电子商务协议中的可信第三方角色*

卿斯汉+

(中国科学院 信息安全技术工程研究中心,北京 100080)
(中国科学院 软件研究所 信息安全国家重点实验室,北京 100080)

TTP Roles in Electronic Commerce Protocols

QING Si-Han

(Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China)
(State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)
+ Corresponding author: Phn: 86-10-62635150, Fax: 86-10-62635150, E-mail: qsihan@yahoo.com
http://www.ercist.iscas.ac.cn
Received 2003-05-19; Accepted 2003-06-30

Qing SH. TTP roles in electronic commerce protocols. *Journal of Software*, 2003,14(11):1936~1943.
http://www.jos.org.cn/1000-9825/14/1936.htm

Abstract: TTP (trusted third party) plays an important role in electronic commerce protocols. Different roles of TTP in inline TTP protocols, online TTP protocols and offline TTP protocols are pointed out through three protocols of different types, i.e., Coffey-Saidha protocol, CMP1 protocol and Asoken-Shoup-Waidner protocol. The above protocols are analyzed thoroughly, and their characteristics, defects and approaches to further improvement are discussed respectively in this paper.
Key words: TTP(trusted third party); electronic commerce protocol; non-repudiation; accountability; fairness

摘 要: 在安全电子商务协议中,可信第三方 TTP(trusted third party)担任重要的角色.通过 3 类不同的协议,即 Coffey-Saidha 协议、CMP1 协议和 Asoken-Shoup-Waidner 协议,指出 TTP 在 inline TTP 协议、online TTP 协议和 offline TTP 协议中的不同作用.对上述协议进行了全面的分析,分别指出它们的特点、缺陷与改进方法.
关键词: 可信第三方;电子商务协议;非否认性;可追究性;公平性
中图法分类号: TP309 **文献标识码**: A

随着 Internet 的日益发展与普及,电子商务与电子政务的需求也越来越迫切.然而,电子商务与电子政务的研究重点是不同的.电子政务研究的重点是认证与授权,而电子商务研究的重点是隐私性与公平性.电子商务协议的安全性是安全地进行网上电子交易的基础.安全的电子商务协议不但应当具备安全认证协议[1~3]的全部功能和性能,还需要具备非否认性、可追究性、公平性、隐私性等安全性质.非否认性是安全电子商务协议的基本性质,否认是电子交易中最主要的威胁之一,它包括:(1) 否认拥有某个消息;(2) 否认发送过某个消息;(3) 否

* Supported by the National Natural Science Foundation of China under Grant No.60083007 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035810 (国家重点基础研究发展规划(973))
第一作者简介: 卿斯汉(1939－),男,湖南隆回人,研究员,博士生导师,主要研究领域为信息系统安全理论和技术.

认接收到某个消息;(4) 否认递交过某个消息;(5) 否认在规定的时间内收到或发送消息,等等.

通常,争议涉及到以下几个方面:一个事件是否发生、何时发生,哪些主体参与了这一事件,哪些信息和它相联系.争议方必须出示证据,在仲裁者的调停下解决争议.非否认服务的目的是为某一特定事件的参与方提供证据,使他们对自己的行为负责.什么是"否认"呢?我们将否认定义为通信的参与方否认参与了全部或部分通信.在一次通信会话中,有两种传递消息的可能方式:(1) 发送方直接向接收方发送消息;(2) 发送方把消息提交给一个可信任的第三方 TTP(trusted third party),再由 TTP 将消息传递给接收方.这时,TTP 的角色是交付中心(delivery authority).一般假定 TTP 是诚实的,且协议的参与方都信任 TTP.

可追究性(accountability)是与非否认性密切相关的另外一个重要性质,可追究性是安全电子商务协议必须满足的基本要求.电子商务协议的可追究性是通过发方非否认和收方非否认两个基本目标[4]达到的.发方非否认证据 EOO(evidence-of-origin)是指电子商务协议向接收方提供的不可抵赖证据,用于证明发送方发送过某个消息.收方非否认证据 EOR(evidence-of-receipt)是指电子商务协议向发送方提供的不可抵赖证据,用于证明接收方收到发送方发送的某个消息.

