ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.1, January 2006, pp.124−133
DOI: 10.1360/jos170124

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

自动信任协商研究*

李建欣+, 怀进鹏, 李先贤

(北京航空航天大学 计算机学院,北京 100083)

Research on Automated Trust Negotiation

LI Jian-Xin+, HUAI Jin-Peng, LI Xian-Xian

(School of Computer Science, Beihang University, Beijing 100083, China)

+ Corresponding author: Phn: +86-10-82316342, 013521215768, E-mail: lijx@act.buaa.edu.cn, http://act.buaa.edu.cn

Li JX, Huai JP, Li XX. Research on automated trust negotiation. *Journal of Software*, 2006,17(1):124−133.
http://www.jos.org.cn/1000-9825/17/124.htm

Abstract: The proliferation of the Internet has given opportunities on different entities to share resources or conduct business transactions. However, how to establish trust among strangers without prior relationship and common security domain poses much difficulty for these activities. To resolve these problems, a promising approach known as Automated Trust Negotiation (ATN), which establishes the trust between strangers with iterative disclosure of credentials and access control policies, is proposed. In this paper, a comprehensive survey of research on ATN is presented, and some basic techniques, e.g. negotiation model and architecture, access control policy specification, credential description and credential chain discovery, are introduced and compared. Then based on the analysis of the shortcomings and problems of the techniques, the trend of research and application is discussed. All these work may contribute to the further work on trust establishment for entities with privacy protection and autonomy in open internet.

Key words: information security; trust negotiation; access control policy; credential; negotiation strategy

摘 要: 在 Internet 日益孕育新技术和新应用的同时,交互主体间的生疏性以及共享资源的敏感性成为跨安全域信任建立的屏障.自动信任协商是通过协作主体间信任证、访问控制策略的交互披露,逐渐为各方建立信任关系的过程.系统介绍了这一崭新研究领域的理论研究和应用进展情况,并对信任协商中的协商模型、协商体系结构、访问控制策略规范、信任证描述及发现收集、协商策略及协商协议等多项关键技术的研究现状进行分析和点评,最后针对目前研究工作中存在的一些问题,对未来的研究方向及工作进行展望.通过对自动信任协商的研究及其进展的介绍,希望有助于在维护开放网络中主体自治性和隐私性的同时,研究更高效、实用的信任自动建立技术.

关键词: 信息安全;信任协商;访问控制策略;信任证;协商策略
中图法分类号: TP309 文献标识码: A

*Supported by the National Natural Science Foundation of China under Grant No.90412011 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2003AA144150 (国家高技术研究发展计划(863))

Received 2004-12-22; Accepted 2005-07-11

近年来,基于网络的商务、政务以及科学实验活动逐渐成为一种主流应用模式,因此,网络环境下的资源共享和业务协作理论、方法和实现机理成为当前计算机技术的主要方向之一,其中,“如何在分布式计算环境中的通信和交易主体间建立信任关系”成为一个重要问题.传统的访问控制技术主要基于请求方的身份进行授权,需要设定统一的安全管理域.然而,在开放的互联网中,由于参与主体数量的规模大、运行环境的异构性、活动目标的动态性以及自主性等特点,各资源主体往往隶属于不同的权威管理机构,使得基于身份的访问控制技术在跨多安全域进行授权及访问控制时显得力不从心,暴露出许多弱点.因此,需要寻求一种更为有效的信任关系建立方法,实现从基于身份的访问控制技术到新技术的转化.

1996 年,AT&T 实验室的 Blaze 等人首先提出信任管理(trust management,简称 TM)的概念[1,2],为解决分布式环境中新应用形式的安全问题提供了新思路,Winsborough 等人[3]称这类信任管理系统为基于能力(capability-based)的授权系统,它们仍需要服务方预先为请求方颁发指定操作权限的信任证,无法与陌生方建立动态的信任关系.依赖主体属性(property-based)授权,是为陌生方之间建立信任关系的一种有效方法[4],Li 等人提出了一种基于角色的信任管理框架(role-based trust-management framework,简称 RT)[5,6],代表了信任管理的最新研究水平.

由于信息安全的隐患源于多个方面,在对陌生方建立信任所依赖的属性信任证和访问控制策略中,都可能泄露交互主体的敏感信息,特别是陌生方之间很难再协定出彼此信任的第三方,来协助它们建立信任关系;在基于“服务为中心”的网格计算(grid computing)环境、应急处理、供应链管理和在线服务等具有多个安全管理自治域的应用中,为了实现多个虚拟组织间的资源共享和协作计算,需要通过一种快速、有效的机制为数目庞大、动态分散的个体和组织间建立信任关系,而服务间的信任关系常常是动态地建立、调整,需要依靠协商方式达成协作或资源访问的目的,并能维护服务的自治性、隐私性等安全需要.

为解决上述问题,Winsborough 等人[3]提出了自动信任协商(automated trust negotiation,简称 ATN)的概念,并成为当前的一个重要研究方向,它是“通过信任证、访问控制策略的交互披露,资源的请求方和提供方自动地建立信任关系”[3,7].迄今为止,ATN 的研究已得到迅速发展,提出了多种领先的研究方法和技术,但是,ATN 整体性研究工作尚处于初级阶段,就其研究和应用前景来看,是一个值得予以关注的方向.本文主要是较为全面地分析了 ATN 研发内容及相关工作,并通过对应用需求和关键技术问题的比较分析,基于我们的研发实践工作,提出了未来的技术发展趋势,以使得读者能够全面、准确地了解这一新兴领域的研究进展.

