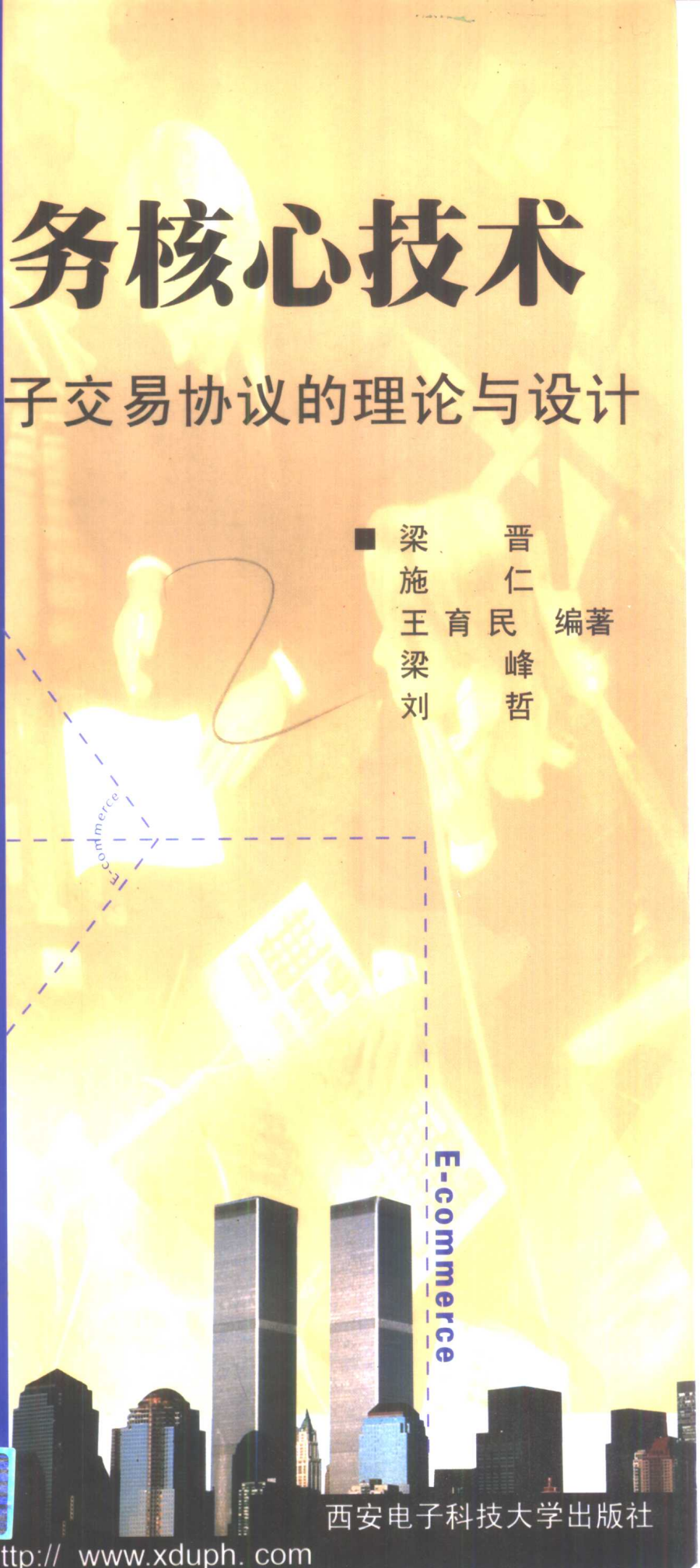
E-commerce

电子商务核心技术

——安全电子交易协议的理论与设计

梁　晋
施　仁
王育民　编著
梁　峰
刘　哲



西电出版社
西安电子科技大学出版社
http:// www.xduph. com

电子商务核心技术

——安全电子交易协议的理论与设计

梁晋 施仁
王育民 梁峰 刘哲 编著

西安电子科技大学出版社

2000

内容简介 电子商务是目前 Internet 发展的热点，支付协议是电子商务的核心问题。以安全电子交易协议(SET)为代表的支付方式和协议逐渐被人们所熟悉。SET 协议是目前支付协议中最为复杂的标准，涉及电子商务、密码理论、计算机网络技术等各方面的知识。目前国内有关电子商务的介绍性书籍不少，但有关电子商务支付协议的技术资料却不多。本书立足 SET 协议的理论和设计，向读者全面系统地讲解了目前电子商务支付系统的理论和设计技术，重点是 SET 协议的标准和扩展技术。通过本书的学习，读者不但能够对 SET 协议有较深刻的理解，并且能够熟悉其它支付协议和标准。

