一种分析电子商务协议的知识与信念模型*

刘文远[1]，魏　刚[1]，司亚利[2]
（1. 燕山大学 信息科学与工程学院，河北 秦皇岛 066004；2. 燕山大学里仁学院，河北 秦皇岛 066004）

摘　要：针对现阶段电子商务协议形式化分析的处理比较混乱、表述精确度不高且通用性较差、存在一些不合理的假设等问题，运用现代模态逻辑理论，结合知识与信念，提出了一种分析电子商务协议的模型：知识与信念模型。该模型主要包含安全环境、知识集、信念集、能力集、切入点和知识化等因素。知识与信念模型很好地解决了上述问题，能够细致、精准地对各种电子商务协议进行形式化描述，并为不同的分析方法提供了模型支持。

关键词：知识与信念模型；电子商务协议；现代模态逻辑
中图分类号：TP311　　**文献标志码**：A　　**文章编号**：1001-3695(2012)05-1702-05
doi:10.3969/j.issn.1001-3695.2012.05.026

Knowledge and faith model of electronic commerce protocols

LIU Wen-yuan[1], WEI Gang[1], SI Ya-li[2]
(1. *College of Information Science & Engineering, Yanshan University, Qinhuangdao Hebei* 066004, *China*; 2. *Liren College of Yanshan University, Qinhuangdao Hebei* 066004, *China*)

Abstract: At this stage, the process of electronic commerce protocol formal analysis is chaotic; description have low versatility and accuracy, usually has some unreasonable assumptions. This paper presented a model—knowledge and faith model—used modern theory of morden modal logic according to knowledge and faith. The model contained the security environment, knowledge sets, faith sets, capability set, the tangent point and toknowledge. The model put forward a good solution to those problems, could formal descript different electronic commerce protocols precisely, and provided a support for different analysis method.

Key words: knowledge and faith model; electronic commerce protocols; morden modal logic

0　引言

近年来电子商务活动发展迅速，已经成为日常消费行为和国家经济活动的重要组成部分。如何保证电子商务的安全，如何保证所采用的电子商务协议的安全可靠，成为当今研究的热门课题。

目前分析安全协议的方法大体可以概括为四类：

a）移植分析通用协议的形式化技术和验证方法，对安全协议进行建模处理和分析验证，此方法不是专门针对安全协议而设计的，可以分析部分协议的部分性质，但对安全协议不具有通用性。

b）在协议设计过程中同步进行的安全性分析，协议设计者通过设计专门的验证方案来验证所设计的安全协议，此方法仅针对于特定的安全协议。

c）基于密码学系统的代数特性对协议进行形式化分析，侧重对协议的算法安全。

d）基于模态逻辑对协议进行形式化分析，侧重协议的逻辑安全。电子商务协议分析是由安全协议分析发展而来的，在认证协议和密钥交换协议的基础上对协议进行分析。基于模态逻辑的分析方法主要有 BAN 类逻辑、串空间和 SPI 演算[1]等。BAN 逻辑主要是对协议主体所拥有的信念进行推理，主体信念单调递增，协议运行结束时，各方达到最终信念，但不考虑知识和不诚实的协议主体[2]；串空间是用图的形式表达协议的执行过程，协议的一个丛就是协议的一个并发运行，协议安全性质通过所有丛保持的性质来刻画。SPI 演算是利用 PI 演算来描述和分析基于密码学的安全协议分析方法，给每个通道和消息赋予类型，将协议安全性的达到归结为协议执行过程中类型的保持，类型的破坏将导致安全性的丧失。

Kailar 和卿斯汉等人对电子商务协议的分析作出了重大贡献。Kailar 逻辑提出了一种可以用来分析电子商务协议可追究性的方法，完善了公理系统和推理过程的概念。卿斯汉等人在分析 Kailar 逻辑的基础上，指出其三个缺陷并对其进行改进，进一步优化 Kailar 逻辑的分析方法。

电子商务协议的建模处理研究不多，多数电子商务协议的分析方法仅进行了粗糙的初始化假设，对于协议的描述不够精确，同时也存在一些不合实际情况的假设。在安全协议分析方面有 D-Y 模型、GSPM[3]等。D-Y 模型在分析过程中引入攻击者的概念，为分析协议的安全性作出了重要贡献。GSPM 的分类思想使得对协议的形式化表述更加精确，但是这些模型对电子商务协议不具有通用性，不能分析电子商务协议的可追究性[4]、公平性[5]、隐私性等性质。

本文在现有方法的基础上，通过对电子商务协议的深入研

收稿日期：2011-10-15；**修回日期**：2011-11-23　**基金项目**：国家自然科学基金资助项目(60970123)；河北省自然科学基金青年科学基金资助项目(G2011203195)

作者简介：刘文远(1968-)，男，教授，博导，CCF 高级会员，主要研究方向为软计算、数据库、电子商务等；魏刚(1985-)，男，硕士研究生，主要研究方向为电子商务协议(wozhaoweigang@163.com)；司亚利(1981-)，女，讲师，硕士，主要研究方向为电子商务.

