SET 协议的分析与改进措施

武汉大学计算机科学与技术系　陈 凡　许先斌

针对SET安全协议不能担保“非拒绝行为”，没有提及在事后处理及在线商店提供的货物不符合质量标准，消费者提出异议，责任由谁来负等问题，本文提供了一种改进措施。

SET 电子商务交易安全协议的优点及存在的问题

在开放的因特网上处理电子商务，如何保证买卖双方传输数据的安全成为电子商务能否普及的最重要的问题。为了克服SSL(Secure Sockets Layer)安全协议的缺点，两大信用卡组织，Visa 和 Master 联合开发了 SET (Secure Electronic Transaction)电子商务交易安全协议。这是一个为了在因特网上进行在线交易而设立的一个以电子货币为基础的电子付款系统规范。SET 在保留对客户信用卡认证的前提下，又增加了对商家身份的认证，这对需要支付货币的交易来讲是至关重要的。

从1996年4月SET安全协议面市以来得到许多大公司的支持，有良好的发展趋势。但也暴露出一些问题，这些问题包括:

问题一:　协议没有担保“非拒绝行为”，这意味着在线商店没有办法证明订购是不是由签署证书的消费者发出的。

问题二:　SET安全协议没有提及在事务处理后，如何安全地保存或销毁此类数据，是否应当将数据保存在消费者的计算机里，还是应当保存在在线商店或收单银行的计算机里？这种漏洞可能使这些数据以后受到潜在的攻击。

问题三: 协议没有说明收单银行给在线商店付款前，是否必须收到消费者的货物接受证书。否则，在线商店提供的货物不符合质量标准，消费者提出异议，责任由谁来负。

由于以上几个方面的不足，使得许多电子商务网站使用SSL安全协议而没有采用SET安全协议。如上海市长途电信局的电子商务系统采用了如下的安全机制:

在服务器一端上海市长途电信局申请了 Verisign 的认证,使得客户和商务服务器之间可以用SSL方式加密传送，在商务服务器与支付网关之间采用软件加密传送,并设有防火墙。在支付网关收单机构之间用专线方式并用硬件加密。这样,用层层加密的方式来提高网上购物的安全性，目前国外许多电子商务网站都采用这种方式。

SET 安全协议的工作原理流程图分析

在阐述关于SET安全协议修改建议之前，先了解一下SET安全协议的工作原理:

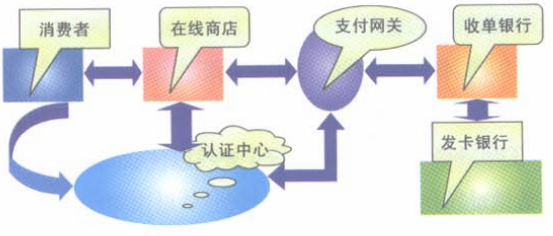

图 1　SET 安全协议的工作原理流程图

SET安全协议的工作原理流程图，分为如下七个步骤:

(1)　消费者利用自己的PC机通过因特网选定所要购买的商品，并在计算机上输入订货单。订货单上需包括在线商店，购买物品名称及数量，交货时间及地点等相关信息。

(2)通过电子商务服务器与有关在线商店联系，在线商店作出回答，告诉消费者所填订货单的货物单价，应付款数，交货方式等信息是否准确，是否有变化。

(3)消费者选择付款方式，确认订单，签发付款指令。此时SET开始介入。

(4)　在SET中，消费者必须对订单和付款指令进行数字签名，同时利用双重签名技术保证商家看不到消费者的帐号信息。

(5)　在线商店接受订单后，向消费者所在的发卡银行请求支付认可。信息通过支付网关到收单银行，再到发卡银行确认。批准交易后，返回确认信息给在线商店。

(6)　在线商店发送订单确认信息给消费者。消费者端软件可纪录较易日志，以备将来查询。

(7)在线商店发送货物或提供服务，并通知收单银行

将钱从消费者的帐号转到商店帐号，或通知发卡银行请求支付。

针对SET安全协议的工作原理流程图中存在问题的改进措施

针对SET安全协议的几点缺陷，我们对SET安全协议的工作原理流进行如下改动：增设一个电子交易认证中心（E_business Transactions CA），电子交易认证中心与传统的认证中心CA的区别如下：电子交易认证中心是构思出来用以确认电子交易有效性的机构，而传统的认证中心（CA）只确认交易双方身份的有效性。

