电子商务支付安全技术研究

王 龙

（陕西广播电视大学延安分校，陕西 延安 716000）

摘 要：电子支付安全问题是电子商务发展过程中所面临的最大问题，也是电子商务研究的重点。笔者通过对当前 SSL 电子支付安全模型和 SET 电子支付安全模型的安全性分析，针对当前 SET 电子支付模型所存在的不足，提出更加简单易用和安全性更高的 SSSEP 安全体系结构。

关键词：电子商务；电子支付；信息安全

中图分类号：TP393.08 **文献标识码：**A **文章编号：**1003-9767（2018）04-182-03

Research on Electronic Commerce Payment Security Technology

Wang Long

(Yan´an Branch of Shaanxi Radio and Television University, Yan´an Shaanxi 716000, China)

Abstract: The security problem of electronic payment is the biggest problem in the development of e-commerce and also the focus of e-commerce research. In this paper, we analyze the security of current SSL electronic payment security model and SET electronic payment security model, and put forward the SSSEP security architecture that is more simple and more secure and more secure in view of the shortcomings of the current SET electronic payment model.

Key words: e-commerce; e-payment; information security

1 引言

随着 Internet 技术的不断发展和完善，其应用越来越广泛。电子商务是在 Internet 发展下的一个非常重要和典型的应用，借助电子商务人们可以更便捷地进行商业活动，同时，电子商务也正逐渐改变人们的消费习惯。但是，在电子商务建设和发展过程中，正面临着法律、安全等问题。其中，如何完善电子支付安全体系，如何提高电子支付安全性，已成为电子商务现阶段所重点关注的问题。

2 电子支付安全模型分析

2.1 SSL 电子支付安全模型

SSL（Secure Socket Layer）是一个 Web 安全传输协议[1]，IETF 组织对 SSL 进行标准化处理后，提出 TLS（Transport Layer Security）安全协议。TLS 协议和 SSL 协议的差别非常小，所以在本文的研究中认为 SSL 和 TLS 在电子支付领域是等价的。SSL 协议建立在传输层和应用层之间，用于保证两个通信实体间通信的认证性、完整性和机密性。SSL 协议的层次结构如图 1 所示。

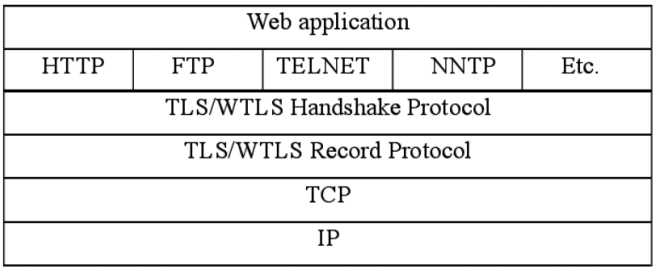

图 1 SSL 协议层次结构图

在数据发送之前，通过 SSL 握手协议产生会话状态的加密参量，在客户和服务器通信之前，两者就需要在加密算法、协议版本选择方面达成一致。客户端和服务器的握手协议过程如图 2 所示。

2.2 SET 电子支付安全模型

SET 安全电子交易协议是一种基于消息流的协议，是电子支付系统规范。SET 协议不仅实现了对两个通信实体之间的单个会话的加密，同时，还准确反映了交易各方之间的关系。实际上，SET 远远不只保证了在线交易安全，同时，还保证了在线交易各方所持有数字证书的合法性，通过响应信息和数字证书来记录交易各方的动作，实现交易各方的责任分担[2]。