以BAN逻辑[5]为代表的BAN类逻辑是一种基于信念逻辑的形式化方法,可以用于分析认证协议的安全性,但不能用于分析电子商务协议的可追究性.其根本原因在于信念逻辑证明某个主体相信某一公式,而可追究性的目的是某个主体向第三方证明另一方对某个公式负有责任.为此,Kailar 提出了新的逻辑[6],用于分析电子商务协议的可追究性.尽管Kailar逻辑扩展了BAN类逻辑的分析范围,可以分析电子商务协议的可追究性,但它仍有一些不足之处.文献[7]指出,Kailar 逻辑的主要缺陷在于:(1) 不能分析协议的公平性;(2) 对协议语句的解释及初始化假设是非形式化的,存在局限性;(3) 无法处理密文.文献[8]对 Kailar 逻辑进行了改进,提出了一种新的形式化分析方法.与 Kailar 逻辑相比,这种新的形式化分析方法主要有 3 个优点:(1) 可以分析协议的公平性;(2) 初始化拥有集合只依赖于环境,不需要人为地引入初始化假设;(3) 增加了密文理解规则,能有效地分析签名的加密消息.

安全电子商务协议应当满足的另外一个基本要求是公平性(fairness).公平性包含两层含义:首先,正确执行协议后,应当保证发送方收到 EOR 且接收方收到 EOO.其次,如果协议异常终止,协议应当保证通信双方都处于同等地位,任何一方都不占任何优势.或者说,协议的执行在任何一步异常终止时,消息接收方收到 EOO 当且仅当消息发送方收到 EOR.

安全电子商务协议可以分为以下两类:

(1) 逐步交换协议(gradual exchange protocol).亦即,参与协议的主体只有两个,他们通过许多步骤一步一步地暴露所交换的消息.此外,还有一类协议可以实现所谓"概率公平性".这类协议类似于逐步交换协议:第 1,它无须第三方参与;第 2,通过许多回合一步一步地交换消息.

(2) 可信第三方协议,亦即,协议主体通过可信第三方交换消息,保证实现协议的各种安全目标,例如原子性、非否认性、可追究性、公平性、隐私性等.

对逐步交换协议,通常需要对它作一种不合理的假设,即参与协议的两个主体具有相同的计算能力.此外,实现这类协议需要进行大量的消息交换,因此效率很低.基于以上原因,目前主流的电子商务协议都采用可信第三方协议方法.逐步交换协议在现实中很少应用,它们只具有理论上的研究价值.

在可信第三方协议中,根据 TTP 介入的程度与介入方式的不同,又可以分为 inline TTP 协议、online TTP 协议和 offline TTP 协议 3 种.在 inline TTP 协议中,TTP 扮演协议主体之间的中介角色.协议主体之间不交换任何消息,协议主体之间所交换的消息都通过 TTP 进行.此外,TTP 直接提供可信第三方的各种服务.在 online TTP 协议中,每次需要提供可信第三方的服务时,TTP 都直接参与;而在 offline TTP 协议中,只有在必须提供可信第三方的服务时,TTP 才介入.由此可见,TTP 在 inline TTP 协议中介入程度最高,而在 offline TTP 协议中,TTP 的介入程度最低.

通常,在安全电子商务协议中,TTP 所能担当的角色有:

(1) "证书(certification authority)中心"角色.证书中心负责为参加认证的主体颁发公开密钥证书,公开密钥证书中包含主体名、主体的公开密钥、公开密钥的有效期等.

(2) “公证(notary)中心”角色.参与协议的主体相信公证中心能提供正确的证据,并为他们验证数据的正确性和数据交换的正确性.

(3) “交付(delivery authority)中心”角色.作为交付中心,参与协议的主体相信 TTP 能正确地将消息传送给对方并提供相应的证据.

(4) “仲裁(adjudicator)中心”角色.可信第三方服务的最终目的是解决有关某一事件是否发生的争议.仲裁中心能够根据争议双方提供的证据作出正确的判断.除非争议发生,仲裁中心一般不参与可信第三方服务.