本文第 1 节简要介绍 ATN 中解决的主要问题和研究内容.第 2 节对当前 ATN 的前瞻性研究工作现状进行阐述分析.第 3 节介绍 ATN 的实现及主流应用领域.第 4 节分析当前工作存在的不足并展望新的研究契机.第 5 节为结束语.

1 自动信任协商的研究问题

跨安全域的联合协作属于组织频繁变化的活动(如图 1 所示),ATN 主要研究跨多安全域的信任建立问题,下面结合实例 1 简要说明目前面临的问题,并由此引出主要研究内容.

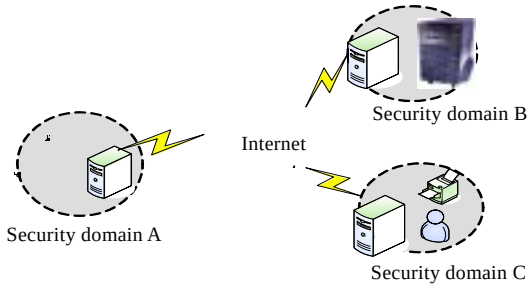

Fig.1 Trust negotiation across multiple security domains
图 1 跨安全域的自动信任协商

实例 **1**(医疗紧急救助). 在对 Alice 实施的一次医疗急救中,急救中心 FirstAid 需要向 Alice 曾就医的医院 Hospital 请求访问其电子病历 *R*,然而,*R* 涉及到 Alice 的个人隐私信息,属于敏感资源,所以,Hospital 制定了相应的保护资源 *R* 的访问控制策略:只有 Alice 本人及急救中心才能调阅 *R*.在协议消息交互过程中,各方会根据其独立的协商策略(strategy)披露相应的消息项,如,FirstAid 只要提交当地卫生署为其签发的急救中心信任

证,就能快速地访问到病历 *R*.

因此,建立跨安全域之间的信任通常面临着如下几项本质问题:(1) 当隶属类似于实例 1 中的机构 FirstAid 和 Hospital 两个独立安全域的陌生主体进行资源访问时,如何提供一种有效的方法和机制,以动态地建立两者的信任关系?(2) 当开放网络中的协商主体在维护其自治性和隐私性时,需要什么样的访问控制策略和信任证(如实例 1 中 Hospital 制定的访问控制策略和 FirstAid 拥有的信任证)?(3) 对资源的访问控制结论,不再是单纯的 Yes 或 No,需要根据各自的协商策略给出相应的提议,以支持进一步的协商:既要实施信息保护,又要达成联合协作.因此,如何建立协商策略机制以兼顾二者的要求?(4) 此外,信任的建立将依赖于一套完整的协议,例如,在实例 1 中体现为机构 FirstAid 和 Hospital 的消息交互过程.

概括地讲,基于 ATN 的工作原理和应用需求(如图 2 所示)的研究主要涵盖 4 个方面:体系结构及基础模型、访问控制策略及信任证、协商策略(strategy)、协商协议.

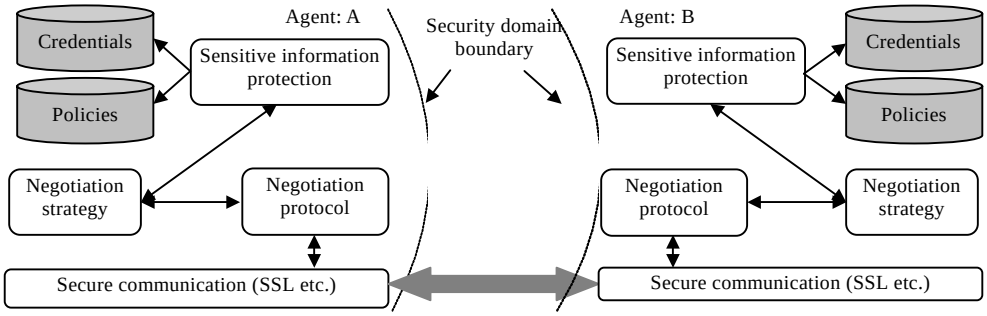

Fig.2 The work principal of ATN application

图 2 ATN 应用的工作原理

从 ATN 的研究和应用角度出发,文献[8,9]提出 3 项基本要求:(1) 自动化(automated),即易于应用,避免过多的人工交互,具有可扩展性的管理能力;(2) 普适性(ubiquitous),即能够以一项网络服务的形式提供;(3) 应用独立性(application independence),即具有一定自治性维护能力,适合分布式管理机制.

2 自动信任协商研究现状分析

目前,ATN 的研究已经得到国际学术界的广泛关注,BYU 大学 ISRL 实验室的 Seamons 和 UIUC 大学 Winslett 等人联合承担了 ATN 的研究项目 TrustBuilder[7−10],前者主要担负 ATN 应用系统的研制;后者主要从事关键理论和技术的突破.他们开展了大量的研究工作,奠定了扎实的应用基础.此外,Stanford 大学的“动态协作的快捷管理(agile management of dynamic collaborations,简称 AMDC)”项目和 NAI 实验室的“基于属性访问控制(ABAC)”项目[11,12]也在开展有关 ATN 的理论和应用研究;其他如 IBM Haifa 研究院的 Trust Establishment 项目[13]、德国 Hannover 大学的 PeerTrust 项目[14,15]也在积极从事相关的研究和应用工作.

