吝啬语义信任协商

张 妍[1)] 冯登国[2)]

[1)](中国科学院软件研究所信息安全国家重点实验室 北京 100190)

[2)](信息安全共性技术国家工程研究中心 北京 100190)

摘 要 自动信任协商是通过数字证书的交互披露在陌生实体间建立信任的过程,现有的自动信任协商框架要求主体出示完整属性证书来证明自己满足对方资源披露策略中的身份断言约束条件,导致了属性证书中身份信息过度披露问题.该文中作者提出一种通过交换 DL-TNL 语义身份断言来建立信任关系的吝啬语义信任协商框架,避免了完整属性证书的直接出示,减少信任建立过程中身份信息被披露的程度,并提出一种正确、完备且有效的吝啬语义信任协商策略.在该策略下,交易双方的协商引擎可以快速有效地从由身份断言权威签发的包含多个 DL-TNL 语义身份断言的身份断言证书中,自动计算出批露最少信息且符合对方策略的身份断言集进行出示,以最大限度地减少信任建立过程中被披露的身份信息,并保证理论上存在成功可能性时,使用该策略必然可以有效地帮助主体最终获得网络资源的访问权限.有关该策略完备性和正确性的证明以及策略实施中所使用的符合性检测算法的实现和分析均在文中给出.

关键词 自动信任协商;语义方法;隐私保护;协商策略;符合性检测

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2009.01989

Parsimonious Semantic Trust Negotiation

ZHANG Yan[1)] FEN Deng-Guo[2)]

[1)](*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

[2)](*National Engineering Research Center of Information Security, Beijing* 100190)

Abstract Automated Trust Negotiation (ATN) is a process in which two unfamiliar entities exchange their digital attribute certificates in turn to set up mutual trust relationship with each other. Since existing ATN frameworks require entities to release entire attribute certificates to prove that they satisfy the identity constraint condition stated by the other entities' access control policies, private identity information of entities is often over-revealed in many circumstances. In this paper, the authors propose a novel parsimonious semantic trust negotiation framework in which entities can build trust relationship by exchanging DL-TNL semantic identity assertions instead of entire attribute certificates. This framework can greatly reduce the degree of disclosed private identity information. Under the framework, the authors propose a correct, complete and efficient parsimonious semantic trust negotiation strategy to allow the negotiation agencies of participants to compute and disclose a satisfying set of DL-TNL assertions which contains least private identity information at every exchange step. In a word, the parsimonious semantic trust negotiation strategy can minimize the disclosed private identity information in the trust negotiation processes and guarantees the resource requesters participating in the processes to get the access rights finally if there does exist a theoretical successful trust negotiation sequence. All of the proofs about

收稿日期:2009-07-15;最终修改稿收到日期:2009-08-24.本课题得到国家"八六三"高技术研究发展计划项目基金(2007AA120404,2007AA120405)资助.**张 妍**,女,1983 年生,博士研究生,主要研究领域为分布式授权、空间数据库安全.E-mail: zhy0202@is.iscas.ac.cn.
冯登国,男,1966 年生,教授,博士生导师,主要研究领域为网络与信息系统安全、密码理论与技术.

the properties of the strategy are given in this paper, so are the relevant compliance checking algorithms and their analyses.

Keywords automated trust negotiation; semantic method; privacy protection; trust negotiation strategy; compliance checking

1 引 言

身份属性证书交换是一种在不同安全域里共享资源或进行商业事务交易的陌生主体之间建立双方信任关系,帮助主体获得资源访问权限的重要手段. 属性证书往往包含敏感的隐私信息,如年龄、职业、个人特征等等,需要有一种方法来规范属性证书的交换. 一种灵活的管理身份属性证书交换的方法是自动信任协商(Automated Trust Negotiation,ATN). 自动信任协商根据主体设定的披露策略,和对方已经披露给自己的属性证书集合,判定是否可以进一步披露自己的属性证书和/或资源给对方,从而在交易双方之间建立多轮安全证书披露过程,保护主体的属性证书信息与个人隐私.

自 Winsborough 等人提出自动信任协商的概念以来,学者们对自动信任协商方法的各个相关领域展开了研究,包括自动信任协商语言[1-3]、协商策略[4-5]和符合性检测算法[6-7]、自动信任协商系统[8]等等,现有的研究所提出的方案普遍需要出示完整的属性证书来证明自己满足对方要求的某些身份断言——关于属性证书的约束条件,因而在协商过程中仍揭示了许多非必要的身份信息. 比如为满足对方"驾龄大于 10 年,准驾中型客车,住址在北四环以内"的要求,司机 Bob 在协商过程中不得不出示他的驾照:"名字:Bob,出生年月:1956 年 1 月,住址:北京市海淀区知春路某号某栋,类型:B1,发证日期:1997 年,签发者:交通管理局",根据交通法规,驾照类型为 A2 或者 B1 的司机准驾中型客车,因而该司机的驾照符合对方的要求,但是却造成了属性信息的过度披露:首先,无关属性信息,如 Bob 的生日被连带披露,其次,为满足身份断言对属性证书的抽象约束、发证日期、驾照类型、住址等属性的具体属性值被披露.

为此,本文提出一种改进的自动信任协商框架——吝啬语义信任协商,以身份断言的交换取代属性证书的直接交换,来进一步保护身份属性信息. 在吝啬语义信任协商框架中,我们提出了一种具有强推理能力和表达能力的属性证书,身份断言和策略描述语言 DL-TNL,并引入一个身份断言权威在检查主体拥有的所有属性证书后,为主体签发包含多个身份断言的身份断言证书,使得协商双方的协商引擎程序可以在协商过程中,执行符合性检测算法对 DL-TNL 所描述的证书、断言和策略进行自动解析和推理,计算出身份断言的组合出示方案来代替属性证书的完整出示,因而可从以下 3 个方面隐藏主体的身份信息:

(1)证书信息拆分. 每一种类型的属性证书通常包含了多个属性,在协商过程中对方可能只关注其中的一部分,而身份断言可以只对单个属性的信息进行声明,并单独出示,相当于对属性证书进行了拆分,避免了无关属性信息的出示.

(2)证书信息泛化. 身份断言可以实现 3 种信息的泛化,一是数值属性值的泛化,如使用"$>20(age)$"来代替"$age=30$"的出示,二是对象属性值的泛化,使用领域知识本体中的概念值来代替具体实例值的出示,如"address:北四环以内"代替"address:海淀区知春路某号某栋",三是证书颁发者具体信息的泛化,身份断言可以只对证书颁发者所满足的一些属性条件进行抽象描述,而不透露具体的证书颁发者名字.

(3)证书持有信息隐藏. 在信任协商的环境里,各种属性证书 CA 可发布委托授权声明,指明拥有某些其它 CA 颁发的属性证书的主体可视为拥有本 CA 颁发的虚拟属性证书,身份断言证书内同样可以包含这种虚拟属性证书所满足的身份断言,从而向对方隐藏其所拥有的真实属性证书.

为了最大化对协商参与方隐私的保护力度,我们在吝啬语义协商的框架下,进一步给出一种正确、完备并且有效的吝啬语义信任协商策略:在该策略下,协商双方的协商引擎程序可调用 extSSGen 算法计算出所有的身份断言替代出示方案并自动推理出其中泄露最少信息的方案以供出示,从而在交易双方之间建立包含最少隐私信息的身份断言披露序列和信任关系. 吝啬语义信任协商策略一方面可最大限度减少信任建立过程中披露的身份隐私信息,

另一方面其保证了只要理论上存在成功的可能,使用该策略必然可以有效地帮助主体最终获得网络资源的访问权限.

本文第 2 节介绍相关工作;第 3 节介绍进行吝啬语义信任协商的参考模型和主要框架;第 4 节介绍具有强表达能力和推理能力的身份断言和策略表达语言 DL-TNL;第 5 节介绍符合性检测算法;第 6 节介绍吝啬语义信任协商策略及其性质分析;最后是结束语.

2　相关工作

2.1　自动信任协商

2000 年,Winsborough 等人[4]提出了自动信任协商(Automated Trust Negotiation,ATN)的概念,并给出 ATN 的抽象模型定义,将双方实体间的信任建立抽象为构造一条证书披露序列.按照披露序列进行协商,虽然可保证所有证书和资源只出示给符合披露策略的合法权限拥有者,但是仍存在隐私泄露的隐患.在自动信任协商的隐私保护研究方面,主要的研究内容有两类,一类是属性证书内容的隐私保护[9-10],即如何最大限度地限制对身份属性信息的合法访问,减少不必要的信息披露,第二类是对是否拥有属性证书的隐私保护[11-12],防止协商主体的响应和信息流动作为旁通道隐式地暴露其是否拥有某些敏感证书.

在对属性证书内容的隐私保护方面,Winsborough 等人在文献[4]中给出了一种吝啬协商策略(parsimonious strategy),允许协商双方在建立证书披露序列的同时,建立一条证书请求序列,证书请求是关于下一步对方提供的证书所应满足的约束说明,在吝啬策略下,协商双方只根据对方的请求提交相关的证书,直到建立起信任关系,吝啬策略避免了与协商目的无关的属性证书的披露,但是仍然必须提交完整的属性证书来证明其对对方策略的满足关系,无法细粒度地避免过度隐私披露问题.

