.2 基础支撑技术	7
1.2.3 主动防御技术	8
1.2.4 被动防御技术	9
1.2.5 面向管理的技术	9
1.3 信息安全管理方法	10
1.3.1 信息安全风险评估	10
1.3.2 信息安全事件管理	11
1.3.3 信息安全测评认证	11
1.3.4 信息安全工程管理	12
1.4 信息安全保障体系	12
1.4.1 信息安全保障体系的概念	12
1.4.2 信息安全组织	14
1.4.3 信息安全法规	14
1.4.4 信息安全标准	16
1.5 本书的内容安排	18
习题	19

第 2 章 信息安全控制规范

2.1 概述	20
2.2 信息安全策略	22

2.3	信息安全组织	23
2.3.1	信息安全的基本架构	23
2.3.2	第三方访问的安全	25
2.3.3	外包	28
2.4	资产分类和管理	28
2.4.1	资产的可计量性	28
2.4.2	信息分类	29
2.5	人员安全	30
2.5.1	工作定义和外包的安全	30
2.5.2	用户培训	31
2.5.3	安全事故响应	31
2.6	物理和环境的安全	33
2.6.1	安全区域	33
2.6.2	设备安全	35
2.6.3	一般性管理措施	38
2.7	通信和运营管理	38
2.7.1	操作过程和责任	38
2.7.2	系统规划和验收	41
2.7.3	防止恶意软件	42
2.7.4	内务管理	43
2.7.5	网络管理	44
2.7.6	备份介质处理和安全	45
2.7.7	信息和软件的交换	46
2.8	访问控制	50
2.8.1	访问控制的业务需要	50
2.8.2	用户访问管理	50
2.8.3	用户责任	52
2.8.4	网络访问控制	53
2.8.5	操作系统访问管理	56
2.8.6	应用程序访问控制	58
2.8.7	检测系统访问和使用	59
2.8.8	移动计算和远程工作	61
2.9	系统的开发与维护	62
2.9.1	系统的安全需要	62
2.9.2	应用软件系统的安全	63

2.9.3	密码管理措施	64
2.9.4	信息文件的安全	66
2.9.5	开发和支持过程中的安全	68
2.10	业务连续性管理	69
2.11	符合性	72
2.11.1	符合法律要求	72
2.11.2	安全策略和技术符合性的检查	75
2.11.3	系统审查相关事项	76
	本章小结	76
	习题	77

第3章 信息系统安全审计

3.1	概述	78
3.1.1	信息系统安全审计的概念	78
3.1.2	信息系统安全审计的功能	79
3.1.3	信息系统安全审计的分类	79
3.2	安全审计系统的体系结构	80
3.2.1	信息安全审计系统的一般组成	80
3.2.2	集中式安全审计系统体系结构	81
3.2.3	分布式安全审计系统体系结构	82
3.3	安全审计的一般流程	83
3.3.1	策略定义	83
3.3.2	事件采集	83
3.3.3	事件辨别与分析	84
3.3.4	事件响应	84
3.3.5	结果汇总	84
3.4	安全审计的分析方法	84
3.5	安全审计的数据源	86
3.6	信息安全审计与标准	88
3.6.1	TCSEC 对于审计子系统的要求	89
3.6.2	CC 中的安全审计功能需求	89
3.6.3	GB 17859—1999 对安全审计的要求	90
3.6.4	信息系统安全审计产品技术要求	91
3.7	计算机取证	92
3.7.1	计算机取证的发展历程	92
3.7.2	什么是计算机取证	93

