广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):287~291
Vol. 23,No. 4 November 2007

基于组合设计方法的安全支付协议的设计与验证*
Design and Verification of Secure Payment Protocol Based on Composition Method

李晓乐[1,2],董荣胜[1],吴光伟[1,3]
LI Xiao-le[1,2],DONG Rong-sheng[1],WU Guang-wei[1,3]

(1.桂林电子科技大学计算机学院,广西桂林 541004;2.广西职业技术学院计算机技术系,广西南宁 530226;3.中南林业科技大学计算机科学学院,湖南长沙 410004)
(1. College of Computer Science, Guilin University of Electronic Technology, Guilin, Guangxi, 541004, China; 2. Department of Computer Technology, Guangxi Polytechnic College, Nanning, Guangxi, 530226, China; 3. Department of Computer Science, Central South University of Forestry and Technology, Changsha, Hunan, 410004, China)

摘要:针对银行、商家和客户对电子支付协议提出的11条安全需求,应用组合设计方法设计一个新的安全支付协议,并用SMV工具分析新协议的原子性。新协议满足指定的安全需求和电子商务协议的原子性要求,实现了电子商品和实物商品在线支付的设计目标,适用于多个客户和商家对同时进行交易。

关键词:组合设计方法 协议原语 支付协议 原子性
中图法分类号:TP393 **文献标识码**:A **文章编号**:1002-7378(2007)04-0287-05

Abstract: This paper designs a new secure payment protocol by means of the composition method, and verifies its atomicity by SMV. It will meet the needs of the banks and the customers who propose the eleven requirements for secure payment and can be used for transaction of electronic or physical goods, even for multiple payment between different customers and merchants.

Key words: composition method, protocol primitive, payment protocol, atomicity

电子支付是指单位或个人通过电子终端,直接或间接向银行或其它金融机构发出支付指令,实现货币支付与资金转移,是电子商务活动中的一个重要环节。随着科学技术的高速发展,电子支付的安全性正受到越来越严峻的挑战。安全支付协议是电子商务协议的一种,主要用于确保电子支付安全有效地进行。

本文研究了组合设计方法[1]在安全支付协议设计中的应用,针对银行(B)、商家(M)和客户(C)3个参与方提出的11条安全需求,设计了一个新的安全支付协议。用SMV工具对该协议的原子性进行了分析并验证了其可行性。该协议能满足指定的安全需求,实现了电子商品和实物商品在线支付的设计目标,满足匿名性、隐私性和可追究性,适用于多个客户和商家对同时进行交易。

1 11条安全需求

根据Choi[1]对电子支付过程中每个参与者的安全需求分析,归纳出银行、商家和客户3方对安全支付协议会提出如下安全需求。

(1)银行拥有客户对交易授权的证据,(2)银行拥有商家对交易授权的证据,(3)商家拥有银行对交易授权的证据,(4)商家拥有客户对交易授权的证据,(5)商家拥有客户对商品接收的证据,(6)客户未授权支付不可行,(7)商家拥有银行对交易授权的证据,(8)客户拥有来自商家的收据。

另外,除认证性和保密性外,安全支付协议还应

收稿日期:2007-08-30
作者简介:李晓乐(1982-),男,助教,主要从事网络安全、形式化技术研究。
*广西自然科学基金项目(0542052),广西研究生教育创新计划项目(2007105950812M17)资助。

满足下列安全属性:(9)隐私性(10)匿名性,(11)可追究性。

2 安全支付协议的组合设计

设计过程分为四个阶段:交易协商、客户支付、商品发送和退货处理。

2.1 交易协商

该阶段包括价格协商和品质协商,由于这两个过程类似,可使用同一个设计框架。

交易协商的协议描述如下。

P_1 $C\rightarrow M:\beta_1,\{|RQ,\beta_1|\}_{ekM},auth_{skC}(RQ,\beta_1)$,

$M\rightarrow C:C,\{|DP|\}_{ekC},<c_{MC1}>_{skM}$,

其中 $\beta_1=(C,M)$,$c_{MC1}=(RQ,DP,\beta_1)$,RQ 表示客户发出的协商请求,DP 表示商家回复的描述信息;$auth_{skC}(RQ,\beta_1)$表示使用客户的签名密钥 skC 对协议参数集合(RQ,β_1)进行单向哈希操作;$<c_{MC1}>_{skM}$表示使用商家的签名密钥对协议参数集合(RQ,DP,β_1)进行单向哈希操作。