(5) “时戳(time-stamping authority)中心”角色.可信第三方提供在非否认证据中加入可信时戳的服务.

本文所采用的基本符号如下:

(m,n):表示消息 m 与消息 n 进行级连;

f_X:字段名,其中下标表示字段的含义,用于标识消息交换的目的.例如,f_{EOO} 表示 EOO 字段,说明该条消息发送 EOO 证据;

K_a:主体 A 的公开密钥,用于验证 A 的数字签名. K_a^{-1} 是与 K_a 对应的 A 的秘密密钥;

$h(m)$:应用于消息 m 的单向散列函数.

下面,我们通过一个简单的例子,说明 TTP 如何担任交付中心的角色.在该 inline TTP 协议中,我们假设通信信道是可靠的(在实用中,这种假设显然是过强了).协议如下:

$$EOO=\{f_{EOO},TTP,B,m\}_{K_a^{-1}},$$

$$EOD=\{f_{EOD},A,B,m\}_{K_{up}^{-1}}.$$

(1) $A\rightarrow TTP: f_{EOO},TTP,B,m,EOO$.

(2) $TTP\rightarrow B: f_{EOO},TTP,B,m,EOO$.

(3) $TTP\rightarrow A: f_{EOD},A,B,EOD$.

在上述协议中,TTP 作为交付中心,忠实地将 A 发送的消息传送给 B,并向 A 提供非否认交付证据 EOD(evidence-of-delivery).注意,EOD 与 EOR 是不同的.

本文通过 3 类不同的可信第三方协议,详细阐述 TTP 在安全电子商务协议中所扮演的角色,并对这 3 个具体的协议进行全面的分析与评价.

1 Inline TTP 协议的例子——Coffey-Saidha 协议

1.1 Coffey-Saidha协议

Coffey-Saidha 协议[9]是 1996 年提出的,其目的是协议发起方 A 向接收方 B 发送消息 m,并保证在协议结束时,A 获得 EOR 且 B 获得 m 与 EOO.

在 Coffey-Saidha 协议中,使用下述符号和记法:

t_1,t_2:时戳;

N_a,N_b:临时值;

TSA:作为时戳中心的 TTP;

NRS:提供非否认服务的 TTP;

$EOO=\{\{f_{EOO},A,B,m\}_{K_a^{-1}},TSA,t_1\}_{K_{tsa}^{-1}}$:发送 m 的非否认证据;

$EOR=\{\{f_{EOR},B,A,h(EOO)\}_{K_b^{-1}},TSA,t_2\}_{K_{tsa}^{-1}}$:收到 m 的非否认证据;

$P\_EOO=\{f_{EOO},A,B,m\}_{K_a^{-1}}$:发送 m 的部分非否认证据;

$P\_EOR=f_{EOR},B,A,h(EOO)$:收到 m 的部分非否认证据;

$S\_P\_EOR=\{f_{EOR},B,A,h(EOO)\}_{K_b^{-1}}$:收到 m 的签名部分非否认证据.

Coffey-Saidha 协议如下,其示意图如图 1 所示.

(1) $A\rightarrow TSA:\{P\_EOO\}_{K_{tsa}}$.

(2) $TSA \to A:\{EOO\}_{K_a}$.

(3) $A \to NRS:REQ$.

(4) $NRS \to A:\{N_a\}_{K_a}$.

(5) $A \to NRS:\{\{N_a,EOO,P\_EOR\}_{K_a^{-1}}\}_{K_{nrs}}$.

(6) $NRS \to B:\{\{N_b,P\_EOR\}_{K_{nrs}^{-1}}\}_{K_b}$.

(7) $B \to TSA:\{S\_P\_EOR\}_{K_{tsa}}$.

(8) $TSA \to B:\{EOR\}_{K_b}$.

(9) $B \to NRS:\{\{N_b,EOR\}_{K_b^{-1}}\}_{K_{nrs}}$.

(10) $NRS \to B:\{EOO\}_{K_b}$.