Bauer 等人在文献[10]中提出了一种细粒度属性出示方案,使用 merkle Hash 树结构来构建拥有多个细粒度身份断言的身份断言证书,允许证书拥有者选择出示其中的哪一个断言,而不泄漏其它断言或属性的信息,从而降低了身份信息的披露程度,该方案可以实现证书信息的拆分和证书数值属性值的泛化,但无法实现更复杂的信息泛化和证书持有的隐藏,此外,由于其并未给出身份断言的描述语言和符合性检测算法,也无法自动推理计算泄露最少身份信息的身份断言组合的方案,因此无法将隐私的保护程度最大化.

Li 等人提出的无记忆属性证书(Oblivious Attribute Certificates,OACerts)[9]使用零知识协议来隐藏属性值.协商双方通过输入不同的属性值计算授权函数,以向对方证明自己拥有的属性证书中的属性值在其要求的范围内,从而避免直接出示完整证书.然而无记忆属性证书方案只能通过谓词来证明具体证书类型的属性值在某一良序数值范围之内,即对证书的数据属性值进行泛化,无法进行更复杂的信息泛化和证书持有信息隐藏.

2.2　描述逻辑

描述逻辑是一族知识表示语言,它以结构化和易理解的形式来表示领域知识,具有正式的基于逻辑的语义和很强的表达能力,是一阶谓词的可判定子集.描述逻辑中最基本的两个术语是概念(concept)和关系(role).概念是一类事物的抽象,而关系则刻画了事物之间的各种联系.描述逻辑中的真假通常用$\top$和$\bot$分别表示,析取和合取分别用$\sqcup$和$\sqcap$表示,而蕴含和等价则分别用$\sqsubseteq$和$\equiv$表示.现有的描述逻辑族中的描述逻辑基本都是在描述逻辑 ALC 的基础上通过引入新的概念/关系构造子、引入具体域或增加新的知识库形式扩展而成.

目前最为通用的描述逻辑 SHOIN(D)是通用本体表示语言 OWL DL 的语义基础.本体是一种共享概念模型,使用类、属性以及各种公理来刻画人类世界中的各领域客观知识及规律. OWL DL 语言描述的本体类、类的对象属性(objectProperty)、数据属性(dataProperty)可以直接转化成 SHOIN(D)的概念、关系与特征,OWL DL 本体中的各种公理则可以转化为 SHOIN(D)公理以构成描述逻辑知识基,从而在逻辑层对领域知识进行推理. SHOIN(D)知识基由两组公理组成,一组为断言事实公理的集合 $Abox$,陈述领域个体对概念和关系的隶属关系,如 $Person(a)$,$isChild(a,b)$分别表示个体 a 为概念 $Person$ 的成员及个体 a,b 之间具有关系 $isChild$;另一组为术语公理集合 $Tbox$,$Tbox$ 中的公理表示概念间的蕴含和等同关系等,如 $Female \sqsubseteq Person$ 表示概念 $Female$ 蕴涵于概念 $Person$.在具体的 SHOIN(D)知识基约束下,可以对新公理或断言进行推导,SHOIN(D)支持的推理问题有概念满足、概念蕴涵、实例检查等等,本文的方案仅关注概念蕴涵推理,在此我们给出概念蕴涵推理问题的介绍:在

知识基 KB 下，可以推导出概念 C 蕴含于概念 D，当且仅当任意 KB 的模型 I，满足 $C^I \subseteq D^I$，记为 $KB \models C \sqsubseteq D$.

SHOIN(D)是一阶谓词逻辑的可判定子集，Lutz 等人在文献[13]中已经证明其概念蕴涵问题是可判定的，是 NEXPTIME-complete 问题. 虽然在理论上只能得出指数时间可判定的结论，但是在 pellet 等各种有效的描述逻辑推理工具的协助下，SHOIN(D)概念蕴涵问题实际推理效率很高.

3 参考模型与吝啬语义信任协商框架

吝啬语义信任协商的参考模型如图 1 所示，其中主要参与方有：

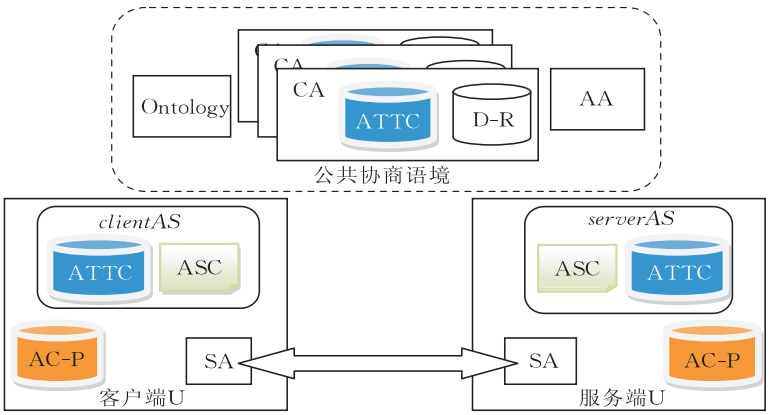


图 1 吝啬语义信任协商参考模型

U：协商主体，包括客户端主体 client 和服务端主体 server，他们通过自己所安装的协商引擎(SA)进行协商，协商双方各自持有多个属性证书(ATTC).

CA：颁发属性证书的权威机构，其自身也可拥有其它 CA 颁发的属性证书.

AA：颁发身份断言证书的权威机构.

参考模型中其它相关要素含义如下：

ATTC：属性证书，是由 CA 颁发的关于主体身份特性的电子证书，其证书主题内容(subject)由一个证书类型和多个身份属性-属性值对构成，CA 可使用 OWL DL 本体语言将其证书类型建模成一个证书类(class)，各种身份属性建模成该证书类所拥有的各种对象属性(objectProperty)或数据属性(dataProperty)，这些类和属性词汇与特定的名空间在一个公开的证书本体 CredOntology 中绑定发布，以帮助开放环境下的各种应用软件识别和翻译主体持有的属性证书. 其中，证书的属性如果建模为对象属性，则其取值可以为某指定名空间下的领域知识本体内的对象实例，如果是数据属性，则取值为某一确定数值或常量.

Ontology：属性证书所涉及的证书本体和各领域知识本体.

D-R：委托声明. 属性 CA 使用委托声明来表明拥有某些其它属性 CA 所签发的属性证书的主体可视为拥有其本身所签发的某类属性证书，相当于将其签发该类属性证书的能力委托给其它属性 CA.

公共协商语境：证书本体和各种知识领域本体(Ontology)，属性 CA 自持的属性证书(ATTC)及其签发的委托授权声明(D-R)构成了所有信任协商参与方进行信任协商所依托的公共协商语境.

ASC：身份断言证书. 在公共协商语境中，主体从多个 CA 处获得属性证书，其所拥有的属性证书可证明其符合许多身份断言 AS. AA 根据主体提交的其所拥有的属性证书和请求验证的身份断言集合 Request_ASSet，验证主体对 Request_ASSet 中的每一条身份断言的符合性，如是否“拥有年龄大于 20 岁的身份证”，“拥有中国科学院某研究所颁发的研究员证明”等等，将所有符合的身份断言写入一个身份断言证书 ASC 并签发. 每一个主体只拥有一个身份断言证书 ASC，但该证书中包含了多条可单独出示的身份断言.

AC-P：资源披露策略. 声明在对方满足何种身份断言要求的条件下，可以将该资源披露给对方.

本地资源包括服务资源和属性证书.

clientAS/*serverAS*：由于属性证书本身可被视为包含较多信息量的身份断言，因此 client/server 所有的属性证书和 ASC 中的所有身份断言一起构成一个身份断言集合 *clientAS*/*serverAS*.

在吝啬语义信任协商框架下，双方 SA 以身份

断言的交换取代了属性证书的交换:双方 SA 首先预协商出一条属性证书披露序列,但并不实际交换属性证书,随后进入身份断言交换阶段,在该阶段中的每一步,SA 并不直接披露事先确定的属性证书集,而是挑选符合对方策略,待披露属性证书集可以推导出的身份断言集进行出示.如在引言中所述事例中,Bob 只需出示"准驾中型客车","驾龄大于 10 年"两条断言,即可证明其符合 Alice 的信用卡披露策略,无需出示完整证书,从而保护了身份隐私.

身份断言证书中包含多个抽象的身份断言,并可能包含多个有关同一属性证书的同一属性值的身份断言,如针对 *age* 属性的"$age>20$","$age>30$"断言.因此,在身份断言交换阶段中的每一步,协商主体面临着多种可用于代替待披露属性证书集的身份断言出示方案的选择.为了强化对参与方隐私的保护,从中挑选透露最少信息的出示方案是非常有必要的.在第 6 节中我们将给出一种正确、完备并且有效的吝啬语义信任协商策略,帮助协商双方建立包含最少身份信息的身份断言披露序列和信任关系.在此之前,我们将首先在第 4、5 节中对支持 SA 在吝啬语义信任协商过程中自动完成证书断言的解析和推理的信任协商语言 DL-TNL 以及 SA 在 DL-TNL 语言的支持下用以计算最小证书符合解和披露最少身份信息的身份断言解的符合性检测算法分别展开介绍.