2.1 基础体系结构和模型

2.1.1 体系结构

ATN 体系结构是基于 P2P(peer to peer)的协作模式.文献[3]提出了一种 ATN 应用层体系结构,该体系结构采用访问控制策略保护敏感信任证,消息类型包括信任证请求和信任证提交两类,从而实现了双方的信任攀升式建立,但是,该结构明显的不足之处在于,它所描述的受保护资源类型单一.随着 ATN 研究工作的逐渐深入,文献[16,17]提出了一种与 ATN 研究和应用更相一致的技术体系结构,该结构较清晰地勾绘出当前 ATN 的研究内容及其层次结构,并强调了访问控制策略的核心地位,泛化了受保护资源的类型,不但包括属性信任证,还包括访问控制策略本身,同时还涉及到“协商策略”和“协商协议”等技术.尽管如此,该体系结构还未完整体现出 ATN 的特殊应用环境,如开放的网络体系下,信任证的分散式存储等特征.此外,在文献[18]的未来工作展望中,还提及将双方式 ATN 扩展到多方安全计算的想法,但迄今为止,尚未有公开的研究结论.

2.1.2 模型与框架

Winsborough 等人在提出 ATN 概念的同时,还相应地定义了 ATN 的抽象模型,将双方实体间的信任建立抽象为构造一条信任证披露序列(credential disclosure sequence).

定义 **1**(**ATN** 抽象模型)[13]. 设请求方信任证集为 *ClientCreds* ,提供方信任证集为 *ServerCreds* ,对于每份信任证 C 的保护,记作 $gov_{client}(c)$ 或 $gov_{server}(c)$,协商的信任证披露序列定义为

$$\{C_i\}_{i\in[0,2n+1]}=C_0,C_1,\ldots,C_{2n+1},\text{其中 } n\in N,\ C_{2i}\subseteq ClientCreds,\ C_{2i+1}\subseteq ServerCreds.$$

该模型较为简洁,其贡献在于抽象出双方信任建立过程的状态表示,后续许多研究工作都沿用了该思路.

Yu 等人[16]提出披露树(disclosure tree)模型表述 ATN 的状态,并证明了信任协商的目标就是构造出一棵信任证完全披露树.Winsborough 等人[11,12]则基于信任证描述语言 RT_0,定义了 ATN 框架[12].

在这 3 类 ATN 的模型和框架中,披露序列和完全披露树是等价并可相互转换的;披露序列简洁、直观地表示出信任证的披露过程;披露树则进一步描述了策略、信任证的结构关系.但是,为了简化协商策略的研究,披露树存在的一个显然不足是采用命题式语言描述信任证,不过文献[18]在其后续的工作中对此进行了扩展.ATN 框架主要针对的是 RT_0 信任证语言,具有清晰的语法、语义,同时,该框架首次较为完整地抽取出 ATN 模型中的关键元,将协商主体的状态定义为有限域上的四元组配置,特别是将很先进的敏感信息保护技术 Ack 统一进来.

2.2 访问控制策略与信任证

2.2.1 访问控制策略

访问控制策略属于 ATN 研究的一项关键内容[11,19,20],它规定了访问受保护资源所需提供的信任证集.尽管 Internet 颇具随意性,但并不能要求策略语言包罗万象,关键在于:倘若策略语言表达力过分强大,整个系统的策略一致性检查器将变得极为复杂.所以,必须对访问控制策略进行合理的约束,才能保证 ATN 的可应用性.

Seamons 等人[19]通过分析 4 类访问控制策略语言,总结出信任协商策略语言需要满足的要求.其中一项关键特征是强调单调性(monotonicity),因为在分布式广域协作环境中,很难判断某实体不拥有某种信任证.例如,某策略定义:如果你不是 ACM 的会员,就可以访问某类服务.在分布式环境中,用户只要不提供 ACM 颁发的信任证就能访问该服务,这就违背了策略定义的本意.换言之,单调性就是保证在披露信任证减少的条件下,不会导致最终授权集的增加.对于访问控制策略的规范和管理,Leithead 等人[21]基于本体论(ontology)来研究如何在避免敏感信息泄漏的同时,简化策略的管理工作;而 Skogsrud 等人[22]借助状态机描述了 ATN 中访问控制策略的结构,并探讨了策略的生命周期管理等问题.

2.2.2 属性信任证

属性信任证是一种经权威中心(信任证颁发机构)签名的数字断言,且具有可存储性和可验证性.信任证中包括所有方的属性信息,其优势在于能够为陌生方进行授权,从而无须为信任证建立统一的管理机构.

Winsborough 等人[3]最初提及的信任证概念,并不直接支持委托授权.Li 等人[5,6]提出的 RT 语言描述的信任证,能够方便于权限的委托,为 ATN 的广泛应用奠定了良好的基础.在广域网络环境中,进行访问控制决策需要包括从授权源到请求方信任证链的发现过程,Li 等人[6]主要针对 RT_0 中描述的信任证类型,研究了信任证的图形化表示,并给出了一种基于目标制导的信任证链发现和收集(credential chain discovery and collection)算法,该算法从一个访问控制查询开始,寻找同该查询相关的信任证,避免考虑与本地的访问控制决策不相关的大量信任证,既适用于信任证集中存储,也适用于信任证分布式存储.