(11) $NRS \to A:\{EOR\}_{K_a}$.

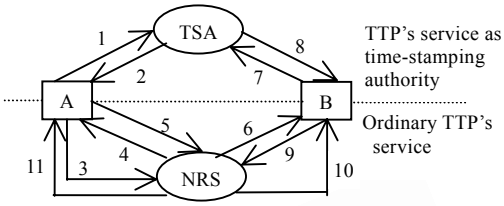

Fig.1 Coffey-Saidha protocol

图 1 Coffey-Saidha 协议

协议的第 1 步,A 生成 P_EOO,并用 TSA 的公开密钥加密后发送给 TSA.在 Coffey-Saidha 协议中,除第 3 步以外,所有的消息均用接收者的公开密钥加密传送.在以下的协议描述部分,我们不再重复阐述这一加密过程.第 2 步,TSA 对 P_EOO 加上时戳并签名,形成完全的 EOO,然后发送给 A.第 3 步,A 向 NRS 发送 REQ,请求进行与 B 的通信.第 4 步,NRS 生成临时值 N_a,并发送给 A.第 5 步,A 将(N_a,EOO,P_EOR)签名后发送给 NRS.第 6 步,NRS 通过 N_a 校验 EOO 的新鲜性后,生成另一个临时值 N_b.NRS 对(N_b,P_EOR)签名,并发送给 B.第 7 步,B 对 P_EOR 签名,并发送给 TSA.第 8 步,TSA 对 S_P_EOR 加入时戳并签名,形成完全的 EOR,并发送给 B.第 9 步,B 将(N_b,EOR)签名后发送给 NRS.NRS 通过 N_b 校验 EOR 的新鲜性后,在第 10 步与第 11 步分别向 B 与 A 发送 EOO 和 EOR.

2.2 TTP 的角色与 Coffey-Saidha 协议分析

选择 Coffey-Saidha 协议作为我们考查的典型例子,其原因是该协议在一个协议中定义了两种不同的 TTP 角色,即提供时戳中心服务的 TTP 角色 TSA,提供非否认证据和可追究服务的 TTP 角色 NRS.我们从分析 TSA 开始.

类似于交付中心角色,时戳中心角色承担的任务比较明确,也比较简单.协议中共有 4 个步骤与 TSA 相关,即第 1、2、7、8 步.从分析可知,TSA 的任务是在证据中加入可信时戳,形成完整的 EOO 和 EOR.其操作流程是,协议主体 A 或 B 向 TSA 提出服务请求并向 TSA 发送消息 m,TSA 对 m 加入可信时戳,形成 n=(m,TSA,时戳),对 n 签名后发送给主体 A 或 B.

在实用中,上述 TTP 所提供的可信时戳服务是十分重要的.证书中心所颁发的 X.509 公开密钥证书,规定了证书应用的有效期.当电子商务协议运行时,不能使用过期的证书与证书中的公开密钥.但是,纠纷仲裁程序往往是在协议运行完成之后离线进行的,这时证书具有过期的可能性.然而,为了解决争议,我们不得不使用过期的公开密钥对协议运行时的签名进行验证.由此,可信时戳服务的重要性可见一斑.在具体实现中,我们还必须注意以下细节.注意到,签名生成的时间与加入时戳的时间之间,有一个短时间的时间延迟.因此,对于请求可信时戳服务的主体,有责任确保在 TTP 提供可信时戳服务期间,该主体的公开密钥证书不会过期.

NRS则提供通常的TTP服务,保证协议的可追究性与公平性等.由于Coffey-Saidha协议是inline TTP协议,TTP参与协议的每一步运行,因此TTP的负荷很重.当协议正常结束时,B获得EOO,A获得EOR.因此Coffey-Saidha协议满足可追究性.在通信信道可靠的情形下,最终协议将正常终止.此时,B通过EOO可以证明A发送了m.A通过EOR可以证明B收到了m.因此,Coffey-Saidha协议满足公平性.在通信信道不可靠的情形下,协议的第10或第11步有可能未成功执行.此时,或者B收到EOO但A未收到EOR;或者A收到EOR但B未收到EOO.所以,Coffey-Saidha协议不满足公平性.此外,由于在协议的执行过程中,m必须暴露给TTP,因此,Coffey-Saidha协议未能有效地保护A与B之间传送的消息的隐私性.