4　DL-TNL,一种证书与披露策略描述语言

在吝啬语义信任协商框架下,陌生的协商双方之间属性证书交换序列预协商,身份断言替代方案推导以及身份断言交换均由其各自的 SA 自动完成.因此,一种可以被 SA 所解析和理解,并可用于计算推理的证书、断言和策略描述语言是框架实现的关键.以下我们给出一种基于描述逻辑 SHOIN(D)的 DL-TNL 语言,它具有如下优势:(1)与证书本体和各种领域知识本体融合,其所描述内容的含义是计算机程序可理解的,使得 SA 可以感知开放环境下具有不同词汇风格的属性证书和身份断言的含义,并推导出其内部的符合关系.(2)SHOIN(D)是一阶谓词逻辑的可判定子集,其出色的知识基推理能力和现存的各种实用的推理工具为我们在吝啬语义信任协商过程中进行符合性检测和语义蕴含关系判定提供了高效的底层支持.在介绍 DL-TNL 的语法与语义之前,我们先给出一个贯穿全文的运行实例.

运行实例. Ebey,ICB,BankA 分别为公共协商语境中的 3 个 CA. ICB 为颁发经营执照的工商局 CA,BankA 是一家银行,可以为客户颁发信用卡证书,Ebey 可为其用户(买家和卖家)颁发声誉证书,并拥有 ICB 颁发的经营执照证书证明其为合法网络商城.Ebey 在公共协商语境中发布委托声明称:所有拥有 Ebey 声誉证书证明其声誉值大于 500,或拥有 BankA 签发的额度大于等于 5000 元的信用卡的用户是 Ebey 的 VIP 用户.

某天,装修公司的经理 Tom 在网上向灯具公司 B 购买一批进口灯具 E_Lamp,B 公司规定,该类灯具只能卖给 Ebey 的 VIP 用户.已知 Tom 对自己的信用卡的披露策略为只将其出示给拥有工商局 ICB 颁发的经营范围为装修材料的经营执照的公司,而对自己的 Ebey 声誉证书的披露策略为只将其出示给拥有 ICB 认证过的网络商城颁发的声誉证书且声誉大于 500 的主体,B 公司的证书无披露策略,那么 Tom 和 B 是否可以协商出一条成功的交互序列使 Tom 最终签订这笔订单,并在此过程中尽可能隐藏自己的身份信息?

4.1　语　法

4.1.1　属性证书与身份断言

定义 1(属性证书).　DL-TNL 属性证书的主要内容可表示为一个六元组$\langle Issuer, Owner, Subject, pubKey, ValidTime, Signature\rangle$,其中 *Issuer* 为证书签发者的标识,*Owner* 为证书所有者,*Subject* 为证书主题,*pubKey* 为证书拥有者公钥,*ValidTime* 为证书有效时间,*Signature* 为证书签名.其中证书主题域的语法结构为 $Subject ::= T(op_0 : I_0, \cdots, op_m : I_m, dp_0 = d_0, \cdots, dp_n = d_n)$,其中 T 是证书本体中已发布的证书类,op_i,dp_i分别为该证书类所具有的某一对象属性和数据属性,$\forall i \neq j$ 满足 $op_i \neq op_j$ 且 $dp_i \neq dp_j$, I_i为某一知识领域本体中的实例对象, d_i是某一确定数值或常量.

表 1 中我们给出运行实例中的两个参与方各自持有的属性证书示例,为了简化篇幅,在本文示例中我们将省略所有本体词汇的名(字)空间标识.其中证书 B_2中的 *licence* 是对象属性,其值 *lamp* 为装修公司的领域本体内的概念 *decoMaterial* 的一个实例.本例中其余证书的属性域均为数据属性.

表 1 属性证书示例

No.	*Issuer*	*Owner*	*Subject*	描述
T_1	BankA	Tom	*credit*(*amount*=15000)	额度为 15000 元的信用卡证书
T_2	Ebey	Tom	*reputation*(*value*=600)	声誉值为 600 的声誉证书
B_1	Ebey	B	*reputation*(*value*=1500)	声誉值为 1500 的声誉证书
B_2	ICB	B	*company*(*license*: *lamp*, *fund*=1000000)	经营范围为灯具,注册资金为 100 万的经营许可证书
C_1	ICB	Ebey	*NetMall*(*rating*=1)	分类为一级的网络商城证书

定义 2(身份断言). 身份断言是对主体所拥有的属性证书的一个约束断言,身份断言的语法格式如下:

$assertion::=credClaim@CAClaim$

$credClaim::=T(op_0:C_0,\cdots,op_m:C_m,p_0(dp_0),\cdots,p_n(dp_n))$

$CAClaim::=issuer|assertion.$

可见,单个身份断言由两部分组成,*credClaim* 是对属性证书内容的约束,包括证书的种类约束和关于证书属性值的约束. 证书种类约束 T 指明了对方所拥有的属性证书的类型必须为 T 或其子类类型;$op_i:C_i$ 为关于证书对象性值的约束,其中 C_i 为知识领域本体中的简单或者复杂类,$op_i:C_i$ 指明了该属性证书的 op_i 属性值是 C_i 的一个实例;$p_i(dp_i)$ 为关于数据属性值的约束,其中 p_i 为建立在 dp_i 的数据域上的一个一元谓词,若 dp_i 的数据域为整数域或实数域等,常见的谓词为 $>c$,$<c$,c 为 dp_i 数据域中的常量,$p_i(dp_i)$ 限定了证书 dp_i 的属性值必须使得 p_i 为真.

CAClaim 是对属性证书签发者的约束,如果 *CAClaim*=*issuer*,则表示满足此断言的属性证书必须由标识为 *issuer* 的 CA 签发,若 *CAClaim* 为一个 *assertion*,则表示签发 CA 自持的属性证书应当满足该 *assertion*.

在属性证书的 *Subject* 中,每一个 $op_i:I_i$ 属性域中的 I_i 等价于一个只包含实例对象 I_i 的枚举概念,而 $dp_i=d_i$ 属性域可以看成是一个 $(=d_i)$ 谓词作用于 dp_i 上表达式,因而每一个属性证书的 *Subject* 和 *Issuer* 域可综合表示为一个形式如下的平凡身份断言:

$$T(op_0:\{I_0\},\cdots,op_n:\{I_n\},=d_0(dp_0),\cdots,=d_n(dp_n))@issuer$$

多个身份断言可以进一步组成身份断言表达式,每一个身份断言表达式 $Fc(a_1,a_2,\cdots,a_n)$ 是由身份断言 $a_1,a_2,\cdots,a_n$ 和布尔运算符 $\wedge$,$\vee$ 构成的逻辑表达式. 身份断言表达式用于构建委托声明和资源披露策略.

例 1. 以下身份断言表达式指明了主体应当拥有 GUCAS 签发的证明其研究领域为计算机科学,年龄大于 30 岁的教师证书或拥有信用额度大于 10000 元的 BankA 信用卡:

$$Teacher(rField:CScience,>30(age))@GUCAS\vee credit(>10000(amount))@BankA.$$

4.1.2 委托授权声明和资源披露策略

定义 3(委托授权声明). 每一个属性 CA 公布的委托授权声明具有如下格式:*subjectClaim*@*issuer*←Fc,其中 Fc 是身份断言表达式,*issuer* 为该 CA 的标识.

属性 CA 发布的每一个委托授权声明指明了主体拥有的属性证书集如果满足身份断言表达式 Fc,那么该用户可视为拥有由该 CA 颁发的一个满足断言"*credClaim*@*issuer*"的属性证书. 有效的委托授权声明必须由该声明头部断言"*credClaim*@*issuer*"中的 CA *issuer* 签名.

例 2. Ebey 发布委托授权声明称,所有拥有 Ebey 声誉证书证明其声誉值大于 500,或者拥有 BankA 的额度大于等于 5000 的信用卡的用户是 Ebey 的 VIP 用户,该声明表示为

$$VIP@Ebey\leftarrow credit(\geq 5000(rating))@BankA\vee reputation(>500(value))@Ebey.$$

披露策略描述了对方身份满足何种条件时本地资源可以向其披露,其中,条件表示为身份断言表达式.

定义 4(披露策略). 令 R 为某一属性证书或服务资源,资源 R 的披露策略格式如下:R: Fc,其中 Fc 是身份断言表达式.

例 3. 运行实例中 B 对进口灯具订单的披露策略表示为

$$E\_Lamp: VIP@Ebey.$$

Tom 对其证书 T_1,T_2 的披露策略分别表示为

T_1: *company*(*license*:*decoMaterial*)@ICB;

T_2: *reputation*(>500(*value*))@(*NetMall*@ICB).

4.1.3 身份断言证书

身份断言证书借鉴了文献[10]中基于 merkle Hash 树细粒度控制证书属性出示的方案,其格式定义如下.