2.2.3 信息的敏感性

访问控制策略和信任证属于 ATN 中的特殊资源.与一般的文件、服务资源相类似,策略和信任证中也可能包含敏感信息.综合来说,目前所研究资源(主要指访问控制策略和信任证)涉及的敏感信息不外乎两大类:

(1) 资源的内容敏感:访问控制策略本体(实例 2),信任证中的某些属性值(实例 3),属于显式敏感信息;

(2) 资源的拥有敏感:协商方的响应和信息流动会隐式地暴露其保密信息(实例 4),属于隐式敏感信息.

实例 **2**. *A* 公司制定了一项秘密联合计划,协定只有 *B* 公司的 CEO 和 *C* 公司的职员才能访问 *A* 公司的专用资源 *R*,访问控制策略为 $R\leftarrow(C_B.titile=\text{“CEO”})\vee C_C$,$C_B$,$C_C$ 为信任证.如果该策略公开,势必会暴露其合作的伙伴.

实例 **3**. Alice 的驾照 *C* 属于交通部门颁发的信任证,但在某些情况下,Alice 并不希望将其中的年龄属性值 age 随意提供给陌生方,也就是说,*C.age* 属于信任证中的敏感属性.

实例 **4**. Alice 属于某保密组织 *S* 的成员,拥有 *S* 为其颁发的信任证 *C*,如果单纯制订 *C* 的访问策略 *P*,Alice 在向 *C* 的请求方披露策略 *P* 或无响应时,都会隐式地暴露 Alice 是否拥有 *C* 的事实.

Seamons,Winslett 等人[9]从信任证角度划分出属性敏感信任证(attribute-sensitive credential)和拥有敏感信任证(possession-sensitive credential)两类,分别包含在上述的显式和隐式敏感信息分类范围内.

2.2.4 敏感信息的保护

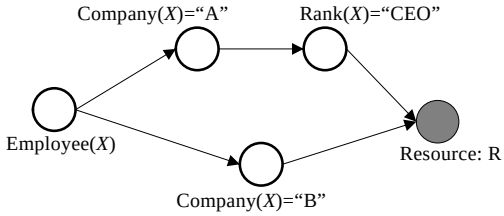

Fig.3 Policy graph of the second example
图 3 实例 2 的策略图

出于对访问控制策略中敏感信息的保护,Seamons 等人[8]提出策略图(policy graph)的概念,采用不带量词和否定关系的一阶谓词表示访问控制策略.策略图为一有向无环图,其终止节点为资源 *R*,其余节点由保护资源 *R* 的访问控制策略组成.例如,对实例 2 所述的敏感策略,对应的策略图如图 3 所示.

Yu,Winslett 等人[20,9,23]提出了一套细粒度的资源保护方案——UniPro(unified scheme for resource protection),为体现应用的广泛性和灵活性,UniPro 并未绑定到一种特定的访问控制策略语言.Yu 区分了策略的可满足性和可视性(visible),例如,对资源 *R* 制定的保护策略记作 *R*:*P*,*P* 仅仅是访问控制策略的一个标识,具体内容为 *p*=*content*(*P*).如果 *P* 是可满足的,并不保证 *p* 是可视的,即:不一定会向协商对端披露 *P* 的内容 *p*.

Yu 等人[18]提出了策略过滤(policy filter)和策略迁移(policy migration)的方法,分别用于解决信任证中可能涉及的两类敏感信息.其中,策略过滤是对信任证中的敏感属性设置一层新的访问控制策略;策略迁移的核心思想是:将保护拥有性敏感信任证的策略迁移到其他可公开披露信任证之上.Winsborough 和 Li 等人[11,12,24]以 RT 为基础,引入属性确认策略(attributed acknowledge policies,简称 Ack)的概念,可用于保护信任证中涉及的两类敏感信息.Ack 策略与访问控制策略的一个典型差异是:主体 *a* 可以采用 Ack 策略,保护其并不一定拥有的敏感属性 *t*,也就是说,虽然主体 *a* 披露了 *Ack*[*t*]策略,但并不能判定 *a* 是否具有属性 *t*.

就资源体的拥有敏感保护而言,无论采用什么方案,其制订和应用过程都需要大量的额外工作.安全协议在信息安全领域占有主导地位,相应地,借助成熟的安全协议保护敏感级别高的信息,成为值得推广的方法.

在实例 4 中,当具有这类属性特点的两个主体交互时,就会产生回环策略依赖问题,这是 ATN 中一个非常棘手的问题.Li 等人[25]将该问题抽象为双方安全函数评估(secure function evaluation)问题,并提出了相应的解决方案——不经意的基于签名信封方案(obvious signature-based envelope,简称 OSBE).最近,Holt,Bradshaw 等人[26,27]提出了 Hidden Credential 技术,借鉴基于身份密码系统思想,将协商方拥有的信任证作为"私钥",实现属性与身份的关联,实现了一套高效信任证披露协议.

