基于智能卡的身份认证及其应用①

Smart Card Based Authentication and Application

李　栋　（北京邮电大学信息安全中心 100876）
杨义先　（北邮国家重点实验室）

摘要：本文总结了当前常用的身份认证方式，并且评价了其优缺点。这些身份认证方式大多数都是在线认证方式。借鉴当前电话卡（智能卡）的一种离线认证的方式，提出了电子商务应用中的离线认证模型。然后，根据电子商务的支付方式，设计出一种基于智能卡的离线认证和安全通信的电子商务应用系统，并且分析了该系统的安全性。

关键词：智能卡 身份认证 离线 电子商务

1 引言

在网络世界中，人的身份是虚拟的，人可以掩盖自己的本来身份，伪装成一个完全陌生的人。正是由于这一点，网络成了人们的乐园，人们可以不用顾忌自己的本来身份而为所欲为。但是，在某些场合，恰恰需要验证人们的真实身份。比如，在电子交易中，双方都希望与自己交易的对方是可信赖的。又比如，在某些涉及保密信息的场合，只有合法的用户才能访问这些信息。因此，身份认证技术是开展网络应用必须面对和解决的一个难题。

2 常用的身份认证技术

2.1 基于用户名和口令的认证方式

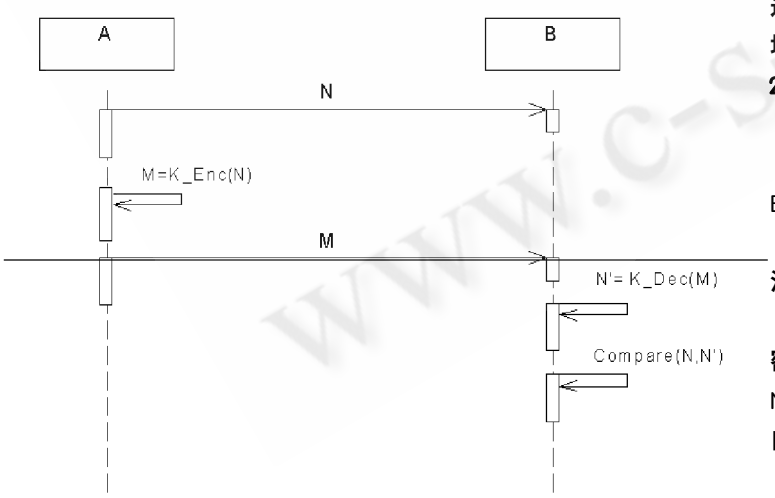

图 1　基于对称密钥的认证原理图

这类是最常见的身份认证方式，电子邮件服务、BBS 系统等都属于此类。

用户在客户端输入的用户名和口令直接在网络上传输，服务器接收到用户名和口令后与其数据库中的数据进行对比来验证用户是否是有效的用户。

在这种基本方式上可以进行变化，比如可以对用户的口令值进行 Hash 计算，服务器数据库存放的是用户口令的 Hash 值，这样既可以避免用户口令在网络上的输出，又可以避免泄漏用户的一些隐私。但是，这种方式很容易被攻击者窃取到用户的用户名和口令信息，这样他就可以冒用别人的帐号来进行网络活动。另外，当合法用户认证通过后，攻击者也可以窃取到合法用户与服务器之间交换的信息。所以，这种方式一般都是用在一些安全性要求很低的场合。

2.2 基于对称密钥技术的认证方式

最典型的应用是 Kerberos 体制。

此类认证方式的基础是双方（用户 A 和用户 B）共享一个对称密钥 K。其原理如图 1 所示。

A 发送消息 N 和消息 M 给 B。其中消息 M 是消息 N 经过对称密钥 K 加密后的结果。

B 接收到来自 A 的消息 N 和 M。B 使用对称密钥解密 K 解密消息 M 得到 N'，然后比较 N' 和 N。如果两者一致，那么 B 可以确认这条消息是来自 A 的。否则，B 对这些消息不作处理。

在身份认证的过程中，A 和 B 可以协商来生成一个临时对称密钥（会晤密钥），使用临时密钥来保证消息的安全性。产生临时密钥需要的参数可以包含在加密的消息

① 国家自然科学基金资助项目（No. 90204017，60372094）

中,这样只有用户 A 和 B 才能产生需要的临时密钥。

另外,为了解决多方认证的难题,还可以增加一个认证服务器作为代理。

但是,这种方式不能解决的难题是电子商务交易中的不可抵赖性。比如 A 发送了一个消息给 B,事后 A 可以否认曾经发送过这样的消息。因为对称密钥是用户 A 和 B 共享的,A 可以声称是 B 自己发送给自己的。

