

<<信息安全管理平台理论与实践>>

图书基本信息

书名：<<信息安全管理平台理论与实践>>

13位ISBN编号：9787121043130

10位ISBN编号：7121043130

出版时间：2007-5

出版时间：第1版(2007年5月1日)

作者：王代潮

页数：362

字数：598000

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>

<<信息安全管理平台理论与实践>>

前言

前言 随着信息化的飞速发展,信息安全技术和管理都受到了广泛的关注。信息安全管理体系和标准特别强调,信息安全不仅强调技术,还应重视管理,要做到二者有机结合。如何体系化、流程化、平台化地进行信息安全平台的建设,是当前业界不断讨论和完善的重要话题之一。

信息安全平台涵盖了广泛的信息安全技术和理念。机构资产的梳理、防火墙的配置、入侵检测系统的事件分析甚至整个信息系统的脆弱性和威胁分析等等,单一的因素都不能构成完整的信息安全。机构的信息安全不仅仅要求技术人员对于细节的关注,更需要管理者宏观地对整体的安全现状和态势进行了解和把握,果断有效地传达旨意采取措施。所以信息安全平台建设的重要价值就是通过技术的实现手段加强对安全管理的关注。

本书将通过信息安全平台建设理论与实践的方方面面,阐述信息安全的理论基础和设计思路,并从实际应用出发探讨如何切实地落实信息安全工作。

本书将以信息安全平台的建设理论和实践为引线,分为三大部分:理论篇、设计篇和应用篇。

第一部分阐述了信息安全的理论基础。

此部分涉及广泛的安全概念和技术知识,从信息安全的发展和未来趋势谈起,涉及诸多的安全技术,如防火墙、入侵检测、防病毒等等;并涵盖目前流行的安全理论基础,如可信计算理论、信息安全服务模型、风险管理等等;并且涉及国际国内的信息安全现状和趋势,所遵从的信息安全相关标准和规范体系,如ISO/IEC 15408 (Common Criteria)、FIPS 140-2、ISO/IEC 27001 (原BS7799)的安全要求,以及国内的标准现状、等级保护要求等。

第二部分从设计的角度出发,阐述了平台建设的设计理念。

首先从平台的基础体系入手,介绍体系架构和开发环境;然后探讨平台涉及的接口协议和格式,中间件概念及设计思路;安全域的网络设计和平台的结合;随后探讨平台的保障功能设计,如身份认证;并着重以模块的形式探讨信息安全平台的设计思路和技术细节,并提出相关的增强辅助模块设计,如自身安全考虑等。

第三部分阐述了信息安全平台建设的实践和应用。

首先给出某机构实现信息安全管理平台的实例描述;之后从目前应用面最广泛的微软产品线入手,介绍信息安全建设的应用模型和实例;从行业发展来看,政府、电力、通信、军工军队、金融,各个领域对于信息安全的要求不断增加,具有其共同点又存在差异。

金融机构从网络基础建设、数据大集中以来,安全建设将是重中之重。

中国的信息安全起步和发展都处于世界前列,特别是在金融领域,2000年以来信息安全的技术和管理层面都已经做了大量的工作。

本部分将对各行业的信息安全态势进行分析和介绍,并着重于金融行业信息安全,分析其如何为金融客户提供高可靠、高质量的服务,使得金融机构稳步健康地发展。

最后在本部分中,针对平台相关的标准应用进行分析和介绍,如等级保护的实践。

本书将以信息安全平台建设为出发点,谈及了如何切实地落实信息安全工作,特别是从安全管理理念考虑。

平台的建设是整个信息安全管理体系 (ISMS) PDCA过程的重要的工作,各机构在信息安全建设中,应配合其实施和应用,加强安全策略的制定、资产的梳理、风险评估工作、安全域的划分、安全意识和培训、建立应急响应等等安全工作,从而将安全管理与技术手段有效地结合。

在本书的编写过程中,我们获得了业界专家和同仁的巨大帮助。

在此我们特别感谢潘柱廷、肖立昕、赵呈东、徐刚、吴茂标、任平为本书提供宝贵的思路和参考资料;感谢郭斌、马丹、杨帆在编写过程中的帮助;感谢白海蔚、刘辉对本书进行审核;感谢所有为本书的出版做出贡献的人。

本书内容深入浅出,涵盖信息安全建设的各个方面,特别是从管理的角度探讨信息安全并致力于技术实现。

<<信息安全管理平台理论与实践>>

本书适用于广泛的读者群体，包括但不限于各行业机构的IT管理者、机构高层决策者、信息安全专家、研究学者、产品开发者等。

我们希望和各方面的信息安全参与者共同研究，提高整体信息安全的管理和技术水平。

作者 2007年3月

<<信息安全管理平台理论与实践>>

内容概要

本书遵循由一般到具体、由理论到实践的原则阐述了当前国内外信息安全领域的相关话题，探讨了信息安全平台建设的理论基础和设计思路，并从实际应用出发探讨如何切实地落实信息安全工作。本书有助于组织构建以风险管理为核心的保障体系，构建符合ISO/IEC 15408 标准的系统，实现ISO/IEC 27001信息安全管理体系统要求的控制措施，贯彻ISSE和IATF纵深防御的信息安全设计思路，从而能够实际强化信息安全意识，提高安全防护水平。