就这些技术而言,策略图需要将访问控制策略进行层次化组织,在实际应用中,当涉及到类似 XACML,SAML 等复杂的策略语言时,层次组织将会是一项繁杂的工作.策略过滤利用访问控制策略保护敏感信任证,这本身仍属于传统的信息保护技术,而策略迁移的思路虽巧妙,但存在的缺陷[11]在于:攻击者可以记录多次协商响应动作,当向协商方的两次不同信任证请求出现披露策略雷同情况时,就会泄露信任证的拥有信息;此外,策略迁移由于采用无关策略控制其他可公开信任证的披露,容易导致协商的意外失败.Ack 方案则要求对协商方并不拥有的敏感资源也制订保护策略,当涉及的属性组特别庞大时,势必会导致生成太多的冗余策略,对策略的管理和应用都是不小的负担.安全协议的设计与应用同样也要基于特定的假设条件,例如,OSBE 协议的应用存在两方面的限制:一是协商主体的保密信任证必须是由同一个信任证权威机构颁发;另一个是需要协商方无条件信任协商对端的公钥[27].

2.3 协商策略

Winsborough 等人[3]将协商状态抽象为资源请求方和提供方之间信任证披露序列 $Q=\{C_1,C_2,\ldots,C_n\}$的构造过程,如果协商过程中每份信任证 C_i 都是可公开的,则称 Q 为安全披露序列(safe disclosure sequence).在协商双方对隐私信息的自治保护技术控制下,一个显然的问题就是:如何控制这条披露序列的生成?

Winsborough 等人[3]首次提出协商策略的概念,意在控制信任关系的合理建立,并提出 3 项约束条件:可完成性、可结束性和高效性.据此提出了两种协商策略:一种是积极(eager)策略,要求协商方在接收到协商对端披露的信息后,披露所有可满足访问控制策略保护的信任证;另一种是谨慎(parsimonious)策略,协商双方在披露足量的访问控制策略后才会披露所需的信任证.积极策略往往会披露过多与信任建立无关的信任证;而在谨慎策略中,协商者从信任标的出发,按照严格受控的方式,通过交换指定的访问控制策略,尽可能地减少无关信任证的披露.这两种协商策略控制的协商交互次数与两方持有的信任证数量呈线性关系[3,28].

Yu 等人[28]在对上述两类策略进行研究的基础上,提出了削减(prunes)协商策略,该策略属于一种改进型的回溯策略,按深度优先方式对“安全披露序列”空间进行搜索.由于削减策略是一种暴力搜索策略,虽然完备但搜索代价颇为昂贵——在最坏情况下,通信量和计算量与双方拥有的信任证数量呈指数关系.为了降低复杂度,削减策略通过监控协商方的交互状态(当对某些信任证的请求失败且尚未达到新信任级别的情况下,采用一种避免重发对这类信任证的请求,或对这类信任证请求的监控机制),能够在有效减小安全披露序列搜索空间的同时,尽可能地保证协商的成功率.经过 Yu 等人[28]的证明,削减策略是高效且完备的,其通信复杂度为 $O(n^2)$,其中 n 为双方请求的信任证数目,计算复杂度为 $O(mn)$,n,m 分别为双方拥有的信任证和访问控制策略数目.Yu 等人[16,17,19,28,29]对协商策略进行了深入研究,并将其规范为集合上的映射.

值得注意的是,鉴于 ATN 所研究主体的自治性特征,各主体的协商策略具有差异性,如何保证理论上存在的信任关系能够自动协商建立?这就需要研究协商策略间的互操作性问题.Yu 等人[20,16]采用图论的研究方式,在披露树概念的基础上,演绎出披露树策略(disclosure tree strategy,简称 DTS)来控制披露树的生成.经证明,披露树策略可以生成封闭披露树策略族(DTS family).族的概念保证协商方只要从同一披露树策略族选取协商策略,就能满足协商的互操作性,封闭性则保证了协商方可以最大限定地自由选择信息的披露方式.也就是说,如果向封闭的披露树策略族增加新的披露树策略,将不会再构成一个新的披露树策略族.

2.4 协商协议

在 TrustBuilder 项目中,以统一的资源保护方案为基础,并嵌入协商策略技术,通过定义“空”消息项为协商失败信号等,构成 UniPro 协议[18,20].出于对访问控制策略的保护,UniPro 协议将策略披露细分为策略声明披露(policy declaration disclosure)和策略定义披露(policy defination disclosure)两类.同时,借鉴披露树的表示方法,采用 UniPro 树表示协商状态,基于 DTS 族的原理,UniPro 协议同样构造出 UTS(UniPro tree strategy)族,用于保证协商策略的互操作性.

在基于属性访问控制(ABAC)项目中,基于 RT_0 语言,定义了信任目标图(trust target graph,简称 TTG)协议[11].TTG 为一有向无环图,由协商双方共同构造而成.TTG 协议交互包含 3 种消息类型:TTG 更新消息、协商成功消息和协商失败消息.当协商方接收到 TTG 消息时,则对其储存的信任目标图进行更新;当接受到协商成功消息时,表示原始标的为可满足状态;当接受到协商失败消息时,表示原始标的为不可满足状态,或双方共享的信任目标图无法继续得到更新.由于 TTG 协议是绑定到具有清晰语法、语义的信任管理语言 RT_0,因此,节点处理算法的可操作性要比 UniPro 协议具有一定的优势.

3 信任协商系统及其应用

近几年是 ATN 的理论和技术研究的主要发展时期.在系统实现方面,主要体现为对传统安全传输协议的扩展以及研制相应的 ATN 中间件;在系统应用方面,则主要集中在网格计算和移动通信领域等.

3.1 ATN的实现

Hess 和 Jacobson 等人[30]通过扩展 SSL/TLS 握手协议,增加了 ATN 功能,称为 TNT(trust negotiation in TLS)协议,在握手阶段,通过协商方式交换信任证,客户方同样也可对服务方进行鉴别,提供了高级的 C/S 认证服务,克服了原始 SSL/TLS 协议采用简单 C/S 认证方式存在的缺陷[30].