在交易协商阶段,客户向商家先后提出价格协商和品质协商请求。价格协商请求中包括商品的产品号和身份标识,商家返回商品的报价和一个唯一的交易号 TID;商品品质协商请求发出后,商家返回商品的规格说明 G。交易双方对商品的品质、发送方式以及最迟送货日期等进行协商。价格协商和品质协商可以反复执行,直到客户和商家达成共识。

2.2 客户支付

若交易双方对商品的价格和品质都已达成共识且客户决定进行交易,则进入客户支付阶段。该阶段可划分为两个双方子协议 P_{21}:客户和商家之间;P_{22}:商家和银行之间。

P_{21} $C\rightarrow M:\beta_{21},\{|PA,\beta_{21}|\}_{ekM},auth_{skC}(PA,\beta_{21})$,

$M\rightarrow C:C,\{|PR|\}_{ekC},<c_{MC2}>_{skM}$,

其中 $\beta_{21}=(C,M)$,$c_{MC2}=(PA,PR,\beta_{21})$。协议中添加了 PA 的绑定组 β_{21},既用于确认发送者和接收者的身份并确保一致性测试,又可以在$\{|\beta_{21},PA|\}_{ekM}$中为商家提供客户身份信息,以便选用合适密钥对 PA 解密得到客户付款授权信息,适用于多个客户和商家对并行交易的情况。

P_{22} $M\rightarrow B:\beta_{22},\{|TR,\beta_{22}|\}_{ekB},auth_{skM}(TR,\beta_{22})$,

$B\rightarrow M:M,\{|PR|\}_{ekM},<c_{BM1}>_{skB}$,

其中 $\beta_{22}=(M,B)$,$TR=\{PA,Macct\}_{skM}$,$c_{BM1}=(TR,PR,\beta_{22})$。同理,协议中添加了 TR 的绑定组 β_{22},为银行明确商家的身份并确保一致性测试,适用于银行处理多个商家请求交易的情况。

在 P_{21}中,客户首先向商家发送购物的定单,$PA=\{|G,TExpire,TID,\{PI\}_{ekB}|\}_{skC}$为支付授权,其中的商品规格说明 G、交易时限 Texpire 和交易序号 TID,是商家能够读取的信息;而支付指示 PI 只有银行能够读取。商家收到该支付授权后,检查 PA 中的 G、TExpire 和 TID。若商家认为有问题则可拒绝交易,若无问题则商家在 PA 后附上自己的账号,并对其数字签名后发送给银行。若银行中的电子支付成功,则商家将支付收据 PR 返回客户,包括交易成功与否的标识 Result、交易序号 TID、商品规格说明 G 等。

在 P_{22}中,商家在同意交易的情况下,在 PA 后面附上自己的账号,将其数字签名后发送给银行,向银行发出交易请求 TR。银行收到这个既被客户签名又被商家签名的消息后,检查交易序号 TID 是否唯一,交易时限 TExpire 是否已过期以及客户账户余额是否足够,若确认没有问题则进行转账工作。银行的转账过程按照数据库提交的方式在银行内部原子地进行。交易成功后,银行将支付收据 $PR=\{|Result,TID,G|\}_{skB}$发送给商家,该收据可作为客户已经付款的凭证使用。商家收到该收据后,将收据的一个拷贝发送给客户。若客户未收到此收据,可向银行索取。

为了将 P_{21}和 P_{22}结合在一起,应添加绑定者 $c_{MB1}=(C,M,B,PA,TR)$,其中包含必要的绑定信息。但由于隐私性需求,为保证商家账号不为客户所知,不能直接让客户验证 TR,故令 $c_{MB1}=(PA,<TR>,\beta_2)$,其中<TR>表示对 TR 进行单向哈希操作后得到的结果。

客户支付协议 P_2描述如下。

P_2 $C\rightarrow M:\beta_2,\{|PA,\beta_2|\}_{ekM},auth_{skC}(PA,\beta_2)$,

$M\rightarrow B:\beta_2,\{|TR,\beta_2|\}_{ekB},auth_{skM}(TR,\beta_2),<c_{MB1}>_{skM}$,