Coffey-Saidha 协议具有以下明显的缺陷:首先,协议的效率很低.因为,协议除第 3 步以外,对所有的协议步骤都进行公开密钥加密运算.另外,A 传送给 B 的消息,需要通过 TTP 再次传送一次,进一步降低了协议的效率.其次,这种公开密钥加密运算不但不必要,也未必真正保证安全.为确保安全,应当使用临时生成的会话密钥.最

后,协议应用临时值 N_a 和 N_b 保证 EOO 和 EOR 的新鲜性,这种技术手段的采用也是错误的.事实上,EOO 与 EOR 很容易复制.EOO 与 EOR 副本的数目未必等于消息 m 被发送与接收的次数.如果一条消息需要重复传送,可以在非否认证据中说明.例如,通过不同的时戳表示;或将交易标识符引入 EOO 和 EOR.

2 Online TTP 协议的例子——CMP1 协议

2.1 CMP1协议

1995 年,Deng 等人提出了两种挂号电子邮件协议[10]方案 CMP1 与 CMP2.其中,CMP1 协议没有邮件加密功能,CMP2 协议具有邮件加密功能.CMP1 协议如下:

$$EOO = \{A, B, TTP, m\}_{K_a^{-1}},$$

$$EOR = \{A, B, TTP, h(m)\}_{K_b^{-1}},$$

$$EOD = \{B, m, EOR\}_{K_{ttp}^{-1}}.$$

(1) $A \to B: A, B, TTP, h(m), \{k\}_{K_{ttp}}, \{EOO\}_k$.

(2) $B \to TTP: EOR, \{k\}_{K_{ttp}}, \{EOO\}_k$.

(3) $TTP \to B: \{EOO\}_{k_{ttp}^{-1}}$.

(4) $TTP \to A: EOD$.

协议的第1步,A生成发送m的非否认证据EOO;生成随机会话密钥k,并用k将EOO加密;计算邮件m的摘要$h(m)$;用TTP的公开密钥加密k;然后将消息(1)发送给B.第2步,B生成收到满足$h(m)$的消息的非否认证据EOR,并将消息(2)发送给TTP.TTP收到消息(2)后,通过两次解密运算获得EOO,并校验A签名的有效性.同时,TTP对EOR校验B签名的有效性.然后,TTP通过由EOO获得的m计算摘要$h(m)$,并与EOR中的$h(m)$进行比较.如果二者一致,则TTP在第3与第4步分别向B与A发送消息(3)和(4).

2.2 TTP的角色与CMP1协议分析

CMP1 协议是典型的 online TTP 协议,如果将 CMP1 协议改变为 inline TTP 协议,则协议至少需要执行 5 步,如图 2 所示.

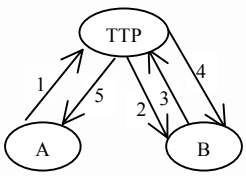

Fig.2 Inline TTP CMP1 protocol

图 2 Inline TTP CMP1 协议

协议的第 1 步,A 向 TTP 发送 m 与 EOO.第 2 步,TTP 向 B 发送接收邮件 m 的请求.第 3 步,B 向 TTP 发送 EOR.TTP 完成各种校验工作后,在第 4 与第 5 步分别向 B 与 A 发送(m,EOO)和 EOD.

在挂号电子邮件协议中,至少需要交换 4 条消息.事实上,邮件发送方 A 至少需要发送一条包含(m,EOO)的消息,邮件接收方 B 至少需要发送一条包含 EOR 的消息.作为可信投递方的 TTP,担任交换(m,EOO)和 EOD 的角色,至少需要发送两条消息:一条发送给 A,另一条发送给 B.由以上分析可见,online TTP CMP1 协议在协议步数上达到最优.

当协议正常结束时,B获得EOO,A获得EOR与EOD.因此CMP1协议满足可追究性.

