一种基于 RBAC 的电子商务匿名性与可追究性实现方案*)

马 勇[1,3] 卿斯汉[1,2] 贺也平[1]

(中国科学院软件研究所 信息安全技术工程研究中心 北京 100080)[1]

(北京中科安胜信息技术有限公司 北京 100080)[2] (中国科学院研究生院 北京 100080)[3]

摘 要 提出了一种基于 RBAC 思想对可信第三方功能进行分类并结合其他一些技术实现电子商务中匿名性与可追究性的解决方案,主要涉及三个主要过程:用户的注册控制、交易过程的控制及投诉处理过程。通过对注册用户的信息进行加密并对加密密钥进行分割保存来实现匿名性,通过对交易过程安全协议的设计及 TTP 功能的划分达到可追究性要求,并对可追究性的实现给予证明。

关键词 RBAC,电子商务,匿名性,可追究行,安全协议

A RBAC Based E-commerce Solution for Anonymity and Accountability

MA Yong[1,3] QING Si-Han[1,2] HE Ye-Ping[1]

(Engineering Research Center for Information Security Technology, Institute of Software, Chinese Academy of Sciences, Beijing 100080)[1]

(Beijing ZhongkeAnsheng Corporation of Information Technology, Beijing 100080)[2]

(Graduate School of Chinese Academy of Sciences, Beijing 100080)[3]

Abstract A resolution for anonymity and accountability requirement in E-commerce is proposed which bases on the thought of BRAC and implicates some other skills. There are three main processes: user's registration, process of trade, and the resolution of complaint. Anonymity of this solution is realized by encryption of the private information of user and the way to save the key in which the key is divided and saved in different places, Accountability is realized by the design of secure protocol and the division of power of the TTP, and the provision of accountability is also given.

Keywords RBAC, E-commerce, Anonymity, Accountability, Secure protocol

1 引言

电子商务的应用已经越来越广泛,而且交易过程中匿名性与可追究性的研究也越来越深入,但是也有一些交易可能同时需要实现匿名性与可追究性的要求,比如一些疾病的网络咨询或者私人物品的购买及其他一些交易方不想透露自己身份但是还必须通过可追究性以保证交易正常完成的场合。

对于这方面的研究已经有了一些进展,并提出了一些解决方案。Kristina A. Keeson 在文[11]中通过一个案例分析论述了匿名性与可追究性实现的重要意义。Csilla Farkas 在文[6]中提出了一个在自组织社区中实现匿名与可追究性要求的框架,本文将会借鉴其中的一些思想。Micheal Backes 在文[10]中提出了一种基于属性实现匿名性与可追究性的访问控制系统。

电子商务中匿名性与可追究性主要是通过可信第三方和安全协议的设计来实现,但是现在的问题往往是对于可行第三方的安全假设过强,如果可信第三方出现问题则会造成比较大的损失。D. F. Ferraiolo 和 D. R. Kuhn 在文[1]中提出了一种基于角色的访问控制(RBAC)的思想,Sandhu 在文[2]中提出了基于该思想的访问控制框架模型。本文借鉴了它的思想将可信第三方的权力进行有效的划分,提出了一种基于 RBAC 的电子商务匿名性与可追究性实现方案,使匿名性与可追究性的实现的控制权限分配到不同的第三方,使其相互协作但又互不干涉,共同实现匿名性与可追究性要求,从而减弱了单个可信第三方的权力提高了电子商务的可信性。

本文第 2 节将对此解决方案进行描述,包括各可信第三方的职能划分以及匿名性与可追究性实现的方法。第 3 节中我们会给出在各个过程中用到的协议及其说明。在第 4 节中将使用一个现有的协议分析框架对交易过程的协议进行分析,从而证明可追究性的实现。最后是总结和展望。

2 框架的设计与实现

在安全操作系统的设计和实现中,RBAC 机制是将管理员 root 的权限进行划分,将不同的管理控制权力分配给不同角色的管理员,其思想类似于西方民主制度中的"三权分立",即行政、立法、司法的权力分别由不同的机构控制,通过它们之间的相互协作和制约达到公平民主和安全的目的。对应的在安全操作系统的 RBAC 机制中设置系统管理员、安全管理员和审计管理员分别控制系统的日常管理、安全策略的制订和实施以及安全事件的审计工作。本文正是借鉴其中思想将可信第三方的权力进行合理划分从而达到相互牵制并相互协调完成匿名性与可追究性的实现。