$B\rightarrow M:M,\{|PR|\}_{ekM},<c_{BM1}>_{skB}$,

$M\rightarrow C:C,\{|PR|\}_{ekC},<c_{MC2}>_{skM},<c_{MB1}>_{skM}$,

其中 $\beta_2=\beta_{21}\cup\beta_{22}=(C,M,B)$。

2.3 商品发送

根据2.1中的协商结果,商家可以对不同类型的商品采取不同的发送方式。对于实物商品在此不加赘述。对于电子商品,可以采取网络发送的方式,分3个双方子协议实现。

P_{31} M→C:β_{31},{|1,GD,β_{31}|}$_{ekC}$,auth$_{skM}$(1,GD,β_{31}),

C→M:M,{|RA|}$_{ekM}$,<c_{CM1}>$_{skC}$,

P_{32} M→B:β_{32},{|2,MRA,β_{32}|}$_{ekB}$,auth$_{skM}$(2,RA,β_{32}),

B→M:M,{|GR|}$_{ekM}$,<c_{BM2}>$_{skB}$,

P_{33} M→C:β_{33},{|3,GR,β_{33}|}$_{ekC}$,auth$_{skM}$(3,GR,β_{33}),

C→M:M,<c_{CM2}>$_{skB}$,

其中,β_{31}=(M,C),β_{32}=(M,B),β_{33}=(M,C),为保证不同子协议中相同结构的消息项不会互相干扰,使用索引区分不同的原语;GD={DID, TID, {EG}$_{kG}$},包括商品发送序号DID,交易号TID和电子商品EG(EG可能进行加密处理);RA={|DID, TID,CSG|}$_{skC}$,包括商品发送序号DID,交易号TID和加密后商品的密码学校验和CSG;MRA={{|DID,TID,CSG|}$_{skC,kG}$}$_{skM}$,包括RA和商品密钥k_G;GR={DID,TID,k_G,CS({EG}$_{kG}$)}$_{skB}$,包括DID、TID、商品密钥k_G及商品的密码学校验和c_{CM1}=(GD,RA,β_{31}),c_{BM2}=(RA,GR,β_{32}),c_{CM2}=(GR,β_{33})。

P_{31}:商家向客户发送商品并收到客户返回的接收确认RA;P_{32}:商家向银行转发RA并收到银行返回的商品收据GR;P_{33}:商家向客户转发商品收据GR的一个拷贝。若客户未收到,也可以直接向银行索取。

三个子协议需要严格按照先后顺序执行,并采用索引编号的方式将它们简单合并为商品发送协议P_3。

2.4 退货处理

前3个阶段,已经实现了电子商务交易的基本要求。考虑到与传统市场相比,虚拟性的电子商务交易市场有诸多不确定因素,极易发生由于实际物品与订购商品不符而造成的退货[2]。因此,本文特别讨论了安全支付协议中的退货处理问题,在此处引入了一个仲裁方。

若客户认为收到的商品存在问题,例如商品品质与协商结果不符,则可以申请退货处理。分为3个子协议实现。P_{41}:客户向仲裁方发送退货请求及相关商品,后者根据国家和各在线商家的退货标准来确定该商品能否退货,若进行退货,则仲裁方负责将退货后的相应收据发送给客户;P_{42}:仲裁方若认为应该退货,则通知商家将货款退返客户账户,商家完成退款后,将银行出具的转账证明发送给仲裁方;P_{43}:仲裁方将加密后的商品退返商家,商家收到退货后,向仲裁方发送退货收据。

退货处理子协议的设计过程与前面三个过程类似。

2.5 安全支付协议

若忽略协议中与资金、商品及交易证据无关的步骤,抽象后的协议描述如下。

1)C→M:PA;2)M→B:TR;3)B→M:PR;4)M→C:PR;5)M→C:EG;6)C→M:CSG;7)M→B:MCSG;8)B→M:GR;9)M→C:GR。

3 协议的验证

采用SMV分析工具对协议的原子性进行验证。

3.1 协议中消息的数据结构

消息的数据结构记录了消息的发送方、接收方以及消息中的各类数据。定义如下:

```
typedef message struct
    {
      type: {idle, msg1, msg2, msg3, msg4,
msg5,msg6,msg7,msg8,msg9};
      source: {ag _ null, ag _ C, ag _ M, ag _
B};
      dest: {ag _ null, ag _ C, ag _ M, ag _ B};
      msgCM: {null, PA, CSG};
```

——null表示空消息,ag _ null表示消息没有发送方

```
      msgMC: {null, PR, EG, GR};
      msgMB: {null, TR, MCSG};
      msgBM: {null, PR, GR};
    }
```

