第一图书网, tushu007.com

<<电子商务安全>>

图书基本信息

书名：<<电子商务安全>>

13位ISBN编号：9787111269809

10位ISBN编号：7111269802

出版时间：2009-7

出版时间：机械工业出版社

作者：王忠诚 主编

页数：251

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

前言

本书是普通高等教育“十一五”国家级规划教材。
本书第1版出版以来，受到了多家高职高专院校电子商务专业及相关专业师生的广泛好评，得到了社会其他人士的认可和肯定。
在广泛吸纳各方建议的基础上，在保留第1版主体框架和基本特色的前提下，突出对基本技能的掌握和技术应用能力的培养，吸收电子商务理论及实践领域的最新研究成果，对全书的内容进行了修订。
与第1版相比，本书的主要特色表现在以下几个方面：1.整合内容体系第2版的内容体系主要从电子商务安全基础、电子商务安全问题、电子商务安全技术以及电子商务安全实际应用四个方面进行章的划分。
这种划分使电子商务安全的层次更加分明，这种结构安排能够更加体现电子商务安全的全貌，让学生在学习的同时体会电子商务各知识点之间的关系，增加学习的灵活性。
2.增加全新案例第2版中保留第1版中的精华内容，加大了对电子商务安全技术和方法的研究，尤其是加入了最新的案例，让学生在解决案例的过程中完成相关课程内容的学习和操作。
3.加大实践操作在第2版编写中仍旧坚持电子商务安全的实践应用环节。
对原有的过时的实践操作内容进行了更新和更换，尤其在原有的实践基础上，根据企业应用现状增加了一些新的实践内容。
4.对全书重点内容进行摘要式介绍为了方便学习，在第2版中还增加了摘要式的全书重点内容总结，系统讲解了电子商务安全中的重要问题，既起到引导学生学习电子商务安全的导航作用，又能够作为教师讲授该门课程的教学大纲。
全书共分8章，分别介绍了电子商务安全概述、电子商务安全面临的问题及解决方法、电子商务安全技术、电子商务的认证与安全电子邮件技术、电子商务安全支付技术、安全电子交易（SET）协议、安全套接（SsL）协议、安全电子商务应用等。
由于是面向高职高专学生的教材，所以，本书在理论上以够用为度，结合案例，深入浅出，实用性强，突出对基本理论、基本技能的掌握和技术应用能力的培养，使学生尽快掌握电子商务安全知识及其应用技术。
本书力求内容丰富、形式简练，既考虑学生的自我学习，也考虑给教师留下一定的教学空间。
本书既可作为高职高专院校的教材，也可作为各界人士的学习用书及专业培训用书。

第一图书网, tushu007.com

内容概要

本书主要围绕保障电子商务活动的安全性，针对电子商务应用的基本安全问题及解决方案进行了详细介绍与阐述。
全书共分8章，分别介绍了电子商务安全概述、电子商务安全面临的问题及解决方法、电子商务安全技术、电子商务的认证与安全电子邮件技术、电子商务安全支付技术、安全电子交易（SET）协议、安全套接层（SSL）协议、安全电子商务应用等内容，并根据每章的具体内容安排了相应的习题和实践实训环节。
　本书内容新颖，结构合理，案例生动，论述深入浅出，实用性强，突出对基本理论、基本技能的掌握和技术应用能力的培养。
本书可作为高职高专电子商务、市场营销、计算机应用、计算机信息管理、工商管理和经济贸易等专业的教材，也可作为有关电子商务的培训用书以及企业管理人员参考用书。
　本书配有电子教案及习题参考答案，凡使用本书作为教材的教师可登录机械工业出版社教材服务网www.cmpedu.corn下载。
咨询邮箱：cmpgaozhi@sina.corn。
咨询电话：010-88379375。

