

<<金融信息安全>>

图书基本信息

书名：<<金融信息安全>>

13位ISBN编号：9787302307815

10位ISBN编号：7302307814

出版时间：2013-1

出版时间：清华大学出版社

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>

内容概要

《服务外包工程教育规划教材:金融信息安全》围绕金融信息化发展与金融服务创新过程中引起社会公众广泛关注的金融信息安全主题展开。

第1章介绍金融信息化的内容、特点,分析其必然性和重要性及其系统的基本构成;第2章介绍金融信息化与服务外包中金融信息面临的安全问题及金融信息安全的重要性与复杂性;第3章涵盖金融信息安全体系,包括信息安全体系的基本结构、信息安全体系的组成、信息安全防御模型以及信息安全风险分析与评估;第4章重点介绍主要信息安全技术,包括物理层安全技术、网络层安全技术、系统层安全技术、应用层安全技术、数据安全技术与内容安全技术;第5章涵盖信息安全管理体制、信息安全规划、信息安全风险评估技术、信息安全策略的制订、信息安全管理标准、信息安全的法律法规与道德规范等;第6章分析金融服务外包所面临的各种新的金融信息安全问题以及对这些新金融信息安全问题的应对措施。

书中包含大量金融信息安全的案例,每章后附有适量的练习与思考,供读者学习与复习。

书籍目录

第1章金融信息化概述 1.1金融信息化概述 1.1.1金融信息化的基本概念 1.1.2金融信息化电子化的内容 1.1.3金融信息化的特点 1.2金融信息化的意义 1.2.1金融信息化的必然性 1.2.2金融信息化的意义 1.2.3金融信息化的影响 1.3 国内外金融信息化的发展与现状 1.3.1国外金融信息化发展概况 1.3.2中国金融业信息化的发展过程与现状 1.3.3我国金融信息化面临的问题 1.4金融信息系统的组成 1.4.1金融信息系统的空间结构 1.4.2金融信息系统的逻辑结构 1.4.3银行事务处理系统的结构 1.4.4金融事务系统中的交易 练习与思考 第2章金融信息安全 2.1金融信息安全的基本概念 2.1.1信息安全的概念 2.1.2信息安全的发展过程 2.1.3金融信息安全的目标 2.2金融信息安全面临的风险 2.2.1金融信息安全的几个概念 2.2.2金融信息系统可能面临的安全威胁 2.2.3电脑病毒 2.2.4金融信息系统信息安全风险产生的原因 2.2.5金融信息安全的主要风险点 2.2.6金融交易中的风险点 2.3金融信息安全的重要性 2.4金融信息安全的复杂性 2.4.1金融信息系统本身的复杂性 2.4.2金融信息系统安全风险的科技特性 2.4.3计算机金融犯罪的特性 2.4.4金融信息安全的特性 练习与思考 第3章信息安全体系 3.1金融信息安全体系概述 3.1.1面向目标的知识体系结构 3.1.2面向应用的层次型技术体系结构 3.1.3面向过程的信息安全保障体系结构 3.2信息安全体系框架 3.2.1技术体系 3.2.2组织体系 3.2.3管理体系 3.3信息安全防御模型 3.4信息安全风险分析 练习与思考 第4章信息安全技术 4.1物理层安全技术 4.1.1物理访问控制 4.1.2防灾 4.1.3防信息泄露 4.1.4容错容灾 4.2网络层安全技术 4.2.1防火墙技术 4.2.2虚拟专用网 (VPN) 技术 4.2.3新一代安全网关 4.3系统层安全技术 4.3.1安全扫描技术 4.3.2入侵检测技术 4.3.3防病毒技术 4.4应用层安全技术 4.4.1身份认证技术 4.4.2访问控制技术 4.4.3安全审计技术 4.5数据安全技术 4.5.1数据加密技术 4.5.2数字签名技术 4.5.3数据备份与恢复技术 4.6内容安全技术 4.6.1内容安全概述 4.6.2内容安全监测技术 4.6.3反垃圾邮件技术 4.6.4数字水印技术 练习与思考 第5章信息安全管理 5.1信息安全管理概述 5.1.1信息安全的概念 5.1.2信息安全管理的重要性 5.1.3信息安全管理的内容与要素 5.1.4信息安全管理的原则 5.1.5信息安全管理体系 5.2信息安全规划 5.2.1信息安全规划的设计原则 5.2.2安全规划基本构成 5.2.3信息安全规划内容 5.2.4金融机构信息安全管理实施内容 5.3信息安全风险评估 5.3.1信息安全风险评估的概念 5.3.2信息安全风险评估的目的和意义 5.3.3信息安全风险模型 5.3.4信息安全风险评估方法 5.3.5风险评估工具 5.4信息安全策略 5.4.1信息安全策略基本概念 5.4.2制定信息安全策略的原则与要求 5.4.3信息安全策略的制订过程 5.4.4安全策略的评价准则 5.4.5信息安全策略框架 5.5信息安全管理标准 5.5.1信息安全标准概述 5.5.2信息安全管理体系标准 5.5.3信息安全评估标准 5.5.4我国的信息安全管理标准与GB17859—1999 5.5.5 ISO / TC68与银行业务有关的信息安全标准 5.6信息安全法律法规与道德规范 5.6.1 国际的信息安全法律法规 5.6.2 中国的信息安全法律法规 5.6.3信息安全道德规范 5.7我国金融信息安全管理对策 练习与思考 第6章金融服务外包中的信息安全 6.1金融服务外包信息安全的重要性 6.1.1金融服务外包潜在的信息安全风险 6.1.2金融服务外包信息安全事故的影响 6.2金融服务外包影响信息安全的因素 6.3金融服务外包中产生信息安全风险的根源 6.4金融服务外包安全风险的内部管理与控制 6.4.1 发包金融企业对外包业务安全的控制与管理 6.4.2接包商对外包项目安全的管理和控制 6.5对金融服务外包的安全监管 6.5.1金融监管概述 6.5.2相关国家与国际组织对金融服务外包的监管 6.5.3 中国对金融服务外包的监管 6.5.4中国对金融服务外包监管的分析 练习与思考 附录A我国已发布的相关信息安全标准 (至2010年) 附录B我国已颁布的信息安全管理体系标准 附录C与银行业务有关的国际信息安全标准 附录D我国涉及信息安全方面条款的法律法规