3.2 协议参与各方的状态转移图

3.2.1 客户方的状态转移图

协议中,客户方的状态转移如图1所示。

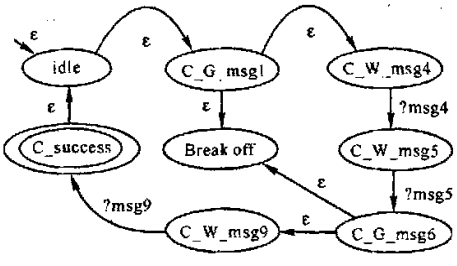

图1 SEP协议中客户方的状态转移

客户在协议开始时处于空闲状态idle,随后转移到C _ G _ msg1状态,并发送消息(付款授权)给

商家。发送该消息后，客户的状态可能因为网络中断而进入 breakoff 状态，或者继续正常地参与协议并转移到状态 C _ W _ msg4状态等待商家的响应消息。如果收到了商家的响应消息(付款收据 RptB)，客户将转移到状态 C _ W _ msg5并等待商家发送商品。同时，设置了一个变量 C _ has _ PR 来记录客户是否获得了这个收据，若客户收到，则 C _ has _ PR =1，否则为0。

客户收到商家发送的商品后，使用变量 C _ has _ M _ EG=1来记录客户已经得到了商家加密后的商品。随后，客户转移到状态 C _ W _ msg9上，并等待商家返回银行的商品收据 GR。收到商品收据后，会将变量 C _ has _ GR 置为1以表示客户收到了该收据。最后，交易成功而客户转移到状态 C _ success。

3.2.2 商家的状态转移图

协议中，商家的状态转移如图2所示

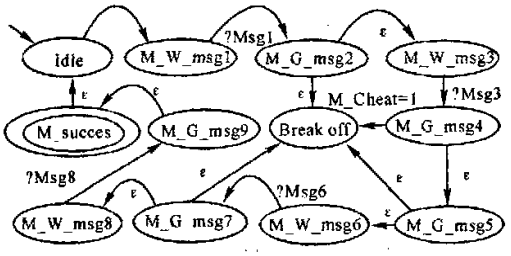

图2 协议中商家的状态转移

协议开始时，商家由 idle 状态自动进入 M _ W _ msg1状态并等待客户的购买请求。在收到客户的付款授权后，商家将其签名并提交给银行，随后进入 M _ W _ msg3状态等待银行的转账结果。收到银行的转账结果后，商家进入状态 M _ G _ msg4，并将付款收据转发给客户。

根据协议，若客户没有收到商家发送的付款收据，则可以直接和银行联系并获得该收据。因此，为了简化模型，假设客户能够得到付款收据 PR，同时还设置了变量 M _ has _ PR 来记录商家是否获得了付款收据 PR。

商家向客户发送了付款收据 PR 之后，如果商家是诚实的，那么他将在收到客户付款之后向客户发送商品；如果商家是不诚实的，那么他可以选择不向客户发送商品，并终止协议。因此，在此处设置变量 M _ Cheat 来表示商家是否诚实。若 M _ Cheat= 1，则表示商家不诚实，此时，商家将中断和客户的联系；否则，商家是诚实的，并向客户发送商品。

如果商家是诚实的，那么商家将进入状态 M _ G _ msg5，并向客户发送电子商品。随后，商家进入状态 M _ W _ msg6并等待客户的响应。在收到客户的响应后，商家将这些信息签名后发送给银行，并进入状态 M _ W _ msg8等待银行的商品收据。在收到银行发送的商品收据 GR 之后，商家将收据的一个拷贝发送给客户，随后交易成功，商家进入 M _ success 状态。此处设置变量 M _ has _ GR 来记录商家是否收到了商品收据。

同样，如果客户没有收到 GR，客户可以直接向银行索取，所以，此处假设客户能够收到商品收据且在发送 GR 的过程中没有出现通信中断。

3.2.3 银行的状态转移图

协议中，银行的状态转移如图3所示。

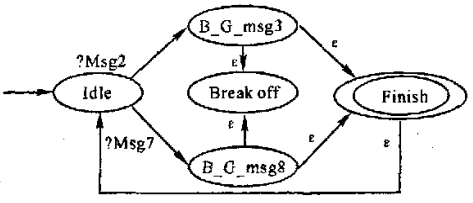

图3 协议中银行的状态转移

在协议开始时，银行处于 Idle 状态并等待商家的请求。如果收到的是交易请求，那么转移到状态 B _ G _ msg3并发送付款收据；如果收到的是商品的发送请求，那么转移到状态 B _ G _ msg8并发送相应的商品收据。然后，银行将进入 Finish 状态表示一个请求已经处理，随后，银行将自动回到 Idle 状态并接收其它的请求。

3.3 协议原子性要求的描述

3.3.1 钱原子性[3]

由于协议中资金的转换是在银行内部原子性提交的，客户账户减少的资金等于商家账户中资金的增加，因此协议满足钱原子性。

3.3.2 商品原子性

客户只有在付款之后才能得到商品，或者是商家只有在发送了商品之后才能得到钱。据此，可以给出以下 CTL 属性描述：

若客户 C 没有付款，则收不到商品。

R0. AG((customer. C _ has _ PR=0)->
(AF customer. state _ customer ~ = C _ success))

