信息安全系列教材

信息安全工程

主　编　赵俊阁
副主编　陈泽茂　薛丽敏　王春东　刘　可

WUHAN UNIVERSITY PRESS
武汉大学出版社

信息安全系列教材

信息安全工程

主　编　赵俊阁
副主编　陈泽茂　薛丽敏　王春东　刘　可
参　编　周立兵　朱婷婷　柳景超　魏国珩
　　姜浩伟　王志锋　张　琪　赵树林

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

信息安全工程/赵俊阁主编;陈泽茂,薛丽敏,王春东,刘可副主编.—武汉:武汉大学出版社,2008.9
信息安全系列教材
ISBN 978-7-307-06529-1

Ⅰ.信… Ⅱ.①赵… ②陈… ③薛… ④王… ⑤刘… Ⅲ.信息系统—安全技术—高等学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2008)第 143847 号

责任编辑:黄金文 乞慧希 责任校对:黄添生 版式设计:支 笛

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)
(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.whu.edu.cn)
印刷:湖北金海印务公司
开本:787×1092 1/16 印张:14.5 字数:357 千字
版次:2008 年 9 月第 1 版 2008 年 9 月第 1 次印刷
ISBN 978-7-307-06529-1/TP·313 定价:24.00 元

信息安全系列教材

编　委　会

何明星，西华大学数学与计算机学院副院长，教授
代春艳，重庆工商大学计算机科学与信息工程学院
陈　龙，重庆邮电大学计算机科学与技术学院，副教授
杨德刚，重庆师范大学数学与计算机科学学院
黄同愿，重庆工学院计算机学院
郑智捷，云南大学软件学院信息安全系主任，教授
谢晓尧，贵州师范大学副校长，教授

华　东

徐炜民，上海大学计算机工程与科学学院，教授
楚丹琪，上海大学教务处，副教授
孙　莉，东华大学计算机科学与技术学院，副教授
李继国，河海大学计算机及信息工程学院，副教授
张福泰，南京师范大学数学与计算机科学学院，教授
王　箭，南京航空航天大学信息科学技术学院，副教授
张书奎，苏州大学计算机科学与技术学院，副教授
殷新春，杨州大学信息工程学院副院长，教授
林柏钢，福州大学数学与计算机科学学院，教授
唐向宏，杭州电子科技大学通信工程学院，教授
侯整风，合肥工业大学计算机学院计算机系主任，教授
贾小珠，青岛大学信息工程学院，教授
郑汉垣，福建龙岩学院数学与计算机科学学院副院长，高级实验师

中　南

钟　珞，武汉理工大学计算机学院院长，教授
赵俊阁，海军工程大学信息安全系，副教授
王江晴，中南民族大学计算机学院院长，教授
宋　军，中国地质大学（武汉）计算机学院
麦永浩，湖北警官学院信息技术系副主任，教授
亢保元，中南大学数学科学与计算技术学院，副教授
李章兵，湖南科技大学计算机学院信息安全系主任，副教授
唐韶华，华南理工大学计算机科学与工程学院，教授
杨　波，华南农业大学信息学院，教授

内容提要

本书力图从工程的角度出发，对信息安全从规划与控制、需求与分析、实施与评估全过程的描述，并结合具体的信息安全工程的实现，描述了信息安全工程的内容。本书主要介绍了信息安全工程基础、系统安全工程能力成熟度模型（SSE-CMM）、信息安全工程实施、信息安全风险评估、信息安全策略、信息安全工程与等级保护和数据备份与灾难恢复，并详细叙述了安全规划与控制、安全需求的定义、安全设计支持、安全运行分析、生命周期安全支持等信息安全工程的过程。并通过几个实施案例加强对信息安全工程的认识。通过本书的学习，学生可对信息安全工程的原理与技术有所了解，并明确信息安全工程过程所包含的内容。

本书适合作为信息安全专业学生的教材，也可供从事相关工作的技术人员和对信息安全感兴趣的读者阅读参考。

序　言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006 年 9 月 19 日

前　言

信息是社会发展的重要战略资源。信息技术和信息产业正在改变传统的生产、经营和生活方式，成为新的经济增长点。信息网络国际化、社会化、开放化、个人化的特点使国家的“信息边疆”不断延伸，国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全成为维护国家安全和社会稳定的一个焦点，各国都给以极大的关注与投入。