定义 5(身份断言证书). 身份断言证书由公开与隐私两个部分组成.公开部分包括了证书的属主、签发者、证书有效期以及对隐私部分的 merkle Hash 树的根节点值的签名.隐私部分包括一个 merkle Hash 树,其中每个叶子节点携带的信息格式如下:

$$\langle c, assertion, random\rangle.$$

即每个叶子节点的内容由一个标签 c、一个关于证书属主的身份断言 *assertion* 和一个随机填充 *random* 构成.每一个 *assertion* 都是在公共协商语境下,主体持有的属性证书可以证明其所满足的断言.由于每一个 *assertion* 都是对某个真实或者虚拟属性证书的泛化,标签 c 是主体设置的对该真实或者虚拟属性证书的唯一标识,对同一属性证书的泛化身份断言拥有相同的标签.

如果主体需要出示身份断言证书中的任意断言子集,只需出示这些断言对应的叶子节点的值以及其它必需的 merkle Hash 树的中间节点,以帮助对方重构 merkle Hash 树的根节点值,与公开部分的断言 CA 签名过的根节点值进行比较验证.根据 Bauer 等人对基于 merkle Hash 树的属性证书的安全性进行的分析和证明[10],其它实体无法根据已获得部分身份断言子集的和断言证书的公开部分获知断言证书隐私部分中包含的其它身份断言,这为实现披露最少语义信息的自动协商策略提供了基本安全技术保障.表 2 中我们给出运行示例的参与双方各自持有的身份断言证书中的身份断言节点(省略了随机填充),它们分别对证书中的属性或者颁发者信息进行了泛化隐藏,其中 T_3 还进一步对证书持有信息进行了隐藏.

表 2　身份断言证书示例

No.	Tom 持有的身份断言	No.	B 持有的身份断言
E_1	T_1: *credit*(>10000(*amount*))@BankA	H_1	B_1: *reputation*(>1000(*value*))@Ebey
E_2	T_1: *credit*(>6000(*amount*))@BankA	H_2	B_1: *reputation*(>600(*value*))@(*NetMall*@ICB)
E_3	T_2: *reputation*(>500(*value*))@Ebey	H_3	B_2: *company*(*license*: *lamp*)@ICB
E_4	T_3: VIP@Ebey	H_4	B_2: *company*(*license*: *decoMaterial*)@ICB

4.2　语　义

DL-TNL 的语义基础是描述逻辑,其所描述的内容可以转化成描述逻辑的概念和公理.

(1) CredOntology 中的每一个证书类转化成一个 SHOIN(D)的概念,每一个对象属性转化为一个 SHOIN(D)的关系(role),数据属性转化为特征(feature).除此之外领域知识本体中的类、对象属性、数据属性也可转化成对应的描述逻辑概念、角色和特征.证书本体与知识本体中的每一条公理转化为描述逻辑公理.

(2)引入一个表示主体的原子概念 Principle、一个表示证书的概念 Cred.每一个证书类都是 Cred 的子类.引入两个特别的描述逻辑关系(role): *hasID* 和 *issuerIs*,其中 *hasID* 将 principle 实例联系到它所拥有的 Cred 实例,*issuerIs* 将 Cred 实例关联到签发它的 Principle 实例.

(3)身份断言与身份断言表达式均可以转换成 SHOIN(D)概念,我们定义一个转换函数 DLP,可以将每一个身份断言,身份断言表达式转换成 SHOIN(D)概念,DLP 的递归转换过程如表 3 所示.

表 3　DLP 函数

X	$DLP(X)$
$Fc_1 \vee Fc_2$	$DLP(Fc_1)\sqcup DLP(Fc_2)$
$Fc_1 \wedge Fc_2$	$DLP(Fc_1)\sqcap DLP(Fc_2)$
(Fc)	$(DLP(Fc))$
$Fc=credClaim@CAClaim$	$\exists hasID.(DLP(credClaim)\sqcap\exists issuerIs.DLP(CAClaim))$
$credClaim=T(op_0:C_0,\cdots,op_m:C_m,\ p_0(dp_0),\cdots,p_n(dp_n))$	$T\sqcap(\exists op_0.C_0)\sqcap\cdots\sqcap(\exists op_m.C_m)\sqcap p_0(dp_0)\sqcap\cdots\sqcap p_n(dp_n)$
$CAClaim=issuer$	$\{issuer\}$
$CAClaim=assertion$	$(DLP(assertion))$

例 4.　使用 DLP 函数,例 1 中的身份断言表达式可以转化为如下 SHOIN(D)概念:

$$\exists hasID.(Teacher\sqcap\exists rField.CScience\sqcap>30(age)\sqcap\exists issuerIs.\{\text{GUCAS}\})\sqcup$$
$$\exists hasID.(Credit\sqcap>10000(rating)\sqcap\exists issuerIs.\{\text{BankA}\})$$

每一个身份断言表达式从语义上来说是一个形如 $\exists hasID.E$ 的 SHOIN(D)概念,主体满足该表达

式，意味着该主体是属于 $\exists hasID.E$ 概念下的一个个体，该个体和单纯描述身份信息的概念 E 之间存在 $hasID$ 的关系. 由于每一个属性证书的 *subject* 域和 *issuer* 域可以被综合表示成一个身份断言，因此 DLP 也可作用于任意属性证书 $attc$，将其转化为 SHOIN(D)概念：

$$DLP(attc)=\exists hasID.(DLP(credClaim)\sqcap\exists issuerIs.\{issuer\}),(attc.Subject=credClaim,\ att.Issuer=issuer).$$

(4) 委托授权声明 $T(op_0:C_0,\cdots,op_m:C_m,p_0(dp_0),\cdots,p_n(dp_n))@issuer\leftarrow Fc$ 转化成概念蕴含公理：

$$DLP(Fc)\sqsubseteq DLP(T(op_0:C_0,\cdots,op_n:C_m,p_0(dp_0),\cdots,p_n(dp_n))@issuer).$$

(5) 将每一个 CA 持有属性证书 $attc$ 的事实转换成实例断言公理：$DLP(attc)(owner)$.

(6) 披露策略与协商参与方自持的属性证书并不需要转变为公理，因其只在协商过程中被出示，并不影响公共协商环境下其它所有的协商实体. 在委托授权声明、CA 属性证书以及领域本体组成的公共协商语境中的各种公理集下，它们以如下方式参与协商：

① 身份断言权威 AA 将主体提交的 n 张自持属性证书中的每一张转化成一个描述逻辑概念 A_i(包括 *Subject* 域和 *Issuer* 域信息)，当主体请求的身份断言 B 满足 $KB\models A_i\sqsubseteq B$ 时，或存在某一虚拟属性证书转化成的概念 C_j，满足 $KB\models A_1\sqcap\cdots\sqcap A_n\sqsubseteq C_j$ 且 $KB\models C_j\sqsubseteq B$ 时，AA 将其加入身份断言证书中予以证明.

② 协商过程中披露策略中的身份断言表达式被转化成复杂的描述逻辑概念 A，对方发送的属性证书或身份断言集转化成复杂的描述逻辑概念 B. 如果在公共协商公理集下，可以推理出 $B\sqsubseteq A$，那么即可说明对方的身份信息满足本地披露策略.

5 符合性检测算法

信任协商顺利实施的一个重要保障是符合性检测算法. 现有的符合性检测算法分为 3 种类型[6-7]：第 1 类用于判定对方出示的凭证集合是否符合本地的资源披露策略；第 2 类用于计算符合对方策略的最小本地证书集合(一般认为其兼容了第 1 类算法的能力)；由于本地可能会出现多个证书集合满足一个策略，为了尽可能保证协商成功，一个可以找出所有满足策略的证书集合的第 3 类符合性算法也是非常必要的. 由于吝啬语义信任协商以身份断言来代替属性证书进行出示，我们首先设计出了一种可以计算符合对方策略的最小本地身份断言解的第 3 类符合性检测算法 complianceChecker，并在 Smith 等人提出的第 3 类符合性算法基础上进行改进，设计出 extSSGen 算法，可计算出所有满足 DL-TNL 策略的最小身份断言集合，并从中推理出透露信息最少(最空泛)的身份断言集合以供出示.

5.1 搜寻一个最小身份断言解的算法

定义 6(公共协商知识基). 公共协商知识基 $KB=\langle OKB,A,D\rangle$ 是一个由公共协商语境中的各种公共知识转化而成的 SHOIN(D)知识基，它所蕴含的公理包括 3 个部分，其中 OKB 为公共协商语境中所有的领域知识本体公理和 credOntology 本体公理转化成的 SHOIN(D)公理，A 为所有 CA 持有某一属性证书的事实转化成的实例断言公理，D 为所有的委托授权声明转化成的概念蕴涵公理.

如前所述，协商主体满足某语义断言表达式 Fc，意味着该主体是属于 $DLP(Fc)=\exists hasID.E$ 概念的一个个体，实际上，若该主体出示了满足 $KB\models DLP(a)\sqsubseteq DLP(Fc)$ 的属性证书 a，即可证明自己是 $DLP(Fc)$ 概念的一个个体，因为属性证书 a 可以证明该主体为 $DLP(a)$ 概念的个体. 同理，若主体出示的是身份断言证书中的一个身份断言节点 a，满足 $KB\models DLP(a)\sqsubseteq DLP(Fc)$，也可证明自己满足断言表达式 Fc. 因此我们可以将主体出示的语义断言和/或属性证书对身份断言表达式的满足关系转换为概念蕴含问题来进行判定.

