<<电子商务信息安全技术>>

图书基本信息

书名：<<电子商务信息安全技术>>

13位ISBN编号：9787111323020

10位ISBN编号：7111323025

出版时间：2011-1

出版时间：沈美莉、陈孟建、郁晓红、 等 机械工业出版社 (2011-01出版)

作者：沈美莉，陈孟建，郁晓红 等 著

页数：268

前言

随着互联网技术的发展，网络安全成了新的安全研究热点。
电子商务是互联网应用发展的必然趋势，也是国际金融贸易中越来越重要的经营模式。
安全是保证电子商务健康有序发展的关键因素。
由于Intemet本身的开放性，使电子商务系统面临着各种各样的安全威胁。
目前安全问题已成为电子商务的核心问题。
大量的事实说明，要保证电子商务的正常运作，就必须高度重视电子商务的安全问题。
电子商务的安全涉及方方面面，不是一堵防火墙或一个电子签名就能简单解决的问题。
安全问题是电子商务成功与否的关键所在：因为电子商务的安全问题不仅关系到个人的资金安全、商家的货物安全、企业的交易安全，还关系到国家的经济安全，关系到国家经济秩序的稳定问题。
而要保障电子商务的安全，除了要充分依靠现代信息技术，尤其是信息安全技术手段来进行保护外，还需要安全管理的制度和手段来约束，需要法律、法规环境的保障。
本书从电子商务信息安全技术角度出发，讲授构建和实施安全电子商务系统所必需的基本理论、方法和技术。
全书在编排上由简到繁、由浅入深和循序渐进，力求通俗易懂，简捷实用。
主要内容包括电子商务信息安全概述、电子商务网络安全基础、电子商务密码技术、电子商务安全认证技术、防火墙技术、电子交易及其安全、电子支付安全协议、移动电子商务安全、电子商务信息安全实训等。
本书观点新颖，论述深入浅出，内容丰富，可读性好，实践性强，适合作为高职高专学校电子商务、信息安全、管理信息系统、计算机科学技术等专业的教材，也可作为计算机和电子商务领域研究人员与专业技术人员的参考书。
本书由浙江工商大学沈美莉、郁晓红，浙江经贸职业技术学院陈孟建等编著。
参加编写的还有张贵君、陈奕婷、李锋之、袁志刚。
由于写作时间仓促和作者水平有限，书中不当之处敬请读者批评指正。

<<电子商务信息安全技术>>

内容概要

《电子商务信息安全技术》从电子商务信息安全技术角度出发，讲授构建和实施安全电子商务系统所必需的基本理论、方法和技术。
主要内容包括电子商务信息安全概述、电子商务网络安全基础、电子商务密码技术、电子商务安全认证技术、防火墙技术、电子交易及其安全、电子支付安全协议、移动电子商务安全、电子商务信息安全实训等。
本教材观点新颖，论述深入浅出，内容丰富，可读性好，实践性强。
《电子商务信息安全技术》适合作为高职高专学校电子商务、信息安全、管理信息系统、计算机科学技术等专业的教材，也可作为计算机和电子商务领域研究人员与专业技术人员的参考书。

<<电子商务信息安全技术>>

书籍目录

章节摘录

插图：5.证书的获取在验证信息的数字签名时，用户必须事先获取信息发送者的公钥证书，以对信息进行解密验证，同时还需要CA对发送者所发的证书进行验证，以确定发送者身份的有效性。
证书的获取可以有以下几种方式。
1）发送者发送签名信息时，附加发送自己的证书。
2）单独发送证书信息的通道。
3）可从访问发布证书的目录服务器获得。
4）或者从证书的相关实体（RA）处获得。
在PKI体系中，可以采取上述的某种或几种方式获得证书。
在发送数字签名的证书的同时，可以发布证书链。
这时，接收者拥有证书链上的每一个证书，从而可以验证发送者的证书。
检验过程是，通过检查发送者证书的发放机构CA，从CA中的目录服务器取得该CA证书，并重复这证书链上的CA根证书的验证。
6.证书和目录查询因为证书都存在周期问题，所以进行身份验证时要保证当前证书是有效而没过期的；另外，还有可能密钥泄露，证书持有者身份、机构代码改变等问题，证书需要更新。
因此在通过数字证书进行身份认证时，要保证证书的有效性。
为了方便对证书有效性的验证，PKI系统提供对证书状态信息的查询，以及对证书撤销列表的查询机制。
CA的目录查询通过LDAP协议，实时地访问证书目录和证书撤销列表，提供实时在线查询，以确认证书的状态。
这种实时性要求是由金融业务或其他电子政务应用的高度敏感性和安全性的高要求所决定的。
7.证书撤销证书在使用过程中可能会因为各种原因而被废止，例如，密钥泄露，相关从属信息变更、密钥有效期中止或者CA本身的安全隐患引起废止等。
因此，证书撤销服务也必须是PK|.的一个必需功能。
该系统提供成熟、易用、标准的证书列表作废系统，供有关实体查询，对证书进行验证。
8.密钥备份和恢复密钥的备份和恢复是PKI中的一个重要内容。
因为可能有很多原因造成丢失解密数据的密钥，那么被加密的密文将无法解开，会造成数据丢失。
为了避免这种情况的发生，PKI提供了密钥备份与解密密钥的恢复机制，即密钥备份与恢复系统。
在PKI中密钥的备份和恢复分为CA自身根密钥的备份和恢复和用户密钥。
CA根密钥由于其是整个PKI安全运营的基石，其安全性关系到整个PKI系统的安全及正常运行，因此对于根密钥的产生和备份要求很高。
根密钥由硬件加密模块中加密机产生，其备份由加密机系统管理员启动专用的管理程序执行备份过程。
备份方法是将根密钥分为多块，为每一块生成一个随机口令，使用该口令加密该模块，然后将加密后的密钥块分别写入不同的Ic卡中，每个口令以一个文件形式存放，每人保存一块。
恢复密钥时，由各密钥备份持有人分别插入各自保管的Ic卡，并输人相应的口令才能恢复密钥。

编辑推荐

《电子商务信息安全技术》：21世纪高职高专规划教材系列

<<电子商务信息安全技术>>

版权说明