在一个系统中,每一对用户之间都要有一个共享的对称密钥,随着系统用户的数量的增多,需要的密钥数量将会指数性增加。不过为了解决多方认证的难题,还可以增加一个认证服务器作为代理,每一个用户都通过认证服务器来与其他用户进行认证。这样可以显著的减少系统中需要的对称密钥的数量,只需为每个用户分配一个对称密钥。

2.3 基于非对称密钥和数字证书技术的认证方式

此类认证方式使用数字证书和数字签名来验证用户的身份。此类方式又可以分为以下两种:一次认证,多次通信的方式;每次通信都进行认证的方式。其主要缺陷在于应用数字证书的体系很复杂,目前难以实际使用。

3 离线认证模型

从上文的讨论中,我们可以看出当前使用的身份认证的方式都是在线的,也就是客户端需要向服务端提交某种信息,由服务端来完成对用户身份的认证。如果换一种角度思考,是否可以在客户端来完成用户身份的认证工作,只有合法的用户才能使用客户端,这样服务端认为它是与一个可信任的客户端在通信,凡是能够与服务端通信的客户端就是合法的。这种认证方式将客户端和服务端结合成一个整体,只有在客户端完成了用户身份的认证后,客户端才能与服务端进行通信,服务端不再需要对客户端进行认证。其优势在于用户的认证信息不需要在网络上传输,而且客户端可以分担服务器的负担。

我们可以参考当前电话卡市场上的用户身份认证方式。一种是基于传统的用户名和口令方式的,比如 201 电话卡。通信网络对用户身份的认证是在网络服务中心来完成的,用户在电话机上输入自己的卡号和密码,然后这些信息通过电话网传送到网络服务中心,服务中心根据其数据库中的信息来决定这个用户是否合法。这种方式是属于在线认证方式的,但是显然是不太安全的。

国外有一些电话卡采用了智能卡技术,在智能卡设计中使用身份认证算法,对用户身份的认证(也就是对电话卡的认证)是在电话机上完成的。这种认证方式属于客户端认证方式。电话卡通过电话机的认证后,用户就可以使用网络了。这种方式避免了用户信息在网络上传输的安全隐患,是一种离线方式的认证。

这种电话卡是如何实现身份认证呢? 电话机必须能够鉴别出电话卡的身份,也就是说必须保证只有合法的电话卡才能使用电话机。为了达到这种鉴别目的,电话卡和电话机都包含了相同的鉴权算法,对于相同的输入进行特定算法的计算,比较两者的输出是否相同,如果相同证明电话卡是合法的。

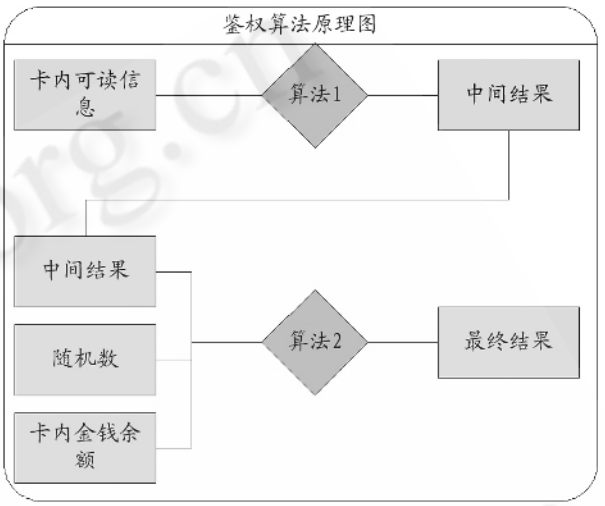

图 2　鉴权算法原理图

电话机为了鉴别电话卡的真伪性,首先根据卡内的一些可读信息作为输入,比如用户的名称,通信地址等,使用算法 1 来生成一个若干 bit 的输出结果(中间结果);然后将这个中间结果、一个随机数和电话卡中的金钱余额作为输入,使用算法 2 进行计算,输出若干 bit 的结果(最终结果)。

电话卡的电路设计需要完成上面类似的操作,不同的是上述的中间结果是在制造智能卡时被预先写入到卡中的,而且这个中间结果是外部不可读的。电话卡只用算法 2 进行的计算,读取卡中预先写入的中间结果,将这个中间结果、一个的随机数和卡内的金钱余额作为输入,计算后得到若干 bit 的输出结果(最终结果)。

这时,电话机比较自己进行计算的最终结果和电话卡计算后的最终结果,如果这两个结果是一致的,那么证明这个电话卡是规定的厂家生产的,而不是假冒的。

其中算法 1 和算法 2 是相互独立的,其功能类似于单向散列函数,与单向散列函数的不同之处在于它们的输入和输出的是固定长度的数据。算法 1 和 2 的特点:输入不同,输出是不同;输入相同,输出是相同的;不可预见的;不可逆的。