全书分七部分。第一部分综述电子商务支付系统和 SET 协议；第二部分是有关 SET 的安全和密码理论知识；第三部分是 SET 协议设计综述；第四部分是 SET 协议的证书管理；第五部分是 SET 协议的支付管理；第六部分是 SET 协议的接口扩展；第七部分是支付系统的探讨和 SET 协议的最新扩展，对比了 SSL 协议，介绍了目前 SET 的最新扩展，以及微支付方式。

本书可作为有关专业的大学本科或研究生教材，也是有关计算机和网络行业从业人员进行电子商务设计、研究和开发的有价值的参考资料。

图书在版编目(CIP)数据

电子商务核心技术：安全电子交易协议的理论与设计/梁晋等编著. —西安：西安电子科技大学出版社，2000.8

ISBN 7-5606-0894-9

Ⅰ.电… Ⅱ.梁… Ⅲ.计算机网络—商业经营—支付方式—安全—协议 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2000)第 35257 号

责任编辑 李惠萍 殷咸安

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)8227828 邮 编 710071

http://www.xduph.com E-mail：xdupfxb@pub.xaonline.com

经 销 新华书店

印 刷 陕西画报社印刷厂

版 次 2000 年 8 月第 1 版 2000 年 8 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印张 30

字 数 704 千字

印 数 1～4000 册

定 价 36.00 元

ISBN 7-5606-0894-9/TP·0476

前言

电子商务的发展将计算机技术(特别是 Internet 技术)拓展到社会各个领域。电子商务的一个核心问题是支付，目前比较流行的支付协议有 SSL、SET 等。SSL 比较简单，应用得比较多，但其问题也比较多，发展潜力不大。在本书第十九章对 SSL 和 SET 作了详细比较。SET 协议在商业上得到了 VISA 和 MASTER 等大的支付卡品牌的支持，在技术上得到了计算机大厂商(如 IBM、Microsoft、HP 等)的支持，是目前支持力量最大的支付协议。虽然 SET 协议从 1997 年正式公布以来，其应用存在一些问题，迫使 SET 协议的标准组织 SETCo 在 1998 年和 1999 年提出了许多 SET 协议扩展，这些扩展针对 SET 协议在应用中出现的问题作了一些改进，如支持 IC 卡、智能卡、借记卡；对商家和持卡者之间支持非 SET 消息，如持卡者可以通过电话、传真、SSL 等非 SET 协议进行交易。这些扩展的推出解决了 SET 协议应用中的一些问题。另外，在电子商务中还有许多支付协议和方式，如目前兴起的微支付方式。在本书第 21 章，将对微支付协议进行介绍。

一、本书读者对象

1. 相关专业的工程技术人员

这些读者可能比较关心如何建立一套电子商务系统，而不是开发一个 SET 应用程序。此类读者需要详细阅读本书，但因为只有了解了支付协议的内容，才能有效地建立支付系统。例如，即使用户买了一套 SET 支付软件，如 IBM 的 Net.commerce，但因为 SET 协议有许多可变因素和扩展协议，不了解消息协议也很难进行应用。

2. 研究和开发人员

对于研究和开发人员，在阅读本书的基础上，建议读者阅读 SET 协议的 ANSI.1 表示，也就是“SET Secure Electronic Transaction Specification Book 3：Formal Protocol Definition Version 1.0”。