著名信息安全专家沈昌祥院士指出：“信息安全既不是纯粹的技术，也不是简单的安全产品的堆砌，而是一项复杂的系统工程——信息安全工程”。其复杂性体现在信息安全具有全面性、生命周期性、动态性、层次性和相对性等特点。作为系统工程，就要用系统工程的观点、方法来对待、处理信息安全问题。安全体系结构的设计、安全解决方案的提出必须是基于信息安全工程理论。对企业来讲，在建立与实施企业级的信息与网络系统安全体系时，必须考虑信息安全的方方面面，必须兼顾信息网络的风险评估与分析、信息网络的整体安全策略、安全模型、安全体系结构的开发、信息网络安全的技术标准与规范的制定、信息网络安全工程的实施等各个方面。对工程实施单位，必须严格按照信息安全工程的过程，规范实施。只有这样才能实现真正意义的信息安全。

信息安全工程的实施方法有许多种，总的指导思想是将安全工程与信息系统开发集成起来。本书以信息系统建设为基础，在分析常见的信息安全问题上，指出具有生命周期的信息安全工程建设流程。并具体描述了信息安全工程过程的目的是使信息系统安全成为系统工程和系统获取过程整体的必要部分，从而有力地保证客户目标的实现，提供有效的安全措施以满足客户的需求，将信息系统安全的安全选项集成到系统工程中去获得最优的信息系统安全解决方案。

本书共分 9 章，第 1 章信息安全工程基础，介绍信息系统建设中常见的信息安全问题及信息安全工程的概念、建设流程和特点；第 2 章系统安全工程能力成熟度模型（SSE-CMM），介绍 SSE-CMM 的基础、体系结构与应用；第 3 章信息安全工程与实施，介绍安全规划与控制、安全需求定义、安全支持设计、安全运行分析、生命周期安全支持和信息安全工程过程；第 4 章信息安全风险评估，介绍风险评估的方法、风险评估的过程和风险评估的实施；第 5 章信息安全策略，介绍信息安全策略的概念、规划与实施以及环境安全、系统安全、病毒防护安全策略；第 6 章信息安全工程与等级保护，介绍等级保护的概念及其在信息安全工程中的实施；第 7 章数据备份与灾难恢复，包括数据备份的概念与技术、灾难恢复概念、计划和技术；第 8 章信息安全工程案例，分别介绍了涉密网安全建设规划设计、信息系统网络安全

工程实施和政府网络安全解决方案；第9章介绍了部分信息安全组织。每章后面附有习题，以利于学生学习时使用。

本书的撰写目的是弥补当前市场上《信息安全工程》教材的缺乏。我们希望编写这样的教材满足信息安全专业教学。

本书的编写是集体共同努力的结晶，包括北京海军司令部的赵树林高级工程师和刘可工程师、南京海军指挥学院的薛丽敏老师、天津理工大学的王春东老师以及武汉海军工程大学信息安全教研室的相关老师。赵俊阁和陈泽茂共同完成编写大纲的制定。赵俊阁和朱婷婷完成第1章、赵俊阁和薛丽敏完成第2章、周立兵完成第3章、柳景超完成第4章、魏国珩完成第5章、刘可完成第6章、姜浩伟完成第7章、王春东和赵树林完成第8章、王志锋完成第9章，张琪完成习题编写与插图。陈泽茂完成了全书的统稿工作。

由于作者水平有限，因此对于本书中出现的错误，恳请读者提出宝贵意见，以便再版时修改和完善，甚为感谢。

作　者

2008年7月

目 录

第一章 信息安全工程基础……1
1.1 信息系统建设……1
1.1.1 信息系统建设的周期阶段……1
1.1.2 信息系统建设计划……2
1.1.3 软件开发工作量和时间估算……5
1.1.4 开发进度估算……6
1.2 常见信息安全问题……6
1.2.1 信息安全问题的层次……6
1.2.2 信息系统的安全问题……6
1.2.3 信息安全问题分类……7
1.3 信息安全工程概念……9
1.4 信息安全工程建设流程……10
1.5 安全工程的生命周期……12
1.6 安全工程特点……13
本章小结……14
习题一……14

第二章 系统安全工程能力成熟度模型……15
2.1 概述……15
2.1.1 安全工程……15
2.1.2 CMM 介绍……16
2.1.3 安全工程与其他项目的关系……18
2.2 SSE-CMM 基础……19
2.2.1 系统安全工程能力成熟度模型简介……19
2.2.2 系统安全工程过程……22
2.2.3 SSE-CMM 的主要概念……25
2.3 SSE-CMM 的体系结构……28
2.3.1 基本模型……28
2.3.2 域维/安全过程区……29
2.3.3 能力维/公共特性……31
2.3.4 能力级别……32
2.3.5 体系结构的组成……33
2.4 SSE-CMM 应用……34

