在NetBill交易协议中引入对商家的时限责任的追究*)

彭 勋 董荣胜 郭云川 蔡国永
(桂林电子工业学院计算机系 桂林541004)

摘 要 NetBill电子交易系统是一个用于网上信息商品以及可通过网络发送的服务的微交易系统。本文从时限责任的角度指出了NetBill交易协议中存在的一种商家欺骗行为,并通过在NetBill交易协议中引入受信任的时间戳服务器的方法,使得修改后的NetBill交易协议能够支持对商家的时限责任的追究。最后本文采用时限逻辑证明了修改后的NetBill协议满足期望的时限属性。

关键词 NetBill协议,时限责任,时间戳服务器

Introducing Temporal Accountability to the Merchant in the NetBill Transaction Protocol

PENG Xun DONG Rong-Sheng GUO Chuan CAI Guo-Yong
(School of Computer Science, Guilin University of Electronic Technology, Guilin, 541004)

Abstract NetBill is a micropayment system for information goods and services on the Internet. This paper points out a merchant fraud in the NetBill protocol from the temporal accountability view, and fixs the problem by introducing a timestamp server into the NetBill system. By using a temporal logic, this paper also proves that the modified NetBill system has the ability to hold the merchant's temporal accountability.

Keywords NetBill protocol, Temporal accountability, Timestamp server

1 引言

电子商务协议需要满足一定的安全特性。对于一类协议的运行被加上了时间限制的电子商务协议而言,要满足的一个重要特性是时限性。时限性是指协议中各个主体的行为必须在规定的时间范围内完成,而对于违反了时限要求的主体行为,这类协议都应能够追究该主体的时限责任。

1993年,Syverson[9]首先在BAN逻辑[10]中引入了时态公式,并能对认证协议的因果一致性攻击进行有效的分析,然而以AT逻辑[11]作为语义模型的Syverson逻辑体系较为复杂,难于操作。同时由于AT逻辑是BAN逻辑的扩展,它不能有效地分析电子商务协议中的责任性问题。1998年,Kudo[12]在Kailar逻辑的基础上引入了时态公式和相应的假设,提出了时限责任的问题。2002年,梁坚等人[7]指出Kudo提出的逻辑在分析时没有加入对消息新鲜与否的判断,导致了Kudo逻辑不能分析发生消息重放时各方的时限责任,为此提出了一种新的时限逻辑系统。该逻辑系统在Kailar逻辑的基础上加入了4条时态公式和相应的2条推理规则。

本文从时限责任的角度对NetBill交易协议进行分析,发现该协议中存在一种可能的商家欺骗行为,并对该协议进行了修改,同时采用时限逻辑给出了修改后NetBill协议中商家的时限责任的可追究性证明。

本文第2节介绍NetBill协议并指出该协议中存在的一种商家欺骗行为;第3节对原有协议进行修改;第4节对修改后NetBill协议中商家的时限责任进行证明。

2 NetBill协议简介

NetBill是由J.D.Tygar和他的同事在1995年提出的一个电子商务交易系统[1,2],它是一个用于网上信息商品以及可通过网络发送的服务的微交易(micropayment)系统。该交易协议包含3方:客户、商家和NetBill交易服务器。一个交易过程包含3个步骤:价格协商、商品发送和付款。对于可通过网络发送的信息商品,NetBill协议将商品发送和付款链接为一个单一的原子交易。

NetBill交易中,在前两个阶段只有客户和商家相互通信。在交易的第3个阶段,用户决定购买商品并准备付款时,NetBill服务器才介入并处理商家提交的交易请求。在整个交易过程中,客户不会和NetBill服务器直接通信。客户只在通信失败或者是需要管理功能的情况下才直接和NetBill服务器联系。各方的通信如图1所示。