书籍目录

第2版前言第1版前言第1章　电子商务安全概述 1.1　电子商务及其系统构成　1.1.1　电子商务的定义、内涵及特征　1.1.2　电子商务系统构成 1.2　电子商务安全概况　1.2.1　电子商务安全概念与特点　1.2.2　电子商务的风险与安全问题　1.2.3　电子商务系统安全的构成 1.3　电子商务安全的保障　1.3.1　电子商务安全技术　1.3.2　电子商务安全国际规范　1.3.3　电子商务安全法律要素　实践项目　练习与实训题　案例分析第2章　电子商务安全面临的主要问题及解决方法 2.1　电子商务安全面临的主要问题　2.1.1　网络信息安全目标　2.1.2　网络信息系统中的威胁与对策　2.1.3　网络信息安全管理原则 2.2　电子商务安全整体解决方法　2.2.1　电子商务安全体系概述　2.2.2　电子商务安全解决方法 实践项目 练习与实训题 案例分析第3章　电子商务安全技术　3.1　数据加密技术概述　3.1.1　密码学的基本概念　3.1.2　网络加密方式分类 3.2　加密算法　3.2.1　对称加密体制　3.2.2　非对称加密体制　3.2.3　公钥密钥与对称密钥技术的综合应用　3.2.4　密钥管理与自动分配　3.3　数字签名　3.3.1　数字签名概述　3.3.2　数字签名实现方法　3.3.3　数字签名的算法　3.3.4　数字签名的过程　3.3.5　数字签名的标准　3.4　防火墙　3.4.1　防火墙概述　3.4.2　防火墙的关键技术　3.4.3　防火墙技术发展动态和趋势　3.4.4　防火墙系统的设计　3.4.5　选择防火墙的原则　3.4.6　主流防火墙产品介绍　3.4.7　防火墙应用举例　3.5　虚拟局域网　3.5.1 VPN概述　3.5.2 VPN技术　3.5.3 VPN服务器配置　3.5.4 IPSec协议　3.6　入侵检测系统　3.6.1　入侵检测概念　3.6.2　入侵检测系统的模型　3.6.3　入侵检测系统的功能　3.6.4　入侵检测系统的分类　3.6.5　入侵检测技术　3.6.6　入侵检测系统的部署　3.6.7　入侵检测的局限性　3.6.8　入侵检测技术发展方向　3.7　反病毒技术　3.7.1　计算机病毒概述　3.7.2　计算机病毒检测方法　……第4章　电子商务的认证与安全电子邮件技术第5章　电子商务安全技术付技术第6章　安全电子交易协议第7章　安全套接层协议第8章　安全电子商务应用全书内容总结练习与实训题答案参考文献

章节摘录

版权页： 插图： 好的网络管理员应该知道：“ 知道自己被攻击了就赢了一半。
”网络安全防护关键在于如何发现网络被攻击，以及当网络被攻击时应该采取怎样的处理方法，以便将损失控制到最小。
对网络系统加强管理是企业、机构及用户免受攻击的重要措施。
针对网络攻击需要解决的几个问题是：首先，网络可能遭到哪些人的攻击；其次，攻击类型与手段可能有哪些；再者，如何及时检测并报告网络被攻击；最后，如何采取相应的网络安全策略与网绍安全防护体系。
3.网络安全漏洞与对策 网络信息系统的运行一定要涉及到计算机硬件与操作系统、网络硬件与网络软件、数据库管理系统、应用软件以及各种网络通信协议。
而这当中肯定会存在一定的安全问题，它们不可能是100％无缺陷或无漏洞的。
（1）网络协议安全漏洞 网络服务是通过各种协议来完成的，因此网络协议的安全性也是网络安全的一个重要方面。
如果网络通信协议存在安全上的漏洞，那么攻击者就有可能不必攻破密码体制即可获得所需要的信息或服务。
而现在网络中的许多协议都是基于一种非常友好的、通信双方十分信任的基础之上的，在通常的网络环境之下，用户的信息都是以明文方式传输，因此进行网络侦听并不是一件难事。
TCP／IP是目前互联网上使用的最基本的通信协议，同样也可以找到能被攻击者利用的漏洞。
TCP／IP族中如POP、SMTP等协议在协议过程中的交换均是以明文出现的，只要使用网络侦听软件，就有可能将协议交换中的口令、密码监听到。
由于TCP／IP使用IP地址作为网络节点的惟一标志，而IP地址的使用和管理存在很多弊端，比如IP地址的数据包的源地址很容易被发现，而且IP地址是一种分级结构地址，其中包括了主机所在网络，攻击者据此可以构造出目标网络的轮廓。
此外，由于TCP／IP没有建立对IP包中的源地址的真实性的鉴别和保密，所以互联网上任何的主机都可能产生一个带有任意源IP地址的IP包，从而假冒另一台主机进行地址欺骗。
（2）防火墙安全漏洞 防火墙是互联网上公认的网络存取控制最佳的安全措施。
但防火墙的安全与研发的技术是紧密相连的。
很多防火墙产品对配置人员的技术背景要求很高，因为防火墙出产后一旦系统改动，就需要改动相关的安全产品的设置，这时很容易产生安全隐患问题。
防火墙主要是防范外部攻击，而很少顾及内部的隐患。
但内部人员使用信息或操作也可能会有错误发生，如遗失、欺骗、滥用等。
实际上，在系统资源的损失中，来自内部的攻击行为在整个系统受到的攻击中占了主要部分。
为了减少其危害的程度，应尽可能地强化管理制度。
（3）口令漏洞 口令是系统软件、应用软件中最主要和常用的认证方法。
口令设置不要太有规律，即不要选取显而易见的信息作为口令，如使用自己的英文名字、生辰等常用符号；但也不要太复杂，以免自己遗忘；此外，要设置口令尝试次数上限，能够及时锁住用户的账户，从而防止穷举口令；还要限制口令使用时间，定期改变口令，至少要3～6个月改变一次。
另外，系统管理员要时刻关注系统日志，对大量的Login失败记录保持警惕。
最后，需要说明的一点就是，为防止有人窃取口令，在输入口令时应确保安全距离，同时也不要在无意中泄露了自己的口令。
要将可能遭受攻击的风险降到最低。

编辑推荐

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