究,提出了电子商务协议的知识与信任模型。

1　电子商务交易体系

电子商务交易体系是一个包含买卖双方、网络金融服务机构、网络认证机构、电子支付工具和网上银行等各方的网络交易体系(图 1)。要进行电子商务交易一般需要经过以下过程:

a)基础设施建设。首先要建立一套安全可靠的 PKI 信用体系,用于用户的注册和认证;其次银行应具有网络支付和结算能力,通过支付网关及安全可靠的银行网络,确保银行之间的安全结算;最后必须要有基础的 Internet 网络服务。

b)用户注册。各个协议主体要通过 PKI 注册成为合法用户,PKI 为各个主体提供身份证书、公钥和私钥。一般需要注册的主体有交易双方、提供公众服务的可信第三方、各银行。

c)银行开户。主要指参与交易的双方向银行提出开通电子账户的申请,银行根据交易方的实际账户接受申请,并为用户提供支付工具和结算工具。这里银行专指具有网上资金交易和结算功能的机构。

d)交易流程。各协议主体根据需要通过 PKI 相互验证各方身份的合法性:第一步,买方向卖方发送订单,提出交易请求;第二步,卖方验证请求的有效性,反馈确认信息;第三步,买方根据银行提供的支付工具向卖方发送付款信息;第四步,卖方将付款信息转发给银行;第五步,银行验证资金的有效性,并将信息反馈给卖方;第六步,卖方接收到有效信息后发货,买方向银行发送支付指令,银行间完成资金的结算。电子商务交易体系交易流程图如图 2 所示。

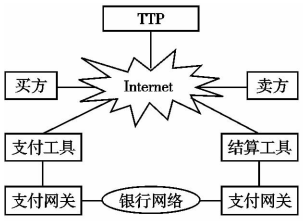

图1　电子商务交易体系结构

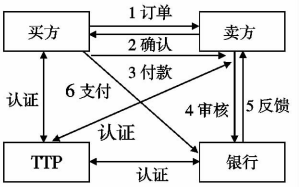

图2　电子商务交易体系交易流程

2　知识与信念模型

知识与信念模型是采用现代模态逻辑理论,以电子商务交易体系为基础提出的一种用于分析电子商务协议的模型。

2.1　模型实体

电子商务是基于计算机网络的利用计算机技术、网络技术和远程通信技术等信息技术实现交易过程中信息流、资金流和数字流的电子化、数字化与网络化的商务活动。

在电子商务交易体系中(图 3)一般认为具有以下实体:买方 P、卖方 S、阴谋者 I、可信第三方 T、银行 B、Internet 网络。合法用户是指协议中明确定义、始终按照协议规定进行执行的诚实用户。其中,阴谋者 I 为非法用户。

买方 P 与卖方 S 是交易构成中最主要的两个实体,双方进行信息与资金的交流,以完成交易活动。其他协议规定实体都是为双方能够安全公平地完成交易服务。

阴谋者 I 是分析电子商务协议时主要考虑的实体,要验证一个电子商务协议是否安全可靠,就是要验证阴谋者 I 的目的是否能够达成,包括窃取交易信息、账户信息等机密、干扰协议执行。

可信第三方 T 是一类机构的统称,包含 PKI 信用体系以及其他提供公共服务的机构。银行由于其直接参与资金交易的特殊性,单列为一类主体,代指一切与银行有关的机构,包含银行支付网关、各银行实体和银行网络。

Internet 网络作为实现信息交换的渠道,在电子商务中占有重要的地位。除了银行间的信息交换在银行专用网络上进行以外,其他交易信息都是通过 Internet 网络来完成的,这是电子商务安全的薄弱环节,也是阴谋者常选的攻击环节。