<<信息安全管理平台理论与实践>>

书籍目录

上篇(理论篇)	第1章 信息安全概述	1.1 信息安全的内涵	1.2 信息安全发展历程	1.2.1
发展的3个阶段	1.2.2 主流技术发展	1.2.3 发展历程小结	1.3 信息安全的发展趋势	
	1.3.1 发展的五大趋势	1.3.2 信息安全管理越来越重要	1.3.3 平台化整合成为必然	1.4
小结	第2章 信息安全管理	2.1 信息安全管理理论	2.1.1 PDCA循环	2.1.2 WPDRR模型
	2.1.3 信息安全保障体系构架	2.1.4 三观安全体系	2.2 信息安全管理标准	2.2.1 IT
治理标准	2.2.2 信息安全评估标准	2.2.3 信息安全风险管理标准	2.2.4 我国信息安全	
管理标准	2.3 ISO/IEC 27001标准	2.3.1 标准的发展历程	2.3.2 标准主导思路	2.3.3
与其他质量管理体系的相关性	2.3.4 与风险管理的相关性	2.3.5 标准的主要内容		
2.3.6 简单评价	2.4 共同准则(CC)	2.4.1 评估准则	2.4.2 标准的历史和未来	
2.4.3 早先的评估标准	2.4.4 标准的组成	2.4.5 评估方法论CEM	2.5 小结	第3章 信
息安全管理平台	3.1 信息安全管理平台概述	3.1.1 平台的需求	3.1.2 信息安全管理平台	
的内涵	3.1.3 平台的原则	3.2 平台体系结构	3.2.1 代表性平台体系结构	3.2.2 基于
三观论思想的平台总体框架	3.2.3 主要功能	3.2.4 辅助功能	3.2.5 与其他平台集成	
3.3 平台关键技术	3.3.1 联动互操作技术	3.3.2 安全代理——数据采集标准化	3.3.3	
可视化技术	3.3.4 基础性支撑协议/技术	3.4 小结	第4章 可信计算与安全平台	4.1 可信
计算概述	4.1.1 TCG的可信计算理论	4.1.2 微软的值得信赖系统	4.2 可信计算基本理论	
	4.2.1 TPM	4.2.2 体系框架	4.3 可信网络连接TNC	4.3.1 TNC概述
TNC构架	4.4 可信计算应用	4.4.1 信息加密保护	4.4.2 操作系统安全	4.4.3 网络
保护	4.5 基于可信计算的安全平台	4.6 小结	第5章 风险管理与安全平台	5.1 风险管理概
述	5.2 一般风险管理模型	5.2.1 ISO13335风险管理模型	5.2.2 AS/NZS4360风险管理模型	
	5.2.3 微软风险管理流程	5.3 风险评估	5.3.1 风险评估与风险管理的关系	5.3.2 风
险评估模型	5.3.3 风险评估过程	5.3.4 风险评估方法	5.3.5 评估工具	5.4 风险管理
理论与安全平台建设	5.5 小结中篇(设计篇)	第6章 平台基础体系设计	6.1 软件体系结构	
	6.1.1 历史和发展	6.1.2 常用体系风格	6.2 基于SOA的体系结构	6.2.1 基本概念
	6.2.2 应用系统框架	6.2.3 结构框架	6.2.4 设计原则	6.3 J2EE体系结构
件——容器	6.3.2 EJB	6.3.3 平台标准服务	6.3.4 多层应用模型	6.3.5 基于J2EE
的平台架构	6.4 .NET体系结构	6.4.1 框架内核	6.4.2 CLR	6.4.3 类库
基于.NET的平台架构	6.5 小结	第7章 平台接口和中间件	7.1 接口设计	7.1.1 简单网络
管理协议	7.1.2 Syslog功能	7.1.3 格式对比	7.1.4 数据标准的分类	7.2 中间件
	7.2.1 概念和分类	7.2.2 主要的中间件类型	7.2.3 面临的一些问题	7.2.4 开发方法
7.3 小结	第8章 安全域网络设计	8.1 安全域简介	8.1.1 基本概念	8.1.2 安全域的作
用	8.1.3 安全域的特性	8.1.4 安全域依存关系	8.1.5 安全域的防护	8.2 安全域设计
思想	8.2.1 划分方法	8.2.2 IATF安全域划分	8.2.3 同构划分	8.2.4 划分步骤
8.3 安全域设计实例	8.3.1 某金融组织案例分析	8.3.2 某电信组织案例分析	8.4 安全	
域与平台的相辅相成	8.4.1 安全域划分的意义	8.4.2 结合的建设成效	8.5 小结	第9章
保障功能设计	9.1 认证体系设计	9.1.1 统一身份认证	9.1.2 密钥管理系统	9.1.3
CA和PKI体系	9.2 平台认证思路	9.2.1 证书的应用	9.2.2 系统平台建设	9.3 安全监
控	9.3.1 原理和要素	9.3.2 体系结构	9.4 可信接入设计	9.4.1 从TNC到可信接入
9.4.2 Cisco自				
防御网络	9.5 小结	第10章 平台模块设计	10.1 远程安全信息采集	10.1.1 概述
	10.1.2 总体设计思路	10.1.3 功能需求	10.1.4 非功能性需求	10.2 综合安全监测
	10.2.1 概述	10.2.2 总体设计思路	10.2.3 功能需求	10.3 安全风险分析
述	10.3.2 总体设计思路	10.3.3 功能需求	10.3.4 非功能性需求	10.4 应急响应支持
	10.4.1 一般处理流程	10.4.2 总体设计思路	10.5 远程安全管理	10.5.1 概述
10.5.2 总体设计思路	10.5.3 功能需求	10.5.4 非功能性需求	10.6 用户终端	10.6.1 概
述	10.6.2 总体设计思路	10.6.3 功能需求	10.6.4 非功能性需求	10.7 互联网安全诱捕