在通信信道可靠的情形下,最终协议将正常终止.此时,B通过EOO可以证明A发送了m.A通过EOR可以证明B收到了$h(m)$;通过EOD可以证明TTP向B交付了m.二者相结合,A可以证明B收到了m.因此,CMP1协议满足公平性.

但是,如果通信信道不可靠,则协议的第3或第4步有可能未成功执行.此时,或者B收到EOO但A未收到(EOR,EOD);或者A收到(EOR,EOD)但B未收到EOO.因此,CMP1协议不满足公平性.

注意,TTP必须忠实地担当其所承担的角色.例如,如果TTP未尽责地校验$h(m)$与m的一致性,则CMP1协议仅能实现下述较弱的可追究性目标:A可以向仲裁方证明,B收到了$h(m)$且B拥有m.

通过以上分析,我们还可以看出,在协议的第3步,用TTP的公开密钥对EOO签名是多余的,因为EOO本身就

足以成为发送m的非否认证据.因此,CMP1协议的第3步可以简化为

(3) $TTP \to B: EOO$.

进一步分析可知,执行协议的第1步之后,B已经拥有$\{EOO\}_k$.所以,在协议的第3步,只需向B发送k,因为B通过k即可获得EOO.因此,CMP1协议的第3步可以进一步简化为

(3) $TTP \to B: k$.

最后,我们分析 CMP1 协议的隐私性保护与效率.由于在协议的执行过程中,m 必须暴露给 TTP,因此,CMP1协议未能有效地保护隐私性.此外,由于 $h(m)$以明文的形式传送,可能会暴露有关 m 的若干信息.改进的方法可以有多种选择,例如,可以用 $h(m,k)$取代 $h(m)$.CMP1 协议的效率不高,因为在协议执行过程中,整条消息 m 被反复传送,且 TTP 的负荷十分沉重.

3 Offline TTP 协议的例子——Asokan-Shoup-Waidner 协议

3.1 Asokan-Shoup-Waidner协议

1998 年,Asokan 等人提出了一种一般性的 offline TTP 协议[11],下面我们对其中的挂号电子邮件协议进行考查与分析.Asokan-Shoup-Waidner 挂号电子邮件协议由 4 个子协议构成:exchange,abort,resolve_A 和 resolve_B.在正常情形下,只执行 exchange 子协议.仅当 A 或 B 认为协议执行出现问题时,才执行其他子协议.

协议的 exchange 子协议如下,其中 N_a 和 N_b 分别为 A 与 B 生成的临时值;m 为 A 向 B 发送的电子邮件; $C = \{m, N_a, K_a, K_b\}_{K_{ttp}}$ 是加密电子邮件.

(1) $A \to B$: $me1 = K_a, K_b, TTP, C, h(m), \{K_a, K_b, TTP, C, h(m)\}_{K_a^{-1}}$.

IF B gives up THEN quit ELSE

(2) $B \to A$: $me2 = h(N_b), \{me1, h(N_b)\}_{K_b^{-1}}$.

IF A gives up THEN abort ELSE

(3) $A \to B$: $me3 = m, N_a$.

IF B gives up THEN resolve_B ELSE

(4) $B \to A$: $me4 = N_b$.

IF A gives up THEN resolve_A

协议的 abort 子协议如下:

(1) $A \to TTP$: $ma1 = aborted, me1, \{aborted, me1\}_{K_a^{-1}}$.

IF B has resolved THEN resolve_A ELSE

(2) $TTP \to A$: $abort\_token = aborted, ma1, \{aborted, ma1\}_{K_{ttp}^{-1}}$.

协议的 resolve_B 子协议如下:

(1) $B \to TTP$: $mrb1 = K_b, me1, me2, N_b$

IF aborted THEN

(2) $TTP \to B$: $mrb2 = abort\_token$

ELSE

(3) $TTP \to B$: $mrb3 = m, N_a$.

