基于PKI的电子商务安全研究

张 琳

(北京建筑工程学院电气与信息工程学院 北京 西城区 100044)

【摘要】网络的飞速发展推动了电子商务的广泛应用，随着网上交易的普及，人们越来越关心电子商务中的保密性、完整性、可用性、认证性和不可否认性等安全问题。本文以电子合同签订的实现过程为例，介绍了系统的核心业务流程、利用SSL技术建立客户端和服务器之间安全传输通道的方法、基于随机数的单向散列函数防止网络欺骗的认证过程以及电子合同的实现过程，全文以PKI理论为基础，利用公钥密码系统确保了电子商务过程中所传输消息的完整性。

关 键 词 电子商务； 电子合同； 信息安全； 公钥基础设施

中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.z1.020

Research on E-Commerce Security Based on PKI

ZHANG Lin

(School of Electricity and Information Engineering, Beijing University of Civil Engineering and Architecture Xicheng Beijing 100044)

Abstract With the rapid development and popularization of internet, E-Commerce is widely used in our daily life. More and more people pay attention to the security problems of E-Commerce: confidentiality, integrity, availability, controllability, non-repudiation and accountability. In cryptology, those problems are solved by public key technology. Public key infrastructure (PKI) is the base and core of network security, it can provide good security services for the world of network, by using asymmetric encryption algorithms. This paper takes E-contract as an example and puts forward the solution of E-Commerce by using technology PKI.

Key words E-commerce; E-contract; information security; public key infrastructure

随着Internet的发展，网络已经渗透到各个方面，改变了人们的生活方式。电子商务作为一种新的营销模式因具有传统商务所不具有的特点越来越被人们所重视，并得到了迅猛的发展。由于Internet的开放性，其安全性一直受到人们的关注。为解决电子商务的安全问题，公钥基础设施(public key infrastructure，PKI)技术作为一种有效安全解决方案被引入到了电子商务中来[1-2]。本文以一个电子商务系统为背景，介绍了PKI的概念及其加密体制，并提出一套完整的基于PKI的安全体系，为电子商务的发展提供安全保障。

1 PKI及其加密体制

1.1 PKI的定义和功能

PKI是对公钥所表示的信任关系进行管理的一种机制，它为Internet用户和应用程序提供公钥加密和数字签名服务[3]。目前，公钥体制广泛地应用于CA认证、数字签名和密钥交换等领域。PKI是信息安全基础设施的一个重要组成部分，是一种普遍适用的网络安全基础设施。数字证书认证中心CA、审核注册中心RA、密钥管理中心KM都是组成PKI的关键组件[4]。PKI的组成框架如图1所示。PKI的主要功能包括：公钥加密、证书发布、证书确认、证书撤销[5]。

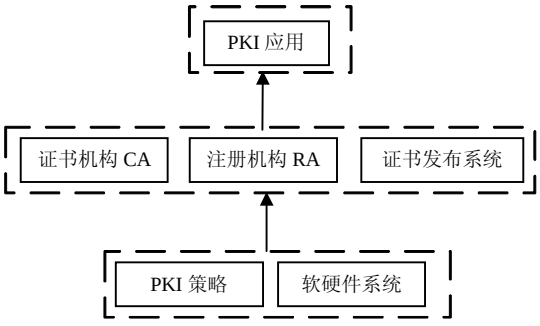

图1 PKI的组成框架图

1.2 PKI的加密体制

PKI的加密体制可分为以下4种。

(1) 对称密码体制。对称密码体制的基本特点是加解密双方在加解密过程中要使用完全相同的一个密钥。在对称密码系统中发送者和接收者之间的密

收稿日期： 2009 ↖ 09 ↖ 15

作者简介：张 琳(1975 ↖)，女，研究生，讲师，主要从事操作系统和软件工程方面的研究.