2.4.1 SSE-CMM 应用方式……34
2.4.2 用 SSE-CMM 改进过程……37
2.4.3 使用 SSE-CMM 的一般步骤……41
2.5 系统安全工程能力评估……43
2.5.1 系统安全工程能力评估……43
2.5.2 SSE-CMM 实施中的几个问题……47
本章小结……49
习题二……49

第三章 信息安全工程实施……50
3.1 概述……50
3.2 安全规划与控制……54
3.2.1 商业决策和工程规划……54
3.2.2 信息安全工程小组……54
3.2.3 对认证和认可（C&A）的信息安全工程输入规划……56
3.2.4 信息安全工程报告……57
3.2.5 技术数据库和工具……58
3.2.6 与获取/签约有关的规划……60
3.2.7 信息系统安全保证规划……61
3.3 安全需求的定义……62
3.3.1 系统需求定义概述……62
3.3.2 安全需求分析的一般课题……64
3.3.3 安全需求定义概述……68
3.3.4 先期概念阶段和概念阶段——信息安全工程的需求活动……70
3.3.5 需求阶段——信息安全工程的需求活动……71
3.3.6 系统设计阶段——信息安全工程的需求活动……71
3.3.7 从初步设计到配置审计阶段——信息安全工程的需求活动……72
3.4 安全设计支持……72
3.4.1 系统设计……72
3.4.2 信息安全工程系统设计支持活动……73
3.4.3 先期概念和概念阶段安全设计支持……75
3.4.4 需求和系统设计阶段的安全设计支持……76
3.4.5 初步设计阶段到配置审计阶段的安全设计支持……77
3.4.6 运行和支持阶段的安全设计支持……77
3.5 安全运行分析……77
3.6 生命周期安全支持……79
3.6.1 安全的生命期支持的开发方法……79
3.6.2 对部署的系统进行安全监控……81
3.6.3 系统安全评估……81
3.6.4 配置管理……82

3.6.5 培训……82
3.6.6 后勤和维护……83
3.6.7 系统的修改……83
3.6.8 报废处置……84
3.7 信息安全工程的过程……84
本章小结……87
习题三……87

第四章 信息安全风险评估……88
4.1 信息安全风险评估基础……88
4.1.1 与风险评估相关的概念……88
4.1.2 风险评估的基本特点……89
4.1.3 风险评估的内涵……89
4.1.4 风险评估的两种方式……90
4.2 风险评估的过程……93
4.2.1 风险评估基本步骤……93
4.2.2 风险评估准备……94
4.2.3 风险因素评估……95
4.2.4 风险确定……100
4.2.5 风险评价……101
4.2.6 风险控制……101
4.3 风险评估过程中应注意的问题……103
4.3.1 信息资产的赋值……103
4.3.2 评估过程的文档化……105
4.4 风险评估方法……107
4.4.1 正确选择风险评估方法……107
4.4.2 定性风险评估和定量风险评估……107
4.4.3 结构风险因素和过程风险因素……107
4.4.4 通用风险评估方法……108
4.5 几种典型的信息安全风险评估方法……111
4.5.1 OCTAVE 法……112
4.5.2 层次分析法（AHP 法）……114
4.5.3 威胁分级法……122
4.5.4 风险综合评价……122
4.6 风险评估实施……123
4.6.1 风险评估实施原则……123
4.6.2 风险评估流程……123
4.6.3 评估方案定制……127
4.6.4 项目质量控制……129
本章小结……130

习题四……130

第五章 信息安全策略……132
5.1 信息安全策略概述……132
5.1.1 基本概念……132
5.1.2 特点……133
5.1.3 信息安全策略的制定原则……133
5.1.4 信息安全策略的制定过程……133
5.1.5 信息安全策略的框架……134
5.2 信息安全策略规划与实施……135
5.2.1 确定安全策略保护的对象……135
5.2.2 确定安全策略使用的主要技术……136
5.2.3 安全策略的实施……139
5.3 环境安全策略……140
5.3.1 环境保护机制……141
5.3.2 电源……141
5.3.3 硬件保护机制……142
5.4 系统安全策略……142
5.4.1 WWW 服务策略……142
5.4.2 电子邮件安全策略……143
5.4.3 数据库安全策略……143
5.4.4 应用服务器安全策略……144
5.5 病毒防护策略……144
5.5.1 病毒防护策略具备的准则……144
5.5.2 建立病毒防护体系……145
5.5.3 建立病毒保护类型……145
5.5.4 病毒防护策略要求……146
5.6 安全教育策略……146
本章小结……147
习题五……147