协议的 $resolve\_A$ 子协议如下:

(1) $A \to TTP$: $mra1 = K_a, me1, me2, m, N_a$

IF aborted THEN

(2) $TTP \to A$: $mra2 = abort\_token$

ELSE

(3) $TTP \to A$: $affidavit\_token = affidavit, mra1, \{affidavit, mra1\}_{K_{ttp}^{-1}}$.

下面,我们详细阐述 exchange 子协议与 resolve_A 子协议的工作流程,abort 子协议与 resolve_B 子协议可以类似地理解.

exchange 子协议的第 1 步,*A* 生成临时值 N_a;计算 $h(m)$;生成加密邮件 *C*;并将消息 *me*1 发送给 *B*.第 2 步,如果 *B* 未在合理的时间内收到 *me*1,则可以终止协议的执行,不会产生任何影响.否则,*B* 生成临时值 N_b,将消息 *me*2 发送给 *A*.第 3 步,如果 *A* 未在合理的时间内收到 *me*2,则可以终止协议的执行,转而执行 abort 子协议.否则,*A* 将消息 $me3=(m,N_a)$发送给 *B*.第 4 步,如果 *B* 未能及时收到 *me*3,则可以终止协议的执行,转而执行 resolve_B 子协议.否则,*B* 向 *A* 发送消息 $me4=N_b$.此后,如果 *A* 未能及时收到 *me*4,则可以终止协议的执行,转而执行 resolve_A 子协议.否则,exchange 子协议正常结束.

resolve_A 子协议的第 1 步,*A* 将消息 mra1 发送给 TTP.第 2 步,如果协议此时已被中断,即 aborted=true,则 TTP 向 *A* 发送 abort_token.否则,TTP 令 resolve_A=true,并向 *A* 发送 affidavit_token.

3.2 TTP的角色与Asokan-Shoup-Waidner协议分析

Asokan-Shoup-Waidner 协议是典型的 offline TTP 协议,只有当必须提供可信第三方服务时,TTP 才参与协议的运行.Asokan 等人将他们的方法称之为“乐观方法(optimistic approach)”,因为他们认为,乐观地讲大多数参与协议的主体都会服从协议的执行,只有少数主体可能会有主动的欺骗行为或被动的失误行为.因此,在满足上述假设的工作环境下,应当对大多数协议主体提高协议的运行效率.基于这种设计思想,Asokan-Shoup-Waidner 协议尽量提高 exchange 子协议的效率.但是,exchange 子协议需要两次传输邮件 *m*,一次通过 *me*1 传送密文邮件 *C*,一次通过 *me*3 传送明文邮件 *m*.因此当邮件 *m* 很大时,协议的效率可能会降低.

当协议正常结束时,亦即执行 exchange 子协议正常终止,未执行其他子协议时,*A* 获得收到邮件 *m* 的非否认证据 $EOR=(me1,me2,N_b)$;*B* 获得发送邮件 *m* 的非否认证据 $EOO=(me1,N_a)$.所以,协议满足可追究性.显然,在通信信道可靠的情形下,协议满足公平性.Asokan-Shoup-Waidner 协议假定,TTP 与协议主体之间的通信信道是可恢复的,亦即协议传送的消息最终可以送达.在这种情形下,协议也满足公平性.

abort 子协议是供邮件发送方 *A* 调用的,目的在于异常终止协议的执行.如果 *B* 已经执行 resolve_B 子协议,则不会向 *A* 发送 *me*4,因此 *A* 必然执行 resolve_A 子协议.但是,abort 子协议在这里出了毛病.因为,如果 *B* 此时未遵守协议,在向 *A* 发送 *me*2 之前即启动 resolve_B 子协议,则 *A* 由于没有 *me*2 就无法执行 resolve_A 子协议.在协议结束时,*B* 将获得邮件 *m* 与发送 *m* 的非否认证据 $EOO=(me1,N_a)$.但是,*A* 既未获得收到邮件 *m* 的非否认证据 $EOR=(me1,me2,N_b)$,又未收到 TTP 发出的交付邮件 *m* 的非否认证据 EOD,即包含 TTP 对 *me*1 和 *me*2 签名的 affidavit_token.因此在这种情形下,协议不满足公平性.