钥必须安全传送，而双方实体通信所用的秘密钥也必须妥善保管。常见的对称加密算法是DES。对称算法最主要的问题是：由于加解密双方都要使用相同的密钥，因此在发送和接收数据之前必须完成密钥的分发。因而密钥的分发便成了该加密体系中的最薄弱风险最大的环节[6]。

(2) 非对称密码体制。非对称密码体制也称公钥密码体制。非对称密码体制的基本特点是存在一个公钥/私钥对，用私钥加密的信息只能用对应的公钥解密，用公钥加密的信息只能用对应的私钥解密。著名的非对称加密算法是RSA。RSA使用的一个密钥对是由两个大素数经过运算产生的结果：其中一个是公钥，为众多实体所知；另外一个是私钥，为了确保其保密性和完整性，必须严格控制并只有它的所有者才能使用。RSA加密算法的最基本特征就是密钥对中的一个密钥加密的消息只能用另外一个解密，这也就体现了RSA系统的非对称性。

(3) 数字证书与数字签名。数字证书是一段包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。身份验证机构的数字签名可以确保证书信息的真实性，用户公钥信息可以保证数字信息传输的完整性，用户的数字签名可以保证数字信息的不可否认性。数字证书是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件[7-8]。

数字签名是指使用密码算法对待发送的数据进行加密处理，生成一段信息，附在原文上一起发送，这段信息类似现实中的签名或印章，接收方对其进行验证，判断原文真伪[9]。

(4) 散列(Hash)函数。Hash函数就是把可变输入长度串转换成固定长度输出串的一种函数，主要用于证明原文的完整性和准确性，是为电子文件加密的重要工具。一般来说，对于给出的一个文件要算它的Hash码很容易，但要从Hash码找出相应的文件算法却很难。Hash函数最根本的特点是这种变换具有单向性，一旦数据被转换，就无法再以确定的方法获得其原始值，从而无法控制变换得到的结果，达到防止信息被篡改的目的。由于Hash函数的这种不可逆特性，使其非常适合被用来确定原文的完整性，从而被广泛用于数字签名。最常用的算法包括MD5和SHA1[10]。

2 系统框架

2.1 核心业务介绍

本文系统是建立在电子商务证书业务和支付体系之上的电子商务应用业务。系统的核心业务如图2所示。

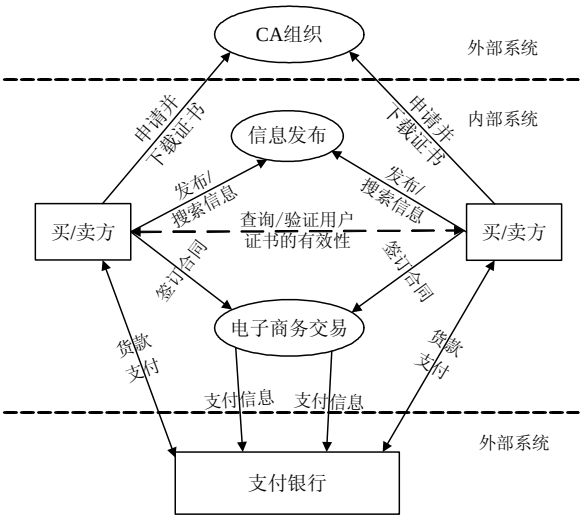

图2 核心业务示意图

系统包括信息发布平台和电子商务交易平台。示意图中的CA机构属于外部系统，完成的是数字证书的产生、发放、撤销等管理工作，系统实用CA机构的数字证书；支付系统也是外部系统；买方和卖方之间、买卖方和交易平台之间、交易平台和银行之间均需要双向的身份认证；合同或订单作为商业机密要进行数字签名、加密保护，以防篡改、抵赖行为发生。

2.2 安全传输通道的建立

本文系统采用了SSL技术在客户端和服务器之间建立一条安全的传输通道，防止网络窃听。安全套接层协议(security sockets layer，SSL)，主要用于提高应用程序之间数据的安全系数，采用了公开密钥和对称密钥两种加密：在建立连接过程中使用公开密钥，在会话过程中使用对称密钥。加密的类型和强度则在两端之间建立连接的过程中判断决定，它保证了客户和服务器间事务的安全性[3-4]。

SSL协议基于C/S和B/S模式，它由两层组成，分别是握手协议层和记录协议层。握手协议层主要是在双方进行正确的保密通信前建立一个连接双方的安全通道。其中主要是相互验证、协商加密算法、生成密钥、初始化向量等。

客户端和服务器之间的相互验证主要通过证书来实现。首先通过对方证书中权威发证机构签字的验证来确定对方的证书是否有效。如果证书有效，就从这个证书中提取公钥，通过对方的签名验证用户是不是非法的。如果两者都通过，则证明对方的身份是真实可信的。