3. 计算机爱好者

有些计算机爱好者，能够熟练操作计算机和上网，对于这些读者，第二部分可以不看，只阅读其它部分内容即可。

二、本书的内容安排

本书以 SET 协议为线索，分为七个部分。如果读者没有密码方面的知识，建议读者先对第二部分网络安全和密码理论作一了解，再阅读其余部分。

第一部分　电子商务和支付介绍

本部分介绍电子商务和支付系统的概念，对 SET 协议作总体描述，包括第 1、2 章。第 1 章 电子商务和支付系统概述，第 2 章 SET 协议的总述，介绍 SET 的概念和支付处理流程。

第二部分　网络安全和密码理论

该部分介绍网络安全和密码理论基础，介绍SET协议涉及的安全密码理论，包括第3～7章。第3章 信息网络安全概述，第4章 密码理论基础，第5章 对称密钥密码技术，第6章 公钥密码技术，第7章 公开密钥基础设施(PKI)。

第三部分　SET系统设计综述

该部分介绍涉及SET的开发工具和应用的设计考虑事项，提供背景信息，介绍突出的特性，包括第8～10章。第8章 SET系统设计介绍，第9章 SET技术要求，第10章 SET系统概念。

第四部分　SET协议证书管理

本部分介绍有关SET协议的证书管理结构、协议、概念等，包括第11～13章。第11章 证书管理结构，第12章 证书格式，第13章 证书请求协议。

第五部分　SET支付系统

本部分介绍SET协议中有关支付系统的处理和描述，包括所有与授权、付款和支付系统管理有关的所有消息，包括第14～16章。第14章 SET一般数据和流程，第15章 持卡者和商家消息，第16章 商家与支付网关的消息。

第六部分　SET协议的外部接口指导

该部分不是SET协议的本身，而是为开发者提供开发交互操作应用程序的指导。主要介绍SET协议没有详细定义的初始消息和传输机制，包括第17、18章。第17章 SET初始消息，第18章 传输机制。

第七部分　电子商务支付系统探讨

本部分主要是有关SET协议的讨论和分析，对比了SSL协议，介绍了目前SET的最新扩展，以及微支付方式，包括第19～21章。第19章 SSL及SET分析，第20章 SET协议扩展及发展趋势，第21章 Internet微支付及其它。

本书主要作者梁晋，博士毕业，现为西安交通大学的教师，工作于西安交通大学信息机电研究所，是中国信息经济学会电子商务分会的常务理事。另两位作者施仁教授、梁峰老师都工作于西安交通大学电子与信息工程学院。王育民教授是西安电子科技大学的老师，也是我国密码安全专家。刘哲是陕西邮电管理局技术人员。同时，本书的编写得到了西安凯辉电子有限责任公司的大力支持。

目前，国外对电子商务支付的研究和产品较多，而国内还处在初级阶段，有关支付系统深层次的技术资料很少，产品研究基本处于空白状态。希望本书能为国内电子商务支付系统的研究提供帮助。

书中错误之处请读者批评指正。

作者梁晋 E-mail：jin_liang@netease.com.

作　者

2000年2月5日

于西安交通大学

目　录

第一部分　电子商务和支付介绍

第二部分 网络安全和密码理论

第三部分 SET 系统设计综述

第四部分 SET 协议证书管理

第五部分 SET 支付系统

第六部分 SET 协议的外部接口指导

第七部分 电子商务支付系统探讨

第一部分

电子商务和支付介绍

本部分介绍电子商务和支付系统的概念，对SET协议作总体描述。电子商务的内容包含两个方面，一是电子方式，二是商贸活动。现在人们所探讨的电子商务主要是由EDI(电子数据交换)和Internet来完成的。尤其是随着Internet技术的日益成熟，电子商务真正的发展将是建立在Internet技术的基础上的。

第1章　电子商务和支付系统概述

介绍电子商务的基本知识(特性、发展过程、分类等)，支付系统的概念(支付服务、支付类型、支付模型选择等)，以及电子商务的安全要求和支付协议(安全要求、现有支付协议等)。

第2章　SET协议的总述

介绍SET的概念和支付处理流程，包括SET标准的组成，SET支付系统参与者，加密概念，证书发行，购物类型，以及SET支付处理的基本步骤。