3.7.3 计算机取证流程	94
3.7.4 计算机取证相关技术	95
3.7.5 计算机取证工具分类	97
本章小结	100
习题	100

第4章 信息安全事件管理

4.1 概述	101
4.1.1 什么是信息安全事件	101
4.1.2 信息安全事件管理的意义	102
4.1.3 信息安全事件管理的主要内容	104
4.2 信息安全事件管理过程	106
4.2.1 NIST SP 800-61 提供的参考流程	106
4.2.2 GB/Z 20985—2007 提供的参考流程	109
4.3 信息安全事件分类分级	112
4.3.1 信息安全事件分类	112
4.3.2 信息安全事件分级	116
4.4 应急响应	118
4.4.1 什么是应急响应	118
4.4.2 应急响应的组织机构	118
4.4.3 应急响应流程	124
4.4.4 应急响应保障措施	126
4.4.5 应急响应计划	127
4.5 信息安全灾难恢复	131
4.5.1 概述	131
4.5.2 灾难恢复的组织机构	132
4.5.3 灾难恢复的工作范围	133
4.5.4 灾难恢复的等级划分	140
4.5.5 灾难恢复与备份	144
4.5.6 灾难恢复工具	150
本章小结	151
习题	152

第5章 信息安全风险评估

5.1 概述	153
5.1.1 信息安全风险评估相关要素	153

5.1.2	信息安全风险评估	156
5.1.3	风险要素相互间的关系	157
5.2	信息安全风险评估策略	159
5.2.1	基线风险评估	159
5.2.2	详细风险评估	160
5.2.3	综合风险评估	160
5.3	信息安全风险评估流程	161
5.3.1	风险评估流程概述	161
5.3.2	风险评估的准备	162
5.3.3	资产识别与评估	163
5.3.4	威胁识别与评估	165
5.3.5	脆弱点识别与评估	168
5.3.6	已有安全措施的确认真	169
5.3.7	风险分析	170
5.3.8	安全措施的选取	173
5.3.9	风险评估文件记录	173
5.4	信息安全风险评估方法	174
5.4.1	概述	174
5.4.2	信息安全风险评估理论基础	175
5.4.3	定量方法	182
5.4.4	定性方法	185
5.5	风险评估案例	187
5.5.1	案例介绍	187
5.5.2	资产识别与评估	188
5.5.3	威胁识别与评估	188
5.5.4	脆弱点识别与评估	189
5.5.5	风险分析与等级划分	190
5.5.6	安全措施的选取	191
	本章小结	192
	习题	192

第 6 章 信息安全管理体系实施

6.1	概述	194
6.2	ISMS 实施模型	194
6.3	ISMS 实施过程	196

6.3.1	建立 ISMS	196
6.3.2	实施和运行 ISMS	199
6.3.3	监视和评审 ISMS	200
6.3.4	保持和改进 ISMS	200
6.4	ISMS 文件要求	200
6.4.1	ISMS 文件	200
6.4.2	文件定义	201
6.4.3	文件控制	203
6.4.4	记录控制	203
6.5	ISMS 审核	204
6.5.1	内部审核	204
6.5.2	管理评审	204
6.6	ISMS 持续改进	205
6.6.1	持续改进	205
6.6.2	纠正措施	205
6.6.3	预防措施	206
6.7	ISMS 实施案例	206
6.7.1	ISMS 规划阶段	206
6.7.2	ISMS 实施阶段	208
6.7.3	ISMS 检查阶段	208
6.7.4	ISMS 处置阶段	209
6.8	信息安全管理工具	209
6.8.1	综合风险管理及评估工具	209
6.8.2	组件评估及测试工具	211
6.8.3	数据及文档管理工具	211
	本章小结	212
	习题	212

第 7 章 信息安全测评认证

7.1	概述	213
7.1.1	什么是信息安全测评认证	213
7.1.2	国外信息安全测评认证现状	214
7.1.3	我国信息安全测评认证现状	215
7.1.4	测试评估相关技术	217
7.2	测评认证有关规范	217

7.2.1	CC	217
7.2.2	GB 17859—1999	222
7.2.3	其他相关标准	224
7.3	测评技术	225
7.3.1	测评认证过程	225
7.3.2	渗透测试	228
7.3.3	代码分析	231
7.3.4	日志分析	234
7.4	信息安全测评实施案例	234
	本章小结	237
	习题	237

