信任管理中基于角色的委托授权研究进展*

张志勇[1,2]，黄 涛[1,3]

(1. 河南科技大学 电子信息工程学院，河南 洛阳 471003; 2. 西安电子科技大学 教育部计算机网络与信息安全重点实验室，西安 710071; 3. 西北工业大学 计算机学院，西安 710072)

摘 要：通过分析委托授权的本质特征和应用背景，综述了现有的基于角色的委托模型及其特征扩展，并给出了它们在信任管理中的研究进展和应用。最后，指出了目前所存在的问题和今后的研究方向。

关键词：分布式计算；访问控制；委托授权；信任管理；证书链

中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2008)06-1601-05

Research advances on role-based delegation authorization in trust management

ZHANG Zhi-yong[1,2], HUANG Tao[1,3]

(1. *College of Electronic Information Engineering, Henan University of Science & Technology, Luoyang Henan* 471003, *China*; 2. *Key Laboratory of Computer Network & Information Security for Ministry of Education, Xidian University, Xi'an* 710071, *China*; 3. *School of Computer Science & Engineering, Northwestern Polytechnical University, Xi'an* 710072, *China*)

Abstract: By the analysis of delegation essential features and application background, this paper surveyed existing delegation models and characteristics extensions, as well as their research progresses and applications in trust management addressed. Finally, it indicated some existing issues and future research directions.

Key words: distributed computing; access control; delegation authorization; trust management; certificate chain

0 引言

近年来依赖于大规模计算机网络(网格)环境的多种计算模式，如分布式计算、移动计算、普适计算、网格计算等得到了广泛的研究和应用，由此所产生的计算环境的安全问题也面临着严峻的考验。嗅探、窃听、身份冒充与欺骗、分布式拒绝服务攻击等手段以及蠕虫病毒、恶意程序的入侵，致使敏感的数据信息被窃取、窜改和滥用，系统安全遭受到严重的威胁。作为信息与网络安全中传统的研究领域，访问控制理论与技术也是目前研究较为广泛、深入且极其活跃的。从 20 世纪 60、70 年代，面向操作系统安全的、经典访问控制模型与机制研究(如访问控制矩阵模型、BLP 与 BiBa 模型、Take-Grant 模型等)，到 90 年代的 RBAC 研究，以及始于 21 世纪初的面向数字版权管理的使用控制等，访问控制策略主要包括 DAC、MAC、RBAC 和 UCON 等。上述策略和模型主要适合于解决用户身份已知的集中式访问控制和授权问题。

从 90 年代后期，信任管理的出现主要为了解决大规模的、开放分布式环境中的授权问题。与传统的安全授权机制相比，信任管理具有灵活性、可扩展性及可靠性等，使得互操作的实体之间能够建立信任关系，从而完成可靠的授权管理和资源分享。这样，传统的集中式授权管理就不再适应于新的计算环境下的安全访问控制要求。委托技术具有分布式、分散授权和系统可扩展的重要特征。作为信任管理中的核心技术，近年来也得到了研究者的关注和广泛研究。基于角色的委托模型(role-based delegation model)就是在 RBAC 策略的基础上提出的一种旨在解决分布式计算环境下访问授权管理复杂性问题的思想和安全机制。

1 委托授权特征与委托模型

1.1 委托授权的思想与基本特征

委托授权[1]是用户实体将自己所具有的角色或许可转授给其他用户，使其可以代表自己的利益行使一定的职责，协同或独立地完成某些任务，最终达到权力和资源共享的目的。此外委托者还可以撤销委托，收回共享的特权。基于角色委托的基本思想是在分布式环境下，用户可以不经过安全管理人员将自身所具有的角色(显式角色)或所继承的角色(隐式角色)委托给其他用户，使他能够代表自己的职责(角色)行使一定的权限。这样便分散了授权管理，增加了分布式系统的灵活性。其中，委托授权后产生的安全性问题可由系统审计来处理。

与基于角色的委托授权相关的实体有委托者(delegator)、被委托角色/许可(delegated-role/permission)和受托者(delegatee)。委托策略主要考虑以下基本特征:

a) 委托粒度。委托的基本单位主要分为 Zhang 等人[2]提出的基于许可的细粒度、Barka 等人[3]和 Na 等人[4]基于角色的中粒度以及 Zhang 等人[5]提出的基于角色—许可的粗粒度。细粒度是指允许用户将角色中的部分许可委托给另一用户，而不只是角色的整体委托。这样降低了可委托授权的粒度，遵循

收稿日期：2007-07-03；修回日期：2007-12-27 基金项目：国家自然科学基金资助项目(60573035)；河南科技大学青年基金资助项目(2005QN019)

作者简介：张志勇(1975-)，男，河南新乡人，CCF 会员，博士研究生，主要研究方向为访问控制策略及其形式化描述、可信计算与可信网络(xidianzzy@126.com)；黄涛(1966-)，男，河南洛阳人，实验师，硕士，主要研究方向为委托授权、CSCW 系统.