作者简介：王龙（1979-），男，陕西延安人，本科，讲师。研究方向：计算机应用。

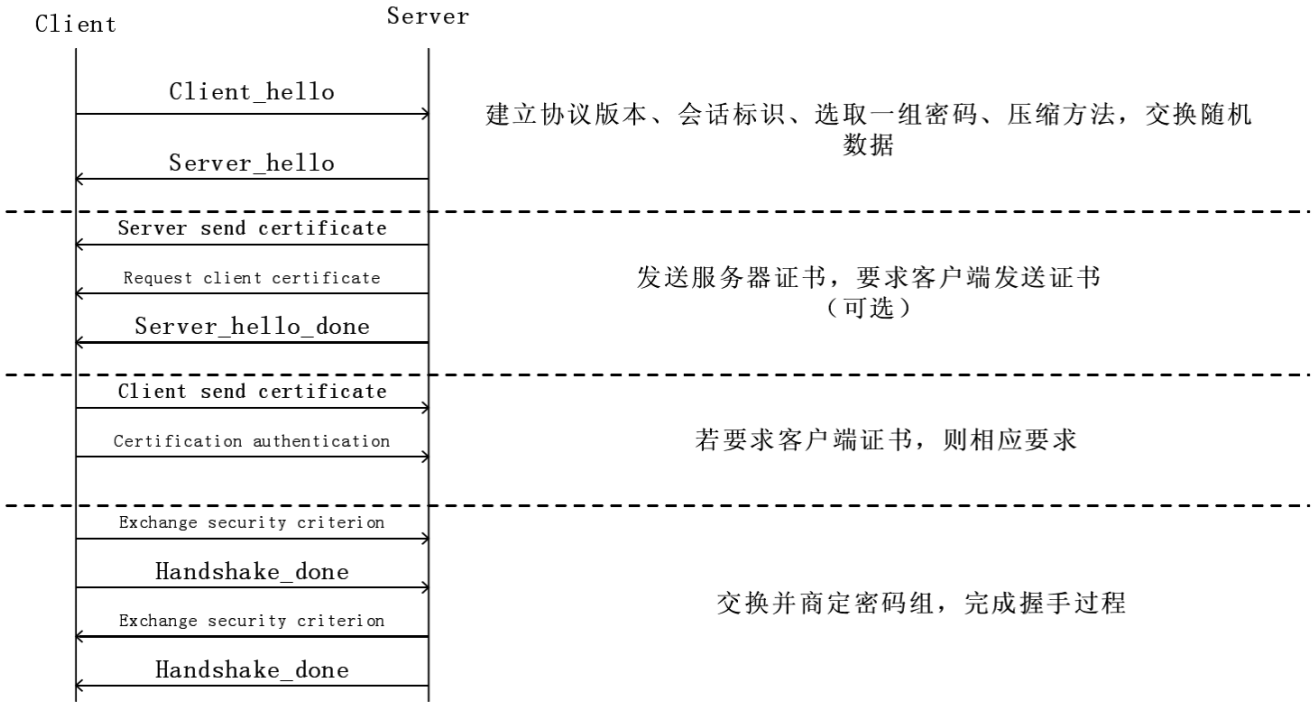

图 2 SSL 协议握手过程图

SET 安全协议的工作流程如图 3 所示。

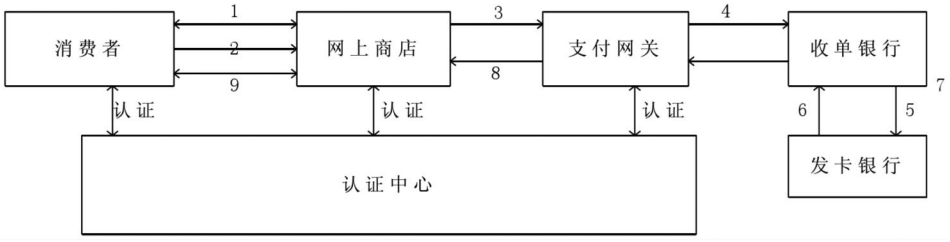

图 3 SET 安全协议工作流程图

2.3 电子支付安全模型的安全性分析

SSL 安全协议模型采用公开密钥技术，以保证两个通信主体之间的通信可靠性和保密性 [3]。在 SSL 安全模型中，要设计一个安全的密钥交换协议非常复杂，因此，在 SSL 密钥管理中，存在如下问题。

（1）通信双方以明文的方式，相互发送自己所能够支持的加密算法，以明文方式发送，就存在被修改的可能。

（2）所有的会话密钥都会产生 master-key，而且通信双方的握手协议完全依赖 master-key 的保护，为此在双方进行通信时要尽可能少地使用 master-key。

SET 使用各种密码技术，定义了完备的电子交易流程，较好实现了电子支付各方的安全连接，保证了电子支付的不可抵赖性、身份合法性、数据完整性和交易机密性。

与 SSL 协议相比，SET 安全协议具有如下优点。

（1）对于店方而言，SET 为店方提供了保护自己的手段，降低店方的欺诈风险，以降低店方的运营成本。

（2）对于消费者而言，SET 可以有效保证店方的安全性，同时，也保证了消费者消费信息的安全性。

（3）对于发卡机构而言，SET 可以降低网络欺骗概率，从而提高了电子支付整体安全性，有利于发卡机构电子支付领域的业务快速扩张。

（4）对于交易平台而言，SET 定义了各方的互操作接口，有助于电子支付系统的构建。

SET 安全模型自面世以来，就得到了广泛的支持，但是在发展了近二十年后，其应用仍然存在问题，具体如下。

（1）SET 协议中并没有说明发卡机构（银行）是否需要在收到消费者的货物接收证书后，才能够将钱支付给店方，从而导致在消费者对店方提供的商品质量提出异议后，责任由谁来承担并不明确。

（2）SET 协议没有“非觉行为”，即店方无法证明订购信息是消费者发出的。

（3）SET 协议具有多层安全保障，提高了系统安全性，但是也增强了系统复杂性，导致 SET 安全模型的实施难度加大。

（4）SET 协议没有规定交易后数据的保存和销毁流程，从而导致可能存在基于交易信息的潜在安全攻击。

（5）SET 协议建设成本高、使用麻烦，而且仅适合于消费者具有电子钱包的场合。

3 SSSEP 安全体系结构设计

SSL 安全模型存在安全性弱等缺陷，但是其具备实现简单、身份验证性能高和负担小等优点。而 SET 安全模型的安全性较高，但是为了保证电子支付的安全性，在其每一步工作中都需要进行加密算法协商，导致系统效率降低，而且这些烦琐的加密算法协商过程并不是必须的。针对 SSL 安全模型和 SET 安全模型所存在的不足，提出 SSSEP（SSL and SET-based Security Electronic Payment）安全体系来保证电子商务的支付安全。