电话卡使用智能卡技术来实现,其电路是很难通过解剖硬件来模仿的。而且算法 1 和算法 2 是独立的,对电话卡提

供了双重的保护。只要鉴权算法的设计足够安全,那么电话机对电话卡的认证就是安全的。

使用智能卡技术,身份认证可以在客户端来完成,这就避免了一些用户信息直接在网络上传输的安全隐患。没有通过认证的用户就不能使用客户端,只有合法的用户才能使用客户端来与服务端进行通信。认证通过以后,客户端和服务器对两者之间交互的数据可以使用对称密钥来加密,这样可以保证数据的安全性和完整性。

基于客户端的身份认证模型如图3。

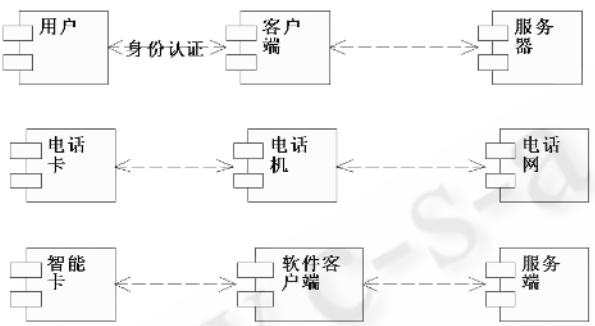

图 3　身份认证模型

4　基于智能卡的离线认证的电子商务应用

在电话卡的应用中,电话卡和电话机分别替代了用户和客户端的角色,电话机对电话卡的认证是通过硬件来实现的,电话机与电话网之间的通信数据是没有经过安全保护的。基于客户端进行身份认证的模型加以扩展后,客户端和服务端之间的数据也可以以安全的方式来传输。

在电子商务应用中,数字证书的使用过于复杂,而且需要一个具有高度权威的机构(CA,Certification Authority)来负责颁发证书。我们的目的在于不使用数字证书和非对称密钥技术,在离线的身份认证基础上开展电子商务应用。

通过使用智能卡,我们设计一套电子商务应用系统来完成用户的身份认证和安全交易。

4.1　体系结构

我们考察电子商务的应用场景,当选择智能卡进行支付时,也可以分为离线支付和在线支付两种方式。

一种方式是离线支付的。用户在商家的网站上浏览商品,发送定单。在商家送货的同时,商家使用专用的读卡设备,对用户的智能卡进行认证,认证通过后,从智能卡的余额中减去货物的金钱数额。

一种方式是在线支付的。用户在商家的网站上浏览商品,发送定单。服务端接收到定单信息后,进行确认,然后发送一个确认定购信息给客户端。客户端接收到确认信息后,先对智能卡中的余额进行减操作,然后返回客户确认信息给服务器。服务器在接收到客户端的确认信息后,明白客户端已经付款了,然后形成发送信息,尽快的将货物发送给客户。当客户接收到商品时,因为商品已经付过款了,这是客户只需要签收即可。这种方式也是很通用,比如想送给朋友或者家人礼物时。

第一种离线支付的模式需要智能卡、读卡设备和普通电子商务网站的配合即可进行操作。

第二种在线支付的模式需要智能卡、客户端软件和特殊的电子商务网站的配合才能进行操作。而这种方式的客户端软件和服务端的设计和实现就比较复杂了,需要满足电子商务的数据安全性、完整性和身份认证的要求。

本文设计了一套系统来完成客户端软件和服务端软件的通信以满足电子商务的安全性要求。在线支付的流程如图4。

4.2　安全性分析

(1) 用户和智能卡之间的相互认证。用户可以通过密码来验证对智能卡的拥有。或者可以通过指纹技术来替代密码。

(2) 智能卡和客户端软件之间的相互认证。一是通过鉴权算法来相互认证。

二是通过客户端软件和智能卡的一一对应来保证。客户端软件在读取卡中一些可读信息进行算法1的计算时,这些可读信息的位置是随机的。在制造商生成智能卡和配套软件时,随机在卡中建立一些目录名称,随机的在这些目录下建立一些文件名称。这样做到智能卡和客户端软件之间是一一对应的,换一个客户端软件或者一张智能卡,客户端软件在读取这些信息时都会出错,从而导致不能通过对智能卡的认证。

这种实现方式将智能卡和客户端软件绑定在一起,跟电话卡相比,在鉴权算法之外,又多了一重的安全性保证。另外,智能卡中存放的对称密钥(2048bit,为了高安全性)的位置也是随机的。

(3) 客户端和服务器的相互认证。服务器接收到客户端的消息,通过判断解密消息后消息的有效性来保证是否从合法的客户端发送的消息。这种消息的有效性格式由发卡厂家自己定义,这样完成了对客户端的认证。

客户端对服务器的认证,也是通过解密消息后消息的有效性验证来保证是从信任的服务器端发送的消息。同时客户端保留了服务器的数字签名,作为服务端的已经接受定单并且扣除客户费用的证据,以便有纠纷时使用。

