多域环境下安全互操作研究进展

金 莉 卢正鼎 赵 峰
(华中科技大学计算机科学与技术学院 武汉 430074)

摘 要 多域安全互操作是通过认证机制、访问控制机制和审计机制来实现多个分布、异构、自治区域间安全的资源共享和信息交互的过程。系统介绍了这一新型研究领域的理论基础和应用现状,从解决访问控制安全和域间策略冲突的角度,对域间角色转换技术、基于信任管理、基于PKI和基于时间限制等方向的多项研究成果和关键技术进行分析和点评,重点探讨了多域环境下各自治域间策略集成算法的建模和实现,最后针对目前研究工作中存在的问题,对该领域未来的发展方向和趋势做出展望。

关键词 安全互操作,多域,RBAC,访问控制

Research Development on Secure Interoperation in Multi-domain Environment

JIN Li LU Zheng-ding ZHAO Feng
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Secure interoperations in Multi-domain can share resources and communicate information in multi distributed, heterogeneous, and autonomy domains, which depends on authentication, access control, and audit mechanisms. A comprehensive survey of research on this novel approach was presented to solve the conflicts of secure policies of domains, and some basic techniques, e. g. role-mapping technique between domains, trust management, Public Key Infrastructure and temporal role based access control, were introduced and compared. Mainly discussed model and architecture of policy-integration in multi-domain. Finally, the trend of research was discussed, which is based on the shortcomings and problems of current research.

Keywords Secure interoperation, Multi-domain, RBAC, Access control

1 引言

Internet和分布式技术飞速发展正在引发信息安全领域的一场大的变革,匿名、动态、分布的新型安全模型对已知、静态、集中的传统安全模型提出挑战。越来越多相对稳定、集中管理的小型局域网分布式系统接入广域网或Internet,形成互连互通的大规模或超大规模分布式系统,随之而来所引发的大规模用户认证和敏感资源共享等安全问题层出不穷。近年来,将大规模分布式系统划分为多个高度自治的管理域或安全域(简称多域系统),从而通过多域间的安全互操作实现对全局信息资源的安全管理和控制已成为分布式访问控制领域的热点问题。

多域间的互操作为分布式环境下资源和服务的最大共享创造了条件,从而大大提高了分布式系统的性能和资源利用率。例如,在P2P网络中,节点间通过交互操作来实现资源共享;在分布式数据库中,用户间通过互操作来实现对多域数据库的访问。目前,跨域互操作技术在政府、军队、金融和医疗等许多重要领域都已得到广泛的应用。

然而,由于跨域互操作在共享本域资源和访问外域资源同时,打开了系统内各个域的诸多安全禁区的大门,因此多域环境下所面临的匿名访问、权限隐蔽提升和指派传递失控等安全问题不容忽视。大量研究表明,未授权的访问请求,特别是来自内部人员的非法访问请求,已经成为分布式环境下的一个主要的安全威胁。由于多域系统必须通过满足各个协同域的应用需求来实现协同工作,因此来自系统内部的安全威胁在多域环境下显得尤为突出。传统集中式管理的安全模型无法适应多域环境下的分布式管理模式,唯一的解决办法就是扩展现有的安全模型或建立新的安全模型来实现多域环境下的安全管理和协同操作,即允许在分属不同安全域的个体和系统之间进行大量的信息交换和数据共享等互操作。

2 多域安全互操作研究的问题

多域安全互操作为多个分布、异构、交互的自治域组成的协同工作环境提供了实现各域间数据和资源的安全交互和共享的有效途径。

2.1 基本概念

定义1(安全域)[1-6] 安全域就是一个有边界的、由受保护的客体和用户群组成,由一位安全管理员来管理和维护一

到稿日期:2008-03-20 本文受国家自然科学基金项目(60403027,60773191),国家高技术研究发展计划(863计划)项目(2007AA01Z403),中国博士后科学基金(20070410282)资助。