2.2　安全环境

根据电子商务交易体系,电子商务协议的环境包含以下四个方面:买方/卖方环境、Internet 网络环境、PKI 环境、银行网络环境。

银行网络采用 VPN、防火墙、内网专线等安全技术,理论及实际应用都证实了这是一种十分安全的网络,因此在分析电子商务协议时,默认银行网络环境为完备的安全环境。同样也认可 PKI 环境是一种完备的安全环境。Internet 网络环境的主要作用是基于 TCP/IP 等协议进行交易信息的传输,是一个比较复杂的环境。由于其环境的多变性和不可控制性,经常成为阴谋者首选的攻击点。

买方/卖方环境是基于计算机终端主机的一种比较复杂的单机环境,客户通过本地计算机环境对协议的客户端进行操作。基于本地计算机环境的信息窃取一般利用操作系统和应用软件的漏洞和后门、hook、进程注入和内存注入等黑客技术直接窃取计算机用户的信息,对电子商务安全产生巨大威胁。买方/卖方环境的安全是电子商务协议能够发挥作用的基础,是其必备的前提条件。据此,将电子商务协议的运行环境分为三个安全层次,即理想环境、自然环境和攻击环境。

1)理想环境　理想环境是一种高度理想化的环境,在现实情况下一般不会存在,但可以作为设计电子商务协议的简单初步模型。在理想环境下,参与协议的各个主体都是协议本身规定的合法用户,没有进行窃取和偷听的攻击者和非法第三方;Internet 网络环境安全可靠,能够及时准确地传输用户的信息和数据,不会在传输过程中泄密;各个协议主体不进行私下传输信息的共谋行为,但不禁止协议单方的伪造、抵赖和终止协议的行为。

2)自然环境　自然环境是电子商务协议在实际运行时所遇到的一般环境。若协议在自然环境下能够可靠运行就算是一个成功的设计。在自然环境中,没有进行阴谋破坏的攻击者,但包含不法的窃听者;Internet 网络能够完成传输用户的信息和数据的功能,但不能保证信息的及时性,并且有泄露信息的可能性;各个协议主体不进行私下传输信息的共谋行为,但不禁止协议单方的伪造、抵赖和终止协议的行为。

3)攻击环境　攻击环境是协议运行时的极端恶劣的环境。电子商务协议由于其自身的特殊性,必须要具有在极限下的安全可靠性。在攻击环境中,除协议规定的合法用户外,还存在阴谋破坏的攻击者[6]。Internet 网络能够完成传输用户的信息和数据的功能,但不能保证信息的及时性,并且有泄露信息的可能性。攻击者对 Internet 网络具有完全的掌控能力,具体表现为以下两个方面:一是攻击者具有截获通过 Internet 的信息和任意阻断通信的能力,造成信息传输的延迟或者中断,特殊的,若攻击者阻断通信并且没有进行伪造或修改转发信

息,造成接收者无法收到信息,协议将终止;二是攻击者具有对截获的信息进行读取、修改、存储和转发的能力,攻击者可以根据自己掌握的信息来对截获的信息进行部分解密或完全解密,依据自身信息对截获的信息进行添加、删除和修改的操作,还可以将修改后的信息发送给原接收者或其他接收者。攻击者除了对 Internet 网络的控制能力外,还可以作为合法用户出现,发起与任意协议主体的合法对话。协议主体可以进行单方的伪造、抵赖和终止协议的行为,并可以进行共谋欺骗。电子商务协议的分析是在攻击环境下进行的。

2.3 协议语句的语义

电子商务协议分析首先要对协议进行简单的形式化表述,即协议语句的理解[7]。根据协议语句的功能,将电子商务协议语句分为两大类:a)处理信息的语句,包含身份认证、信息匹配、字符串处理和加解密操作等;b)交换信息的语句,即通过网络向对方发送信息。在本模型中,将处理信息的语句视为该协议主体的一种处理信息的能力,并作为该协议主体下一条交换信息语句的执行条件。因此将协议视为由一系列有序的交换信息的语句构成。

对于协议主体处理信息的能力,用能力集和信息集来表示。能力集是指协议主体对信息进行处理时可采用方法的集合,是协议设计者在设计阶段所规定的,不随协议语句的执行而变化;信息集是指协议主体所占有的全部信息的集合,用知识集 Ks 和信念集 Fs 来表示。信息集是影响协议主体能力的主要方面,随着协议的进行,知识集和信念集不断变化,协议主体的能力也不断变化。因此,协议的执行过程可以抽象成在分布式环境中运行计算的一个分布式算法。每一句协议语句的执行都会对协议各主体的能力产生不同的影响,协议的执行过程就是分布的各协议主体能力不断变化的过程。电子商务协议的执行如图 4 所示。