了最小特权原则;但是会产生大量逻辑意义上不完整的角色,从而又增加了授权管理的复杂性和实际应用系统的开销。中粒度是指用户只能将自身的角色整体委托给其他用户,从而使其获得该角色所具有的全部许可权限。它在某种程度上违背了最小特权原则。粗粒度委托是用户可以任意将自身的角色和(或)许可委托给他人。这样的委托较前两者更为灵活,然而实现时较为复杂。关于委托粒度需要根据实际应用系统的需求折中选择合适的委托授权基本单位。

b)委托传播。在委托权限进一步传播和转让过程中,可以通过构建委托树来实现。委托树的深度具体可分为单步委托和多步委托两类。前者是指受托者不可以进一步地将委托角色或许可再次委托给其他用户;后者则是允许受托者进一步实施委托,但撤销委托将变得复杂和困难。委托树的广度是指角色或许可可以同时被授权的数量,即针对同一委托权限,它所属的受托者集合的基数问题。

c)委托时限。角色或许可的委托具有临时性、周期性等特征,因此在委托时限内,用户可以合法地执行被委托的能力;超出时限的角色或许可将被系统或委托者收回。

d)委托撤销。委托过程的逆操作称为委托撤销,即完成被委托角色或许可的回收。撤销的主要方式有级联、非级联、独立于授权、非独立于授权、系统自动和用户撤销等。

e)委托约束。针对上述四个特征,对角色(许可)委托过程和委托使用过程的基本约束限制,从而实现更为严格的自定义安全策略和委托策略。主要表现为委托步约束、委托时限约束以及委托实施约束等方面。

1.2 研究动机与应用情景

在分布式计算环境下,传统的集中式授权管理加重了安全管理员的负担。这种繁重的授权工作已经不再适应新的环境。为此提出了角色委托的概念,它是安全分布式计算环境的一个重要因素。委托作为是一种重要的安全策略,通常运用于如下应用场景中[2]:

a)职责备份。当某人临时不在岗位时,他所负责的工作需要由他人继续接管实施。这时需要将其工作权力暂时委托给他人,并通过委托安全策略(涉及 1.1 节委托的五种基本特征)控制委托权限的有效使用。

b)职权分散。当某个组织初始构建或后来重组时,需要按照组织结构将工作职权从高层向低层进行分配。

c)协同工作。在单个组织内部以及多个组织间进行高效协作和资源(权力)共享时,需要资源和权力属主将部分或全部权限临时转让给协作者。

2 基于角色的委托模型研究

2.1 基于角色的委托模型

Barka 和 Sandhu 最早在文献[1]中分析了基于角色委托模型的一些基本特性,包括委托的临时性、单调性、委托角色完整性、委托传播性、管理性等,并提出了角色委托模型的研究方向。其中,单调性是表示委托者在将角色委托授权给其他实体后,是否失去相应的许可;委托角色完整性是指是否将角色作为委托的最小单位,即角色的原子性和委托粒度;委托传播性是被委托的角色仍可以再次进行转让,即委托树的深度问题;委托管理性是对委托过程涉及的多个实体的管理和控制特性。同时,他们提出了一个基于角色的委托模型 $RBDM_0$[3]。该模型是第一个支持用户到用户的角色委托模型,并且非形式化地提出了在委托细粒度、委托传播、支持具有角色层次属性的委托,以及委托撤销等方面的扩展特征。$RBDM_0$ 存在角色委托的时限,并且该模型中委托细粒度和传播特征是通过委托约束机制加以描述,但并不显式支持这些特征,使得模型在使用时效率较低,并具有较大的系统开销。此后,Barka 等人又在文献[6]中基于 $RBDM_0$ 作了角色层次上的扩展,给出了支持角色层次的 $RBDM_1$,但仍然不显式支持委托细粒度和委托传播性。文献[7]基于 $RBDM_0$ 提出了 RDM2000。该模型对 $RBDM_0$ 在委托传播和约束方面作了进一步扩展,并采用基于规则的描述语言形式化地描述了该委托策略。但是,与 $RBDM_0$ 一样,该模型为保持委托角色的完整性,只支持基于角色中粒度的整体委托,然而在职责备份和协同工作情形下,部分委托则是必需的。这时上述模型将不能满足实际需求。