金 莉(1978-),女,博士生,主要研究方向为信息安全、分布式计算等,E-mail:jessiewelcome@126.com;卢正鼎(1944-),男,教授,博士生导师,主要研究方向为信息安全、并行分布式处理;赵 峰(1976-),男,博士,博士后,主要研究方向为网络安全、数据挖掘等。

组安全策略的区域，如图 1 所示。每个域都可以使用不同的安全模型、语法、分类模式和约束来表达自己的信息安全策略，即允许合法请求、阻止非法访问。安全域又被称作协同域或自治域。

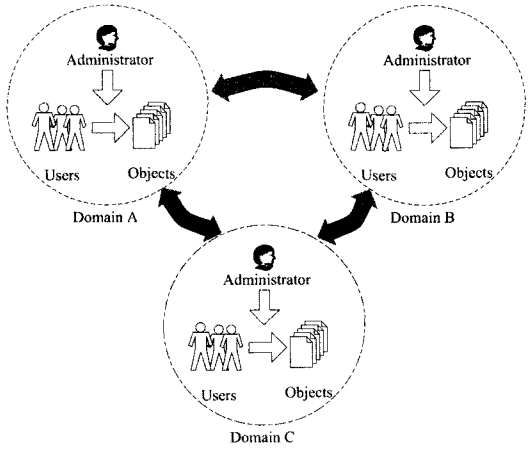

图 1　多域间的安全互操作

定义 2(多域)[7,8]　多域是由多个互为契约关系的安全域组成的。当一个域需要允许以前并不相识的用户或实体访问自己的资源，则必须设置相应的安全机制来确保未知的访问被控制在预先定义的已知共享策略范畴之内。当这样的跨域访问在多个域间被允许，并且各系统仍然沿用自身原有的安全策略时，那么这些域被看作是组成了一个多域环境。

定义 3(多域安全互操作策略)[9,10]　多域安全互操作策略是各域为实现协同工作，集成所有域的本地策略以构成全局策略来控制信息和资源在多个域间的共享。因此，它是一种集成化的高级访问控制策略。

P. Bonatti 等人[11]提出了一种用代数表达式来表示和集成访问控制策略的方法。在该方法中，假设 S，O 和 A 分别表示主体集合、客体集合和主体对客体操作的集合，那么一条授权术语可以表示为(s，o，a)的三元组，一条访问控制策略可以由一组授权术语集合来表示。这种代数表示方法将访问控制的语义转化为形式化的一阶代数，与单一的策略描述语言相比具有支持异构策略(Heterogeneous policy support)、支持未知策略(Support of unknown policies)和可控干预(controlled interference)等优势，在多级安全或 BLP 模型等静态约束的访问控制系统中广泛使用，然而在基于动态约束的访问控制系统下，特别是在表示多域环境下的互操作时，无法表达分布、异构环境下权限的指派和传递。

定义 4(基于角色的访问控制)[12-15]　基于角色的访问控制 RBAC(role-based access control)已成为近年来访问控制领域的主流研究方向，具有代表性的是 Sandhu 等人提出的 RBAC96 及其补充模型、ARBAC97、ARBAC02 和 CL03 等。NIST(National Institute of Standards and Technology)于 2001 年制定了 RBAC 标准，根据标准中的定义，角色表示了用户和权限之间多对多的关系，用来指明用户的职权和责任，这样的访问控制权限不再直接授予用户而是授予角色，用户通过获得角色来取得相应的权限。

在实际系统中，用户的权限会经常变化，而角色和权限之间的映射则相对稳定，所以将权限授予角色，然后再将角色分配给用户，可以大大简化安全管理工作的复杂性。因此，RBAC 模型所表现出的这种灵活性，更适应于多域环境下的动态需求，能够满足域间互操作的安全性、自治性和机密性的需求。目前，多域环境下访问控制策略的研究大都是以基于角色的访问控制模型为基础开展的[16-18]。