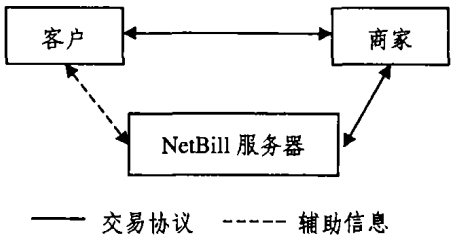

图1 NetBill交易中参与方之间的通信

2.1 NetBill交易协议的目标

1)只有被授权的客户才能从NetBill帐户中提款;

2)客户和商家必须同意要购买的商品和要收取的费用;

3)客户能够选择保护她(本文用"她"代替弱势客户,用"他"代替商家)的身份不让商家知道;

4)客户和商家都保留有从NetBill服务器得到的交易结果的证明;

*)本文得到广西自然科学基金(0229051)的资助。彭 勋 硕士研究生,研究方向:网络安全,形式化技术。董荣胜 副教授,主要研究领域:形式化技术,计算机学科认知理论。郭云川 讲师,主要研究领域:网络安全,形式化技术。蔡国永 副教授,主要研究领域:实时系统,面向对象软件工程,协议验证技术。

5)在客户和商家之间有一个协商过程;

6)客户可以提供证书来说明她有权享有特殊的定价或待遇;

7)客户只有在对商品付款后才能收到信息商品;

8)在 NetBill 服务器进行一次交易前,客户可能需要得到某个第四方的允许;

9)通信的隐私性和完整性不会被参与交易的其他方所观察或修改。

2.2 NetBill 交易协议

本文使用符号"$X \Rightarrow Y$"表示 X 发送指定的消息给 Y。基本的交易协议包含8个步骤:

1)$C \Rightarrow M$ Price request

2)$M \Rightarrow C$ Price quote

3)$C \Rightarrow M$ Goods request

4)$M \Rightarrow C$ Goods, encrypted with a key K

5)$C \Rightarrow M$ Signed Electronic Payment Order

6)$M \Rightarrow N$ Endorsed EPO (including K)

7)$N \Rightarrow M$ Signed result (including K)

8)$M \Rightarrow C$ Signed result (including K)

2.2.1 *价格协商* 在 NetBill 交易协议中,客户和商家之间的价格协商过程发生在协议的前两步。首先客户向商家发送一个价格请求,请求中包含了客户的身份标识(可能是用户的假名)、客户对商品的出价以及交易号 *TID* 等。商家随后向用户返回标价,这个消息中包含了产品号(*ProductID*)、商品的价格和交易号 *TID*。其中,交易号 *TID* 是一个可选项,客户和商家可以使用这个交易号对商品的价格进行反复的协商直到双方满意为止。

2.2.2 *商品发送* 交易协议中的第2和第3步是商家发送电子商品的阶段。客户和商家对商品的价格达成一致后,客户向商家发送商品请求。在接到客户的这个请求后,商家向客户发送用商品密钥 E_K(采用对称密钥机制)加密了的电子商品以及由商家产生的一个唯一的电子定单序号 *EPOID*。

2.2.3 *付款* 客户收到商家发送的已加密的电子商品后,客户就开始决定是否进行交易。如果客户不希望继续交易,那么在这一步她可以安全地终止交易,她的利益不会受到任何损害;如果客户决定继续交易,那么她将不能再终止协议的继续进行。

如果客户决定继续交易,那么她将签名一个电子支付定单 EPO。EPO 包含有两个部分的内容,其中一部分是公开的信息,包括用户的身份标识(可能是假名)、商家的身份标识、产品号、价格、*EPOID*、对收到的电子商品的密码学校验和以及对商品请求数据的密码学校验和等,公开的部分商家和服务器都能够读取;另一部分是加密的,该部分包含客户的帐户信息和真实身份等内容,只有 *NetBill* 服务器才能够读取。整个 *EPO* 的内容如下。

EPO 的公开部分包括:1)客户的身份标识(可能是假名);2)可读的产品号(从第2步得来的);3)协商的价格(从第2步得来的);4)商家的身份标识;5)已加密了的商品的密码学校验和;6)产品请求数据(从第1步得来的)的密码学校验和;7)客户的帐号以及一个帐户验证临时值的密码学校验和;8)全局唯一的 *EPOID*。