2.2 基于许可的委托模型

文献[8]中针对 $RBDM_0$ 和 RDM2000 禁止重复角色委托和不支持细粒度的缺点,提出基于重复和部分角色的转授权模型 RPRDM(repeated-and-part-role-based delegation model),并定义了该模型的组成元素以及转授权和转授权撤销规则等;最后给出了 Linux 实现 RPRDM 的一个实验原型,并指出如何形式化描述与该模型相关的安全策略将是今后的研究方向之一。文献[2]中提出了 PBDM(permission-based delegation model)委托模型家族,其主要特征是支持角色间的基于许可的细粒度委托。其中,部分委托是通过用户创建临时性的委托角色 DTR(delegatgion role)区别于普通授权角色(regular role),将待委托的许可(集)指派给临时委托角色,然后再将其委托给用户。在实现上临时委托角色的引入能够封装多个待委托许可或可委托角色,并可以一次性地进行委托。但这种方式需要创建大量的临时性角色,这些角色可能在组织内部的语义并不完整,同时也导致模型的使用和管理的高复杂性。文献[5]提出了基于许可—角色粗粒度的委托模型。临时委托角色 TDR 不仅可以封装多个许可,也可以将多个普通角色指派给 TDR,即 TDR 是许可和角色的集合。这样可以更灵活地实现许可和(或)角色的同时委托,但在实现上增加了系统的开销和 TDR 的管理复杂性。

2.3 基于特征扩展的委托模型

文献[9]主要针对委托约束的基本特征,提出了一个基于角色的受限委托模型(constrained role-based delegation model, CRDM)。该模型在 $RBDM_0$ 的基础上,通过引入委托票据的概念,并以角色作为委托粒度,着重解决临时性限制约束、常规角色关联性限制约束等问题。其中,在委托的时限约束上表现得较为灵活,可以在委托角色的生命周期内控制激活时间、使用次数;常规角色关联则通过常规角色当前的激活状态这一先决条件,判定委托角色是否可以有效地执行。该模型对于委托角色的使用限制和约束特征,从多个方面进行了讨论,但缺少统一的描述约束框架和形式化语言,并且其中的角色继承和层次以及多步委托问题还有待于进一步研究。文献[10]针对 PBDM 中的委托约束问题,为提高委托过程的安全性,提出了一

种基于属性的委托模型(attribute-based delegation model, ABDM$_A$) 。通过同时实现委托先决条件(CR) 和委托属性表达式(DAE) , 增强对用户和权限的使用限制, 提高了委托过程的安全性。但由于委托实现采用类似于 PBDM 构建临时委托角色集的方法, 该模型在管理上也存在较高的复杂性问题。

文献[11] 针对委托粒度和委托传播特征, 提出了量化角色的概念, 实现了一种强制与自主相结合的细粒度委托约束机制, 给出一个形式化的基于量化角色的可控委托模型(quantified role based controllable delegation model, QBCDM) 。量化角色是对普通 RBAC 角色的扩展, 可以描述其任意部分权限, 能够较好地实现细粒度的委托能力, 并且改进了 PBDM 委托角色的管理复杂性问题。此外, 该模型结合 DAC 和 MAC 基本特征, 实现了更为严格的委托传播限制。

文献[12] 针对委托时限的相关特征, 基于 Bertino 的周期时间自主访问控制模型, 较为详细地形式化构建了一种基于周期性时限的 DAC 委托模型 PDACDM。它主要面向用户到用户的委托访问权限限制, 对权限委托的临时性、时序依赖性和受限传播性等约束特性进行探讨, 并给出了相关的推导规则集和应用实例。此外, 本文提出正负权限的概念。负权限是指用户对于某个客体不该具备的访问权限, 这对于开放系统环境下的委托授权研究是值得关注的。

Bandmann 等人在文献[13] 中针对委托约束特征, 提出一个受限的委托模型及其在协作组织中的委托框架。该模型通过正则表达来描述委托约束, 从而对委托树的构建进行限制。该框架将权限的委托与使用分离。具体的约束限制表现为组成员约束、时间约束和外部数据的依赖约束等。

3　信任管理中的委托授权

3.1　信任管理技术

信任管理[14] 作为一种开放环境下支持分布式授权的技术近年来得到了广泛而深入的研究。它支持匿名主体用户的访问控制, 通过委托授权机制实现信任的传递, 从而支持分布式应用, 并依据相关的信任评估模型, 完成对主体用户的信任评价和计算。信任管理的主要研究内容和实现是解释说明安全策略和信任凭证, 以及判定它们之间的一致性关系; 依据判定结果, 通过信任凭证对某个动作请求进行委托授权, 传递信任关系和拓展信任链。

为了使信任管理能够独立于特定的应用, Blaze 等人[15] 等人提出了一个基于信任管理引擎(trust management engine, TME) 的信任管理模型, 如图 1 所示。TME 是整个信任管理模型的核心, 体现了具有通用性、应用独立性的一致性验证算法, 根据输入的三元组(*r*, *C*, *P*) , 由信任管理引擎判定策略是否被满足, 并对应用系统的动作请求进行响应。其中, 安全策略 *P* 是指本地定义的可信授权规则; 而信任凭证 *C* 表示用户实体间基于委托机制的信任传递。对于请求 *r* 相关的凭证集合 *C* 是否与本地安全策略 *P* 具有一致性的判定和授权则由一致性验证器来完成, 并将判定结果反馈给应用系统来实施访问控制。信任管理引擎负责判定和推荐信任关系, 具体的信任实施则由应用系统实现。这里假设凭证系统、本地策略数据库、信任管理引擎和应用系统都是可信的, 从而构成一个具有信任边界的信任域。