2.2　构造跨域互操作策略

构造跨域互操作策略必须基于跨域角色的权限集合和各协同域的安全需求和自治需求，假设将基于角色的访问控制中的客体划分成一个概念类，例如，账目表单、保险需求、审计报告等，那么同属一个概念类的两个受到跨域访问的客体可以被视作语义相同。基于上述假设，对于两个来自不同域 A 和 B 的客体 O_A，O_B，角色 r_A 和 r_B 对于某权限 a 可能存在以下四种关系[10]：

1. 包含关系：角色 r 的权限集合 $Pset(r)$包括所有直接或间接指派给角色 r 的权限，如果下列条件满足，则 r_A 包含 r_B：

a. 角色 r_A 的权限集合 $Pset(r_A)$包含角色 r_B 的权限集合 $Pset(r_B)$。

$$\forall j \exists i:(O_{B_j},a)\in Pset(r_B)\Rightarrow[(O_{A_i},a)\in Pset(r_A)\wedge(class(O_{A_i})=class(O_{B_j}))] \tag{1}$$

b. 角色 r_B 的权限集合 $Pset(r_B)$与域 A 共享。

$$\forall j:(O_{B_j},a)\in Pset(r_B)\Rightarrow shareable(O,a,A) \tag{2}$$

2. 相等关系：如果 r_A 包含 r_B 且 r_B 包含 r_A，那么 r_A 与 r_B 相等。

3. 相交关系：如果 $Pset(r_A)$和 $Pset(r_B)$有相同的共享权限，且 r_A 不包含 r_B，r_B 不包含 r_A 那么 r_A 与 r_B 相交。

$$\left\{\begin{array}{l}\exists i,j:class(O_{A_i})=class(O_{B_j})\wedge[(O_{A_i},a)\in Pset(r_A)\wedge\\ \quad (O_{B_j},a)\in Pset(r_B)\wedge shareable(O_{A_i},a,B)\wedge\\ \quad shareable(O_{B_j},a,A)\end{array}\right\} \tag{3}$$

$$\wedge(\neg(r_A\ contains\ r_B)\wedge\neg(r_B\ contains\ r_A)$$

4. 无关：如果角色 r_A 和 r_B 不共享任何权限，那么 r_A 与 r_B 无关。

$$\neg\exists i,j:class(O_{A_i})=class(O_{B_j})\wedge\lfloor(O_{A_i},a)\in Pset(r_A)\wedge(O_{B_j},a)\in Pset(r_B)\rfloor \tag{4}$$

因此在 n 个协同域组成多域环境中，可以借助上述 4 类角色关联规则，通过两两相关的迭代方法为不同域的角色建立关联，进行角色传递和权限继承，从而实现跨域安全互操作。在第一次迭代时，用域 1 和域 2 的最高级角色来合成域 1 和域 2 的 RBAC 策略；在随后的迭代中，一条新的 RBAC 策略由前面迭代中产生的合成 RBAC 策略生成；在经过 $n-1$ 次迭代后，n 个域的 RBAC 策略将集成为一条全局性的多域互操作策略。此外，在每次迭代中新产生的冗余角色将从集成 RBAC 策略中删除。

2.3　安全目标

多域安全互操作研究的最终目标就是要在保护各成员域信息系统安全的前提下最大限度地实现域间的资源共享。基于这个最终目标，多域环境下的安全互操作应具备以下特性[19,20]：

- 机密性(Confidentiality)　保证信息不会由于本域或外域的非法授权而泄漏。
- 完整性(Integrity)　保证信息不会由于本域或外域的非法授权而更改。
- 合法性(Validity)　保证信息只能被合法用户获得。

• 责任性(Non-repudiation)　每个行为都可以被追溯到实施行为的唯一用户。

为了实现安全的互操作,由全局策略支持的跨域访问控制策略必须与域内的访问控制策略保持一致性,尤其需要对以下两条策略予以加强[21]:

• 自治策略　如果一个访问在单个域内允许,那么它必须在多域安全互操作下被允许;