当身份断言表达式较复杂时，主体可能需要出示多个身份断言节点和/或多个属性证书构成的集合来证明对该表达式的满足. 由于属性证书是一种平凡的身份断言，我们以下将用“身份断言集”统称由属性证书和身份断言证书中的身份断言节点构成的集合. 任意身份断言集 $\{a_1,a_2,\cdots,a_n\}$ 的出示，相当于证明了主体满足 $\{a_1,a_2,\cdots,a_n\}$ 所代表的概念 A，那么只要 $KB\models A\sqsubseteq DLP(Fc)$，即可证明主体满足 Fc.

据有相同标签的身份断言是由同一个属性证书直接推导而来的，因而同时出示时可能会存在冗余，我们定义如下 $conj$ 函数来将身份断言集 $\{a_1,a_2,\cdots,a_n\}$ 转化成消除冗余的 SHOIN(D)概念.

定义 7($conj$ 函数). 设 P 为某主体拥有的全部身份断言的集合，函数 $conj:2^P\rightarrow CON$ 将 P 中的

任意子集 $A=\{a_1,a_2,\cdots,a_n\}$ 转换为一个描述逻辑概念 $conj(A)=C_1\sqcap C_2\sqcap\cdots\sqcap C_m$. 其中每一个 C_i 唯一对应于一个由 A 中所有拥有同一标签 c 的身份断言节点(或标识为 c 的属性证书)$c:a_{i1},a_{i2},\cdots,c:a_{it}$ 合成的概念,其合成方式为

$$C_i=\exists hasID.(trim(DLP(a_{i1}.credClaim)\sqcap\cdots\sqcap DLP(a_{it}.credClaim))\sqcap \exists issuerIs.trim(DLP(a_{i1}.CAClaim)\sqcap\cdots\sqcap DLP(a_{it}.CAClaim))),$$

其中 $trim$ 函数作用的结果为消除概念冗余,如化简"$C\sqcap C$"为 C,或者化简"$>60(age)\sqcap>30(age)$"为"$>60(age)$"

例 5. 使用 $conj$ 函数,我们可以将 Tom 拥有的身份断言集合$\{E_1,E_2,E_4\}$转化成概念:

$$\exists hasID.(credit\sqcap>10000(amount)\sqcap \exists issuerIs.\{\text{BankA}\})\sqcap \exists hasID.(\text{VIP}\sqcap\exists issuerIs.\{\text{BankA}\}).$$

定义 8(语义满足). 在公共协商知识基 KB 下,设某主体的身份断言集为 C,若存在 C 的非空子集 A 和身份断言表达式 Fc,满足 $KB\models conj(A)\sqsubseteq DLP(Fc)$,则称身份断言集 A 语义满足 Fc,记为 $sat_{KB}(A,Fc)$,A 也称为 Fc 的一个解,如果任意 A 的非空真子集 A' 满足 $KB\not\models conj(A')\sqsubseteq DLP(Fc)$,则称 A 为 Fc 的一个最小解,记为 $msat_{KB}(A,Fc)$. 此外,如果 Fc 的(最小)解 A 中的每一个元素都是该主体的一个属性证书,则称 A 为 Fc 的一个(最小)属性证书解.

下面我们给出一个算法 complianceChecker,从任意主体的身份断言集 C 中计算一个满足身份断言表达式 Fc 的最小解.

算法 1. complianceChecker(KB,Fc,C).

输入:KB:公共协商知识基,Fc:身份断言表达式,
　　C:身份断言集
输出:NS:C 中的一个 Fc 的最小解

```
1. NS=∅;
2. DS=∅;
3. If sat_KB((C∪NS),Fc) is false
4.    return ∅;
5. While C≠∅
6.       If ((NS==∅)&&(|C|==1))
            //若处理到 C 中还剩最后一个元素时,
            //NS 仍为空,则将 C 中元素放入
            //NS 结束循环
7.          PutInto(C,NS);
8.          Return NS;
9.       E=selectACredFrom(C);
                  //从 C 中任意取出一个属性证书
10.      If sat_KB((C∪NS),Fc) is false
11.         PutInto(E,NS);//去除 E 后断言集合 C∪NS
                  //无法满足 Fc 断言,则将 E
                  //从 C 转移到 NS
12.      Else PutInto(E,DS); //去除 E 后断言集合C∪
                  //NS 可满足 Fc 断言,则
                  //将 E 从 C 转移到 DS
13.   Return NS;
```

算法分析.

在分析算法的正确性和完备性前,我们先给出语义满足关系的如下性质.

性质 1. 给定身份断言集合 A 和身份断言表达式 Fc,若 $sat_{KB}(A,Fc)$不成立,则对于 A 的任意子集 A',$sat_{KB}(A',Fc)$不成立.

证明. 根据 $conj$ 函数的定义,对于 A 的任意子集 A',$conj(A)\sqsubseteq conj(A')$,若$sat_{KB}(A,Fc)$不成立,则$KB\not\models conj(A)\sqsubseteq DLP(Fc)$,显然$KB\not\models conj(A')\sqsubseteq DLP(Fc)$,因此 $sat_{KB}(A',Fc)$也不成立. 证毕.

下面我们先对算法 1 的正确性进行分析:在 while 循环的每一步处理后 $C\cup NS$ 集合都使得 $sat_{KB}((C\cup NS),Fc)$成立,因此 while 循环结束后$NS=C\cup NS$ 也使得 $sat_{KB}((NS),Fc)$成立,此外,若 NS 中的任意一个元素 E 被取出,$sat_{KB}((NS-E),Fc)$不成立(若 NS 中只有一个元素 E,显然 $sat_{KB}((NS-E),Fc)$不成立;若$|NS|>1$,且 $sat_{KB}((NS-E),Fc)$成立,则在 while 循环进行到将 E 从 C 中取出的第 j 步时,设 $NS_j\cup C_j$为第 j 步时的 $NS\cup C$ 集合状态,根据性质 1,$sat_{KB}((NS_j\cup C_j-E),Fc)$成立,$E$ 应当放入 DS 集合中,矛盾). 因此算法 1 是正确的.

算法 1 也是完备的. 这是因为,若 C 中至少存在一个最小解 S,满足 $msat_{KB}(S,Fc)$,那么根据性质 1,我们有 $sat_{KB}(C,Fc)$必然成立,则算法 1 一定能返回一个非空集合 NS,且根据算法 1 的正确性知,NS 为 Fc 的最小解.

在算法的复杂性上,由于该算法只遍历了一次集合 C,因此共执行了$|C|$次 sat_{KB}检验,即执行了$|C|$次 KB 下的概念蕴涵判定,由于 SHOIN(D)的概念蕴含推理是 NEXPTIME-complete 问题,因而 complianceChecker 是指数时间内可终止的.

5.2 搜寻所有最空泛语义解的算法 extSSGen

对于同一个断言表达式 Fc,某主体所拥有的所

有属性证书和所有签发身份断言可能构成多个 Fc 的最小解，不同的解透露的信息量并不相同，我们需要判定什么样的最小解透露的信息较少，以保证吝啬语义信任协商的实施.

定义 9(语义蕴涵). 在公共协商知识基 KB 下，给定两个断言集 A_1，A_2，若 $KB \models conj(A_1) \sqsubseteq conj(A_2)$ 则称 A_2 在 KB 下语义蕴涵 A_1，表示为 $A_1 \rightarrow_{KB} A_2$.

显然，若断言集 A_2 在 KB 下语义蕴涵 A_1，则 A_2 决不会比 A_1 透露更多的信息量，因为已知 A_1 可以推出 A_2 必然成立，已知 A_2 却无法反推 A_1 肯定成立(除非 $A_2 \rightarrow_{KB} A_1$ 也为真).

如在公共协商语境中，某 CA 发布了委托授权声明 $A \leftarrow (B \wedge C) \vee D$，那么显然在公共协商知识基 KB 下，我们可以推出 $KB \models conj(\{D\}) \sqsubseteq conj(\{A\})$，即 $\{A\}$ 在 KB 下语义蕴涵 $\{D\}$，此时若某主体 a 持有断言 A 和 D，为了满足协商主体 b 的策略“$R:A$”，a 既可出示 A 也可出示 D，但出示断言 A 透露的信息为“a 可能拥有 D，也可能拥有 B 和 C”，显然比出示一个确定的断言 D 所透露的信息更加空泛，从而进一步隐藏了 a 的隐私.

定义 10(最空泛语义符合解). 在公共协商知识基 KB 下，给定某主体 a 的一个断言集 A_1 和一个身份断言表达式 Fc，若 $msat_{KB}(A_1, Fc)$ 成立，且不存在任何该主体的其它断言集 A_2，使得 $A_1 \rightarrow_{KB} A_2$ 与 $msat_{KB}(A_2, Fc)$ 成立，则称 A_1 为主体 a 在 KB 下关于 Fc 的一个最空泛语义符合解，记为 $mostGeneralSat_{KB,a}(A_1, Fc)$.

extSSGen 算法. 下面我们给出一个 extSSGen 算法的伪代码. 该算法可应用于两种场景：(1) $C \neq \varnothing$ 时，AS 为身份断言集合，C 为 AS 中符合 Fc 的一个最小属性证书解，算法 extSSGen(KB, Fc, C, AS) 从断言 AS 中计算出 Fc 的所有语义蕴涵 C 的最空范语义符合解. (2) $C = \varnothing$ 时，AS 为属性证书集，extSSGen(KB, Fc, C, AS) 计算的结果为 AS 中 Fc 的所有最小属性证书解.