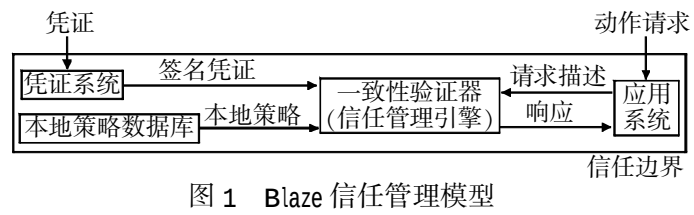

图 1　Blaze 信任管理模型

信任管理涉及信任管理模型、信任评估模型以及具有委托特性的授权模型等。本文主要讨论其中的委托授权机制与相关模型的研究进展情况。

3.2　基于 SPKI/PMI 的传统委托授权

Blaze 等人提出的 PolicyMaker[14] 和 KeyNote[15] 作为经典的信任管理系统, 通过实体凭证集支持委托授权, 但两者主要探讨的是安全凭证和策略的表达、元语言描述以及一致性验证器的判定决策算法等, 对于其中的委托机制和实现涉及较少。Ellison 等人[16] 提出的 SPKI 主要借助于证书机制, 较为灵活地实现了委托授权的表达和传递。这与上述信任管理系统是一致和互补的。SPKI 中包括两种证书, 即授权证书和名字证书。授权证书表达权限的指派, 是公钥或名字等与权限的绑定。SPKI 授权证书使用委托机制进行权限传播, 通过委托字段的关联从而形成从证书初始发布者 CA 到最终被级联委托授权的用户实体之间一条完整的证书链。对于该证书链的搜索通常采用自顶向下或自底向上的搜索算法。

随着基于 X.509 证书格式的 PKI 技术的发展和面向可信域的实际部署, 为表达更为详细的实体属性特征(包括角色、组成员关系、权限等) , X.509 公钥证书进一步向属性证书扩展, 由此产生了 PMI 技术以及委托技术在 PMI 中的相关研究与应用等。基于 X.509 属性证书的 PMI 主要是通过属性证书进行系统用户或其他实体的授权管理与访问控制过程。属性证书 AC(attribute certificate) 不同于 PKI 中的公钥证书 PKC, 它是由 AA(attribute authority) 机构颁发的记录用户特权信息的载体, 具有短期的时效性。PMI 和其他信任管理技术均可以实现基于角色的委托授权, 但是 PMI 关于委托的实现仅限于集中式属性权威机构 AA 的委托授权, 特权声称者 PA(privilege assertion) 及用户本身不具备委托授权能力, 这将不适合于分布式 PMI 应用的创建[17 ~19] 。然而信任管理主要面向于分布式环境, 其中任何一个拥有公私钥对的实体都可以发布证书。因此传统的 PMI 在分布式授权上具有一定的局限性。文献[20] 对于分布式环境下基于证书的委托机制, 提出了主要的研究内容和开放问题, 如权限管理与指派、委托证书链、委托控制和委托撤销等。

3.3　基于 PMI/角色的分布式委托授权

文献[21] 提出了传统 PMI 体系在委托授权方面存在的问题。委托授权者是 SOA 或各级 AA、SOA 具有最高和最广泛的权限, 各级 AA 只具备由上一级 AA 授予的局部权限, 它们可以将所属的特权或特权子集委托给实体 PA。这种委托过程属于集中式特权管理, PA 不具有委托能力。在大型分布式应用环境下, 由于大量实体的存在, 委托授权只能集中在 AA 机构, 将使其承担繁重的管理工作; 并且在委托验证时需要 AA 逐级向上回溯至 SOA, 这又增加了委托验证的时间复杂度。

根据委托特性, 文献[21] 所给出的 DM for PMI(delegation

model for PMI) 模型既弥补了原有委托模型不支持权限级委托授权的缺陷, 又保持了角色级委托授权管理中高效、灵活的特点, 是一种在分布式应用环境下解决委托问题较为完备的模型。同时, 依据 DM for PMI 对传统的 PMI 体系架构进行了扩展, 引入委托证书、委托失效列表、委托审计等组件构成了 EPMI, 使其具有分布式委托特性。鉴于委托授权的短期时效性, 不将委托信息写入属性证书, 而是构建 DC 发放给受托者。除了 SOA、AA 具有委托特权外, 终端实体 PA 也具备委托能力。PA 可以在遵循 SOA 制定的委托策略前提下, 通过终端系统生成的 DC 直接(或间接由 AA 机构托管) 将显式或隐式角色以及权限委托给受托者 PA。当 PA 需要撤销委托或委托时限到达时, PA(或系统) 将在委托失效列表 DEL(delegation expire list) 中添加 DC 的惟一标志, 使 DC 作废, 同时多步委托特权也被具有依赖性的级联撤销。