• 安全策略　如果一个访问在单个域内不允许,那么它在多域间安全互操作下也不能允许。

此外,认证机制、访问控制和审计机制是实现以上安全目标的关键性服务。认证机制为每个用户建立一个身份,这是访问控制的首要条件;访问控制完成认证管理,约束合法用户在系统中的行为和操作;审计机制搜集关于系统行为的数据,检测可能存在的安全隐患。

3　多域安全互操作发展历程和现状分析

多域安全互操作研究是对分布式系统访问控制研究的延伸和发展。20 世纪 80 年代初,分布式系统大量涌现。当时的分布式系统主要分为两类:一类是由松散连接、自治管理的计算机系统组成,通常是通过广域网建立连接,如 APPANET 和 JANET[22];另一类是由紧密连接、集中管理的计算机系统组成,是基于高速局域网的使用,如 Amoeba[23] 和 Cambrige Distributed System[24]。前者的访问需求主要限于虚拟终端的访问、文件传输和电子邮件,用户必须能够准确地验证自己的身份才能获得系统资源;相比前者而言,后者的访问需求主要基于高效的通讯处理机制,而不是文件传输。

到了 20 世纪 80 年代末,基于高速局域网的小型分布式系统开始作为大规模分布式系统的一部分接入到广域网的分布式系统中,这样的分布式系统中既有广域网又有局域网,因此需要一个更加灵活的管理机制来处理和解决这种大规模分布式系统中的复杂管理问题。1988 年,Robison 等人提出了基于域的分布式访问控制模型[25],当时"域"的概念与现在的概念有较大区别,仅仅涉及对部分访问权限和信息资源的划分和管理。到 20 世纪 90 年代,分布式系统的发展有了较大的飞跃,Thomas 等人提出了一种增强分布式授权表达力的逻辑思路[26],Marvin 等人提出了分布委托技术,即用户可以通过一个不可信的第三方访问其所需要的服务[27],这些授权和分布委托理论都为后来的多域环境下的访问控制技术奠定了理论基础。

3.1　基础结构和安全模型

近年来,随着大规模分布、异构环境下的访问控制问题被细分成多个相对集中局域环境下的互操作问题,"域"的概念在分布式安全系统中得到广泛应用,多域安全互操作已经成为信息安全领域的一个重要研究方向。目前,多域安全互操作的研究正处于一个较好的发展势头之上,国内外的诸多研究成果主要集中于多域间角色转换、信任管理、基于 PKI 和基于时限约束等方面。本文较为全面地阐述了多域安全互操作的研究内容及相关工作,并对部分研究成果和关键技术进行分析比较,提出了该领域未来的发展趋势,使得读者能够全面、准确地了解这一领域的研究进展。

3.1.1　基于跨域角色映射机制

Eric Freudenthal 等人[28]提出了一种基于动态结盟环境(Dynamic Coalition Environment)下的多域访问控制模型 dRBAC(Distributed Role-based Access Control)。"结盟环境"指军事上几个国家或者商业上的几个公司联合工作从而实现一个共同的目标。在 dRBAC 中没有公共可信的授权中心,各个域间彼此仅存在有限的信任,每个域保持对其局部资源的完全自治性并且可以自主地加入或退出结盟。dRBAC 通过定义指派(Credentials)、指派链(Credential Chains)、支持链(Support Chains)、证据(Proofs)、子证据(Sub-Proofs)和证据监控(Proof Monitor)等一系列概念来完成多个域间角色的转换。如图 2 所示,根据支持链(Supporting Chain)对主链(Primary Chain)的证明,可以推导出"主体 A 可以获得主体 B 所拥有的角色 role2"这一结论。

