<<信息安全体系结构>>

图书基本信息

书名：<<信息安全体系结构>>

13位ISBN编号：9787302170723

10位ISBN编号：730217072X

出版时间：2008-9

出版时间：清华大学出版社

作者：冯登国　等编著

页数：220

字数：304000

前言

21世纪，人类社会已进入信息时代。
信息时代的重要特征是信息的获取、传输、处理等的高速发展。
伴随信息化的发展，信息安全作用更加突出，成为全球关注的热点问题，为培养高层次信息安全人才，我国的一些高等院校设置了信息安全专业，并出版了或准备出版一系列信息安全教材。
冯登国教授等编著的《信息安全体系结构》是高等院校信息安全专业规划教材之一。
这是一本具有系统性、先行性和实用性等鲜明特点的教材。

（1）系统性。

信息安全的发展，人们已认识到它不仅是安全技术和产品的问题，而是一个涉及信息安全策略、整体架构、完整流程以及涵盖技术、产品、人员、过程、管理等诸多因素的复杂系统。
本书从信息安全整体性出发，系统论述了信息安全的体系结构规划和设计，技术支撑、产品、标准、管理、人员等各个方面以及它们之间的关联，使读者能从更高的层析上去领会信息安全问题。

<<信息安全体系结构>>

内容概要

本书对信息安全涉及的各个层面进行了梳理和论证，并讨论了与安全技术和产品相关的内容，充分反映了信息安全领域的最新研究进展和发展趋势。
本书主要从信息安全体系结构规划与设计、信息安全技术支撑、信息安全产品、信息安全标准、信息安全管理、人员能力成熟度模型以及信息安全应用案例等方面系统地论述了如何解决信息技术应用所带来的信息安全问题。
本书也对信息安全体系结构的概念进行了详细分析和论述，并对构建信息安全体系结构的关键三要素（人、技术和管理）之间的关系进行了详细阐述。
本书的特点是系统性强、内容覆盖面广、体系化程度高。

本书可作为计算机、通信、信息安全、密码学等专业的本科生和研究生的教材，也可供从事相关专业的教学、科研和工程技术人员参考。

<<信息安全体系结构>>

作者简介

冯登国，中国科学院软件所研究员，博士生导师，教育部高等学校信息安全类专业教学指导委员会副主任委员，国家信息化专家咨询委员会专家，国家863计划信息安全技术主题专家组组长、信息安全国家重点实验室主任，国家计算机网络入侵防范中心主任。

<<信息安全体系结构>>

书籍目录

第1章 概述
1.1 基本概念
1.1.1 体系结构
1.1.2 信息安全体系结构
1.1.3 信息安全保障
1.2 三要素
1.2.1 人
1.2.2 技术
1.2.3 管理
1.2.4 三者的相互关系
1.3 小结
习题
第2章 信息安全体系结构规划与设计
2.1 网络与信息系统总体结构初步分析
2.2 信息安全需求分析
2.2.1 物理安全
2.2.2 系统安全
2.2.3 网络安全
2.2.4 数据安全
2.2.5 应用安全
2.2.6 安全管理
2.3 信息安全体系结构的设计目标、指导思想与设计原则
2.3.1 设计目标
2.3.2 指导思想
2.3.3 设计原则
2.4 安全策略的制定与实施
2.4.1 安全策略
2.4.2 制定依据
2.4.3 安全策略分类
2.5 小结
习题
第3章 信息安全技术支撑
3.1 密码服务技术
3.1.1 作用
3.1.2 要求
3.1.3 组成
3.1.4 密码的使用
3.1.5 密钥的配用与管理
3.1.6 密码服务系统接口
3.2 密钥管理技术
3.2.1 作用
3.2.2 体系结构
3.3 认证技术
3.3.1 作用
3.3.2 基本模型

3.3.3 交叉认证与桥CA
3.3.4 体系结构
3.3.5 主要组件的功能要求
3.3.6 其他认证技术
3.4 授权技术
3.4.1 作用
3.4.2 基本结构和应用模型
3.4.3 体系结构与主要功能
3.4.4 性能指标
3.5 容灾备份与故障恢复技术
3.5.1 作用
……
第4章 主要信息安全产品
第5章 信息安全标准
第6章 信息安全管理
第7章 人员能力成熟度模型
第8章 案例研究
附录A 图表目录
附录B 缩略语
参考文献

章节摘录

版权页： 插图： （2）无论知识顾问位于建筑物的任何位置，需要其帮助的员工都可与之保持联系。
通过电子邮件、电子日历和网络聊天，员工无论在开会还是离开办公室，都可保持联机状态。
（3）联机信息随时可用。
如果会议中有人急需检索上个月的图形报告或更新演示文稿，无需中断会议。
这将极大提高会议的质量和效率。
（4）提高了组织的灵活性。
随着团队和项目结构的更改，快速、轻松地移动办公桌，甚至移动整个办公室都会成为可能，员工不会再受到办公位置的束缚。
WLAN技术的主要运营优势是具有较低的资金和运营成本，这可以具体归纳为三点：（1）建筑物联网的成本大幅度降低。
尽管多数办公室空间都铺设了网络电缆，但仍有许多其他工作场所（例如，工厂、仓库和商店）尚未铺设。
无线网络还可以在无法建立有线网络的位置（例如，户外、海上甚至战场）提供。
（2）可以根据组织需求来调整网络（如果需要，甚至可以每天调整），使之满足不同层次的需求；在给定位置部署高度集中的无线接入点（AP）要比增加有线网络的端口数容易得多。
（3）构建基础结构再也不需要考虑资金，可以轻松地将无线网络基础结构移动到新的建筑物，而有线网络永远是固定的。
虽然WLAN具有上述优势，但与其相关的许多安全问题还是限制了这项技术的使用。
金融和政府等比较关注WLAN安全的行业部门，尤其担心通过WLAN将没有得到足够保护的数据传播给周围地区的人，非常危险。
目前，大多数业务已经实施了某种形式的无线安全性，但这种安全性通常只是采用了最为基本的第一代无线安全功能。
而按照现今的需求标准来考虑，它所提供的保护措施是远远不够的。
一般地，WLAN应用主要存在以下几种不安全因素：（1）窃听（数据泄漏）。
窃听网络传输数据可导致机密数据泄漏、未保护的用户凭据泄漏，以及身份被盗用。
还使得有经验的入侵者能够收集用户的IT环境相关信息，然后利用这些信息攻击其他情况下不易遭到攻击的系统或数据。
（2）截获和修改传输数据。
如果攻击者可以访问网络，他（或她）便可插入恶意计算机来截获和修改两个合法方之间交换的网络数据。
（3）哄骗。
如果可以访问内部网络，入侵者便可以采用一些在网络外部无效地方法伪造表面上合法的数据，例如，一封哄骗性的电子邮件。
相比之下，员工（包括系统管理员）通常更容易相信来自企业网络内部的信息，而不是来自网络外的信息。

编辑推荐

<<信息安全体系结构>>

版权说明