鉴于分布式委托的分散性, 为保证 PA 委托的安全和合法, 在 EPMI 中引入委托审计机制。系统对 PA 每一次委托授权和撤销过程进行跟踪监视, 将审计信息存储在审计数据库中, 以便将来进行安全检测。

3.4 基于逻辑/角色的委托授权

委托技术是信任管理中的一项核心技术, Li 等人[22] 首先于 1999 年提出了一种基于逻辑的知识描述语言——委托逻辑(delegation logic, DL) 。它主要用于描述大规模、开放、分布式环境下的授权机制。该文献提出对于任意系统在判定一个请求动作是否应当被授权的关键是授权委托、授权否定和授权冲突的表达。DL 基于已有的委托技术和信任管理研究, 以及在逻辑语言和非单调推理方面的否定和冲突研究, 形式化地给出了 DL 相关语法及语义说明。与已有的基于逻辑的授权方法所不同的是, DL 基于逻辑程序显式地表述了委托深度, 并且支持广泛的负责策略, 其中包括(n, k) 门限等; 与现有信任管理方法所不同的是, 一致性验证是基于理论模型的语义。该语言不仅具备说明性语义, 其一致性证明也是基于完备的逻辑基。同时, DL 可在分布式授权中描述复杂的信任关系和委托特征。DL 和 PolicyMaker、KeyNote 等系统在一致性证明上有所不同, 它的一致性证明是基于逻辑程序的模型理论语义来实现的, 具有实现独立性。

此后, 在文献[23, 24] 中将信任管理与基于角色的访问控制进行结合, 提出了基于角色的信任管理框架 RT。该框架是描述用于分布式授权策略和安全凭证的基于角色的信任管理语言集合, 它将 RBAC 角色易于组织和管理的优势, 与信任管理系统相结合, 使其适合于基于属性的访问控制。通过简单的证书形式, 提供了对角色的本地授权、角色委托定义、关联角色、参数化角色等; 此外 RT 引入簇角色来表述授权限制和职责分离策略, 以及激活角色的委托。通过在框架中实现从证书到 datalog 逻辑语言规则的翻译, 形式化地定义了证书的语义。文献[25] 针对信任管理中不同类型的委托深度控制方案, 将基于正整数值的委托深度控制方法引入到 RT 框架中, 提出了 $RT+_0$ 模型及形式化描述了证书的相关语法, 并将其翻译为可操作的逻辑规则, 增强了委托深度控制的语义表达能力。

3.5 基于 RBAC 模型的委托授权

Freudenthal 等人[26] 在 RT 框架的基础上提出并形式化定义了一个动态结盟环境下的分布式 RBAC 模型 dRBAC(distributed RBAC) 以及基于图方法的证书搜索和验证。dRBAC 是一种面向跨多个管理域的具有分布式可扩展性、非集中式的信任管理和访问控制策略。它利用 PKI 机制定义信任域, 通过角色指派实现多许可的分配, 并且可实现跨域的角色委托。dRBAC 的主要特征体现在来自于域的名空间之外引入的第三方角色委托依赖于显式的委托指派; 使用与角色关联的数量值属性实现权限转移; 对时间较长的交互进行持续的实体信任关系监控, 从而确保信任关系的有效性和延续性。dRBAC 实现了一个较为完整的访问控制系统用于分发、搜索、验证和撤销基于角色的委托, 适用于较大规模的分布式安全环境的构建。

面向信任管理的委托授权, 结合 RBAC 模型中角色和组织结构的一致性、可管理性、高效灵活性等优势, 已经取得了广泛的研究, 但在角色授权级联撤销方面仍缺乏高效的机制。由于委托的临时性和时限性, 有效地实现委托角色不同方式的回收机制是一个完备的授权系统所必需的。此外, 基于角色的委托授权在角色继承、角色层次构建和委托基数(委托树的广度) 等方面同样缺少深入的研究。现有机制能够隐式地支持角色层次关系, 但相比显式机制而言, 在实施代价和效率方面将有待于进一步提高, 这对于信任管理系统最终得到广泛的应用和部署至关重要。

3.6 基于信任度/角色的委托模型

现有的委托模型在分布式环境下基于认证用户的访问控制中得到了深入研究, 尤其是在委托的周期性、委托树的深度, 以及委托中角色的相关属性进行了不断扩展和完善。然而这些模型不能满足分布式环境下基于匿名和未知用户的访问控制问题, 同时由于它们未考虑委托中的信任问题, 也不适用于信息管理的应用。首先, 在信任管理中委托授权需要考虑两个实体之间的信任程度, 而此时的信任度并非只是处于信任与不信任二值之间, 还应考虑更全面的信任度量, 即当信任度处于二值之间时的委托情形, 这是信任管理所必需的。其次, 现有的信任管理系统对委托的深度控制还没有很好的方案, 因此需要在模型或实现机制层次上给出委托控制问题的解决。基于信任度的委托授权模型(trustworthiness based authorization delegation model, TBAD) 使用信任度来刻画授权实体和被授权实体之间的信任程度, 满足分布式开放环境中的信任管理, 并有效地解决了委托的深度控制问题[27] 。