在我们提出的框架模型中有以下主体:真实客户 U,真实服务提供商 S,虚拟用户 Vu,虚拟服务提供商 Vs,以及可信

*)北京市自然科学基金(批准号:4052016),国家自然科学基金(批准号:60573042)和国家重点基础研究发展规划(973)(批准号:G1999035802)。**马 勇** 硕士生,主要研究方向为安全操作系统,安全协议;**卿斯汉** 研究员,CCF 高级会员,主要研究方向为大型网络安全,安全协议分析,密码学;**贺也平** 研究员,CCF 会员,主要研究方向为网络安全,安全协议,可信平台。

第三方组 TTP_group。其中 TTP_group 包括三个可信第三方，并负责不同的任务：匿名管理可信第三方 TTP_A 负责用户的注册并负责真实用户信息的保密工作和虚拟用户密钥的分发；可追究管理可信第三方 TTP_C 负责交易过程的监测并保存必要的证据消息；投诉管理可信第三方 TTP_M 负责对客户或者服务提供商的投诉做出裁决，获取证据并在需要的情况下提供客户或服务商的真实情况数据。框架结构如图 1 所示。

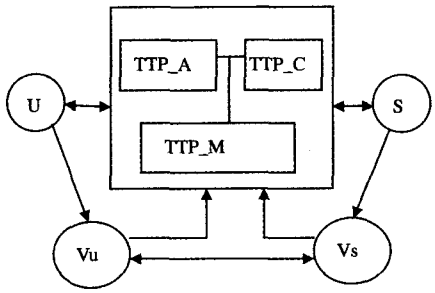

图 1

下面将对各 TTP 的工作过程进行详细的描述。

首先是用户的注册过程：

真实用户 U 或服务提供商 S 向 TTP_A 提出注册申请并提交个人真实信息，如果允许则 TTP_A 将为该用户生成一个虚拟身份 Vu 或 Vs，作为在以后的交易中客户和服务提供商身份，同时为其生成一对公私钥并发送给该用户和其他 TTP_group 成员用于交易及其他一些过程的加密和认证操作。为了进一步完善匿名和用户真实资料的保密，TTP_A 将会为该注册用户或服务提供商生成一个新的密钥 K_{US} 或 K_{SS}，用该密钥将用户的真实身份信息进行加密保存，然后将该密钥划分为三份，分别发给包括自己在内的 TTP_group 成员，并在本机上将此密钥删除。在需要的时候（一般是 TTP_M 接到投诉并确认了确实需要被投诉人的真实身份时）三部分密钥将重新组合而解密用户的真实身份。这种方法保证了用户真实身份的的保密性，从而实现了交易过程中的匿名性，而在需要的时候既能获取用户的真实资料又为可追究性提供了基础。文[6]中曾提出了类似思想，但其将密钥分割后发送给自组织社区中的每一个成员，其处理方式有两个问题：

1）没有考虑社区成员人数的变化，当有成员退出社区时其所拥有的密钥部分如果不妥善处理将会造成其他成员的真实信息永远不能解密；当有新的成员加入社区时由于其不占有任何密钥所以没有民主决策的权力。

2）单个社区成员的权力过大，类似于一票否决的情况，即使只有一个人反对解密真实信息都不能完成，没有实现真正的民主。

本文对其方法做了改进，将密钥分配给 TTP_group 的成员，类似于民主集中的思想，只要 TTP_group 成员一致决定即可解密信息，而且密钥划分的方法也能更好地保护用户的信息。

注册以后的用户将使用注册的虚拟身份进行交易和其他一些操作，在交易的过程中 TTP_C 将对交易过程作有一些可追究性的记录以完成可追究性的要求，并为 TTP_M 的投诉处理过程提供裁决的证据。按照文[4]的分类，TTP_C 属于 OnlineTTP 类型，即只在需要的时候直接参与交易的过程，但是该 TTP 没有双方的真实信息，完全根据 TTP_A 提供的注册虚拟用户信息和为交易方提供的公私钥队来对交易方进行识别。TTP_C 在交易过程中的主要工作是接受交易方发送的非否认证据，其中包括接受价格的证据、服务接收确认消息等。具体的过程将在第 3 部分详细描述。