3.1 用户支付网关结构设计

SSSL 体系结构由消费者、店家、支付网关和金融机构四个部分组成，SSSL 安全体系结构设计如图 4 所示。

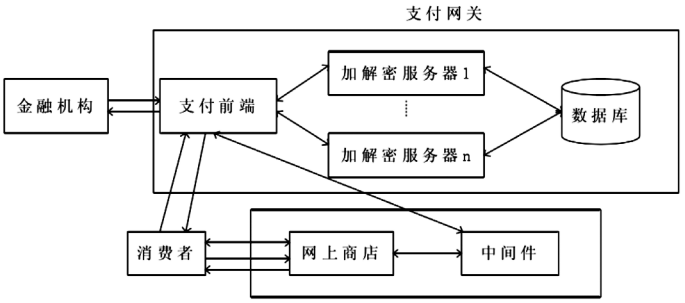

图 4 SSSL 系统框架图

消费者与店方交换安全证书，并进行密钥、加密算法等安全参数协商；店家在接收到订单后，将订单信息通过中间件转发给支付网关；消费者在支付网关进行支付或授权；支付网关根据消费者的身份认证信息，向金融机构认证消费者身份，并按照需求进行授权和支付，并通过中间件，将授权和支付信息发给店方；店方根据支付机构返回的授权和支付信息，为消费者提供服务或产品。

3.2 支付网关设计

支付网关是因特网与银行金融系统之间的接口，支付网关也是本文基于 SET 安全模型建设 SSSEP 安全体系架构的改进重点。在 SET 安全模型中，电子支付过程中的密钥、银行账号、消费者信息和证书等信息都存储在支付网关中。因此，在 SET 安全模型中，一旦支付网关被侵入者攻破，就能轻易获得交易过程中的消费者信息、帧数信息、密钥信息和银行账号信息。

为此，本文提出 SSSEP 安全体系结构来保证支付网关的安全性，SSSEP 安全体系中的支付网关设计如图 5 所示。

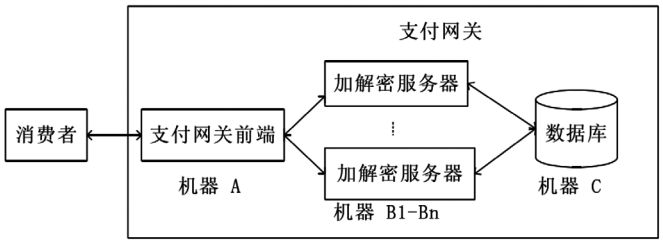

图 5 支付网关设计

在 SSSEP 安全体系结构中，支付网关负责消息的接收和转发，数据库用于存储支付网关操作过程信息和支付结果信息。由于支付网关只负责信息的接收和转发，而相关数据在加密后存储到数据库中，因此，外界无法直接访问加密后的数据库信息，从而有效防止来自网关外部的攻击，进一步增强了电子支付系统的安全性。

3.3 中间件设计

中间件起着在支付网关和店家之间传输数据的中介作用，主要从如下三个方面满足支付网关和店方的要求：（1）安全性，支付网关和店家之间的信息需要通过因特网进行传输，因此，中间件必须要满足安全性需求；（2）方便性，店家需要关注为消费者所提供服务和产品的质量，因此，中间件必须要保证方便性，以方便信息技术能力较为薄弱的店家能非常方便简单地使用中间件；（3）灵活性，能够为具有不同业务特点的店家提供灵活的支付服务，并且还需要考虑中间件配置和管理的灵活性。

针对如上需求，中间件的设计如图 6 所示。

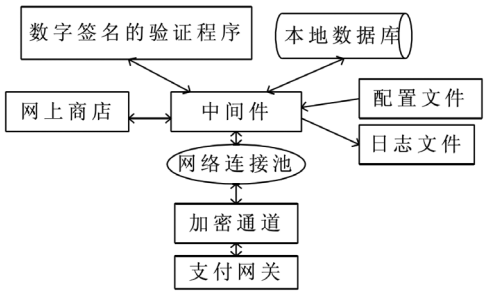

图 6 中间件框架设计

4 结 语

本文通过对当前 SSL 电子支付安全模型和 SET 电子支付安全模型的安全性分析，针对当前 SET 电子支付模型所存在的不足，进行 SSSEP 电子支付安全体系结构的设计，以进一步提高 SET 电子支付模型的安全性，提高安全体系结构应用的便捷性。但是，本文研究的 SSSEP 电子支付模型只是一个简单的原型，还需要通过不断改进和完善，才能够保证电子支付模型的安全性。

参考文献

[1] 闫鹏 . 基于 SSL 和 SET 协议的电子支付安全研究 [J]. 通讯世界 ,2016(22).

[2] 薛安松 . 电子支付安全协议的探讨 [J]. 数字技术与应用 ,2016(11).

[3] 刘洋 . 电子支付安全问题与分析 [J]. 电子技术与软件工程 ,2015(22).