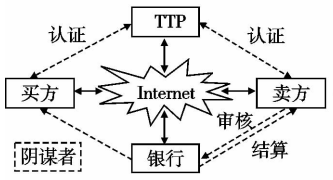

图3 电子商务交易体系

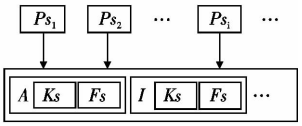

图4 电子商务协议的执行

同时,协议的执行过程还有一个重要的特性,即可中断性。协议主体可以拒绝执行协议规定的自身当前操作,使协议终止。可信第三方 TTP 是协议中的一个特殊存在,总是按照协议规定执行当前的所有操作,不会主动终止协议的执行,被其他各方所共同信任。

为方便表示,将协议的语句记为 Ps,协议的第一句记为 Ps_1,协议的第 i 句记为 Ps_i。协议 P 即可以记为

$$P=\{Ps_1,Ps_2,\cdots,Ps_i,\cdots\}$$

协议 P 的第 i 步语句 P_{si}:A 向 B 发送信息 M,表示为

$$Ps_i:A\rightarrow B:\{A,B,M\},\{\ \text{limit}\ \}$$

其中:A、B 为参与协议的任一主体;{ limit } 为执行条件。

将协议的状态记为 T,协议的初始状态为 T_0,协议语句 Ps_i 执行完成后,协议状态转换为 T_i。

2.4 知识与信念

电子商务协议中包含有多种类型的信息,为了对协议进行更精确的描述,将协议中的信息分为以下两类:

a)原子信息 Am,即不可进行分解的信息,包含公开密钥 Ek、私密密钥 Dk、对称密钥 Sk、临时变量 TV、明文 m。

b)复合信息 Cm,即由原子信息 Am 经过拼接、删减、加密等操作合成的信息。Cm 是网络中传输的正式信息,包含 Am、$M\mid m$、$K(M)$、hash(M)等。$M\mid m$ 表示原子信息和复合信息的相互拼接;$K(M)$ 表示对原子信息或复合信息的加密变换;hash(M)表示对原子信息或复合信息的哈希变换。

定义 1 对电子商务协议主体 A 所占有的信息集 $M=\{m\mid m\in A\}$,将满足 $m\in Am$ 的信息归为集合 Ks,即 $Ks=\{m\mid m\in M$ 且 $m\in Am\}$,则 Ks 就叫做协议主体 A 的知识集,并将集合 M 中的其余信息归为另一类 Fs,即 $Fs=\{m\mid m\in M$ 且 $m\notin Am\}$,则 Fs 就叫做协议主体 A 的信念集。

知识集是由一系列原子信息构成的信息集合,信念集是由一系列复合信息构成的信息集合。任何一个协议主体的信息集都是由其知识集和信念集构成,随着协议语句 Ps 的执行,Ks 和 Fs 都不断变化,协议主体的能力也不断增强,最终达到协议设计的目的。

定义 2 某协议主体对任一信息 m 依据自身处理信息的能力,通过解密、拼接、删减等操作得到新信息的集合 $Ft=\{m_1,m_2,\cdots\}$,且集合 Ft 中的任一元素 m_i 不能通过其余元素的拼接、删减、加密等复合操作来构成,则将信息 m 到集合 Ft 的转换过程称为因子化,并将集合 Ft 称为信息 m 的全因子。

若信息 m 的全因子 Ft 中的任一元素都不能再进行因子化,则称集合 Ft 为信息 m 的最简全因子。

若 $Ft\subset Ks$,即 Ft 中所有元素都是原子信息,则称集合 Ft 为信息 m 的全质因子。

若信息 m 的全因子 Ft 能够依据协议主体自身处理信息的能力,通过其中元素的拼接、删减、加密等复合操作,还原成为 m,则称 m 到 $Ft=\{m_1,m_2,\cdots\}$ 的过程为完全因子化。

协议主体因子化的能力与该主体处理信息的能力有着直接的关系。协议主体处理信息的能力由能力集和信息集共同构成,其中能力集固定不变,信息集不断变化。因此,协议主体因子化的能力随着协议语句的执行以及协议主体的知识集 Ks 和信念集 Fs 的变化而不断变化。