交易过程中也会出现一些问题，比如交易一方对交易过程进行否认拒绝接受交易结果，或者收到服务后拒绝支付等，在这种情况下交易的另一方可以通过向 TTP_M 提出投诉要求做出相应处理。TTP_M 在框架中扮演类似司法机关的角色，接受投诉方提出的处理请求，根据投诉方提供的证据和 TTP_C 提供的证据做出裁决，如果必要将向另外两个 TTP 提出被投诉方真实信息加密密钥请求，获取该用户或服务提供商的真实信息从而做出相应处理。

3 协议的具体实现

框架用到的协议主要由三个部分组成：用户的注册过程、交易过程和投诉过程，而且三个 TTP 分别参与其中的过程。下面将对三部分进行详细的描述，描述所用的符号定义如下：

K_a：主体 a 的公开密钥，用于验证 a 的数字签名，K_a^{-1} 是 K_a 对应的 a 的秘密密钥。

(m,n)：消息 m 和消息 n 的连接。

$(m)_{K_a}$：用 K_a 对消息 m 进行加密或签名。

3.1 注册过程

这部分协议主要是真实用户和 TTP_A 之间的消息交换，完成真实用户注册虚拟用户的过程，并为新注册的用户分配密钥。

1 $U \rightarrow TTP\_A$

$(U, Vu, (R)_{Ku^{-1}}, t1)_{K_{TTP\_A}}$

用户 U 向 TTP_A 发送的注册申请消息，内容包括用户的真实身份信息 U、想要申请的虚拟身份 Vu、用 U 的私钥加密的申请请求 R 以及时间戳 $t1$，整个消息用 TTP_A 的公钥加密，保证只能由 TTP_A 解密该消息。

TTP_A 收到该消息以后，如果确定 U 符合注册条件，则为该用户生成一对公私钥并连同申请的虚拟身份一起发送给 U。

2 $TTP\_A \rightarrow U$

$(R, Vu, K_{Vu}, K_{Vu}^{-1}, t2)_{K_U}$

在这个消息中，TTP_A 将生成的公私钥 K_{Vu}/K_{Vu}^{-1}、U 申请的身份 Vu、以及解密后的申请请求 R 连同时间戳 $t2$ 用 U 的公钥加密后发送给 U。U 收到该消息以后向 TTP_A 发送一个接收确认消息。

3 $U \rightarrow TTP\_A$

$((Acknowledge)_{Ku^{-1}})K_{TTP\_A}$

该消息首先用 U 的私钥签名然后用 TTP_A 的公钥进行加密。

注册结束后 TTP_A 将进行 U 的真实身份加密处理过程。首先 TTP_A 将生成一个密钥 K_{US}，用此密钥将用户的真实身份加密：$(U)_{K_{US}}$，然后将此密钥分为三份：$K_{US}1$、$K_{US}2$、$K_{US}3$，并将 $K_{US}2$ 和 $K_{US}3$ 连同新注册用户的公私钥对 K_{Vu}/K_{Vu}^{-1} 分别发送给 TTP_C 和 TTP_M 并将本机存储的 K_{US} 删除。

到这里用户的注册过程结束，在以后的交易活动中用户将使用注册后的虚拟身份 Vu 进行操作。

3.2 交易过程

本过程中所使用的协议参考了卡耐基·梅隆大学的 IBS (Internet Billing Server Protocl)协议[9],并做了一些修改。其中去掉了价格协商部分和发票分发部分的协议,并将原协议中多个项目申请简化为一个。本框架假设在交易之前已经协商好了价格交易过程只包括服务的申请、获得及接收服务确认。TTP_C 在该过程中以 OnlineTTP 的形式参与交易过程,主要工作是记录交易方的一些非否认证据保证交易的公平性,并为 TTP_M 处理投诉时提供证据。以下是协议的具体描述:

1 $Vu \rightarrow Vs$

$((Price)_{K_{Vu}^{-1}})_{K_{Vs}}$

首先客户 Vu 向服务提供商 Vs 发送价格确认,并以自己的私钥进行签名,然后经过 Vs 的公钥加密后发送给 Vs。

2 $Vs \rightarrow TTP\_C$

$((Price)_{K_{Vu}^{-1}})_{K_{TTP\_C}}$

Vs 收到 Vu 发送的价格确认消息后,如果确认价格没有问题则立即将该消息转发给 TTP_C 作为 Vu 的价格确认非否认证据。

3 $Vs \rightarrow Vu$

$((Serice)_{K_{Vs}^{-1}})_{K_{Vu}}$

Vs 发送 Vu 申请的服务,并以自己的私钥签名,然后用 Vu 的公钥签名后发送给 Vu。

4 $Vu \rightarrow Vs$

$(Acknowledge)_{K_{Vu}^{-1}}$

收到 Vs 的服务以后,Vu 会向 Vs 发送一个自己签名的确认消息。

5 $Vs \rightarrow TTP\_C$

$((Acknowledge)_{K_{Vu}^{-1}})_{K_{TTP\_C}}$

Vs 将收到的确认消息转发给 TTP_C 作为 Vu 收到消息的非否认证据。

交易过程的协议满足可追究性要求,本文将在第 4 部分做出相应证明。

3.3 投诉处理

本部分协议在交易方对交易提出异议时使用,TTP_M 在收到投诉后对投诉者提供的证据进行辨别,并向 TTP_C 索要该交易过程的非否认证据,如果确定被投诉者违规则向另外两个 TTP 提出真实信息解密密钥请求,并从 TTP_C 处获取该用户或服务提供商的真实信息并做出相应处理。该部分协议具体描述如下(描述过程将不对客户和服务提供商做区分,统一用 Vu 标识):

1 $Vul \rightarrow TTP\_M$

$(Vu2, Proof, (R1)_{K_{Vu1}^{-1}}, t1)_{K_{TTP\_M}}$

用户 $Vu1$ 向 TTP_M 发送投诉请求消息,投诉对象为 $Vu2$ 并提供相应的证据 $Proof$,签名的投诉请求标志 $R1$,以及时间戳 $t1$,整个消息用 TTP_M 的公钥加密过后发送给 TTP_M。

2 $TTP\_M \rightarrow Vul$

$(Confirm, R1)_{K_{TTP\_M}^{-1}}$

如果 TTP_M 接受 $VU1$ 的投诉,则向 $Vu1$ 发送一个确认消息,包括确认信息 $Confirm$ 以及解密后的投诉请求 $R1$,消息用 TTP_M 的私钥加密。

3 $TTP\_M \rightarrow TTP\_C$

$(Vu1, Vu2, (R2)_{K_{TTP\_M}^{-1}}, t2)_{K_{TTP\_C}}$

接受 $Vu1$ 的投诉后 TTP_M 将向 TTP_C 索要 $Vu1$ 与 $Vu2$ 交易过程的记录。消息主要内容是投诉方和被投诉方的信息,以及用 TTP_M 私钥加密的请求 $R2$,时间戳 $t2$,整个消息用 TTP_C 的公钥加密。

4 $TTP\_C \rightarrow TTP\_M$

$(Info, R2)_{K_{TTP\_C}^{-1}}$

收到 TTP_M 的请求后,TTP_C 将 TTP_M 要求的信息 $Info$ 并解密后的 $R2$ 用自己的私钥签名后发送给 TTP_M。

如果 TTP_M 根据 $Vu1$ 提供的证据并参考 TTP_C 提供交易记录确定被投诉者违规,则向 TTP_A 和 TTP_C 提出解密密钥请求,得到 $Vu2$ 的真实信息加密密钥并用该密钥从 TTP_A 处得到 $Vu2$ 的真实信息并对其进行相应的处理或惩罚。

在文[6]中曾提出了密钥分割的思想,但是其将真实信息的加密密钥平均分给自组织内的所有成员,在第 2 部分中已经对其进行了分析。本文对该思想进行改进,实行民主集中的思想,将用户的加密密钥分配给有限的 TTP,一方面实现了安全与民主,另一方面也解决了用户数量变化的情况。

4 可追究性证明

本文中协议的三个部分涉及到可追究性要求的只有第二部分即交易过程的协议,所以只对该部分进行可追究性的证明。本文将利用 Kailar 在文[8]中提出的协议可追究性证明框架对该部分协议进行证明。

首先作为初始状态的假设我们有:

A1:Vs CanProve(K_{Vu} Authenticates Vu)

A2:Vu CanProve(K_{Vs} Authenticates Vs)

A3:Vs,Vu CanProve(K_{TTP_C} Atlthenticates TTP_C)

A4:(Vu Says Price)⇒(Vu agrees to $Price$)

A5:(Vs Says Serice)⇒(Vs sends Service)

A6:(Vs Says Acknowledge)⇒(Vu Received Service)

假设 A1 说明:服务提供商可以证明 K_{Vu} 可以确认用户 V_u,即任何使用 K_{Vu}^{-1} 加密的消息的 Vu 发送的。$A2$ 和 $A3$ 是同样的情况。$A4$ 的意思是如果 Vu 提出了服务请求则说明 Vu 已经同意了协商好的价格。$A5$ 和 $A6$ 说明 Vu 已经发送了服务并且 Vu 已经确定收到了服务。

下面对交易过程的各条协议进行分析我们得到关于一些消息的解释:

1 $Vu \rightarrow Vs$ $((Price)_{K_{Vu}^{-1}})_{K_{Vs}}$

⇒Vs Receives($Price$)SignedWith K_{Vu}^{-1}

3 $Vs \rightarrow Vu$ $((Serice)_{K_{Vs}^{-1}})_{K_{Vu}}$

⇒Vu Receices($Serice$)SignedWith K_{Vs}^{-1}

4 $Vu \rightarrow Vs$ $(Acknowledge)_{K_{Vu}^{-1}}$

⇒Vs Receices

($Acknowledge$)SignedWith K_{Vu}^{-1}

对于消息 1:当 Vs 收到 Vu 的消息后,根据假设 A1 可以确定是 Vu 发送的消息,即:

Vs CanProve(Vu Says $Price$)

根据假设 A4,又可以得到:

Vs CanProve(Vu Agrees to Price)

对于消息 3:根据假设 A2,Vu 可以证明是 Vs 发送了消息,即:

Vu CanProve(*Vs* Says *Service*)

再根据假设 A5，又可以得到：

Vu CanProve(*Vs* Sends *Service*)

对于消息 4：根据假设 A1，*Vs* 可以确定是 *Vu* 发送了消息，即：

Vs CanProve(*Vu* Says *Acknowledge*)

然后根据假设 A6 得到：

Vs Canprove(*Vu* Received *Service*)

根据以上证明，交易过程的协议已经达到了可追究性的目标。

结论与展望 随着电子商务的发展，对于同时实现匿名性与可追究性的要求也越来越强烈。本文通过将 RBAC 的思想应用到电子商务交易的可信第三方的角色分配过程，并通过对注册用户真实信息加密并将加密密钥分段保存的方法实现了交易过程中的匿名性和可追究性要求。根据 RBAC 最小特权的原则对可信第三方的角色进行合理分配使其够协调工作又能相互牵制，既减弱了单个可信第三方的权力并将单个可信第三方出现问题造成的损失降到最低，又能实现匿名性与可追究性同时实现的要求。这种方法对于长期以来可信第三方安全假设要求过强的问题也提供了一些思路。

在下一步的工作中，需要进一步研究是投诉处理过程中的证据确认原则及各可信第三方之间的通信过程处理及协议。更长远的研究包括使用零知识证明等方法实现进一步的匿名要求。

参 考 文 献

1 Ferraiolo D F, Kuhn D R. Role Based Access Control. In: 15th National Computer Security Conference, 1992

2 Sandhu R S, Coyne E J, Feinstein H L, et al. Youman, Role-Based Access Control Models. IEEE Computer, 1999, 29(2): 38～47

3 Qing SH. Cryptography and Computer Network Security. Beijing: Thinghua University Press, 2001 (in Chinese)

4 Qing S H. TTP roles in electronic commerce protocols. Journal of Software, 2003,14(11):1936～1943

5 Qing, S H. Design and logical analysis of security protocols. Journal of Software, 2003,14(7):1300～1309 (in Chinese with English abstract)

6 Farkas C, Ziegler C, Meretei A, et al. Anonymity and Accountability in Self-Organizing Electronic Communities. In: WPES'02, Nov. 2002

7 Kailar R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, 1996,22(5):313～328

8 Kailar R. Reasoning about Accountability in Protocols for Electronic Commerce. Security and Privacy. In: Proceedings, 1995 IEEE, 1995