从以上分析可知,Asokan-Shoup-Waidner 协议存在冗余.首先,协议将临时值 N_a 作为 EOO 中的部分证据,这是没有必要的.事实上,*me*1 本身就是完整的发送 *m* 的非否认证据.在协议中,令 $EOO=me1$ 即可满足要求.因此,可以在整个协议中取消 N_a.其次,在 resolve_A 子协议中,*A* 没有必要向 TTP 发送 *m* 与 N_a.因为 *me*1 中含有 *C*,TTP 解密 *C* 后即可获得 *m* 与 N_a.

类似于 Coffey-Saidha 协议与 CMP1 协议,当执行 abort,resolve_A 和 resolve_B 子协议时,邮件 *m* 中的内容向 TTP 公开,因此 Asokan-Shoup-Waidner 协议未能有效地保护邮件 *m* 的隐私性.

4 小 结

在安全电子商务协议中,可信第三方 TTP 的角色日益重要.几乎在所有实用的安全电子商务协议中,TTP 都在不同程度地发挥作用.本文通过 3 类不同的协议,即 Coffey-Saidha 协议、CMP1 协议和 Asoken-Shoup-Waidner 协议,指出 TTP 在 inline TTP 协议、online TTP 协议和 offline TTP 协议中的不同作用,并对上述协议进行了全面的分析.本文从电子商务协议的安全性质出发,如非否认性、可追究性、公平性、隐私性以及冗余性和效率等方面,分别指出了上述协议的特点、缺陷与改进方法.

对 TTP 的信任程度,不同的协议作了不同的假设.例如在极端情形,假设 TTP 的所有行为均可信赖.又如,对 TTP 作“允许 TTP 失误,但 TTP 不与协议主体合谋欺骗”的假设等.在理论上,对 TTP 的信赖程度越高,越容易证

明协议满足安全需求,但在实用上,越难找到这样的可信第三方.今后,我们将在这一方向作更为细致的形式化工作.

References:

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

[2] Qing, SH. Design and logical analysis of security protocols. Journal of Software, 2003,14(7):1300~1309 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1300.htm.

[3] Qing, SH. 20 Years Development of Security Protocols Research. Journal of Software, 2003,14(10):1740~1752 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1740.htm.

[4] ISO/IEC 3rd CD 13888-1. Information technology--Security techniques Part 1: General model. ISO/IEC JTC11/SC24 N1274, 1996.

[5] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems, 1990,8(1):18~36.

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

[7] Zhou DC, Qing, SH, Zhou ZF. Limitations of Kailar logic. Journal of Software, 1999,10(12):1238~1245 (in Chinese with English abstarct).

[8] Zhou DC, Qing SH, Zhou ZF. A new approach for the analysis of electronic commerce protocols. Journal of Software, 2001,12(9): 1318~1328 (in Chines with English abstract).

[9] Coffey T, Saidha P. Non-Repudiation with mandatory proof of receipt. Computer Communication Review, 1996,26(1):6~17.

[10] Deng RH, Gong L, Lazar AA, Wang W. Practical protocols for certified electronic mail. Journal of Network and Systems Management, 1996,4(3):279~297.

[11] Asokan N, Shoup V, Waidner M. Asynchronous protocols for optimistic fair exchange. In: Proceedings of the 1998 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998. 86~99.

附中文参考文献:

[1] 卿斯汉.密码学与计算机网络安全.北京:清华大学出版社.2000.

[2] 卿斯汉.安全协议的设计与逻辑分析.软件学报,2003,14(7):1300~1309. http://www.jos.org.cn/1000-9825/14/1300.htm.

[3] 卿斯汉.安全协议 20 年研究进展.软件学报, 2003,14(10):1740~1752. http://www.jos.org.cn/1000-9825/14/1740.htm.

[7] 周典萃,卿斯汉,周展飞.Kailar 逻辑的缺陷.软件学报,1999,10(12):1238~1245.

[8] 周典萃,卿斯汉,周展飞.一种分析电子商务协议的新工具.软件学报,2001,12(9):1318~1328.