(4) 通信流程的安全性分析。对称密钥是智能卡和服务端共享的,而且客户端软件只能使用智能卡中的对称密钥进行加解密操作而不能读取密钥的信息。这样保证了所有符合商家消息格式的消息都是从有效的客户端和服务端发送的。

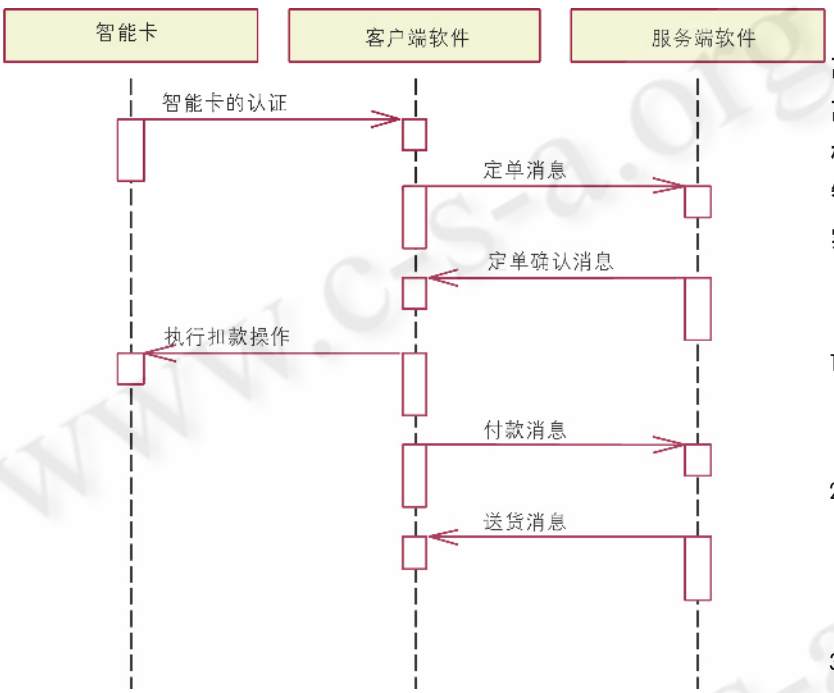

图 4　在线支付流程图

为了防止过期消息的攻击,每次进行一次完整的电子交易流程都会在客户端和服务端生成一对随机数(客户端定单号和服务端定单号),确认消息包含这对随机数来保证当前交易的有效性。

4.3 缺陷

由于客户端没有数字证书,所以没有方法对客户端的信息生成数字签名,因而不能保证服务器不会冒充客户端来进行电子交易。但是,这种预付款的方式就决定了客户是信任服务器的,否则也不会事先把钱交给服务器。在这种假设下,服务器是不会冒充客户端的。

因此,这种缺陷是可以忽略的。

另外本设计方法中,每次使用的加密密钥是同一个。为了提高对已知明文的攻击,可以设计一套协议来生成会晤密钥,这样每次连接时使用的密钥都是变化的。但是,提高对称密钥的长度,或者使用 3 个独立密钥进行 3 重 DES 计算,这样的安全性将维持十年[1]。所以,本方案采用的方式是安全的。

智能卡中的鉴权算法和电子交易中的消息格式是特定的,导致不同发卡厂家之间不能通用。

5 结束语

本文借鉴当前电话卡(智能卡)的一种离线认证的方式,提出了电子商务应用中的离线认证模型。利用智能卡的物理安全性,根据电子商务的支付方式,设计出一种基于智能卡的离线认证和安全通信的电子商务实现方案。

参考文献

1 Bruce Schneier 著,吴世忠等译,应用密码学——协议、算法与 C 源程序,机械工业出版社,2000 年。

2 J. T. Kohl and B. C. Neuman. RFC 1510: The Kerberos Network Authentication Service (V5). IETF Request for Comments 1510. September ,1993。

3 SSL Specifications version 3. 0. April 1996. see: http://www. netscape. com/eng/ssl3/

4 TLS Specifications version 1. 0. January 1999. see: RFC 2246.

5 朱华飞、刘建伟、王新梅、肖国镇, 密码安全杂凑算法的设计与分析, 电子学报,1998 ,26 (1) :126 ~128。

6 李中献、詹榜华、杨义先,认证理论与技术的发展,电子学报,1999 ,27(1) :98 -102。

7 曹鹏、乔秦宝、翁清、王荣,一种使用智能卡的网络身份认证密钥分发体制,武汉大学学报(自然科学版),1998 ,44 (3) :369 -372。

8 刘玉珍、涂航、张焕国、覃中平,实用智能卡操作系统的设计与实现,武汉大学学报(自然科学版),2000 ,46 (3) : 309 -312。