定理 1 在协议主体的固定 Ks 和 Fs 环境下,信息 m 的最简全因子 Ft 的中元素组成是唯一的。

证明 设该协议主体为 A,信息 x、y 不能进行因子化,存在一种 A 能够处理的运算 *,构成信息 x^*y。

因为 A 的 Ks、Fs 都是固定的,A 所能够处理的运算 * 的集合是固定的;因为对于信息 x^*y,当对其进行因子化必然存在唯一的最简全因子形式 $\{x,y\}$,所以根据递推原理可得,信息 m 的最简全因子 Ft 的中元素组成是唯一的。

定义 3 将信念集中的信息依据自身的能力进行因子化,此过程中新生成的原子信息并入知识集,新生成的复合信息并入信念集,若完全因子化则将此复合信息从信念集中删除,这一过程叫做知识化。对所有信息进行知识化处理后,新生成的知识集称为最大知识集,新生成的信念集称为最简信念集。一般地,当谈及知识集 Ks 时即指最大知识集,信念集 Fs 即指最简信念集。

定义 4 信息 M 为最简信念集 Fs 中的一个信息,Ft 为信息 M 的完全因子化后的全质因子,定义集合 $Is=\{m\mid m\in Ft$

且 $m \notin Fs\}$ 为信息 M 的索引因子。

协议开始执行时,按照协议的规定,每个协议主体对自身的知识集和信念集进行初始化。一般地,对于拥有 PKI 的体系结构,根据 PKI 的功能可知知识集 Ks 包含所有协议主体的公开密钥、自身的私密密钥,信念集合为空。

在协议执行过程中,主体通过发送或者接收取得信息 M 时,进行以下操作:

a)对信息 M 进行因子化得到 M 的最简全因子 $Ft = \{m_1, m_2, \cdots\}$。

b)对 Ft 中的信息进行分类:$Ft_1 = \{m \mid m \in Ft$ 且 $m \in Am\}$;$Ft_2 = \{m \mid m \in Ft$ 且 $m \notin Am\}$。

c)生成新的知识集和信念集:$Ks = Ks \cup Ft_1$;$Fs = Fs \cup Ft_2$。

d)对于新生成的信念集 Fs,对其中的元素按照 $Ft = \{m_1, m_2, \cdots\}$ 检索索引因子进行最简因子化。若存在一个信息 M' 可以进行因子化,则重复步骤 c);若完全因子化将 M' 从信念集 Fs 中删除;若不存在,则操作终止。

e)重复上述过程直至信念集 Fs 中的所有元素都不能进行因子化。

2.5　主体能力

协议主体的能力具体体现为协议主体处理信息的能力,在本模型中通过信息集和能力集来描述。信息集体现了协议主体占有信息的情况,能力集体现了协议主体在处理信息时所能够采用的方法。在模型中能力集由三种基本能力和一种扩展能力—切入点构成。

1)基本能力

在协议设计的过程中,设计者使用了许多不同的安全策略,同时也对协议主体的动作和行为进行了详细的规定,协议主体具有多种特有的能力,如对信息进行拼接修改、加密解密、数字签名、身份认证、哈希运算等。

由于不同的电子商务协议所使用的安全技术各不相同,为了增强模型的通用性,在此将协议主体所具有的对信息处理的能力归纳为以下三类:

a)不可逆操作 $Hs()$。主要包含生成信息摘要,加盖时间戳等操作。

b)同因子可逆操作 $Sk()$。这一类操作是可逆的,且变化和逆变换所使用的因子是相同的,对称加解密算法是典型的例子。类似地,将对字符串的添加、删除、修改等一般字符变换也归为此类,变换因子为所操作的字符串。

c)异因子可逆操作 $Ek/Dk()$。此类操作主要是公开密钥加密算法。

在分析电子商务的过程中,借鉴 D-Y 模型的假设,认为协议中所采用的安全算法都是具有强可靠性的完美密码体制,即在截获密文而不知道密钥的情况下,无法通过暴力破解、猜测攻击等破解手段获得明文。忽略安全算法的内部计算,能更加关注协议的结构以及由此产生的安全问题,而不是纠缠于所使用的安全算法本身,使分析更具有目的性和针对性。