TBAD 是基于信任度和角色概念的模型, 它非形式化地定义了其基本组件, 包括实体、角色、客体(委托的对象)、主体(被委托的对象) 等。此外该模型引入信任度的概念, 即指一个实体对另一个实体的信任程度, 这里可用一个区间整数表示信任度。信任度的值刻画了实体之间彼此的信任程度。在实现上, TBAD 仍采用访问控制列表 ACL 作为资源所有者的授权源。一个 ACL 元组由权限、主体和信任度三部分组成。其中信任度不是表示资源所有者对主体的信任程度, 而是表示权限能够被授予的一个信任度阈值, 即只有当该权限的请求者所拥有的信任度达到该条目中的信任度阈值时, 才能将该权限授予给请求者。

在 TBAD 中, 证书的发布者、受托者具有一定的信任程度, 用证书表示委托关系, 并用自己的私钥对证书进行数字签名,

该证书具有有效期等相关属性。该模型的一致性验证问题就是证书链查找和信任度的传递计算。TBAD 为了能够快速地查找合法的证书链,需要对访问请求者提供的所有证书和本地安全策略(即 ACL)进行预处理。首先验证证书的有效性,包括证书是否过期、信任度的取值是否合法,以及证书的数字签名是否正确,从而提高证书链查找的效率。此外,用简单的形式表示合法的证书和访问控制列表的条目。证书链搜索可以从访问控制列表条目中的权限开始(前向搜索法),也可以从委托(即证书)的主体开始(后向搜索法),还可以同时从权限和主体开始(双向搜索法)。

关于信任传递计算模型,TBAD 在满足信任函数单调递减性和有界性的基础上简化了计算模型,把它表示为 $f(t_1, t_2)$,即信任链上相邻的委托信任度的值。通过计算证书链上每个主体拥有相应权限的信任度,结合 ACL 的信任度阈值来判定委托是否有效,即受托者是否能得到相应的委托角色或权限,从而达到了对委托深度进行有效控制的目的。

作为信任管理中的委托模型研究,TBAD 将信任度引入委托模型中,根据信任度的不同和基于证书链的信任传递,初步实现了信任管理中的委托授权机制,并给出了一个应用举例。然而,该模型还存在若干问题:

a) TBAD 的实体中定义角色实体,但在委托形式化定义时并未涉及角色与信任度的关系,信任度仍然与用户直接关联。因此在应用中,未能体现角色实体的意义。

b) 该模型对委托深度的控制采用信任传递模型计算从委托者到受托者的信任值,然后与权限信任阈值比较,判定此次委托是否有效。TBAD 没有使用显式的委托深度控制,不利于委托者直接控制权限的传播。委托信任值的计算复杂度是 $O(n)$,而基于委托树深度值的判定时间开销只有 $O(1)$。

c) TBAD 没有涉及委托授权的回收,因此该模型是不完备的,需要完整定义委托撤销的方式和实现机制。

d) TBAD 模型缺少具体的形式化工作,包括委托的时限描述以及基于角色的委托约束规则等。

4　结束语

近年来委托模型研究得到了深入的研究,并且在重要组件上得到了扩展和完善。信任管理作为分布式计算环境下的访问控制研究对象,它依赖于证书链机制实现了系统对匿名用户的信任管理和访问授权。分布式环境下用户间的资源共享必然涉及到委托授权问题,同时这也是解决集中式授权服务器负荷过重的有效方案。委托授权在传统基于角色的访问控制中的研究已比较成熟,如何将它应用在信任管理中将是今后信任管理的一个重要研究方向。目前这个方向的研究仍然不足,所面临的问题和研究内容包括:

a) 用户间的信任度差异使得委托授权的范围和时限不同,因此信任管理中需要细粒度的、具有委托时限的委托模型。目前这个方面已有相应成果,但需要考虑如何将信任度引入模型之中。

b) 目前的信任管理模型是基于用户实体的信任度管理,当用户具有多个角色或权限时,单一的用户信任度将不能满足系统要求。因此,还需要将信任度与角色联系,根据受托者信任度和角色信任度的比较,判定是否委托该角色。

c) 信任管理中的委托撤销除了通过证书期限由系统判定委托的有效性之外,委托者根据应用系统的变化和实际需求,如何实现用户主动撤销委托以及证书链的修正,也将是今后待解决的主要问题。

d) 信任委托树的深度和广度研究并重,委托树的深度研究涉及到权限委托的安全传播和高效的级联撤销等问题,目前研究较为深入。然而,委托树的广度研究相对薄弱,它主要涉及到同一权限受托者集合的基数控制。在某些应用场景下这也是必不可少的。如何描述这种基数控制策略也是今后值得关注的方向。

参考文献:

[1] ARKA E, SANDHU R S. Framework for role-based delegation models[C]//Proc of the 16th Annual Computer Security Application Conference. New Orleans: IEEE Computer Society Press, 2000: 168-176.