TrustBuilder[10,23]是目前唯一用于自动信任协商的中间件,它采用 TNT 协议保证信息传输的安全性.TrustBuilder 中的协商 Agent 内部运行结构如图 4 所示.其中,"策略一致性验证器"属于信任管理和 ATN 中的研究热点,它既能根据请求方的访问控制策略,计算出满足策略的信任证集,也能够判定请求方披露的信任证集是否满足其访问控制策略.Smith 等人[10]还专门研究了将信任管理中的"一致性验证器"用于 ATN 所需进行的扩展.

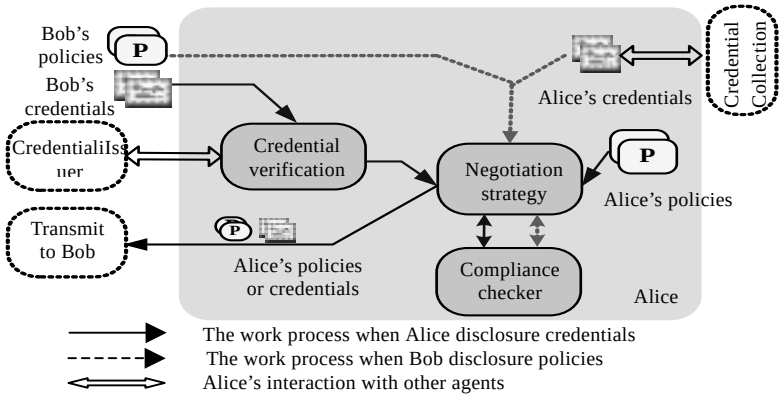

Fig.4 The structure of TrustBuilder negotiation agent
图 4 TrustBuilder 协商主体的内部结构

3.2 ATN的应用

从 ATN 的研究伊始,研究人员就关注着其潜在的应用前景,目前已经涉及到网格计算[15]、Semantic Web[14]和移动通信[31]等多个应用领域.

在 GT3 中,网格安全基础设施 GSI 的认证和授权分别是基于 X509 身份证书和访问控制列表(grid-mapfiles)完成的.然而,这种机制存在诸多不足:首先,在多数应用场景中,参与方通常来源于特定的组织或团体,具有一定的属性,所以兼容基于属性授权方式很有必要;其次,GT3 继续沿用 GT2 的授权机制,将远程用户的授权信息存储在本地的 grid-mapfiles 文件,该文件又将用户 X.509 证书中标识的身份映射到本地标识上(一般为系统账户),维护数量庞大的身份证书库,势必会影响 Grid 安全基础设施的可扩展性和灵活性;最后,虽然新的 GT4 框架中将遵循 WS 系列安全规范,但都尚未考虑信任证中的敏感信息保护,具备了 ATN 功能的 Grid 安全基础设施会占据许多方面的优势[15].

近年来,移动通信技术得到飞速发展,而移动设备在跨安全域间的活动最具动态性,建立信任关系所面临的问题也尤为突出.但移动设备的计算能力是非常具有局限性的,很难独立部署一套完整的 ATN 系统.文献[31]介绍了一种 Surrogate Trust Negotiation 方法来缓解协商对节点性能的要求,该方法将 ATN 的核心功能(例如一致性验证器)从那些"瘦"客户端剥离出来,实现移动设备代理与其他安全域主体的协商功能.

4 现有研究工作的不足及展望

4.1 现有工作的不足

目前,ATN 的研究虽颇具成果,应用领域也不断扩展,但研究内容仍有待不断深入和拓展.

首先,如何建立有效的基础信任模型?现在,ATN 的信任决策模型仍凸显单薄,Yu 寄希望于将 TM 和 ATN 通

过一个有机模型融合起来[18].而在现实社会中,陌生方之间信任的确立往往需要凭借主观和非主观信任相结合的方式.主观信任(计算信任)模型[2]的研究比 ATN 的研究起步要早,它主要侧重于从主观性入手研究信任的数学模型,解决信任的表述、度量、推导和综合运算等问题.因此,探究一种综合式的信任模型将为跨域协作提供更有力的理论基础;

其次,访问控制策略是 ATN 中的一个重要研究内容,时至今日,有关策略语言的研究仍属于一个热点.ATN 的广泛实用需要表达力强、计算效率高而且使用友好的策略语言来支持.策略语言不仅局限于对信任证属性的约束,而且要能够表达跨安全域间复杂的委托约束关系.目前,文献[5]提出的 RT 语言在这方面已初见端倪.同时,在访问控制策略动态变化的情况下,需要研究其对协商策略的影响,即二者间的一致联动关系;

第三,从协议角度研究协商策略的安全性.协商策略主要控制协商协议的交互过程,对于传统的协议,交互消息项是一一对应的;但对于协商策略的消息迁移,不同的本地资源会对应不同的消息映射.这样,在安全协议中容易出现的各类攻击,就同样会在策略协商过程中出现.所以,在保证策略能够互操作的同时,切不可忽视由于策略间交互可能引入的安全漏洞.例如,在对策略迁移的弱点评述中[11],就属于攻击者发起的主动攻击,通过分析协商协议交互信息,从而获取主体是否拥有保密信任证的信息.