2)切入点

除去上述三种基本操作,根据协议语句的功能引入切入点 Tf 的概念。

定义 5　切入点是协议主体设计的一种特定功能,是由与协议主体相关的前后相联系的一个接收信息语句和紧接其后的一个发送语句抽象而得的多元参数函数。函数的输入集为当前接收语句所包含的信息;执行条件为当前主体所进行的信息处理;输出集为当前发送语句所包含的信息。

$$\mathrm{tf} = \begin{cases} \{\mathrm{limit}\}.A & \text{执行条件} \\ \mathrm{In}(ft(m)).A & \text{函数的输入信息集} \\ \mathrm{out}(M).\mathrm{A} & \text{函数的输出信息集} \end{cases}$$

其中:$ft(m)$ 表示输入信息的全因子的集合。

协议主体的上述四类功能是协议达成既定的安全目的的必须的功能,同时也为攻击者留下了攻击方式,作为攻击者的一种能力而存在。

2.6　攻击实例

下面就 D-Y 模型所提及的攻击实例,用切入点进行简单分析。

实例中具有两方 A 和 B,A 发送信息 M 给 B,B 反馈给 A 一个信息证明自己已经接收到该信息 M。协议的具体步骤如下:

a)A 向 B 发送信息$(A, B, E_B(E_B(M) \mid A))$;

b)B 应答 A,回应$(B, A, E_A(E_A(M) \mid B))$。

进行形式化转换,以使协议内容更加清晰,并利于后面的分析处理。该协议可进行如下表述:

$$P = \{Ps_1, Ps_2\}$$
$$Ps_1 : A \rightarrow B : \{A, B, E_B(E_B(M) \mid A)\}$$
$$Ps_2 : B \rightarrow A : \{A, B, E_A(E_A(M) \mid B)\}$$

在攻击者 I 存在时,D-Y 给出的攻击模式过程如下:

a)A 和 B 正常通信,执行协议语句 Ps_1。

b)Ps_1 经过 Internet 网络,攻击者 I 截获信息 $E_B(E_B(M) \mid A)$,并构造信息 $M' = E_B(E_B(E_B(M) \mid A) \mid I)$。

c)I 向 B 发起新的会话,执行协议语句 Ps_1,发送信息 M',即执行 $Ps_1 : I \rightarrow B : \{I, B, E_B(E_B(E_B(M) \mid A) \mid I)\}$。

d)B 收到 I 的信息后应答,执行:$Ps_2 : B \rightarrow I : \{B, I, E_I(E_I(E_B(M) \mid A) \mid B)\}$。

e)在过程 c)d)中,I 作为合法用户存在,有自己的公钥和私钥,I 接收到信息 $E_I(E_I(E_B(M) \mid A) \mid B)$ 后,利用自己的私钥进行解密:

$E_I(E_I(E_B(M) \mid A) \mid B)$

$\xrightarrow{D_I} E_I(E_B(M) \mid A) \mid B$　用 I 的私钥 D_I 解密

$\xrightarrow{B} E_I(E_B(M) \mid A)$　删除字符串 B

$\xrightarrow{D_I} E_B(M) \mid A$　用 I 的私钥 D_I 解密

$\xrightarrow{A} E_B(M)$　删除字符串 A

f)I 再次发起新的会话,发送信息 M'':

$$M'' = E_B(E_B(M) \mid I)$$
$$Ps_1 : I \rightarrow B : \{I, B, E_B(E_B(M) \mid I)\}$$
$$Ps_2 : B \rightarrow I : \{B, I, E_I(E_B(M) \mid B)\}$$

g)I 接收到信息 $E_I(E_I(M) \mid B)$,进行解密处理得到 A 和 B 之间的通信信息 M。

利用本文模型的方法可以简化分析过程,使逻辑推理更为清晰,得到此类问题的通用解法。分析过程如下:

a)对 I 的知识集 Ks 和信念集 Fs 进行初始化。

$$Ks = \{D_I, E_I, E_A, E_B, I, A, B\}$$
$$Fs = \Phi$$

b)经过 Ps_1、Ps_2,对截获到的信息 $E_B(E_B(M) \mid A)$,E_A

$(E_A(M) \mid B)$进行知识化,可以得到

$$Ks = \{D_I, E_I, E_A, E_B, I, A, B\}$$
$$Fs = \{E_B(E_B(M) \mid A), E_A(E_A(M) \mid B)\}$$

c)分析协议的结构,得到主体 B 的切入点

$$Tf = \begin{cases} \{\text{limit} \mid .B & \text{执行条件} \\ \text{In}(ft(m)).B & \text{函数的输入信息集} \\ \text{out}(M).B & \text{函数的输出信息集} \end{cases}$$

