<<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：9787121103612

10位ISBN编号：7121103613

出版时间：2010-3

出版时间：电子工业出版社

作者：王丽芳 主编

页数：278

<<电子商务安全>>

前言

电子商务是以互联网（Internet）为基础的商务活动。
每一个商务活动都是由客户机、通信网络、服务器组成的电子商务链实现的。
但是由于互联网的开放性、共享性和无序性，使得电子商务面临着多种风险和威胁。
电子商务安全问题一直困扰着电子商务的发展。
因此，电子商务专业人才应该具备保障电子商务安全的能力。
电子商务安全是电子商务专业重要的专业基础课程。
电子商务安全需要多层面提供保障，它是人、技术和管理的合理均衡。
本书的目的就是向学生系统地阐述电子商务面临的安全问题，并深入分析问题产生的根源，利用先进适用的技术解决这些问题。
本书的主要特点如下。
（1）结构完整，内容全面。
电子商务以ICT（Information and Communication Technologies）技术为基础，不仅深入阐述了主要的电子商务安全技术，而且也论述了电子商务安全管理和电子商务安全法律法规的主要内容。
（2）先进、适用。
精心选择教材内容，既重视基础知识，又紧跟学科领域的发展。
使学生既打下坚实的学科基础，又能掌握最新的思维方法和技术的进步。
（3）深入浅出、循循善诱。
本书用矛盾分析的方法，先找出问题，然后分析原因并找出解决的办法。
（4）理论和实践相结合。
电子商务安全实践性强，本书结合著名IT企业的电子商务安全解决方案，将理论与实践相结合。
从而使学生知道如何实施和部署各种技术以解决安全问题。
参加本书编写的有西北工业大学王丽芳、蒋泽军、吴健、刘志强、邓磊，西安邮电学院秦成德，由王丽芳任主编，并负责全书的统稿，蒋泽军、吴健任副主编，具体分工如下。
第1章、第6章由王丽芳编写，第2章、第3章由邓磊编写，第4章、第5章由蒋泽军编写，第7章、第8章由刘志强编写，第9章、第10章由吴健编写，第11章由秦成德编写。
在编写过程中，西北工业大学计算机学院博士研究生张志珂，信息安全与电子商务技术系的硕士研究生张英、张萌、周陈超、段勤等给予了很大的帮助，在此表示衷心的感谢！
教材编写过程中，参阅了大量的著作和教材、著名IT公司的理念和解决方案、互联网上相关的文献资料，在此向参考文献的作者表示最诚挚的感谢！
在本书出版之际，感谢国家信息办专家委员会与教育部电子商务教学指导委员会各位专家，感谢电子工业出版社，感谢国内外从事电子商务安全的同行。
电子商务安全涉及众多的学科，各种理念、技术和方案在实践中不断地推陈出新。
由于作者水平有限，书中不足之处，希望读者谅解，并恳请读者批评指正，以便进一步完善本书内容。

<<电子商务安全>>

内容概要

本书全面、系统地分析了电子商务面临的安全问题，以及问题产生的根源。
在此基础上从技术、管理和法律法规等方面，深入阐述了实现电子商务安全的思想、技术、方法和策略。
全书共11章，主要内容有电子商务安全概述、密码学基础、密钥管理、公钥基础设施与应用、身份认证与访问控制技术、互联网安全技术、电子商务安全协议、数据高可用技术、电子商务安全评估与管理、电子商务安全解决方案和电子商务安全法律法规。
　通过本书的学习，读者将具备确保电子商务安全的能力。
本书既可作为高等学校电子商务及电子安全等相关专业本科生、研究生的参考书，也可以供相关专业科研人员、管理人员参考使用。

<<电子商务安全>>

书籍目录

章节摘录

插图：1）对称加密对称加密又称私钥加密，加密密钥与解密密钥是相同的。
它的优点是算法简单，密钥较短，且破译困难，加密和解密的速度快，适合对大数据量进行加密。
但是密钥管理困难。
首先，密钥必须通过安全可靠的途径传递，如果通信的双方能够确保密钥在交换阶段未曾泄露，那么就可以采用对称加密方法对信息进行加密。
其次，有大量的私钥需要保护和管理，因为与不同的客户交互信息需要不同的私钥加密。
因此，密钥管理是对称加密应用系统安全的关键性因素。
目前常用的对称加密算法包括DES、3DES、AES和IDEA等。
2）非对称加密非对称加密又称公钥加密，加密和解密使用不同的密钥.每个用户有唯一的一对密钥，公开密钥（公钥）和私有密钥（私钥）。
公钥是公开的，存放在公共区域；私钥是保密的，必须存放在安全保密的地方。
如果用公钥对数据进行加密，那么只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。
非对称加密算法中，无论用户与多少客户交互，都只需要两个密钥：公钥和私钥。
公钥即加密密钥是公开的，因而解决了对称加密算法中密钥传递问题。
私钥即解密密钥，只有一个，因而解决了对称加密算法中用户管理众多私钥的问题。
非对称加密算法的保密性比较好，因为最终用户不必交换密钥.但其加密和解密花费时间长、速度慢，不适合于对文件加密，只适用于对少量数据进行加密。
常用的非对称加密算法有RSA、ECC等。

<<电子商务安全>>

编辑推荐

《电子商务安全》：普通高等教育“十一五”国家级规划教材，“信息化与信息社会”系列丛书之高等学校电子商务专业系列教材

版权说明