第四,提供统一的敏感信息保护方案.目前,针对典型的敏感信息泄漏问题包括多项技术,如 Ack、策略过滤、策略迁移以及 UniPro 方案等.从安全协议从发,更多时候需要借助一些经典的密码协议,例如 OSBE 等协议的应用,一些研究人员也逐渐提出新的想法,“如何能够将零知识证明、公平交易等经典的密码协议技术无缝平滑地集成到 ATN 中?”.但这些技术在某种程度上具有重叠性,例如 Ack 技术完全包含策略过滤技术.因此,将这些技术和协议纳入统一体系下,将更有助于研究适用的 ATN 系统中间件.

4.2 ATN研究的展望

在其他领域,有关协商和隐私信息保护的研究相对成熟,能否借鉴这些领域的研究方法和结论呢?如电子商务和 MAS(multi-agent system)中对交易协商的研究,包括了博弈论(game theory)、启发式搜索等方法.在 ATN 中,具有自治性的协商方依靠策略来指导行为活动:一方面,出于对隐私信息的保护,各方都会制订最优策略;另一方面却不希望过分严格的策略影响协商的成功率和效率.同时,多级数据库(multilevel database)、统计数据库(statistical database)和演绎数据库(deductive database)中对推演控制(inference control)的研究[11],便于防范攻击者利用多次查询得到的结论破解私密信息.此外,信任协商具有与现实生活组织行为活动相一致的属性特征,既要维护信息的隐私性,又要促使资源的广泛共享和协作的顺利进行.

5 结束语

自动信任协商技术解决了跨多安全域隐私保护、信任建立等问题,成为广域安全协作中一个崭新的研究领域,其研究和应用在国际上倍受关注.伴随着 Internet 技术的发展、商务信息的全球化,其应用领域也将不断拓展.同时,任何一种新技术从它的诞生、发展到被广泛接受,都需要进行不断的探索和实验.因此,了解动态、开放网络环境下协作的迫切需求,把握当前国际上 ATN 的研究现状,继续展开深入的研究,将有助于维护多安全域协作中主体的自治性及隐私性,乃至构建开放网络中可信协作的基础设施.

致谢 本文的工作得到了项目组薛伟、林莉、颜强等同学的建议和帮助,在此谨表感谢.同时,特别感谢 North Carolina State University 计算机系的 T. Yu 博士和匿名审稿专家对本文提出的一些建议.

References:

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. In: Proc. of the 1996 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 1996. 164−173. http://citeseer.ist.psu.edu/blaze96decentralized.html

[2] Xu F, Lü J. Research and development of trust management in Web security. Journal of Software, 2002,13(11):2057−2064 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/13/2057.htm

[3] Winsborough WH, Seamons KE, Jones VE. Automated trust negotiation. In: DARPA Information Survivability Conf. and Exposition. New York: IEEE Press, 2000. 88−102. http://isrl.cs.byu.edu/pubs/discex2000.pdf

[4] Johnson W, Mudumbai S, Thompson M. Authorization and attribute certificates for widely distributed access control. In: IEEE Proc. of the 7th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. Washington: IEEE Computer Society Press, 1998. 340−345. http://portal.acm.org/citation.cfm?id=715185

[5] Li NH, Mitchell JC, Winsborough WH. Design of a role-based trust management framework. In: Proc. of the 2002 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 2002. 114−130. http://citeseer.ist.psu.edu/533810.html

[6] Li NH, Winsborough WH, Mitchell JC. Distributed credential chain discovery in trust management. In: Proc. of the 8th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2001. 156−165. http://www.cs.purdue.edu/homes/ninghui/pubs.html

[7] Barlow T, Hess A, Seamons KE. Trust negotiation in electronic markets. In: Proc. of 8th Research Symp. in Emerging Electronic Markets. Maastricht, 2001. http://isrl.cs.byu.edu/pubs/rseem2001.pdf

[8] Seamons KE, Winslett M, Yu T. Limiting the disclosure of access control policies during automated trust negotiation. In: Network and Distributed System Security Symp. (NDSS 2001). Internet Society Press, 2001. http://isrl.cs.byu.edu/pubs/ndss2001.pdf

[9] Seamons KE, Winslett M, Yu T, Yu L, Jarvis R. Protecting privacy during on-line trust negotiation. In: Dingledine R, Syverson PF eds. Proc. of the 2nd Workshop on Privacy Enhancing Technologies. LNCS 2482, Springer-Verlag, 2003. 129−143. http://isrl.cs.byu.edu/pubs/pet2002.pdf

[10] Smith B, Seamons KE, Jones MD. Responding to policies at runtime in TrustBuilder. In: Proc. of the 5th Int'l Workshop on Policies for Distributed Systems and Networks. Washington: IEEE Computer Society Press, 2004. 149−158. http://isrl.cs.byu.edu/pubs/pet2002.pdf

[11] Winsborough WH, Li NH. Towards practical automated trust negotiation. In: Proc. of the 3rd Int'l Workshop on Policies for Distributed Systems and Networks (POLICY 2002). Washington: IEEE Computer Society Press, 2002. 92−103. http://www.cs.purdue.edu/homes/ninghui/pubs.html

[12] Winsborough WH, Li NH. Safety in automated trust negotiation. In: IEEE Symp. on Security and Privacy 2004. Washington: IEEE Computer Society Press, 2004. 147−160. http://www.cs.purdue.edu/homes/ninghui/pubs.html