该算法由文献[6]中的 SSgen 算法扩展而来，在 extSSGen 算法中，1～5 行首先判断 C 是否为空集，若为空集 $AN = AS$，否则算出 AS 中所有语义蕴涵 C 的身份断言，记录在集合 AN 中，6～32 行借鉴 SSgen 思想从 AN 中搜索所有 Fc 的最小解，并且当 C 不为空集时，需要进一步搜寻出最空泛语义断言解，其方法为：在搜寻到一个最小解 E 时，则将其与 R 中所有现有最小解比对，若任意 R 中的最小解 E' 在 KB 下被 E 语义蕴涵，则将 E' 从 R 中去除，并将 E 加入 R 中，当算法结束时，R 中记录了 AS 中语义蕴涵了 C 的 Fc 所有最空泛语义符合解.

算法 2. extSSGen(KB, Fc, C, AS).

输入：KB：公共协商知识基；
　　Fc：身份断言表达式；
　　C：(1)$\varnothing$或(2)Fc 的一个最小证书解；
　　AS：(1)属性证书集合或(2)身份断言集合

输出：R：
　　(1) AS 中 Fc 的最小证书解集合
　　(2) AS 中 Fc 的所有语义蕴含 C 的最空泛语义断言解

符号定义：
AN：AS 中所有蕴涵 C 的断言的集合
B：已经找到的所有 Fc 的最小解的集合
E：已知不能语义符合 Fc 的 AN 的子集的集合
U：B 中所有最小解的并集；
n-subset：有 n 个成员的子集
$P(U)$：U 的幂集

```
1. If (C is ∅)
2.    Let AN=AS;
3.    Let C=complianceChecker(KB,Fc,AS);
4.    If (C is ∅)return ∅;
5. Else Let AN=pickSatByC(AS,C);
6. flag=0;
7. J=C;
8. R=B∪{J};
9. B=B∪{J};
10. Let n=|U|;
11. Let S=P(U) //令 S 为 U 的幂集
12. while (n>0)
13.    Let T 为所有 S 中(n−1)-subset 集合
14.    For each set D∈T
15.     A=D∪(AN\U)
16.     If A 不是 B 中某集合的超集或子集且
              不是 E 中某集合的子集
17.       J=complianceChecker(KB,Fc,A);
18.       If (J is ∅)   E=E∪{A}
19.       else
20.         flag=0;
21.         If (C is not ∅)
22.           for each set G∈R
23.             If (G→KB J)   Delete(R,G);
                //在 R 中删除 G
24.             Else if(J→KB G)
25.                   flag=1; break;
```

```
26.      If (J\U!=∅) && (!flag) goto 8;
27.      Else if (J\U!=∅) goto 9;
             //|U|增长了
28.      B=B∪{J};
29.      If(!flag)   R=R∪{J};
30.  If (∀t∈T(t∪(AN\U)⊆E))   n=0
31.  else n=n-1
32. End-while
```

算法分析.

在分析算法的完备性和正确性前,我们先给出如下可由定义 8、9 和性质 1 推导出的性质.

性质 2.　若首次调用 complianceChecker(KB, AS,Fc)无法获得一个最小解,根据性质 1,则 AS 中不存在任何最小解,更不存在任何最空泛语义符合解.

性质 3.　给定断言集合 E 和身份断言表达式 Fc,若 $msat_{KB}(E,Fc)$成立,根据定义 8,对于任意 E' 满足 $E'?E$ 或者 $E?E'$,$msat_{KB}(E',Fc)$都不成立,因此若 complianceChecker 返回一个最小解 E,任何一个 E 的真子集或真超集都不可能成为最小解.

性质 4.　$A_1 \rightarrow_{KB} A_2$,当且仅当对 A_2 中的任意断言 a,有 $A_1 \rightarrow_{KB} \{a\}$.

算法正确性与完备性:在文献[6]中,Smith 等人证明了 SSgen 算法的正确性与完备性,SSgen 算法在计算证书集合中所有符合策略的最小解时,所适用的策略是受限的,而在 etxSSGen 中调用的符合性检查算法 complianceChecker 可计算出任何身份断言表达式的最小解(如果存在),因而不受限制.在 extSSGen 算法中,当 $C=\varnothing$,AS 全为属性证书的断言集时,extSSGen 与 SSgen 算法等价,因而其正确性与完备性可以得到保证.$C\neq\varnothing$ 时,AS 为身份断言集合,extSSGen 算法首先从断言 AS 中算出所有语义蕴涵 C 的身份断言,记录在集合 AN 中,随后使用 SSgen 算法计算出 AN 所有的 Fc 的最小解(由性质 4,若任意断言集 A_2 蕴涵 C,当且仅当 A_2 中的任意一个断言都蕴涵 C).由于身份断言集合 AN 符合 Fc 的最小解集的结构满足性质 1～3,足以使其满足 SSgen 算法的实施前提[6],因而可应用 SSgen 方法从 AN 中计算出所有 Fc 的最小解,进一步,从最小解集中挑选最空泛语义符合解的代码也并未删除掉任何潜在的最空泛语义符合解,因此 extSSGen 算法在 $C\neq\varnothing$ 时也是正确和完备的.

$C=\varnothing$ 时,extSSGen 算法的时间复杂度来自于使用 SSgen 方法最坏情况下调用 $2^{|U|}$ 次 complianceChecker 来搜索所有最小证书解;$C\neq\varnothing$ 时,extSSGen 算法的时间复杂度来自 3 个方面:(1) extSSGen 需要执行 $|AS|$ 次 sat_{KB} 检验来计算 AN;(2) 使用的 SSgen 方法最坏情况下需要调用 $2^{|U|}$ 次 complianceChecker 来搜索所有最小解;(3) 从所有最小解中挑选最空泛语义符合解所需要调用的 sat_{KB} 检验的次数$\leq|(M-1)\times M|<2^{|U|}$,$M$ 是搜索到的最小解的个数.因而 extSSGen 算法是指数时间可终止的.

6　吝啬语义信任协商策略

信任协商策略决定了成功协商序列的搜索过程,信任协商策略可以决定在协商的每一步所应出示的属性证书以及对方下一阶段所应出示的属性证书.尽管并不是每一次交互都可能获得成功,但是有效的信任协商策略可以保证只要双方拥有的属性证书以及证书保护策略潜在地预示了一个成功协商序列的存在,按照该策略执行的协商过程就一定可获成功.为了减少协商过程中的身份信息暴露,我们对吝啬信任协商策略[4]进行改进,使其由控制属性证书的出示转为控制泄露最少信息的身份断言的出示.在本节中,我们首先介绍扩展后的吝啬语义信任协商策略,然后给出策略的正确性和有效性证明.

6.1　吝啬语义信任协商策略

吝啬语义信任协商发生于一个客户端主体和一个服务端主体之间,设他们各自持有的属性证书集合为 $clientATTC$ 和 $serverATTC$,而各自拥有的身份断言集合为 $clientAS$ 和 $serverAS$.由于属性证书可看成平凡的身份断言,因而我们有 $clientATTC\subseteq clientAS$,　$serverATTC\subseteq serverAS$,对于任意 $clientATTC$ 或 $serverATTC$ 中的证书子集 $C=\{L_1,L_2,\cdots,L_n\}$,令 $Gov(C)=P\_Body(L_1)\wedge\cdots\wedge P\_Body(L_n)$,$P\_Body(L_i)$ 为 L_i 的披露策略的 body 部分,若 $serveAS$ 或 $clientAS$ 中的任一断言子集 A 可以语义满足 $Gov(C)$,即 $sat_{KB}(A,Gov(C))$ 成立,则称 A 解锁 C,表示为 $unlock(C,A)$.若 $Gov(C)$ 为空,则 C 可以被无条件解锁,即 $unlock(C,\varnothing)$ 成立.而对于一个身份断言表达式的集合 $Fcs=\{Fc_1,Fc_2,\cdots,Fc_n\}$,若断言子集 A 可以语义满足其中的任何一个 Fc_i,则称 A 满足 Fcs,记为 $sat(A,Fcs)$,显然,若 $unlock(C,A)$成立,$sat(A,\{Gov(C)\})$也成

立.吝啬语义信任协商策略的执行分为两个阶段:预协商阶段与身份断言交换阶段.每个阶段客户端和服务端轮流发送报文,因此每个阶段均可表示成报文序列,我们用 $end(i)$ 表示发送第 i 个报文的参与方.

预协商阶段. 预协商阶段开始于客户端发送一个资源 R 的请求给服务器,$end(0)=client$. 当服务器收到对 R 的请求时,它检查 R 的披露策略,如果 R 是一个不受保护的服务,它可以被直接发送给对方.否则,若 R 的披露策略为 $R:Fc(a_1,a_2,\cdots,a_n)$,服务器须向客户端请求可以满足 $Fc(a_1,a_2,\cdots,a_n)$ 的属性证书集.