对输入信息集$\{I, B, E_B(E_B(m') \mid I)\}$进行因子化可得到 $ft(m)$的另外形式$\{I, B, E_B, m'\}$;$\{I, B, E_B, E_B(m')\}$。所以 $ft(m) = \{\{I, B, E_B(E_B(m') \mid I)\}, \{I, B, E_B, m'\}, \{I, B, E_B, E_B(m')\}\}$。其中 $M' = \{B, I, E_I(E_I(m') \mid B)\}$,对于攻击者 I 可以进行因子化,得到 $M' = \{B, I, E_I, m'\}$。

d)对于攻击者 I,由于 $E_B(E_B(M) \mid A) \in Fs$,因此可以利用 Tf 中 $ft(m) = \{I, B, E_B, E_B(m')\}$,得到 $m' = E_B(M) \mid A$;对于 m'进行知识化可以得到 $E_B(M)$,此时知识集和信念集为:

$$Ks = \{D_I, E_I, E_A, E_B, I, A, B\}$$
$$Fs = \{E_B(M), E_A(E_A(M) \mid B)\}$$

对于攻击者 $I, E_B(M) \in Fs$ 再次利用切入点 $Tf, ft(m) = \{I, B, E_B, E_B(m')\}$可以得到 $m'' = M$。至此完全破解 A 与 B 之间的通信内容。

3 协议属性分析

本文提出的知识与信念模型是一种通用模型,可以应用于各种不同的形式化分析方法中。在此不限定具体的分析方法,仅对该模型在协议的安全性、可追究性、公平性、隐私性方面作出简单的判定。

3.1 安全性

安全性[8]是电子商务协议首要考虑的内容。在知识与信任模型中采用了类似的攻击者模型来验证。攻击者依据自身占有的知识集和信念集,运用基础能力对信息进行修改处理,运用合法身份通过切入点完成对协议的攻击。

定理 2 若协议 P 是安全的,则对于任一主体 A 对信息集知识化后,除自身私钥 D_A 外的任意私钥都不包含与 A 的知识集 Ks,即不存在集合 $D_X\{X \mid A \notin X\}$ 中的 X,使得 $D_X \in Ks$ 成立。

证明 设某协议主体 D,其私钥为 D_X,若协议主体 A 的知识集 Ks 满足 $D_X \in Ks$,则协议主体 A 具有通过 D_X 处理信息的能力,如破解某些密文信息、伪造 D 的签名等,所以该协议不满足安全性要求。

因此,若协议 P 是安全的,则不存在集合 $D_X\{X \mid A \notin X\}$ 中的 X,使得 $D_X \in Ks$ 成立。

定理 3 若协议 P 是安全的,则对于阴谋者 I 经过信息知识化后,信息 $m \notin Ks$。

证明 设对于阴谋者 I,其知识集 Ks 存在 $m \in Ks$,则表示 I 已经获得了通信双方的信息,密文已经被破解明文信息泄露,所以该协议不满足安全性要求。

因此,若协议 P 是安全的,则对于阴谋者 I 经过信息知识化后,信息 $m \notin Ks$。

3.2 可追究性

可追究性是电子商务协议纠纷处理的重要组成部分。在交易双方产生纠纷时,各方都能证明另一方对该信息的发送或接收负责[9],主要通过发送方非否认证据 POO 和接收方非否认证据 POR 来实现的[2]。发送方非否认证据是由接收方占有的用于证明发送方曾经向接收方发送过信息 M 的一种信息字段;接收方非否认证据是由发送方占有的用于证明接收方已经接收信息 M 的一种信息字段。

定义 6 若协议 P 是可追究的,那么交易双方 A 和 B 进行知识化后必然都满足:对于发送方 A 有 $\text{POR} \in Fs$;且对于接收方 B 有 $\text{POO} \in Fs$。

3.3 公平性

公平性是指在电子商务执行的任意阶段,交易双方都处于公平的地位,都不会优先占有信息或提前作出承诺。一方占有信息必然导致另一方也占有对应的信息,一方作出承诺另一方也必然作出等价的承诺,可以存在时间的先后,但是当一方的行为发生时,必然出现另一方的相应行为[10]。