EPO 中加密的部分包括:

1)证明客户真正身份的票据;2)任何需要的认证代币;3)客户的 NetBill 帐号;4)帐户验证临时值;5)客户的备注字段。

用户将构造好的 EPO 数字签名之后发送给商家。

商家收到客户的电子定单 EPO 后,对定单中的公开部分进行检查,并确认 *EPOID*、产品号、商品的价格以及客户收到的电子商品的密码学校验和等信息是否与自身的记录相符。在这一步,商家可以安全地终止交易,他的利益也不会受到任何损害。如果商家决定继续交易,那么他将不能再终止交易的继续进行。

如果商家决定继续交易,商家将在客户的 EPO 后面附上商家的 NetBill 帐号、商家的注释以及商品密钥 K,随后商家对此消息进行数字签名并将交易提交给 NetBill 服务器。

NetBill 服务器收到商家提交的交易请求后,将检查交易的序号 *EPOID* 是否有重复、交易客户的帐户余额是否足够等信息,并决定是否进行交易。如果交易成功,商家把交易的结果发送给商家,这个结果将作为交易的收据。收据的内容如下:

Result, *Identity*, *Price*, *ProductID*, *M*, *K*, *EPOID*

其中 *Result* 为交易结果代码,*Identity* 为客户的身份标识(可能为客户的假名),*Price* 为商品的价格,*ProductID* 为交易的商品号,*M* 为商家的身份标识,*K* 为商品密钥,*EPOID* 为此次交易的电子定单号。

这个收据包含了交易过程中的有用信息,它可作为商家和客户在争论中的凭证使用。商家在收到服务器的这个收据后,将这个收据的一个拷贝转发给客户。如果客户没有收到商家发送的收据,她可以直接向银行索取。

2.3 NetBill 协议的特点

NetBill 交易协议满足电子商务的原子性要求。电子商务中的原子性概念是由 Tygar 提出的[3]。Tygar 认为电子商务协议应该满足3类原子性的要求,即钱原子性、商品原子性和确认发送原子性。

钱原子性(Money Atomicity):钱既不能被创生,也不能被销毁。客户支付的钱等于商家收到的钱。

商品原子性(Goods Atomicity):客户只有付款后才能收到商品;同理,商家只有发送了商品后才能收到付款。

确认发送原子性(Certified Delivery):客户能够确认商家所发送的商品正是她所订购的,商家也能够证明客户所声称的商品正是商家所发送的。

交易协议满足原子性可以解决交易过程中的很多问题,同时为交易结束后各方之间的争论提供了不可否认的证据。

NetBill 交易协议还提供了构造客户假名的机制,这种机制能够保护客户的真实身份,从而能够保护客户的隐私(如购物习惯和购买数量等信息)。另外,NetBill 交易协议还提供了一种使得客户能够证明自己在组中的成员关系的证书机制,这使得 NetBill 交易协议能够支持商家的打折(例如,若商家对客户采取会员制的管理策略,那么对于不同等级的会员,商家会提供商品不同程度的打折服务)。

NetBill 交易协议还具有其他一些特性,本文就不再一一列举。

2.4 NetBill 交易协议存在的问题

不少研究者从安全性和原子性角度对 NetBill 协议进行了细致的分析[4~6,13]。本文将从时限约束的角度分析 NetBill 交易协议中存在的一种缺陷。

下面举个简单的例子来说明 NetBill 电子交易协议中存在的一个问题。

假设商家 M 决定在时间期限$\{T_s, T_e\}$范围内对所有的购物客户实施打折的优惠。这时,如果有某位客户 C 在接近于 T_e 的时刻 T_c 提出了购物请求,那么商家会怎么处理呢?这时商家有3种选择:

1)接受购物请求并为客户实施打折优惠;2)拒不接受客

户的购物请求;3)接受购物请求,但是将交易的提交时间推迟到 T_e 之后,从而可以不给客户打折优惠。

如果商家拒绝客户的购物请求,那么商家虽然不会受到利益上的损失,但可能会对商家的信誉产生负面的影响。如果商家采用第3种做法,则商家可以在事后向客户解释成网络故障造成了消息传输的延迟,从而使得客户的购物请求超过了打折优惠的期限。客户对此没有任何证据,而商家的名誉也不会受到影响。

解决该问题的一个方法是在付款阶段中引入商家的时限责任。时限责任要求参与者的行为必须在规定的时间范围内完成,若违反了时限要求,协议可以追究参与者的时限责任(temporal accountability)。

3 在 NetBill 协议中引入对商家的时限责任追究

3.1 时限责任

对于一些电子商务协议,如电子投递和电子定单协议,协议的运行被加上了时间限制以确保协议各方在规定的时间范围内完成某项事务或者是阶段性的事务处理。时限责任就是要求这类协议在参与协议的主体违反了时限要求的情况下能够追究该主体的时限责任。

3.2 在 NetBill 交易协议中引入时限责任

通过分析 NetBill 交易协议的交易过程,可以发现交易真正提交的阶段是从客户发送消息5提交付款开始的。在这之前的价格协商和商品发送阶段中,由于交易双方可能对价格有多次的协商,电子商品的传送时间可能较长,而且商家和客户都可以随时终止交易而不会对双方的利益造成任何负面影响,因此在交易协议的前面4个步骤中,没有必要引入交易双方的时限责任。

在 NetBill 交易协议的第5步中,如果客户决定进行交易,那么该客户将不能再终止协议的进行,而商家可以终止协议的最后期限是在收到客户的电子定单之后,因此在协议的第5步也没有必要对客户引入时限约束。

由于商家是在客户提交 EPO 后才决定是否继续进行交易的,此时客户已无权再终止协议的进行,为了防止发生2.4节中商家的不诚实行为,这一步将引入商家的时限责任:要求商家在规定的时间范围内处理客户的购物请求,如果超过了时限将追究商家的时限责任。

由于 NetBill 服务器是受到交易各方信任的,因此不对服务器引入时限责任。

3.3 对 NetBill 交易协议过程的改进

为了在 NetBill 交易协议过程中引入商家的时限责任。可以在 NetBill 交易协议的过程中引入受信任的时间戳服务器 T。参与协议的各方(C,M 和 N)都相信 T 所产生的时间是正确的,同时还假设时间戳服务器 T 处理消息的时间、和商家 M 与 NetBill 服务器的通信时间都可以忽略不计。这样处理后,可将协议原有的消息交换过程改为图3,同时也给出协议原有的消息交换过程(图2)以便比较。

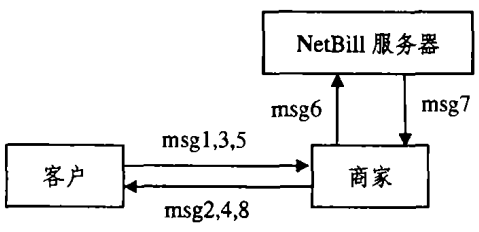

图2 NetBill 电子交易协议的消息交换过程

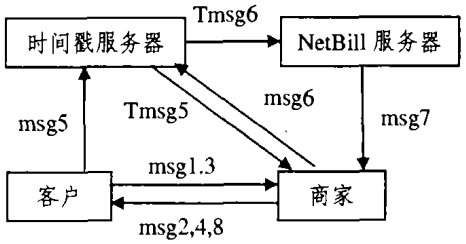

图3 修改后的 NetBill 电子交易协议的消息交换过程

图2中的消息 $Tmsg5$ 表示时间戳服务器 T 在收到客户的购买请求 $msg5$ 后,先将其加盖时间戳,然后再转发给商家。商家在提交交易时,先将提交请求 $msg6$ 发送给时间戳服务器 T,时间戳服务器在加盖时间戳之后,再将消息 $Tmsg6$ 转发给 NetBill 服务器。

由于 NetBill 服务器是受信任的,本文假设 NetBill 服务器会及时地发送交易的收据信息,服务器发出的消息 msg7也没有加盖时间戳。

修改后协议的步骤如下:

1) $C \Rightarrow M$ Price request

2) $M \Rightarrow C$ Price quote

3) $C \Rightarrow M$ Goods request

4) $M \Rightarrow C$ Goods, encrypted with a key K

5) $C \Rightarrow T$ {Signed Electronic Payment Order, $M\}K_T$

6) $T \Rightarrow M$: {Signed Electronic Payment Order, $T_1\}K_T^{-1}$

7) $M \Rightarrow T$ {Endorsed EPO (including K, and T_1), $N\}K_T$

8) $T \Rightarrow N$ {Endorsed EPO (including K, and T_1), $T_2\}K_T^{-1}$

9) $N \Rightarrow M$ Signed result (including K, T_1 and T_2)

10) $M \Rightarrow C$ Signed result (including K, T_1 and T_2)

为了使客户可以得知交易的提交时间间隔,可以在 NetBill 服务器发送的收据中包含由时间戳服务器提供的时间 T_1 和 T_2。

4 修改后的 NetBill 协议的时限责任分析

4.1 时限逻辑

文[7]提出的时限逻辑是在 Kailar 逻辑的基础上扩展而来的。下面先介绍 Kailar 逻辑,然后介绍文[7]提出的时限逻辑。

Kailar 逻辑[8]是 Kailar 提出的一种对电子商务责任性进行形式化逻辑证明的方法。其基本概念是责任性,下面给出 Kailar 逻辑的符号、语法和语义。

A、B 为参与协议的各个主体;K 是密钥,Ka 为主体 A 的公钥,Ka^{-1} 表示与 Ka 相对应的 A 的私钥;K 表示会话密钥,K_{ab} 表示 A 和 B 之间的共享密钥;m 表示消息。TTP 为可信任第三方。

Kailar 逻辑的公式如下:

A CanProve x:表示 A 可以向任何主体证明公式 x 是正确的,而不泄漏任何其他秘密 $y(y \neq x)$ 给其他主体,则将这种证明叫强证明;

A CanProve x to B:表示 A 可以向 B 证明 x,而不泄漏任何其他秘密 $y(y \neq x)$ 给其他主体,则将这种证明叫弱证明;

A IsTrustedOn x:表示任何主体都相信 A 给出的公式 x 是可信的;

A IsTrustedOn x by B:表示 B 认为 A 给出的 x 是可信的,或者说 A 可以向 B 证明 A 能对 x 负责;

Ka Authenticates A:表示可以通过公钥 Ka 来认证 A 的身份;

x in m:表示 x 蕴含在消息 m 中;

A Says x:表示 A 说过 x(因而 A 对 x 负有责任);

A Receives m Signed With K^{-1}:表示 A 收到了用 K^{-1} 签名的消息 m;

$x \Rightarrow y$:表示 x 蕴含 y,即若 x 成立,则有 y 成立;

$x \wedge y$:表示 x 并且 y。

Kailar 逻辑的基本规则:

K_1:

A CanProve x;

A CanProve y

$\Rightarrow A$ CanProve $(x \wedge y)$.

连接规则,即 A 能够证明公式 x,并且 A 能够证明公式 y,那么 A 就能够证明公式 $x \wedge y$;

K_2:

A CanProve x;

$x \Rightarrow y$;

$\Rightarrow A$ CanProve y.

推理规则,即 A 能证明 x,x 蕴涵 y,那么 A 能够证明 y;

K_3:

A Believes $x \Leftrightarrow A$ CanProve x to A 信仰关系,即 A 相信 x,当且仅当 A 能向自己证明 x 成立;

K_4:

A Receives (m SignedWith K^{-1});

x in m;

A CanProve (K Authenticates B)

$\Rightarrow A$ CanProve (B Says x)

签名规则,即 A 收到用私钥 K^{-1} 签名的消息 m,m 中包含了 x,并且 A 能够证明公钥 K 能够验证 B 的身份,那么 A 就能够证明 B 对公式 x 负责;