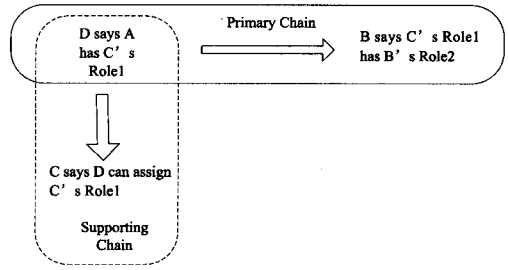

图 2　dRBAC 证据 $A \Rightarrow B.role2$

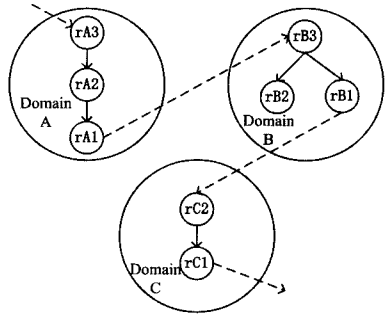

图 3　跨域访问路径的例子

如果说 dRBAC 是一种狭义和微观的跨域角色映射模型,那么 Mohamed Shehab 等人[29]提出的协同域间安全角色映射(SERAT;Secure Role mApping Technique)的分布式协议则是一种广义和宏观的跨域角色模型。SERAT 是将"域"和"角色"抽象成"有限圆"和"点"的形式,引入了访问路径和访问路径约束的概念,通过路径连接规则来实现安全路径的评估和更新。在不改变域内原有的访问路径的前提下,对域间路径的安全性进行研究,它通过数字签名来保持用户访问路径在域间传递时的正确性;通过访问路径发现算法使得用户能够在多域环境下查询可能存在的访问路径。SERAT 将域的访问控制策略表示成有向图的形式,其中节点表示角色,有向边表示角色间的层次关系。为了强调跨域路径,SERAT 特别将位于域边界的角色定义为 $r_{status}^{domain\_name}$ 的形式,其中 $status \in \{(E)ntry, e(X)it\}$,分别表示"进入"和"离开"状态,用户的访问路径可以描述为 $P=\{\cdots, r_{E_1}^{A}, r_{X_1}^{A}, r_{E_1}^{B}, r_{X_1}^{B}, \cdots\}$。如图 3 所示,从域 A 角色 $rA3$ 到域 C 角色 $rC1$ 的访问路径 P 可以表示为 $P=\{\cdots, rA_3, rA_2, rA_1, rB_3, rB_1, rC_2, rC_1, \cdots\}$,其中以 rA_3 和 rA_1 为例,分别代表 r_E^A 和 r_X^A。当域 A 的用户希望获得域 B 或域 C 的角色时,用户将访问请求提交给域 A 的管理员,域 A 的管理员为用户更新访问路径,并进行数字签名,

最后将签名后的路径添加到访问请求中发往域B或域C。域B或域C的管理员在收到访问请求后，提取出用户的访问路径，确认签名认证，对用户请求作出评估，最后决定是否授予用户所需的角色。

3.1.2 基于信任管理

1996年，AT&T实验室的Blaze等人提出了信任管理(TM；Trust Management)的概念，为解决分布式环境中的安全问题提供了新的思路[30]。2001年，Li Ninghui等人提出了基于角色的信任管理(RT；Role-based Trust-management)的初始版本RT0，后来将其扩充为一个框架体系RT[31,32]，它继续沿袭了RBAC和基于逻辑程序的方法，并认为要简化结盟环境下的授权管理，需要采用基于属性的访问控制(ABAC；Attribute Based Access Control)，RT与RBAC进行了紧密的集成，支持角色层次、SOD、基于角色的委托、角色的选择性激活等。

近来，基于信任管理的多域访问控制研究已经成为多域环境下安全访问控制的主流方向。由于信任管理允许资源的控制者以一种受控的方式将相应的权限委托给其它组织中的用户，因此信任管理为多域环境下的开放、分布和动态的系统特征提供了一个合理的安全决策框架[33]。

自动信任协商(ATN；Automated Trust Negotiation)是Winsborough等人[34]为解决跨域的信任建立而提出的一个新方法。TrustBuilder[35]项目是基于ATN的著名安全科研项目，由BYU大学的Seamons和UIUC大学的Winslett等人共同完成。Hannover大学的PeerTrust项目[36]是基于P2P环境下开展的信任协商的研究工作。概括地讲，基于ATN的工作原理和应用需求的研究主要涵盖四个方面[37]：体系结构及基础模型、访问控制策略及信任证、协商策略和协商协议。