在预协商的中间过程($i>0$),每个协商参与方发送给对方的报文都是一个身份断言表达式集合,其生成过程如下:参与方接收到对方的请求报文(一个身份断言表达式集合 Fcs)后,对于 Fcs 中的每一个身份断言表达式 Fc,调用 extSSGen(KB,Fc,$\varnothing$,$clientATTC/serverATTC$),求取所有本地可以符合对方请求的最小属性证书解.若所有的 Fc 都不存在最小属性证书解,则告知对方协商失败,反之若存在且所有最小属性证书解为 $C_1,C_2,\cdots,C_n$,检查是否存在某个 C_i 的 $Gov(C_i)$ 为空,即 C_i 中所有属性证书可以无条件发送.若存在,发送报文"success"通知对方已经寻找到可无条件解锁的最小属性证书解,可以终止预协商,进入身份断言交换阶段;否则,则向对方请求满足身份断言表达式集合 $Fcs=\{Gov(C_1),GovC_2),\cdots,Gov(C_n)\}$ 的属性证书集.

当协商进行到第 $2\times\min(|clientATTC|+1,|serverATTC|+1)+1$ 步时,若任何可无条件解锁的最小属性证书解还未出现,则终止协商,宣告协商失败.否则,预协商阶段成功寻找到了无条件解锁的最小属性证书解,则协商双方发送的请求构建起了一条序列($f_0,f_1,f_2,\cdots,f_{m-1}$),有关此序列我们可以得出如下定理.

定理 1. 成功的预协商阶段建立的请求序列满足如下条件.

(1) $f_0=R$,$f_{m-1}=success$,且 $end(m-1)$ 拥有一个 f_{m-2} 中某身份断言表达式 Fc 的可无条件解锁的最小属性证书解 S.

(2) 任意 $end(i+1)$ 拥有属性证书集 C,$0<i<m-1$,使得 $sat(C,f_i)$ 成立,当且仅当存在一个 $end(i)$ 的属性证书集 C',使得 $sat(C',f_{i-1})$ 成立,且 C 为 $Gov(C')$ 的一个属性证书解,即 $unlock(C',C)$.

证明. 条件(1)显然成立,对于条件(2),根据预协商阶段的协商规则,可以直接推出:

(a) 预协商序列中的任意报文 $f_i=\{Gov(C_1),Gov(C_2),\cdots,Gov(C_n)\}$,$0<i<m-1$,其每个 C_j 都是 $end(i)$ 对 f_{i-1} 中某 Fc 的一个最小属性证书解,即存在 $Fc\in f_{i-1}$,$msat_{KB}(C_j,Fc)$ 成立,因此 $sat(C_j,f_{i-1})$ 也成立;

(b) 对于 $f_i=\{Gov(C_1),Gov(C_2),\cdots,Gov(C_n)\}$,$\{C_1,C_2,\cdots,C_n\}$ 为 $end(i)$ 关于 f_{i-1} 的所有身份断言表达式的所有最小属性证书解的集合.

下面我们先证条件(2)的⇒部分. 若存在 $end(i+1)$ 的属性证书集 C 使得 $sat(C,f_i)$ 成立,由于 $f_i=\{Gov(C_1),Gov(C_2),\cdots,Gov(C_n)\}$,那么至少有一个 $Gov(C_j)$ 被满足,因此至少存在一个 $end(i)$ 的属性证书集 C_j,使得 $unlock(C_j,C)$ 成立,根据推论 a,$sat(C_j,f_{i-1})$ 成立,令 $C'=C_j$,则⇒成立.

我们再证⇐. 若存在一个 $end(i)$ 的属性证书集 C' 使得 $sat(C',f_{i-1})$ 成立,那么必然存在一个 $Fc\in f_{i-1}$ 使得 $sat_{KB}(C',Fc)$ 成立,因此也必然存在 end(i) 对 Fc 的一个最小属性证书解 $C''\subseteq C'$,使得 $sat(C'',f_{i-1})$ 成立;若同时存在一个 $end(i+1)$ 的证书集 C 使得 $unlock(C',C)$ 成立,因为 $KB\models DLP(Gov(C'))\sqsubseteq DLP(Gov(C''))$ 成立,所以 $unlock(C'',C)$,即 $sat_{KB}(C,Gov(C''))$ 也成立,又由推论 b 知,$Gov(C'')$ 定为 f_i 中的一个子句,因此可以推出 $sat(C,f_i)$ 成立. 证毕.

身份断言交换阶段. 预协商阶段成功后,协商转入身份断言交换阶段,身份断言交换阶段是一条长度由预协商阶段决定的序列 $\{g_m,\cdots,g_{2m-2}\}$,$\forall g_j$,$m\leq j\leq 2m-2$,是一个 $clientAS$ 或 $serverAS$ 的子集,且满足如下条件:

(1) $j=m$ 时,g_m 是 $end(m)=end(m-1)$ 的身份断言子集,$end(m)$ 调用 extSSGen(KB,Fc,S,$clientAS/serverAS$)生成所有最空泛语义符合集后随机挑选而得,因而满足 $mostGeneralSat_{KB,end(m)}(g_m,Fc)$,且 $S\rightarrow_{KB}g_m$.

(2) $m<j<2m-2$ 时,g_j 是 $end(j)$ 的身份断言子集,由 $end(j)$ 挑选一个满足 $msat_{KB}(C,fc)$,$fc\in f_{2m-j-2}$ 且 $unlock(C,g_{j-1})$ 的属性证书集 C,再从 extSSGen(KB,fc,C,$clientAS/serverAS$) 生成的最空泛语义符合集中挑选而得,因而满足 $mostGeneralSat_{KB,end(j)}(g_j,fc)$,且 $C\rightarrow_{KB}g_j$.

(3) $j=2m-2$ 时,$g_{2m-2}=R$,且 $unlock(R, g_{j-1})$成立.

6.2　运行实例

在吝啬语义协商策略下,运行实例中的 Tom 和 B 的交互序列如图 2 所示.其中步 1～4 为预协商阶段,Tom 首先发送订单请求,B 检查对进口灯具订单资源的保护策略,随后发送对 Tom 的身份断言请求 F_1,Tom 调用 extSSGen 计算出两个符合 F_1的最小证书解$\{T_1\}$,$\{T_2\}$,于是发送 $F_2=\{Gov(\{T_1\}), Gov(\{T_2\})\}$给 B,在第 4 步中,B 调用 extSSGen 计算出两个符合 F_2的最小证书解$\{B_1\}$,$\{B_2\}$.两个解中的证书都是可以无条件解锁的,B 挑选其中一个无条件解锁解$\{B_2\}$,然后发送 Success 成功结束预协商阶段.

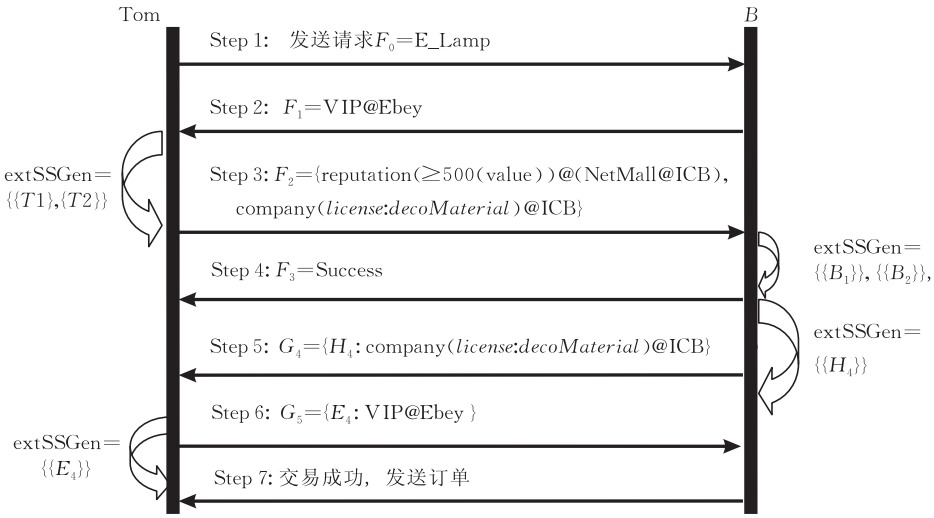


图 2　吝啬语义信任协商运行实例

步 5～6 为身份断言交换阶段,在步 5 中,B 计算出符合 $Gov(\{T_1\})$且蕴涵了无条件解锁解$\{B_2\}$的最空泛断言解为$\{H_4\}$,因此它发送断言 H_4给 Tom,避免了直接出示 B_2:company(*license*: *lamp*, *fund*=1000000)证书,从而自己的营业执照中的具体经营范围这一对象属性信息进行了泛化,也实现了对属性信息 fund 的拆分.在步 6 阶段,Tom 的证书集$\{T_1\}$被对方发送的$\{H_4\}$解锁,且符合身份断言请求 F_1,因此 Tom 调用 exSSGen(KB, F_1, $\{T_1\}$, $TomAS$)计算出一个最空泛语义符合解$\{E_4\}$,他只需发送 E_4即可符合 F_1的要求,尽管 Tom 的身份断言 $E_1(T_1: credit(>10000(amount))@\text{BankA})$,$E_2(T_1: credit(>6000(amount))@\text{BankA})$都满足 F_1且蕴涵 T_1,但他们都被 E_4语义蕴涵,即 E_4比他们更进一步保护了主体的隐私,成为 exSSGen 算法返回的最空泛语义符合解,使得 Tom 在出示 E_4时更加含蓄地透露自己的信息,甚至隐藏了自己的证书持有情况.