第8章 信息安全工程管理

8.1	概述	239
8.1.1	背景简介	239
8.1.2	SSE-CMM 的益处	241
8.2	CMM 概念	242
8.2.1	过程改进	242
8.2.2	期望结果	243
8.2.3	关键概念	243
8.3	模型体系结构	245
8.3.1	安全工程	245
8.3.2	安全工程过程概述	247
8.3.3	SSE-CMM 体系结构描述	250
8.4	能力级别概述	253
8.4.1	0级能力——不执行	253
8.4.2	1级能力——有科学根据地实施	254
8.4.3	2级能力——被设计和跟踪	254
8.4.4	3级能力——恰如其分的定义	255
8.4.5	4级能力——量化的控制	255
8.4.6	5级能力——连续性改进	256
8.5	安全性工程过程区	256
8.6	SSE-CMM 的使用	259
8.6.1	SSE-CMM 适用对象	259
8.6.2	使用 SSE-CMM 进行评定	260

8.6.3	使用 SSE-CMM 改进过程	263
8.6.4	使用 SSE-CMM 获得安全保证	263
8.6.5	如何使用 SSE-CMM	264
	本章小结	266
	习题	267
第 9 章 信息安全法规标准		
9.1	概述	268
9.1.1	信息安全法规的概念	268
9.1.2	信息安全法规的需求	268
9.1.3	信息安全法规的原则	269
9.1.4	信息安全标准概述	271
9.2	国外信息安全法规	271
9.2.1	美国	272
9.2.2	欧洲	277
9.2.3	日本	280
9.3	我国信息安全法规	286
9.3.1	信息安全法规体系	286
9.3.2	《中华人民共和国刑法》	287
9.3.3	《全国人大常委会关于维护互联网安全的决定》	288
9.3.4	《中华人民共和国电子签名法》	289
9.3.5	《中华人民共和国计算机信息系统安全保护条例》	290
9.3.6	《信息网络传播权保护条例》	290
9.4	国外信息安全标准	292
9.4.1	国际信息安全标准发展历史	292
9.4.2	国际信息安全标准化组织	293
9.4.3	国际重要的信息安全标准介绍	295
9.5	我国信息安全标准	298
9.5.1	国内信息安全标准的发展现状	298
9.5.2	国内重要的信息安全标准	299
	本章小结	302
	习题	302
	参考文献	303

第 1 章

绪 论

信息安全管理是保障信息系统安全的有力手段,是当今世界各国都在努力推广与应用的重点课题。它涉及的内容广泛,包括技术、方法、模型、保障体系等多方面内容。本章对信息安全的概念、模型、技术体系、基本方法、保障体系等内容进行了概要的阐述,并对本书的内容安排进行了说明。

1.1 信息安全管理

1.1.1 什么是信息安全管理

信息技术创立、应用和普及是 20 世纪技术革新最伟大的创举之一,藉此,人类正在进入信息化社会,人们对信息、信息技术的依赖程度越来越高。一方面,信息已成为一种崭新的资产,在政治、经济、军事、教育、科技和生活等方面发挥着重要的作用,另一方面,由此而带来的信息安全问题正变得日益突出。由于信息具有易传输、易扩散、易破损的特点,信息资产比传统资产更加脆弱,更易受到损害,信息及信息系统需要严格管理和妥善保护。

网络技术的发展加速了信息的传输与处理,缩短了人们之间的时空距离,方便了交流;同时,对信息安全提出了新的挑战。据统计,全球平均每 20 秒就发生一次计算机病毒的入侵;互联网上的防火墙大约 25% 被攻破;窃取商业信息的事件平均以每月 260% 的速度增加;约 70% 的网络主管报告因机密信息泄露而受到损失。国家与国家之间的信息战问题更是关系到国家的根本安全问题。

关于信息安全,不同组织有不同的定义,国际标准化组织对信息安全的定义是:“在技术上和管理上为数据处理系统建立的安全保护,保护计算机硬件、软件和数据不因偶然和