目前，国内关于多域访问控制的研究也主要集中于信任管理方面，许多研究机构和人员也对基于信任管理的多域访问控制进行了卓有成效的研究和探讨。文献[38]将主要目标放在了解决分布式群组通信的访问控制问题上，提出了一个多域群组协作中基于角色的信任管理的访问控制模式，扩充RT语言以适应群组通信的需求，重点解决了动态联合授权以及基于属性的委托授权，并建立了一个包括安全策略的协商、信任证的颁发、信任证与安全策略的一致性验证及用户访问权限论证等较完整的体系。南京大学的王远等[39]针对信任管理中信任关系的二元值描述、安全凭证表达能力有限和安全信息搜集与处理不足等问题，设计并实现了一个适于开放环境的基于信任管理的分布式访问控制系统DACBTM。中国科技大学的陈颖等[40]将域的概念置于网格环境下，把节点划分成多个域，针对域内和域间的不同特点，分别采用全局信任模型和局部新任模型，基于中心服务器AAC(Authentication and Authorization Center)，融入信任管理的概念，提出了一个基于动态角色的访问控制架构。华中科技大学的朱贤等人[41]在多篇文献中对基于信任管理的多域访问控制进行了全面的探讨和研究，朱贤还在其博士学位毕业论文中从委托深度控制机制、证书链发现问题等角度对基于信任管理的多域访问控制进行了阐述，并提出了一个多域环境下的RBAC模型EMRBAC，但是其主要研究方向还是偏重于从微观的角度对主体间权限委托和证书搜索等安全问题的细化和分析，对整体多域系统的宏观安全把握相对较少。

3.1.3 基于PKI的跨域访问控制

Grit等人[42]提出了一种基于PKI的跨域访问控制管理方法。这种方法是在RBAC的基础上，融入PKI技术来实现对跨域访问的认证。Grit等人认为在大规模跨域环境下应用PKI实现访问控制，一个主要挑战就是可能会产生多个CA(Certification Authority)中心，即各域都有各自的CA中心。因此，他们假设每个组织域都有自己的CA中心，不同的组织之间通过跨域证书(cross-certificate)互相认证。跨域证书中包括组织的名称、可信状态和被另一个组织签名认证的CA公钥信息。由于一个服务组织可能对应许多不同的客户组织，一个客户组织也可能对应许多不同的服务组织，为了便于管理，Grit等人将域分为两类：服务域和客户域。客户域负责向用户(客户)发布证书，授予公钥和角色。服务域则包括一个或多个Web服务器，可以被其它域的用户访问。同一个域可以既是客户域又是服务域。最后，在阐述PKI访问控制模型的基础上，构造了一个跨域访问控制的原型系统XDA，它充分利用了PKI概念和标准，通过跨域证书来支持客户域间的联系，通过用户-角色证书来识别用户，通过角色层次证书来定义角色层次。

3.1.4 基于时限的访问控制

随着电子商务的产生，系统间进行具有时间限制的限时资源共享已成为一种普遍现象。在这有限的合作周期内，合作伙伴之间需要一种更加灵活有效的机制来支持这种限时共享策略，而且不能破坏各系统原有的安全策略。对此，Smithi等人[43]提出基于一般时限角色的访问控制机制(GTRBAC；Generalized Temporal Role Based Access Control)来解决这个问题，它通过使用适当的限时跨域访问策略来扩展或重构本地的GTRBAC策略，实现外域对本地资源的访问，改进的本地GTRBAC策略在保持本地需求的同时促进了域间的访问。GTRBAC模型集成了一组语言结构来定义角色上不同的时间和周期的约束，包括角色有效(role enabling/disabling)、角色激活(role activation)、用户-角色指派(user- role assignment)、角色指派许可(role-permission assignment)等。GTRBAC还特别对角色有效和角色激活两个概念做出明确的区分。角色有效是指用户能够获得角色的权限，只有当用户在会话中获得角色具有的权限时才能称一个有效角色被激活。相反，无效的角色不能被任何用户激活。