[13] Herzberg A, Mass Y, Michaeli J, Ravid Y, Naor D. Access control meets public key infrastructure, or: Assigning roles to strangers. In: Proc. of the 2000 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 2000. http://www.haifa.il.ibm.com/projects/software/e-Business/papers/Paper_Trust.pdf

[14] Nejdl W, Olmedilla D, Winslett M. PeerTrust: Automated trust negotiation for peers on the semantic Web. In: Proc. of the Workshop on Secure Data Management in a Connected World (SDM 2004). LNCS 3178, Springer-Verlag, 2004. 118−132. http://www.l3s.de/~olmedilla/pub/trustVLDB04.pdf

[15] Basney J, Nejdl W, Olmedilla D, Welch V, Winslett M. Negotiating trust on the grid. In: Proc. of the 2nd Workshop on Semantics in P2P and Grid Computing at the 13th Int'l World Wide Web Conf. 2004. http://www.ncsa.uiuc.edu/~jbasney/sempgrid.pdf

[16] Yu T, Winslett M, Seamons KE. Interoperable strategies in automated trust negotiation. In: Proc. of the 8th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2001. 146−155. http://isrl.cs.byu.edu/pubs/ccs2001.pdf

[17] Yu T, Winslett M, Seamons KE. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. ACM Trans. on Information and System Security, 2003,1(6):1−42.

[18] Yu T. Automated trust establishment in open systems [Ph.D. Thesis]. Illinois: University of Illinois, 2003.

[19] Seamons KE, Winslett M, Yu T, Smith B, Child E, Jacobson J, Mills H, Yu L. Requirements for policy languages for trust negotiation. In: Proc. of the 3rd Int'l Workshop on Policies for Distributed Systems and Networks (POLICY 2002). Washington: IEEE Computer Society Press, 2002. 68−79. http://isrl.cs.byu.edu/pubs/policy2002.pdf

[20] Yu T, Winslett M. A unified scheme for resource protection in automated trust negotiation. In: Proc. of the 2003 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 2003. 110−122. http://isrl.cs.byu.edu/pubs/oakland03.pdf

[21] Leithead T, Nejdl W, Olmedilla D, Seamons KE, Winslett M, Yu T, Zhang C. How to exploit ontologies in trust negotiation. In: Workshop on Trust, Security, and Reputation on the Semantic Web, Part of the 3rd Int'l Semantic Web Conf. 2004. http://rewerse.net/publications/download/REWERSE-RP-2004-22.pdf

[22] Skogsrud H, Benatallah B, Casati F. Trust-Serv: Model-Driven lifecycle management of trust negotiation policies for Web services. In: Proc. of the 13th Int'l World Wide Web Conf. (WWW 2004). New York: ACM Press, 2004. 53−62. http://www.www2004.org/proceedings/docs/1p53.pdf

[23] Winslett M, Yu T, Seamons KE, Hess A, Jacobson J, Jarvis R, Smith B, Yu L. Negotiating trust on the Web. IEEE Internet Computing, 2002,6(6):30−37.

[24] Winsborough WH, Li NH. Protecting sensitive attributes in automated trust negotiation. In: Proc. of the ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2002. 41−51. http://mason.gmu.edu/~wwinsbor/index_files/Papers/sensitiveAttributes_WPES.pdf

[25] Li NH, Du W, Boneh D. Oblivious signature-based envelope. In: Proc. of the 22nd ACM Symp. on Principles of Distributed Computing (PODC 2003). New York: ACM Press, 2003. 182−189. http://suif.stanford.edu/collective/podc03.pdf

[26] Bradshaw R, Holt J, Seamons KE. Concealing complex policies with hidden credentials. In: Proc. of the 11th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2004. 146−157. http://eprint.iacr.org/2004/109.pdf

[27] Holt J, Bradshaw R, Seamons KE, Orman H. Hidden credentials. In: Jajodia S, Samarati P, Syverson PF, eds. Proc. of the 2003 ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2003. 1−8.

[28] Yu T, Ma X, Winslett M. PRUNES: An efficient and complete strategy for trust negotiation over the Internet. In: Proc. of the 7th ACM Conf. on Computer and communications Security. New York: ACM Press, 2000. 210−219. http://www4.ncsu.edu:8030/~tyu/pubs/ccs2000.pdf

[29] Yu T, Winslett M. Policy migration for sensitive credentials in trust negotiation. In: Proc. of the ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2003. 9−20. http://www4.ncsu.edu:8030/~tyu/pubs/wpes03.pdf

[30] Hess A, Jacobson J, Mills H, Wamsley R, Seamons KE, Smith B. Advanced client/server authentication in TLS. In: Network and Distributed System Security Symp. 2002. http://citeseer.ist.psu.edu/hess02advanced.html

[31] Sundelin TL. Surrogate trust negotiation solving authentication and authorization issues in dynamic mobile network [MS. Thesis]. Provo: Brigham Young University, 2003.

附中文参考文献:

[2] 徐锋,吕建.Web 安全中的信任管理研究与进展.软件学报,2002,13(11):2057−2064. http://www.jos.org.cn/1000-9825/13/2057.htm

李建欣(1979－),男,内蒙古集宁人,博士生,主要研究领域为网络安全,信任管理.

李先贤(1969－),男,博士,副教授,主要研究领域为信息安全,计算机科学理论.

怀进鹏(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算机软件与理论,中间件与网格技术,网络安全.