K_5:

A CanProve (B Says x);

A CanProve (B IsTrustedOn x);

$\Rightarrow A$ CanProve x

信任规则,即 A 能够证明 B 声明了公式 x,并且 A 能够证明 B 对 x 具有管辖权,那么 A 能够证明 x。

2002年,梁坚等人在 Kailar 逻辑的基础上加入了4条时态公式和2条推理规则,并将 Kailar 逻辑扩展如下:

增加的4条时态公式为:

1)x At t:在时间 t 发生了 x,x 为任意公式。如 A Says x At t 等。

2)x TimestampedWith t:对 x 打上时间标记 t。

3)x FreshstampedWith n:x 打上新鲜标记 n,在某些协议中,时间标记同时也作为新鲜性的标志。

4)x Freshbefore t:x 在时间 t 之前是新鲜的(包含 t 时刻),即 x 在时刻 t 以前是唯一的。

增加的推理规则如下:

$K7$ 新鲜性规则

A CanProve (x FreshstampedWith n SignedWith K^{-1});

A CanProve (x TimestampedWith t SignedWith K^{-1});

A CanProve(K Authenticates TTP);

A CanProve(TTP IsTrustedOn t);

$\Rightarrow A$ CanProve (x Freshbefore t)

$K8$ 时限规则

A Receives (x TimestampedWith t SignedWith K^{-1});

(x in y)Signed With K_b^{-1};

A CanProve (x Freshbefore t);

A CanProve (K_b Authenticates B);

A CanProve (K Authenticates TTP);

A CanProve (TTP IsTrustedOn T);

$\Rightarrow A$ CanProve (B Says y At t)

4.2 商家时限责任的证明

使用时限逻辑来分析协议共有4个步骤:1)列举协议要达到的目标;2)将协议步骤解释成逻辑公式;3)列举协议的初始化假设,这些假设是分析中需要用到的;4)对协议进行分析。

由于只对商家引入时限责任的追究,分析的部分仅涉及修改后协议的第5到第9步。

4.2.1 *协议要达到的时限责任目标* 修改后协议的要满足的目标是:

$G1$: N CanProve (M Submit during T_p)

其中 N 表示 NetBill 服务器,M 表示商家,而 T_p 表示 M 收到来自时间戳服务器 T 的客户请求时刻到提交交易给 NetBill 服务器时刻之间的时间间隔。

这个目标表示的含义是:NetBill 服务器能够证明商家 M 在时间间隔 T_p 内提交了客户的交易请求。为便于分析,修改后协议的第6步到第8步的时间区间可用图4表示。

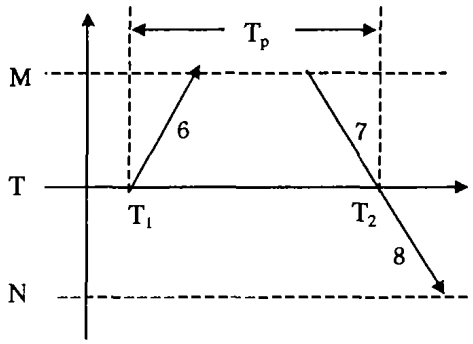

图4

4.2.2 *协议步骤的逻辑描述* 修改后的交易协议的第5步到第9步描述如下:($M5$, $M6$, …, $M9$分别指代协议中的消息)

5)T Receives ($M5$ SignedWith K_C^{-1})

6) M Receives $M6$ TimestampedWith T_1 SignedWith K_M^{-1}

7)T Receives ($M7$ SignedWith K_M^{-1})

8) N Receives $M8$ TimestampedWith T_2 SignedWith K_T^{-1}

9)M Receives (Receipt SignedWith K_N^{-1})

4.2.3 *协议的初始化假设* 协议的初始化假设如下:(A 表示商家 M 或 NetBill 服务器 N)