若客户 C 付了款，则要么 C 收到商品，要么 C 收不到商品收据，M 也收不到商品收据。

R1. AG((customer. C _ has _ PR=1)->

(AF (customer. state _ customer = C _ success | (customer. state _ customer~=C _ success & merchant. M _ has _ GR=0 & customer. C _ has _ GR=0))))

若商家收到了付款,则要么客户收到商品,要么客户收不到商品且商家收不到商品收据。

R2. AG((merchant. M _ has _ PR=1)->
(AF (customer. state _ customer = C _ success |
(customer. state _ customer~=C _ success & merchant. M _ has _ GR=0))))

3.3.3 确认发送原子性

客户和商家都能证明所发送的商品确实是所期望的。由于商品的内容包含在了商品规格说明 G 中,而这个结果将在商品收据 GR 中给出,因此不需考察如果交易成功,双方是否都会得到凭证。

若商家得到了付款收据 PR 和商品收据 GR,则客户最终也一定能收到 PR、GR 和商品 EG。

R3. AG((merchant. M _ has _ PR=1 & merchant. M _ has _ GR=1) ->
(AF (customer. C _ has _ PR = 1 & customer. C _ has _ GR=1 &
customer. C _ has _ EG=1)))

若客户收到了付款收据 PR 和商品收据 GR 及商品 EG,则商家最终也一定能收到了 PR 和 GR。

R4. AG((customer. C _ has _ GR=1 & customer. C _ has _ PR=1 &
customer. C _ has _ EG=1) ->
(AF (merchant. M _ has _ PR = 1 & merchant. M _ has _ GR=1)))

3.4 运行结果

将交易三方的状态转移图以及协议规格说明写入 SMV 程序中并验证,结果表明协议的5条属性都能满足,本文所提出的安全支付协议满足电子商务协议的原子性需求。

4 结束语

本文研究了组合设计方法在安全支付协议设计中的应用,根据 Choi 对电子支付过程中每个参与者的安全需求分析,归纳得到了针对银行、商家和客户三方的11条安全需求,设计了一个新的安全支付协议,分析表明,该协议满足指定的安全需求,实现了电子商品和实物商品在线支付的设计目标,满足匿名性、隐私性和可追究性,适用于多个客户和商家对同时交易的情况;最后使用 SMV 工具对协议的原子性进行了分析并验证了其可行性。

分析组合设计方法,我们发现原语中对协议的规格虽然比较全面和直观,但是非常繁琐且容易出错,尤其是使用该方法得到的协议通常不是最优的[1]。因此,在未来的研究中,应从消息的精炼和优化[4]着手,确保协议设计的高效性。

参考文献:

[1] CHOI HYUN-JIN. Security protocol design by composition [D]. Cambridge, United Kingdom: University of Cambridge, 2006.

[2] 周龙骧. 电子商务协议研究综述[J]. 软件学报, 2001, 12(7): 1015-1031.

[3] TYGAR J D. Atomicity in electronic commerce: proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing[C]. Philadelphia, USA: ACM Press, 1996: 8-26.

[4] DATTA A, DEREK A, MITCHELL J C, PAVLOVIC D. A derivation system for security protocols and its logical formalization: proceedings of the 16th Computer Security Foundation Workshop [C]. Asilomar, USA: IEEE Computer Society Press, 2003: 109-125.

(责任编辑:尹 闯)

美国研究显示一种降脂药物可改善中风患者肾功能

参与强化降低胆固醇预防脑卒中(SPARCL)项目的美国研究人员在研究中发现,一种名为阿托伐他汀的降脂药物,能稳定或改善卒中(俗称"中风")或轻微卒中患者的肾功能。与服用安慰剂的患者相比,服用了80mg 阿托伐他汀的中风或轻微中风患者,无论原先是否患有慢性肾病、代谢综合征或者Ⅱ型糖尿病,其肾功能都得到了显著改善。患有慢性肾病等疾病的卒中患者发生其他心血管事件的风险往往更高。研究人员的新研究表明,与服用安慰剂的患者相比,服用阿托伐他汀的慢性肾病患者发生心血管死亡等主要冠脉事件的风险可降低39%。此外,参与另一项大规模临床试验的研究人员对近8900名以往有心肌梗死病史的患者进行了研究。结果发现,这些患者在服用了阿托伐他汀80mg 片剂后,再发心血管事件的风险大大降低。

(据科学网)