[2] ZHANG Xin-wen, OH S, SANDHU R S. PBDM: a flexible delegation model in RBAC[C]//Proc of the 8th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2003: 149-157.

[3] BARKA E, SANDHU R S. A role-based delegation model and some extensions[C]//Proc of the 23rd National Information Systems Security Conference. Baltimore, Maryland: NIST, 2000: 101-114.

[4] NA S Y, CHEON S H. Role delegation in role-based access control[C]//Proc of the 5th ACM Workshop on Role-based Access Control. New York: ACM Press, 2000: 39-43.

[5] ZHANG Zhi-yong, PU Jie-xin. Permission-role based delegation model and object-oriented modeling[C]//Proc of China National Open Distributed and Parallel Computing Symposium. Beijing: Computer Engineer and Application, 2004: 52-55.

[6] BARKA E, SANDHU R S. Role-based delegation model/ hierarchical roles (RBDM1)[C]//Proc of the 20th Annual Computer Security Applications Conference. Washington DC: IEEE Computer Society, 2004: 396-404.

[7] ZHANG Long-hua, AHN G J, CHU B T. A rule-based framework for role-based delegation[C]//Proc of the 6th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2001: 153-162.

[8] 赵庆松,孙玉芳,孙波. RPRDM:基于重复和部分角色的转授权模型[J]. 计算机研究与发展, 2003, 40(2): 221-227.

[9] 徐震,李斓,冯登国. 基于角色的受限委托模型[J]. 软件学报, 2005, 16(5): 970-978.

[10] 叶春晓,吴中福,符云清,等. 基于属性的扩展委托模型[J]. 计算机研究与发展, 2006, 43(6): 1050-1057.

[11] 翟征德. 基于量化角色的可控委托模型[J]. 计算机学报, 2006, 29(8): 1401-1407.

[12] 张宏,贺也平,石志. 基于周期时间限制的自主访问控制委托模型[J]. 计算机学报, 2006, 29(8): 1427-1437.

[13] BANDMANN O, DAM M, FIROZABADI B S. Constrained delegation[C]//Proc of the 23rd Annual IEEE Symp on Security and Privacy. Oakland: IEEE Computer Society Press, 2002: 131-143.

[14] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society Press, 1996: 164-173.

[15] BLAZE M, FEIGENBAUM J, IOANNIDIS J, *et al*. Request for comments 2704, the KeyNote trust management version 2[S]. Sterling, VA: Internet Engineering Task Force, 1999.

(下转第 1610 页)

[8] GKANTSIDIS C, MIHAIL M, ZEGURA E. Special analysis of Internet topologies[C] //Proc of IEEE INFOCOM 2003. San Francisco: IEEE, 2003: 364-374.

[9] 刘玮. 由认知到感知: 谈信息可视化技术[EB/OL] . (2003) . http: //www. e-works. net. cn/ ewkArticles/xxhyl. htm.

[10] ATTISTA G D, EADES P, TAMASSIA R, *et al*. Algorithms for drawing graphs: an annotated bibliography[J] . Computational Geometry: Theory and Applications, 1994, 4(5) : 235-282.

[11] TOLLIS I G, Di BATTISTA G, EADES P, *et al*. Graph drawing: algorithms for the visualization of graphs[M] . New York: Prentice Hall, 1999.

[12] IAZ J, PETIT J, SERNA M. A survey of graph layout problems[J] . ACM Computing Surveys, 2002, 34(3) : 313-356.

[13] MUNZNER T, HOFFMAN E, CLAFFY K, *et al*. Visualizing the global topology of the MBone[C] //Proc of IEEE Symposium on Information Visualization. San Francisco, California: [s. n.] , 1996.

[14] LOMBARDONI A. The cone tree layout algorithm[EB/OL] . http: //www. inf. ethz. ch/ personal/lombardo/ archives/da/node9. html.

[15] MUNZNER T. Drawing large graphs with H3Viewer and site manager [C] //Proc of GD '98. 1998: 384-393.

[16] GRAHAM J W. Niche works-interactive visualization of very large graphs[C] //Proc of GD '97. 1997.

[17] SUGIYAMA K, TAGAWA S, TODA M. Methods for visual understanding of hierarchical systems[J] . IEEE Trans on Systems, Man, and Cybernetics, 1981, 11(2) : 109-125.

[18] EADES P A. A heuristic for graph drawing[J] . Congressus Numerantium, 1984, 42: 149-160.

[19] FRUCHTERMANN T, REINGOLD E. Graph drawing by force-directed placement[J] . Software-practice and Experience, 1991, 21(11) : 1129-1164.

[20] RODGERS P, MUTTON P. Visualizing weighted edges in graphs [C] //Proc of the 7th International Conference on Information Visualization. 2003.