6.3　正确性与完备性分析

定理 2(策略完备性和有效性).　若协商双方可以建立成功的信任协商属性证书交换序列使得客户端最终获得资源 R 访问权限,则吝啬语义信任协商策略下双方在预协商阶段内一定可以在不超过 $2\times\min(|clientATTC|+1, |serveATTC|+1)+1$ 次交互过程中成功找到无条件解锁证书解,并可以成功形成一条长度为 $m-1$ 的身份断言交换序列,m 为预协商阶段的报文长度

证明.　由定理 1 知,一次吝啬语义信任协商的预协商阶段满足一次吝啬信任协商的信任点(point of confidence)搜寻阶段所应满足的条件,因而预协商阶段建立的报文序列$(f_0, f_1, \cdots, f_{m-1})$中的$(f_0, f_1, \cdots, f_{m-2})$部分可视为一次吝啬信任协商搜寻信任点的证书请求序列,预协商阶段可获得一个无条件解锁证书解当且仅当该证书请求序列到达了信任点.根据吝啬信任协商策略的性质分析,若协商双方可以建立成功的信任协商序列,则存在自然数 k,$k\leq 2\times\min(|clientATTC|+1, |serverATTC|+1)$,使任意一次吝啬信任协商都可在 f_k处达到信任点,因此若协商双方可以建立成功的信任协商序列,吝啬语义信任协商策略下的预协商阶段也可以在 $m-2=k$ 处成功找到无条件解锁证书解,此时双方的交互次数 $k+1\leq 2\times\min(|clientATTC|+1, |serverATTC|+1)+1$.

若预协商阶段成功找到无条件解锁证书解,在

身份断言交换阶段，$end(m)$首先设置 $C_m=S$，与 S 所语义满足的 $Fc\in f_{m-2}$ 为 extSSGen 的输入，获得满足 $mostGeneralSat_{KB,end(m)}(g_m,Fc)$，且 $C_m\rightarrow_{KB}g_m$ 的 g_m，发送给对方，$end(m+1)$获得 g_m 后，根据 f_{m-2}的生成规则，必然存在至少一个最小证书解 C_{m+1}满足 $unlock(C_{m+1},g_m)$，且 $sat(C_{m+1},f_{m-3})$，$end(m+1)$可以进一步以 C_{m+1}为输入获得 g_{m+1}发送给 $end(m+2)$，如此反复，每一步至少存在一个 C_j符合 end_j的挑选要求，身份断言交换阶段不会停滞，直至最终获得成功. 证毕.

定理 3(策略正确性). 若一次吝啬语义信任协商的预协商阶段获得成功后形成一条长度为 $m-1$ 的身份断言交换序列，m 为预协商阶段的报文长度，则客户端最终获得资源 R 的访问权限.

证明. 根据定义，在身份断言交换序列中，$g_{2m-2}=R$，因此客户端最终可以获得资源 R 的访问权限. 证毕.

7 结束语

本文提出一种以身份断言的披露代替属性证书出示的吝啬语义信任协商框架，以对协商参与方的身份信息进行严格保护，并提出一种正确、完备且有效的吝啬语义信任协商策略，在该策略下，交易双方的协商引擎可以从身份断言证书中，快速选择透露最少信息且符合对方策略的身份断言集进行出示，以最大限度地减少信任建立过程中被披露的隐私信息，并保证只要理论上存在成功的可能，使用该策略必然可以有效地帮助主体最终获得网络资源的访问权限. 同时，本文给出了在吝啬语义信任协商框架下，自动实施吝啬语义信任协商策略所需执行的符合性检测算法的设计及分析，并提出了一种具有强推理能力的信任协商描述语言 DL-TNL，可支持协商引擎在吝啬语义信任协商过程中对属性证书与身份断言的含义完成自动的解析和推理，实现高效的符合性检测.

参 考 文 献

[1] Bertino E, Ferrari E, Squicciarini A C. Trust-X: A peer to peer framework for trust establishment. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 827-842

[2] Nejdl W, Olmedilla D, Winslett M. PeerTrust: Automated trust negotiation for peers on the semantic Web//Proceedings of the Secure Data Management. Toronto, Ontario, Canada, 2004: 118-132

[3] Li Jian-Xin, Huai Jin-Peng, Li Xian-Xian. Research on automated trust negotiation. Journal of Software, 2006, 17(1): 124-133(in Chinese)
(李建欣，怀进鹏，李先贤. 自动信任协商研究. 软件学报，2006，17(1)：124-133)

[4] Winsborough W, Seamons K, Jones V. Automated trust negotiation. North Carolina State University at Raleigh: Technical Report TR-2000-05, 2000

[5] Yu Ting, Ma Xiao-Song, Winslett M. PRUNES: An efficient and complete strategy for automated trust negotiation over the Internet//Proceedings of the ACM Conference on Computer and Communications Security. New York, 2000: 210-219

[6] Smith B, Seamons K E, Jones M D. Responding to policies at runtime in Trust Builder//Proceedings of the 5th International Workshop on Policies for Distributed Systems and Networks. Washington, 2004: 149-158

[7] Lee J A, Winslett M. Towards an efficient and language-agnostic compliance checker for trust negotiation systems//Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security. Tokyo, Japan, 2008: 228-239

[8] Li Jian-Xin, Huai Jin-Peng. COTN: A contract-based trust negotiation system. Chinese Journal of Computers, 2006, 29(8): 1290-1300(in Chinese)
(李建欣，怀进鹏. COTN：基于契约的信任协商系统. 计算机学报，2006，29(8)：1290-1300)

[9] Li Jiang-Tao, Li Ning-Hui. OACerts: Oblivious attribute certificates//Proceedings of the 3rd Conference on Applied Cryptography and Network Security. New York, 2005: 122-138

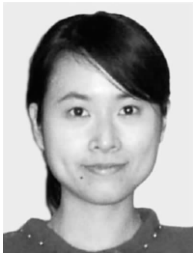
[10] Bauer D, Blough M D, Cash D. Minimal information disclosure with efficiently verifiable credentials//Proceedings of the 4th ACM workshop on Digital Identity Management. Virginia, 2008: 15-24

[11] Bradshaw R W, Holt J E, Seamons K E. Concealing complex policies with hidden credentials//Proceedings of the 11th ACM Conference on Computer and Communications Security. New York, 2004: 146-157

[12] Frikken K, Atallah M, Li Jiang-Tao. Hidden access control policies with hidden credentials//Proceedings of the 3rd ACM Workshop on Privacy in the Electronic Society. New York, 2004: 27-28

[13] Lutz C. An improved NExpTime-hardness result for description logic ALC extended with inverse roles, nominals, and counting. Technical University Dresden, Germany: Technical Report LTCS-Report 04-07, 2004

[14] Frikken B K, Li Jiang-Tao, Atallah J M. Trust negotiation with hidden credentials, hidden policies, and policy cycles//Proceedings of the 13th Annual Network and Distributed System Security Symposium. California, 2006: 157-172



ZHANG Yan, born in 1983, Ph. D. candidate. Her research interests include distributed access control and spatial database security.

FENG Deng-Guo, born in 1965, professor, Ph. D. supervisor. His research interests focus on network and information security, cryptography theory and technique.

Background

The work is supported by the National High Technology Research and Development Program (863 Program) of China under grant Nos. 2007AA120404, 2007AA120405.

In automated trust negotiation, the trust between unfamiliar principals is established by incremental exchange of certificates, protecting sensitive certificates in the process. In recent years, more and more researchers focus on potential privacy problems in ATN. One of the main potential privacy problems is that sensitive information can often be inferred from a response to a request to access a resource, while the other important one is the unnecessary disclosure of information during the negotiation process. This paper focuses on the latter problem.

Several researchers have proposed their approaches to solve the over-revelation problem. Li J. et al. designed a kind of oblivious attribute certificate to hide the sensitive attribute's value by exploiting zero knowledge protocol. Bauer D et al. advanced a fine-grain attribute assertion revelation solution which allows certificate owners to show relevant attribute assertions in a certificate and hide the irrelevant ones. Though these approaches behave well when generalizing the values of attributes of some data type, they can't realize the value generalization of attributes with abstract type or hide the fact of possessing specific certificates. In this paper, authors propose a novel parsimonious semantic trust negotiation framework in which entities can generalize both data type and abstract type of attribute values of their certificates, hide irrelevant attributes and conceal the specific certificates' possession status during the trust negotiation process. Under the framework, the authors propose a correct, complete and efficient parsimonious semantic trust negotiation strategy to allow the negotiation participants to protect their private identity information as much as possible.