<<信息安全管理平台理论与实践>>

10.7.1 概述	10.7.2 总体设计思路	10.7.3 功能需求	10.7.4 非功能性需求	10.8 平
台的多级架构互连	10.9 小结	第11章 增强功能设计	11.1 平台报表管理	11.1.1 概述
11.1.2 报表管理设计	11.1.3 功能需求	11.1.4 非功能性需求	11.2 平台系统配置	
11.2.1 概述	11.2.2 系统配置设计方案	11.2.3 系统功能设计	11.2.4 非功能性需求	
11.3 平台系统安全	11.3.1 系统安全概述	11.3.2 系统安全总体设计	11.3.3 日志和审	
计	11.3.4 用户安全	11.3.5 系统升级管理	11.3.6 系统数据安全	11.3.7 非功能性
需求	11.4 合规性管理	11.4.1 概述	11.4.2 指标体系	11.4.3 典型合规实例
11.5 小结下篇(应用篇)	第12章 平台实现实例	12.1 体系架构	12.1.1 环境与开发语言	
12.1.2 平台结构	12.2 实例总体设计分析	12.2.1 信息资产等级保护	12.2.2 安全事件	
管理	12.2.3 网络行为审计	12.2.4 脆弱性扫描和评估	12.2.5 风险管理	12.2.6 响
应管理	12.2.7 知识管理	12.2.8 综合显示	12.2.9 用户管理	12.3 平台用户管理的使
用	12.3.1 用户登录	12.3.2 用户组管理	12.3.3 用户管理	12.3.4 审计查看
12.4 小结	第13章 微软系统的平台应用	13.1 体系架构	13.2 操作系统	13.3 平台中基于
微软产品的应用	13.3.1 邮件系统	13.3.2 数据库系统	13.3.3 补丁管理	13.4 监控管
理系统	13.5 小结	第14章 行业安全实践	14.1 金融行业安全实践	14.1.1 概述
体系建设思路	14.1.3 技术体系建设	14.1.4 网上银行安全思路	14.1.5 构建信息安全管理	14.1.2
管理平台	14.2 电力行业安全实践	14.2.1 总体建设思路	14.2.2 安全技术要求	14.2.3
安全管理层面	14.3 电信行业安全实践	14.3.1 数据网	14.3.2 办公系统	14.4 政府组
织安全实践	14.4.1 需求分析	14.4.2 现状和威胁分析	14.4.3 建设思路	14.5 军队军
工领域实践	14.5.1 背景	14.5.2 规划原则	14.5.3 需求分析	14.5.4 解决方案
14.5.5 建设步骤规划	14.6 教育行业安全实践	14.6.1 需求分析	14.6.2 总体设计思路	
14.7 小结	第15章 基于标准的应用	15.1 等级保护的思路	15.1.1 背景介绍	15.1.2 概
念	15.1.3 安全等级的划分	15.1.4 等级的保护能力	15.2 准备计划	15.2.1 系统识别
和描述	15.2.2 业务子系统划分	15.2.3 信息系统划分	15.2.4 安全等级确定	15.3 规
划设计	15.3.1 安全需求分析	15.3.2 总体设计	15.4 实施建设	15.4.1 详细设计
15.4.2 管理实施	15.4.3 技术实施	15.5 运行维护	15.6 小结结束语主要参考文献	

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>