第六章 信息安全工程与等级保护……148
6.1 等级保护概述……148
6.1.1 信息安全等级保护制度的原则……148
6.1.2 信息安全等级的划分及特征……149
6.2 等级保护在信息安全工程中的实施……150
6.2.1 新建系统的安全等级保护规划与建设……151
6.2.2 系统改建实施方案设计……155
6.3 等级保护标准的确定……156
6.3.1 确定信息系统安全保护等级的一般流程……156

6.3.2 信息系统安全等级的定级方法……157
本章小结……160
习题六……160

第七章 数据备份与灾难恢复……161
7.1 数据备份的概念……161
7.2 数据备份的常用方法……166
7.2.1 数据备份层次……166
7.2.2 数据备份常用方法分类……168
7.3 灾难恢复概念……171
7.4 安全恢复的计划……172
7.4.1 容灾系统……172
7.4.2 安全恢复的实现计划……173
7.4.3 安全恢复计划……174
7.5 灾难恢复技术……176
7.5.1 灾难预防制度……176
7.5.2 数据库的恢复技术……177
本章小结……182
习题七……183

第八章 信息安全工程案例……184
8.1 涉密网安全建设规划设计……184
8.1.1 安全风险分析……184
8.1.2 规划设计……185
8.2 信息系统网络安全工程实施……188
8.2.1 制定项目计划……188
8.2.2 项目组织机构……188
8.2.3 工程具体实施……190
8.3 政府网络安全解决方案……191
8.3.1 概 述……191
8.3.2 网络系统分析……192
8.3.3 网络安全风险分析……193
8.3.4 网络安全需求及安全目标……193
8.3.5 网络安全方案总体设计……194
8.3.6 网络安全体系结构……196
习题八……200

第九章 信息安全组织……201
9.1 IETF（www.ietf.org）……201
9.2 CERT／CC（www.cert.org）……205

9.3 NSA（www.nsa.gov）和 NIST（www.nist.gov）……205
9.4 ISO……206
9.5 ITU……206

参考文献……209

第一章 信息安全工程基础

【学习目标】

- 了解信息系统建设过程;
- 认识信息系统建设中的安全问题;
- 认识信息安全工程概念;
- 了解信息安全工程特点。

1.1 信息系统建设

20 世纪 40 年代，随着计算机在社会各个领域的广泛应用和迅速普及，使人类社会步入信息时代，以计算机为核心的各种信息系统建设如雨后春笋。同时，信息安全问题伴随而来。

中国著名科学家钱学森院士认为："系统工程是组织管理系统规划、研究、制造、实验、使用的科学方法，是一种对所有系统都具有普遍意义的科学方法。"系统工程通过开发并验证一个集成的和在整个生命周期平衡的系统级产品或过程解决方案，以满足最终用户的需求，其模型包括：开发、制造、验证、部署、运行、支持和培训、处置等过程。系统工程的方法论是合理开发系统或改造旧系统的思想、步骤、方法、工具和技术。

信息系统建设基于系统工程的思想与方法，其建设过程复杂，任何系统均有其产生、发展、成熟、消亡或更新换代的过程。这个过程称为系统的生命周期。

1.1.1 信息系统建设的周期阶段

1. 系统规划

这是信息系统的起始阶段。这一阶段的主要任务是根据组织的整体目标和发展战略，确定信息系统的发展战略，明确组织总的信息需求，制定信息系统建设总计划，其中包括确定拟建系统的总体目标、功能以及所需资源，并根据需求的轻、重、缓、急及资源和应用环境的约束，把规划的系统建设内容分解成若干开发项目，以分期分批进行系统开发。

2. 系统分析与设计

这一阶段的主要工作是根据系统规划阶段确定的拟建系统总体方案和开发项目的安排，分期分批进行系统开发。这是系统建设中工作任务最为繁重的阶段。每一个项目的开发工作包括系统调查和系统开发的可能性研究、系统逻辑模型的建立、系统设计、系统实施、系统转换和系统评价等工作。

3. 系统实施

在信息系统的生命周期中，经过系统规划、系统分析和系统设计等阶段后，便开始系统实施阶段。在系统分析和设计阶段，系统开发工作主要是集中在逻辑、功能和技术设计上。系统实施阶段要继承此前各阶段的工作，将技术设计转化成为物理实现。系统实施的成果是