$A1$: C,M,N CanProve (T IsTrustedOn T_1, T_2)
$A2$: K_C Authenticates C
$A3$: K_M Authenticates M
$A4$: K_N Authenticates N
$A5$: K_T Authenticates T
$A6$: N CanProve (M Recives $M6$ At T_1)
N CanProve (N Receives $M8$ At T_2)
$\Rightarrow N$ CanProve (M Submit during T_p)

$A7$: A Receives x TimestampedWith t SignedWith K_T^{-1}
K_T Authenticates T
A CanProve (T IsTrustedOn t)
⇒A CanProve (A Receives x At t)

$A8$: M CanProve (M Receives x At t)
x in m
N CanProve(N Receives m SignedWith K_M^{-1})
K_M Authenticates M
⇒N CanProve (M Receives x At t)

4.2.4 协议目标的证明 由 M Receives $M6$ TimestampedWith T_1 SignedWith K_T^{-1}

$A5$, $A1$ $\{A7\}$⇒M CanProve (M Receives $M6$ At T_1)

由 N Receives $M8$ TimestampedWith T_2 SignedWith K_T^{-1}

$A5$, $A1$ $\{A7\}$
⇒N CanProve (N Receives $M8$ At T_2)
($M7$ SignedWith K_M^{-1})in $M8$
$M6$ in $M7$
M CanProve (M Receives $M6$ At T_1)
$A3$ $\{A8\}$
⇒N CanProve (M Receives $M6$ At T_1)
⇒N CanProve (M Submit during T_p)

参考文献

1 Sirbu M, Tygar J D. NetBill: an internet commerce system optimized for network delivered services [J]. IEEE Personal Communications, 1995, 2(4): 34～39
2 Cox B, Tygar J D, Sirbu M. NetBill Security and Transaction Protocol. In: Proc. of the First USENIX Workshop on Electronic Commerce, July 1995. 77～88
3 Tygar J D. Atomicity in Electronic Commerce, ACM-Mixed Media, April 1998
4 Heintze N, Tygar J D, Wing J, Wong H C. Model checking electronic commerce protocols. In: Proc. USENIX 1996 Workshop on Electronic Commerce, Nov. 1996
5 Lichota R W, Hammonds G L, Brackin S H. Verifying Cryptographic Protocols for Electronic Commerce. In: Proc. of the 2nd USENIX Workshop on Electronic Commerce, 1996. 53～65
6 郭云川,古天龙,董荣胜,蔡国永. NetBill 协议原子性的符号模型检验分析. 计算机工程与应用,2003,39
7 梁坚, 敖青云, 尤晋元. 安全协议的时限责任分析. 电子学报, 2002,30(10):1450～1454
8 Kailar R. Accountability in electronic commerce protocols [J]. IEEE Trans. on Software Engineering, 1996, 22(5): 313～328
9 Syverson P. Adding time to a logic of authentication [A]. In: Proc. of the 1st ACM Conf. on Computer and Communications Security [C]. Fair-fax: ACM, 1993. 97～101
10 Burrows M, Abadi M, Needham R M. A logic of authentication. Report. 39[R]. Palo Alto, CA: DEC System Research Center, 1989
11 Abadi M, Tuttle M R. A semantics for a logic of authentication [A]. In: Proc. of the 10th Annual ACM Symposium on Principles of Distributed Computing [C]. 1991. 201～216
12 Kudo M. Electronic submission protocol based on temporal accountability [A]. In: Proc. of 14th Annual Computer Security Application Conf. [C]. Phoenix: ACSA, 1998. 353～363
13 Papa M, Bremer O, Hale J, Shenoi S. Formal Analysis of E-Commerce Protocols. In: Proc. of the 5th Intl. Symposium on Autonomous Decentralized Systems. 2001. 19～28

(上接第75页)

用户。而且,由于 I_u 的椭圆曲线离散对数 x_u 是难解的,对用户进行非法攻击从而伪造签名是不可能的。但如果用户丢失电子现金并试图进行恢复时,他必须向银行公开其身份信息,另外,除非用户实施了重复花费,用户身份将不可能被追踪。