从SET协议中可以看出，由于采用公开密钥加密算法，认证中心(CA)就成为整个系统的安全核心，各种证书均由各级认证权威机构产生、颁布、更新、废除和验证。CA的身份证明服务为使用公钥加密的应用提供了可定制的公钥身份证明发放及管理服务，在经Internet、Intranet以及其他非安全网络进行安全通信时，CA能够扮演这种系统中的中心角色。CA可以根据不同组织应用的需要进行定制。CA自身身份的认证由证书的树形验证结构*来完成。具体地说，CA有证书发放、证书更新、证书撤销和证书验证4大职能。

电子交易认证中心（E_business Transactions CA）也可由传统的认证中心（CA）充当，此处仅按功能划分，电子交易认证中心应具有以下功能：

（1）一旦交易成功，双方不得否认此交易的有效性。

（2）对有效交易加盖时间戳，并在一段时间内加以保存，作为交易有效性的法律证据。任何人不得做丝毫改动。

（3）电子交易认证中心在交易确认成功之前，交易双方发生争执时，有权进行仲裁，即此交易是否应当取消或应当生效。

鉴于以上考虑，电子交易认证中心最好由政府职能部门（如商检局和质量监督局）来担任，这样才能有效的发挥电子交易认证中心的功能。此外，电子交易认证中心自身的身份也应由CA来认证。

首先解决第一个问题，即在线商店如何证明订购是由签署证书的消费者发出的。这一点比较容易解决，可利用数字签名技术，消费者发出订单时使用SHA算法或MD5算法得出数字摘要，将数字摘要用自己的私用密钥加密，形成数字签名，再将原文（包括消费者的身份证号码）和加密后的摘要用在线商店的公用密钥加密，然后传给在线商店。在线商店先用自己的私钥解密，得到原文和加密摘要，再用消费者的身份证号码从认证中心得到消费者的公钥，然后用此公钥对加密摘要解密，即可确认订购是由签署证书的消费者发出的。

改进后的SET安全协议的工作原理流程图如下：

图2　改进后的SET安全协议工作原理流程图

再解决第二个问题，即SET安全协议没有提及在事务处理后，如何安全地保存或销毁此类数据，这时就要引用到电子交易认证中心(E_business Transactions CA)。一旦交易成功，双方不得否认此交易的有效性。电子交易认证中心对有效交易加盖时间戳，并在一段时间内加以保存，作为交易有效性的法律证据。任何人不得做丝毫改动。电子交易认证中心在交易确认成功之前，交易双方发生争执时，有权进行仲裁，即此交易是否应当取消或应当生效。

要解决第三个问题比较复杂，要将SET安全协议的工作原理流程图，重新分为如下几个步骤：

(1) 消费者利用自己的PC机通过因特网选定所要购买的商品，并在计算机上输入订货单。订货单上需包括消费者的身份证号码、在线商店、购买物品名称及数量、交货时间及地点等相关信息，利用数字签名技术等加密后传给在线商店。

(2)通过电子商务服务器与有关在线商店联系，在线商店作出回答，告诉消费者所填订货单的货物单价，应付款数，交货方式，在线商店在收单银行的帐户等信息是否准确，是否有变化。

(3)消费者选择付款方式，确认订单，签发付款指令，利用数字签名技术和数字信封技术等加密后包括消费者的身份证号码、在线商店、购买物品名称及数量、交货时间、货物单价、应付款数、交货方式及地点等相关信息传给电子交易认证中心，电子交易认证中心将此记录在案，但交

易成功标志仍然是未确定，然后将信息传给发卡银行。这样，商家根本看不到消费者的帐号信息。

(4)发卡银行核实消费者有能力付款后，将此笔款项扣下，存入一冻结帐户(为保护消费者的利益，一般要求暂存三天，而不是立即划入在线商店在收单银行的帐户)，然后通知在线商店的收单银行，款项已经扣除，可以交货。