.....

章节摘录

版权页：插图：2.信息安全阶段 20世纪80年代至90年代初期，计算机网络逐步产生并发展起来，计算机系统成为信息安全的主要保护对象。

计算机系统是由计算机及其相关的配套设备、设施构成的，按照一定的应用目标和规格，对信息进行采集、加工、存储、传输和检索等处理的系统。

在这一时期，人们认识到，除了信息保密的需要之外，信息在存储、处理和传输的过程中不应被未经授权者进行插入、删除和修改（完整性要求），以及在需要使用的地点可以保证提供使用（可用性要求），也是信息安全的重要、基本需求。

“完整性”和“可用性”需求是保密性之外的两个基本的信息安全属性。

安全重点是确保计算机系统硬件、软件及正在处理、存储、传输信息的机密性、完整性和可控性，主要安全威胁扩展到非法访问、恶意代码、脆弱口令等。

主要保护措施是安全操作系统设计技术（TCB）。

主要标志是1983年美国国防部公布的可信计算机系统评估准则（TCSEC），将操作系统的安全级别分为4类7个级别（D、C1、C2、B1、B2、B3、A1），后补充TN1和TD1。

1991年，欧共体发布了“信息技术安全评价准则”（Information Technology Security Evaluation Criteria，ITSEC）。

ITSEC扩展了人们对信息安全的认识，最早提出了CIA的概念（Confidential机密性、Integrity完整性、Availability可用性），形成了信息安全属性的基本共识。

在这一时期，公开密钥密码技术得到了长足发展，著名的RSA公开密钥密码算法获得了日益广泛的应用。

对用于完整性校验的Hash函数的研究也日趋成熟。

1991年，NIST提出了采用数字签名算法（DSA）的数字签名标准（DSS），为实现对信息完整性的保护奠定了基础。

3.信息保障阶段 20世纪90年代以来，由于互联网技术的飞速发展，无论是对内还是对外，信息都得到极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性3个原则了，由此衍生出了诸如可控性、抗抵赖性、真实性等其他原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障，重点保护信息存储、处理、传输过程中及信息系统不被破坏，确保合法用户的服务和限制非授权用户的服务，以及必要的防御攻击的措施。

除了强调信息的保密性、可用性和完整性，还提出了新的安全属性，如可认证性（Authenticity）、不可抵赖性（Non—repudiation）和可核查性（Accountability）等。

主要安全威胁发展到网络入侵、病毒破坏、信息对抗的攻击等。

主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、PKI、VPN等。

主要标志是提出了新的信息安全评估标准CC（ISO15408）、IPv6等安全性设计。

编辑推荐

《服务外包工程教育规划教材:金融信息安全》由清华大学出版社出版。

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>