客户端和服务器之间需协商安全参数。协商的参数一般包括协议的版本号、密钥交换算法、数据加密算法和Hash算法，通过协商达成一致性。版本号一般要求一致，密钥交换算法和数据加密算法是先由客户端向服务器发送一个列表，其中详细列举了客户端所支持的算法，然后由服务器从中选取自己支持且加密性能优越的算法，并返回给客户端，完成算法的协商；最后由客户端随机产生一个用于数据加密的对称密钥，用一种商定好的密钥交换协议将它传送给服务器端。

SSL协议的通信是保密的，双方的验证使用非对称密钥，在握手协议初始化连接后，具体的通信内容使用对称密钥进行加密。传输中的消息带有一个完整性校验。SSL建立的连接是可靠的，如果传输的数据被截获，没有解密密钥，也无法看到可读的资料。SSL所使用的证书可以是自己创建的，也可以通过一个商业性CA签署证书。本文系统使用支持SSL的Apache Web Server，通过openssl产生3类证书：根证书、服务器证书和客户端证书。根证书用来签发服务器证书和客户端证书。

2.3 防止网络欺骗的认证过程

在开放的网络环境下，如何提供系统的登录验证、实现身份的认证所面临的安全要求要比封闭环境下的安全要求强度大，传统的基于口令的简单认证形式显然不能满足认证的安全性要求。本系统采用基于随机数的单向散列函数的口令传输方式实现了系统的登录过程，原理如图3所示。

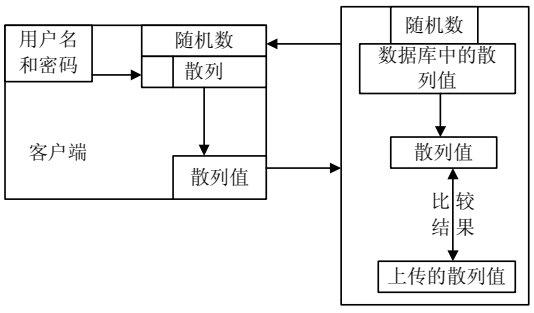

图3　登录原理图

验证开始时，服务器生成一个随机数，送到客户端，客户端对用户名和密码进行散列，其结果再与随机数进行第二次散列，然后发送给服务器；服务器从数据库中取出用户名与密码的散列值与随机数的散列值再求散列后的结果与客户端上传的数据比较，如果相同，则通过服务器的验证并对用户授予相应的权限。

在项目实施过程中，将随机数更改为一个基于一组字符的随机串，每次登录根据会话产生不同的随机串，增加了随机数的复杂度。

系统中求散列的功能使用Bouncy Castle Crypto API的SHA1Digest摘要引擎来计算用户名和密码的散列值。在此没有使用常规的MD5算法设计散列值，因为在当前的技术条件下已经比较容易计算出MD5算法的碰撞，可靠性不高。

2.4 电子合同的实现

当买方和卖方进行交易时，为了明确责任，制约双方的行为，防止和减少经济纠纷，需要签订合同。

(1) 合同的状态。

合同的状态定义如下：

PENDING：合同产生时默认的状态；

PROCESSING：当一方对合同进行签名，其状态由PENDING到PROCESSING；

FAILED：当有任意一方放弃或拒绝，以及到合同截至日期未完成签名，合同的状态转为FAILED；

COMPLETED：合同被双方签名，状态转为COMPLETED。

(2) 合同的生成。

网上交易双方有购买的意向后，由一方生成电子合同发布在网上，合同的制作者要在合同中指定合同的另一方。双方用户登录后可以同时浏览合同的内容，通过其他的通讯方式进行沟通，双方经过数次修改，最终没有分歧时，由合同制作一方填入签名截止日期，提交合同。合同提交后不能修改，此时合同的状态为PENDING。如果截止日期前任意一方没有签名或拒绝签名，合同作废。

(3) 合同的签名。

已经提交的合同，进入待签名状态。只有状态为PENDING的合同可以签名，买卖双方均可对合同进行签名。合同的签名保存在签名表中，买卖双方的签署顺序没有要求，但必须在指定的日期内签署，否则合同的状态转为无效。当有任意一方进行了数字签名后，合同的状态转化为PROCESSING，双方都签过名的合同状态转换为COMPLETED。

3 结 束 语

本文介绍了电子商务和公钥的相关理论，分析了系统实现时可能出现的安全问题，并利用密码学的技术进行了解决。本文以PKI理论为基础，利用公钥密码系统确保电子商务过程中所传输消息的完整性。文章的理论研究和实现方法，对于保障电子商务活动中消息的完整性和机密性具有重要的意义。

(下转第108页)