(5)收单银行得到发卡银行的承诺后，即通过支付网关通知在线商店可以交货。

(6)在线商店接受收单银行通知后，即向消费者发送货物或提供服务。以后可能发生两种情况：

①如果三天内，消费者无异议，则在第四天电子交易认证中心自动通知发卡银行将冻结帐户中此笔资金划入在线商店在收单银行的帐户，等发卡银行发回划款成功信息后，将此笔交易记录标志改为确定，交易即告成功，收单银行通知在线商店款项已到位。要求在线商店发送货物或提供服务。如果第四天款项没有到位，在线商店可向电子交易认证中心发询问，由电子交易认证中心仲裁。

②如果三天内，消费者有异议(即在线商店提供的货物不符合质量标准，则向电子交易认证中心和在线商店同时发消息，要求退货和取消此笔交易。电子交易认证中心通知发卡银行推迟三天将冻结帐户中此笔资金划入在线商店在收单银行的帐户，然后等待在线商店的答复，又有三种情况：

· 在线商店同意退货，则电子交易认证中心要求在线商店和消费者共同签名，然后将此共同签名发给发卡银行，发卡银行将冻结帐户中此笔资金划回消费者的帐户，给电子交易认证中心发冲帐成功信息，电子交易认证中心将此笔交易标志置为无效，加盖时间戳，然后给在线商店和消费者发回冲帐成功信息。

· 在线商店不同意退货，此时只能由电子交易认证中心派人进行调查后，进行仲裁。

a. 如果仲裁结果认为在线商店提供的货物的确不符合质量标准，则电子交易认证中心和消费者共同签名后，然后将此共同签名发给发卡银行，发卡银行将冻结帐户中此笔资金划回消费者的帐户，给电子交易认证中心发冲帐成功信息，电子交易认证中心将此笔交易标志置为无效，加盖时间戳，然后给在线商店和消费者发回冲帐成功信息。

b. 如果仲裁结果认为在线商店提供的货物确实符合质量标准。则电子交易认证中心和在线商店共同签名后，然后将此共同签名发给发卡银行，发卡银行将冻结帐户中此笔资金划入在线商店在收单银行的帐户，发卡银行给电子交易认证中心划款成功信息，电子交易认证中心将此笔交易标志置为确认。加盖时间戳，然后给在线商店和消费者发回划款成功信息。

· 如果在线商店不予答复，则电子交易认证中心每隔三天通知发卡银行推迟三天将冻结帐户中此笔资金划入在线商店在收单银行的帐户，直到在线商店答复同意退货或不同意退货为止。然后按(a)(b)两种方式处理。

改进后的SET安全协议的有效性

(1)在线商店通过消费者的数字签名可以确认订购是否由签署证书的消费者发出的。

(2) 通过电子交易认证中心对有效交易加盖时间戳，并在一段时间内加以保存，作为交易有效性的法律证据。可以避免将电子交易记录放在消费者计算机里或在线商店或收单银行的计算机里。可以避免使这些数据以后受到潜在的攻击。如果日后发生纠纷，以电子交易认证中心加盖时间戳的记录为准。

(3)当消费者与在线商店对货物质量或付款等问题发生纠纷时，改进后的SET安全协议即可避免在线商店提供的货物不符合质量标准，又可避免消费者故意不付款。在电子交易认证中心的监督下，即可以保证消费者的利益，又可以保证在线商店的利益。在一笔交易中，在线商店提供一次货物，消费者付一次款，电子交易认证中心对有效交易确认一次。这样，电子商务的三类原子性，即钱原子性(Money Atomicity)、商品原子性(Goods Atomicity)和确认发货原子性(Certified Delivery)都可得到满足。

结束语

在我国市场经济还不发达、各种法制法规还不健全、电子商务刚刚起步、商家信誉普遍不高的情况下，各种不法分子会利用SET协议的缺陷进行欺诈活动。一方面我们要健全法制法规，加大惩处力度，另一方面要完善SET协议本身。本文针对SET协议的一些漏洞进行了改进，对防范电子商务中欺诈行为有一定的实用价值。■

参考文献

1 王育民 刘建伟 通信网的安全,理论与技术 西安电子科技大学出版社 1999

2 扬坚争 扬晨光 罗来兴 马迁 电子商务基础与应用 西安电子科技大学出版社 1998

3 骆小来 电子商务 人民邮电出版社 1999