本系统能够有效地防止欺诈行为和高手段犯罪。一是如果用户向银行伪报失。虽然系统不能预防此类现象的发生,但当用户恢复得到电子现金时,原有的电子现金因为被列入黑名单而失效。二是商店可能持有用户的电子现金,直到用户丢失其电子现金后他才将其存入银行。表面看来,用户挂失时可能会取得比其丢失数额更大的电子现金。但事实并非如此,若商店迟迟不将电子现金存入银行,银行将拒绝接受,因为它们已经被列入了黑名单。三是对高手段犯罪的预防。高手段的犯罪是电子支付领域出现的一个新问题,由于电子现金的持有者可能被绑架或杀害,犯罪分子将会使用受害人的电子现金。当犯罪分子胁迫用户将电子现金从银行中取出并企图进行花费时,用户可以向银行挂失,通过将这些被盗电子现金列入黑名单且广播告知所有商店,商店都将不会再接收已经失效了的电子现金。

与基于 RSA 和离散对数问题的电子支付系统(如 Okamoto[4]和 Chan[1]提出的电子现金支付系统)相比,本文所提出的可恢复离线电子支付系统由于采用了椭圆曲线密码体制,故所需的安全参数字节较短且易于扩展,在占有较小系统空间的情况下仍能达到与使用模指数运算等其他系统相同的安全水平,因而存储、计算和通信效率大大提高。如 RSA 加密体制进行模指数运算时需要1024比特的密钥,在 ECC 中若要达到相同要求则只需160比特即可。因此 ECC 中密钥的长度较短,内存空间和计算能力都可以降低,尤其适用于存储容量有限的基于智能卡的电子钱包。而且在提取协议中,可以采用将 $a=lB=(R_x(a),R_y(a))$, $M=lP_B+dI_u$, $e'=H(R_x(M)\|R_y(M)$, $R_x(a)\|R_y(a)$和 $\sigma=l-x_ue'$等运算进行前置处理的方法来提高在线处理速度,以减小银行执行取款协议时的计算和通信开销。

结论 本文设计了一个基于 ECC 的高效可恢复离线电子现金系统。与传统的基于效率不高的模指数运算的电子支付系统相比,ECC 具有密钥长度较短和安全性更高的特点,从而使得本系统的存储、计算和通信效率大大地提高。而且用户在丢失电子现金后,通过向银行挂失,并与其执行恢复协议,仍然可以继续使用剩余的未花费的电子现金,而不必向 TTP 公开自己的身份信息。此外,本系统还能有效地防止重复花费、窃听、篡改、非法攻击和犯罪。

参考文献

1 Chan A, Frankel Y. Easy come-easy go divisible cash. In Advances in Cryptology - Eurocrypt 98, LNCS, Springer-Verlag, 1998. 561～575
2 Brand S. Untraceable Off-line Cash in Wallet with Observers. In Advances in Cryptology - Crypto 93, LNCS, Springer-Verlag, 1994. 302～318
3 Chaum D, Fiat A, Naor M. Untraceable electronic cash. In Advanced in Cryptology - Crypto 88, volume 403 of Lectures Notes in Computer Science, Springer-Verlag, 1990. 319～327
4 Eng T, Okamoto T. Single-Term Divisible Coins. In Advances in Cryptology-Eurcrypt 94, LNCS, Springer-Verlag, 1994. 306～313
5 Ferguson N T. Single Term Off-line Coins. In Advances in Cryptology-Eurcrypt 93, LNCS, Springer-Verlag, 1994. 318～328
6 Koblitz N. Elliptic curve cryptosystems, Mathematics of Computation, 1987, 48(17): 203～209
7 Miller V S. Use of elliptic curves in cryptography. In Advances in Cryptology - Crypto 85, LNCS, Springer-Verlag, 1985. 417～462
8 Tsaur W-J, Ho C-H. A Secure Electronic Payment System Based on Efficient Public Key Infrastructure. In: Proc. of the 2002 Intl. Workshop for Asian Public Key Infrastructures (IWAP 2002), Taipei, Taiwan, 2002