

<<信息安全工程>>

图书基本信息

书名：<<信息安全工程>>

13位ISBN编号：9787307065291

10位ISBN编号：7307065290

出版时间：2008-9

出版时间：武汉大学出版社

作者：赵俊阁

页数：210

字数：357000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<信息安全工程>>

内容概要

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。

<<信息安全工程>>

书籍目录

第一章 信息安全工程基础

- 1.1 信息系统建设
 - 1.1.1 信息系统建设的周期阶段
 - 1.1.2 信息系统建设计划
 - 1.1.3 软件开发工作量和时间估算
 - 1.1.4 开发进度估算
- 1.2 常见信息安全问题
 - 1.2.1 信息安全问题的层次
 - 1.2.2 信息系统的安全问题
 - 1.2.3 信息安全问题分类
- 1.3 信息安全工程概念
- 1.4 信息安全工程建设流程
- 1.5 安全工程的生命周期
- 1.6 安全工程特点

本章小结

习题一

第二章 系统安全工程能力成熟度模型

- 2.1 概述
 - 2.1.1 安全工程
 - 2.1.2 CMM介绍
 - 2.1.3 安全工程与其他项目的关系
 - 2.2 SSE—CMM基础
 - 2.2.1 系统安全工程能力成熟度模型简介
 - 2.2.2 系统安全工程过程
 - 2.2.3 SSE—CMM的主要概念
 - 2.3 SSE—CMM的体系结构
 - 2.3.1 基本模型
 - 2.3.2 域维, 安全过程区
 - 2.3.3 能力维, 公共特性
 - 2.3.4 能力级别
 - 2.3.5 体系结构的组成
 - 2.4 SSE—CMM应用
 - 2.4.1 SSE—CMM应用方式
 - 2.4.2 用SSB—CMM改进过程
 - 2.4.3 使用SSE—CMM的一般步骤
 - 2.5 系统安全工程能力评估
 - 2.5.1 系统安全工程能力评估
 - 2.5.2 SSE—CMM实施中的几个问题
- 本章小结

习题二

第三章 信息安全工程实施

- 3.1 概述
- 3.2 安全规划与控制
 - 3.2.1 商业决策和工程规划
 - 3.2.2 信息安全工程小组

<<信息安全工程>>

- 3.2.3 对认证和认可(C&A)的信息安全工程输入规划
- 3.2.4 信息安全工程报告
- 3.2.5 技术数据库和工具
- 3.2.6 与获取/签约有关的规划
- 3.2.7 信息系统安全保证规划
- 3.3 安全需求的定义
 - 3.3.1 系统需求定义概述
 - 3.3.2 安全需求分析的一般课题
 - 3.3.3 安全需求定义概述
 - 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
 - 3.3.5 需求阶段——信息安全工程的需求活动
 - 3.3.6 系统设计阶段——信息安全工程的需求活动
 - 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
- 3.4 安全设计支持
 - 3.4.1 系统设计
 - 3.4.2 信息安全工程系统设计支持活动
 - 3.4.3 先期概念和概念阶段安全设计支持
 - 3.4.4 需求和系统设计阶段的安全设计支持
 - 3.4.5 初步设计阶段到配置审计阶段的安全设计支持
 - 3.4.6 运行和支持阶段的安全设计支持
- 3.5 安全运行分析
- 3.6 生命周期安全支持
 - 3.6.1 安全的生命期支持的开发方法
 - 3.6.2 对部署的系统进行安全监控
 - 3.6.3 系统安全评估
 - 3.6.4 配置管理
 - 3.6.5 培训
 - 3.6.6 后勤和维护
 - 3.6.7 系统的修改
 - 3.6.8 报废处置
- 3.7 信息安全工程的过程

本章小结

习题三

第四章 信息安全风险评估

- 4.1 信息安全风险评估基础
 - 4.1.1 与风险评估相关的概念
 - 4.1.2 风险评估的基本特点
 - 4.1.3 风险评估的内涵
 - 4.1.4 风险评估的两种方式
- 4.2 风险评估的过程
 - 4.2.1 风险评估基本步骤
 - 4.2.2 风险评估准备
 - 4.2.3 风险因素评估
 - 4.2.4 风险确定
 - 4.2.5 风险评价
 - 4.2.6 风险控制
- 4.3 风险评估过程中应注意的问题

<<信息安全工程>>

- 4.3.1 信息资产的赋值
- 4.3.2 评估过程的文档化
- 4.4 风险评估方法
 - 4.4.1 正确选择风险评估方法
 - 4.4.2 定性风险评估和定量风险评估
 - 4.4.3 结构风险因素和过程风险因素
 - 4.4.4 通用风险评估方法
- 4.5 几种典型的信息安全风险评估方法
 - 4.5.1 OCTAVE法
 - 4.5.2 层次分析法(AHP法)
 - 4.5.3 威胁分级法
 - 4.5.4 风险综合评价
- 4.6 风险评估实施
 - 4.6.1 风险评估实施原则
 - 4.6.2 风险评估流程
 - 4.6.3 评估方案定制
 - 4.6.4 项目质量控制
- 本章小结
- 习题四

第五章 信息安全策略

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

<<信息安全工程>>

第六章 信息安全工程与等级保护

6.1 等级保护概述

6.1.1 信息安全等级保护制度的原则

6.1.2 信息安全等级的划分及特征

6.2 等级保护在信息安全工程中的实施

6.2.1 新建系统的安全等级保护规划与建设

6.2.2 系统改建实施方案设计

6.3 等级保护标准的确定

6.3.1 确定信息系统安全保护等级的一般流程

6.3.2 信息系统安全等级的定级方法

本章小结

习题六

第七章 数据备份与灾难恢复

7.1 数据备份的概念

7.2 数据备份的常用方法

7.2.1 数据备份层次

7.2.2 数据备份常用方法分类

7.3 灾难恢复概念

7.4 安全恢复的计划

7.4.1 容灾系统

7.4.2 安全恢复的实现计划

7.4.3 安全恢复计划

7.5 灾难恢复技术

7.5.1 灾难预防制度

7.5.2 数据库的恢复技术

本章小结

习题七

第八章 信息安全工程案例

8.1 涉密网安全建设规划设计

8.1.1 安全风险分析

8.1.2 规划设计

8.2 信息系统网络安全工程实施

8.2.1 制定项目计划

8.2.2 项目组织机构

8.2.3 工程具体实施

8.3 政府网络安全解决方案

8.3.1 概述

8.3.2 网络系统分析

8.3.3 网络安全风险分析

8.3.4 网络安全需求及安全目标

8.3.5 网络安全方案总体设计

8.3.6 网络安全体系结构

习题八

第九章 信息安全组织

9.1 IETF(www.ietf.org)

9.2 CERT/CC(www.cert.org)

9.3 NSA(www.a.gov)和NIST(www.nist.gov)

<<信息安全工程>>

9.4 ISO

9.5 ITU

参考文献

<<信息安全工程>>

编辑推荐

《信息安全工程》由武汉大学出版社出版。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>