[21] SAGIE G, WOOL A. A clustering approach for exploring the Internet structure, EES2003-7[R] . [S. l.] : Tel Aviv University, 2003.

[22] DHAMIJA R, FISHER D, YEE K P. gnuTellaVision: real-time visualization of a peer-to-peer network[EB/OL] . http: //www. sims. berkeley. edu/ ~rachna/courses/infoviz/ gtv/paper. html.

[23] 黄竞伟, 康立山, 陈毓屏. 一个新的无向图画图算法[J] . 软件学报, 2000, 11 (1) : 138-142.

[24] BARRETO A M S, BARBOSA H J C. Graph layout using a genetic algorithm[C] //Proc of International Conference on Neural Networks. 2000: 179-184.

[25] 孙炜, 吴伟民, 陈志峰. 基于遗传模拟退火算法的图的三维可视化[J] . 广东工业大学学报, 2002, 19(1) : 37-41.

[26] MONIEN B, RAMME F, SALMEN H. A parallel simulated annealing algorithm for generating 3D layouts of undirected graphs[C] //Proc of International Symposium on Graph Drawing. 1995: 369-408.

[27] [EB/OL] . http: //www. caida. org/tools/visualization/index. xml.

[28] [EB/OL] . http: //www. isi. edu/ scan/mercator/ mercator. html.

[29] SIAMWALLA R, SHARMA R, KESHAV S. Discovering Internet topology[C] //Proc of INFOCOM. 1999.

[30] BURCH H, CHESWICK B. Mapping the Internet[J] . IEEE Computer, 1999, 32(4) : 97-98.

[31] CHESWICK B, BURCH H, BRANIGRAN S. Mapping and visualizing the Internet[C] //Proc of USENIX Annual Technical Conference. 2000.

[32] AU S C, LECKIE C, PARHAR A, *et al*. Efficient visualization of large routing topologies[J] . International Journal of Network Management, 2004, 14(2) : 105-118.

[33] [EB/OL] . http: //nlanr. net/.

[34] BROWN J A, McGREGOR A J, BRAUN H W. Network performance visualization: insight through animation[C] //Proc of PAM2000. 2000.

[35] CARMIGNANI A, Di BATTISTA G, DIDIMO W, *et al*. . Visualization of the high level structure of the Internet with hermes[J] . J of Graph Algorithms and Applications, 2002, 6(3) : 281-311.

[36] [EB/OL] . http: //delis. udp. de/index-2. html.

(上接第 1605 页)

[16] LLISON C, FRANTZ B, LAMPSON B, *et al*. Request for comments 2693, SPKI certificate theory[S] . Sterling, VA: Internet Engineering Task Force, 1999.

[17] LINN J, NYSTROM M. Attribute certification: an enabling technology for delegation and role-based controls in distributed environments [C] //Proc of the 4th ACM Workshop on Role-based Access Control. Virginia: ACM Press, 1999: 121-130.

[18] CHADWICK D W, OTENKO O. The PERMIS X. 509 role-based privilege management infrastructure[C] //Proc of the 7th ACM Symposium on Access Control Models and Technologies. Monterey: ACM Press, 2002: 135-140.

[19] 许长枫, 刘爱江, 何大可. 基于属性证书的 PMI 及其在电子政务安全建设中的应用[J] . 计算机应用研究, 2004, 21(1) : 119-122.

[20] CANOVAS O, GOMEZ A F. Delegation in distributed systems: challenges and open issues[C] //Proc of the 14th International Workshop on Database and Expert Systems Applications. Washington DC: IEEE Computer Society Press, 2003: 499-503.

[21] 张志勇, 普杰信. 委托授权在 PMI 体系架构中的研究与应用[J] . 计算机工程, 2006, 32(5) : 152-154.

[22] LI Ning-hui, FEIGENBAUM J, GROSOF N B. A logic-based knowledge representation for authorization with delegation[C] //Proc of IEEE Computer Security Foundations Workshop. Washington DC: IEEE Computer Society Press, 1999: 162-174.

[23] LI Ning-hui, MITCHELL J C, WINSBOROUGH W H. Design of a role-based trust-management framework[C] //Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society Press, 2002: 114-130.

[24] LI Ning-hui, MITCHELL J C. RT: a role-based trust-management framework[C] //Proc of DARPA Information Survivability Conference and Exposition (DISCEX III) . Washington DC: IEEE Press, 2003: 201-212.

[25] HONG Fan, ZHU Xian, WANG Shao-bin. Delegation depth control in trust-management system[C] //Proc of the 19th International Conference on Advanced Information Networking and Applications. Washington DC: IEEE Computer Society, 2005: 411-414.

[26] FREUDENTHAL E, PESIN T, PORT L, *et al*. dRBAC: distributed role-based access control for dynamic coalition environments, TR2001-819[R] . New York: New York University, 2001.

[27] 廖俊国, 洪帆, 朱更明, 等. 基于信任度的授权委托模型[J] . 计算机学报, 2006, 29 (8) : 1265-1270.