9 O'Toole K R. The Internet Billing Server Transaction Protocol Alternative. Carnegie Mellon University Information Networking Institute, INI TR, 1994

10 Backes M, Camenisch J, Snommer D. Anonymous yet Accountable Access Control. In: VPES05, 2005 ACM, Nov. 2005

11 Keesom K A. Anonymity, Accountability. In: InfoSecCD Conferece'04, ACM, 2005

(上接第 85 页)

正式进行攻击测试之前，攻击者先试用一次该系统，攻击者可以事先花一定时间查看假冒对象的某一次认证记录结果。每个攻击者轮流假冒每个用户一次，测试过程中还可以查看该假冒对象的相应认证记录结果。正常用户与被假冒时针对该用户的平均识别率和平均认证时间结果分别见图 1 和图 2。

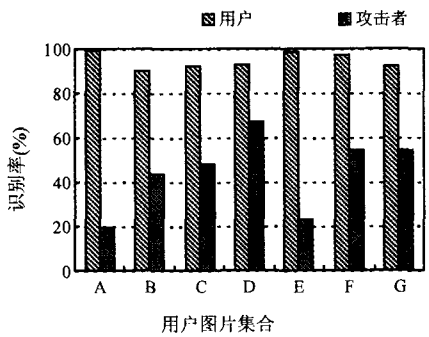

图 1 正常用户和攻击者识别率比较

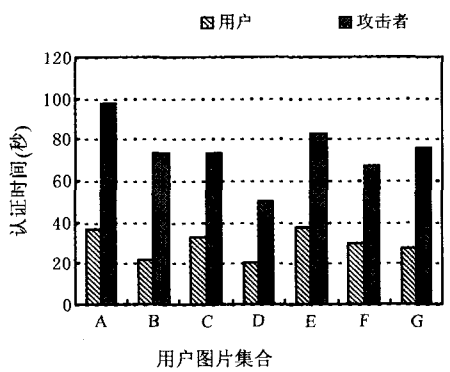

图 2 正常用户和攻击者登录的花费时间比较

由图 1 和图 2 所示结果，从对图片的识别率和平均认证时间两个方面看，攻击者和用户都可以比较明显地进行区分。P 方案中攻击者识别率相对较高，多数达到 60%左右。从图 1 可以看出，本方案显著降低了攻击者对图片的识别率。实验结果显示这种组合方案会在用户最初使用该系统时会出现漏选个别信息的错误。

其他一般性实验显示单独使用一种类型的数字媒体时，使用文本方式时用户识别率略高而攻击难度大，图片次之，视频和音频差一些。如果只提供一种形式的媒体供用户选择，图片为用户的首选。相对传统认证方式，用户本人制作、生成个人收藏集合还是有一定困难，用户总体上感到此种认证方式新颖、有趣，感觉比较安全。但也有部分人担心数字媒体信息集合全部被他人获得，从而可能暴露个人隐私。

结论 本文个性化认证方法由于用户每次登录通过随机选取使用了不同的媒体信息组合，可以抵抗重放攻击。分析与实验结果表明该方法是可行的，安全性得到提高，用户可以接受这种认证方式。该实现方案增加了用户灵活的媒体形式选择，解决了设备多样性问题，同时减少了暴露给攻击者的信息，相对地可以认为扩大了备选的媒体组成的信息空间。

未来可能的研究工作包括改进用户参与配置系统的方式、攻击方法及其对抗措施等。

参 考 文 献

1 Pering T, et al. Photogranphic Authentication through Untrusted Terminals. IEEE PERVASIVE computing,2003,2(1): 30～36

2 Dhamija R, Perrig A. DejaVu: A User Study Using Images for Authentication. In: Proc. 9th Usenix Security Symp., Usenix, Aug. 2000. 45～58

3 徐光佑，史元春，谢伟凯. 普适计算. 计算机学报，2003,26(9): 1042～1050

4 王悦，岳玮宁，王衡，董士海. 手持移动计算中的多通道交互. 软件学报，2005,16(1):29～36

5 Deb S, Zhang Yanchun. An overview of content-based image retrieval techniques. In: 18th International Conference on Advanced Information Networking and Applications, Volume 1, 2004. 59～64