与事件发生概率密切相关的是协议的可中断性,涉及买卖双方、阴谋者和可信第三方。买卖双方可以拒绝执行协议规定的自身的当前操作,使协议终止;阴谋者可以阻断交易双方的通信,致使接收方无法收到信息,协议终止;可信第三方 TTP 是协议中的一个特殊存在,总是按照协议规定执行当前的所有操作,不会主动终止协议的执行,被其他各方所共同信任。由于可信第三方的可靠性,认为 TTP 总会将信息发送给接收者,而不会被阴谋者始终阻断。

定义 7 若协议 P 是公平的,那么交易双方 A 和 B 进行知识化后必然满足:当发送方 A 发生 $\text{POR} \in Fs$ 时接收方 B 发生 $\text{POO} \in Fs$ 的概率为 1;或当接收方 B 发生 $\text{POO} \in Fs$ 时发送方 A 发生 $\text{POR} \in Fs$ 的概率为 1。

3.4 隐私性

由于商业机密和个人隐私需求,在电子商务交易活动中,协议主体不希望暴露自己的身份、交易信息等,因此隐私性也是电子商务协议应该考虑的一个重要方面。

定义 8 在协议 P 中,对于任意协议主体 A,进行信息的知识化后,若存在 $m \in Ks$,则称在协议 P 中信息 m 对协议主体 A 不具有隐私性;若 $m \notin Ks$,则称在协议 P 中信息 m 对协议主体 A 隐私。

4 结束语

知识与信念模型基于现代模态逻辑,通用性强,对协议环境、协议实体、信息字段和主体能力都作了详细分析,并且根据实际进行了分类处理。首创性地提出了知识集、信念集、知识化、全因子、切入点等概念,对电子商务协议进行了清晰、合理、完善的形式化描述。三层安全环境的提出,明确了各安全级别分析所需面对的问题。将协议主体的能力定义为占有信息的能力和处理信息的能力。占有信息的能力由知识集和信念集构成,通过知识化处理信息,更加精确地形式化了该能力,并且有效地解决了状态爆炸问题。能力集中切入点的提出,为攻击者的攻击问题提供了一般通用解决办法,不必再依赖现有的已知攻击模式。该模型细致、精准地对各种电子商务协议进行形式化的描述,并且为多种分析方法提供了理论的模型支持。

随着电子商务协议所采用的安全技术不断发展,新的技术会逐渐引入到电子商务协议中来,该模型的基础能力集会逐渐发生变化。因此模型的基础能力集应当依据安全技术的发展作进一步的更新和分类的细化。另外,本模型(下转第 1712 页)

(上接第 1706 页)提出了可用于攻击的切入点的概念,对切入点采用了简单的符合性匹配,没有对切入点的匹配算法进行研究。依据信息集对切入点的匹配使用应当在算法上作进一步的研究。

参考文献:

[1] 薛锐,冯登国. 安全协议的形式化分析技术与方法[J]. 计算机学报,2006,29(1):1-20.

[2] 卿斯汉. 一种电子商务协议形式化分析方法[J]. 软件学报,2005,16(10):1757-1765.

[3] GU Yong-gen,FU Yu-xi,ZHONG Fa-rong,*et al*. A generic model for analyzing security protocols[C]//Proc of the 3rd International Conference on Mathematical Methods,Models,and Architectures for Computer Network Security. Berlin:Springer Verlag,2005:119-128.

[4] BACKES M,MAFFEI M,UNRUH D. Zero-knowledge in the applieed PI-calculus and automated verification of the direct anonymous attestation protocol[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC:IEEE Computer Society,2008:202-215.

[5] WANG Zhang-kai. Analyzing a fair exchange e-commerce protocol using CSP and FDR[C]//Proc of International Conference on e-Education, e-Business, e-Management and e-Learning. Washington DC: IEEE Computer Society,2010:303-307.

[6] 陈锋,张怡,苏金树,等. 攻击图的两种形式化分析[J]. 软件学报,2010,21(4):838-848.

[7] BRIAIS S,NESTMANN U. A formal semantics for protocol narrations [J]. Theoretical Computer Science,2007,389(3):484-511.

[8] CATHALO J. Provable security and fairness in crypto- graphic identification and signature schemes[D]. Wallonie, Belgique: Université Catholique de Louvain,2007.

[9] SHAIKH S A,BUSH V J,SCHNEIDER S A,*et al*. Specifying authentication using signal events in CSP[J]. Computers Security,2009,28(5):310-324.

[10] 陈明,吴开贵,吴长泽,等. 公平交换协议形式逻辑[J]. 软件学报,2011,22(3):509-521.