3.2 安全模型的分析与比较

角色映射、自动信任协商等安全模型是当前多域安全互操作领域中几个具有代表性的模型，表1是各安全模型对于多域安全互操作需求满足情况的对比，表中Y表示支持，P表示部分支持，N表示不支持。

表1 安全模型性能比较

Security Requirements	Role Mapping		ATN		PKI Based	GTRBAC
	dRBAC	SERAT	TrustBuilder	PeerTrus		
Confidentiality	P	P	Y	Y	Y	Y
Integrity	Y	N	Y	P	P	P
Validity	P	P	P	P	P	P
Non-repudiation	Y	Y	N	N	N	Y

3.3 策略集成

构造一条控制着异构系统互操作的多域策略是一项具有

挑战性的工作，它可能导致不同类型冲突。这些冲突的产生是由于不同的域使用了不同的模型、语法、计划模式、数据标记模式和约束来表达各自的访问控制策略[44,45]。在这样一种异构环境中，建立一个统一的策略表达方式显得十分必要。

Bo Lang 等人[46]提出了一个基于元策略概念的灵活访问控制机制来支持大规模分布式协同环境。元策略是一个通用访问控制策略的结构，三种经典的访问控制模型 DAC，MAC 和 RBAC 都可以分别用元策略表示出来。基于元策略模型，Bo Lang 等人构造了一个面向客体的元策略架构，如图 4 所示。这个架构可以描述当前所有的访问控制策略，并且可以在架构中添加或删除策略，从而实现大规模分布式协同环境下的策略集成。

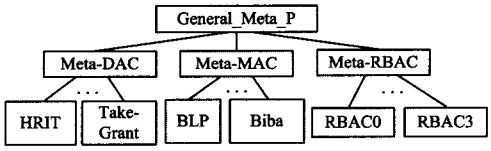

图 4　元策略体系

与文献[46]的策略集成方式不同，文献[47]在进行策略集成时直接引入“域”的概念，将分布式系统逻辑划分为“全局域”和“本地域”，提出了一个基于不同域管理的分布式协同控制系统 ERBAC。ERBAC 模型由下列 5 种实体组成：主体、证书、认证过程、客体和信任域。这里信任域的概念与上文中提到的安全域、自治域的概念相同，都是指一个由单个管理员和安全策略控制的主体和客体的集合。为了实现全局 RBAC 策略，ERBAC 提出了详细的策略集成规则：

- 多域协同环境由多个安全域组成；
- 在单个安全域中认可的操作只能适用于本地安全策略；
- 全局和本域的主体可以共存。对于每个安全域，都存在从全局主体到本域主体的部分映射；
- 在不同安全域间的实体操作需要相互的认证；
- 一个经过认证的全局主体到本域主体的映射等同于那个本域主体在本域的认证；
- 所有访问控制决策由本域主体本地化决定；
- 代表用户进行的程序或进程可以被用户权限的子集指派；
- 在不同域中代表相同主体运行的进程可以共享同一组证书；
- 职责分离约束。

近来，Ajith Kamath 等人[48]提出了一种基于用户证书的多域策略集成方法，它是基于 X-RBAC 语言[9]的。X-RBAC 语言是一种基于 XML、主要描述用户、角色、权限和三者间的关联的 RBAC 语言。用户证书是一组属性值对（Attribute-Value pairs），需要被用户满足来获得相应的权限。例如，与“医生”角色相关的 AV 对集合可能包括（qualification＝Doctor）AND（（level＝4）OR（age＞35））。用户证书可以产生一个由属性、值和操作符组成的同义集合，语义的一致性在多组这样的同义集合中保持。基于这个概念，Ajith Kamath 等人还定义出了 4 种不同类型的跨域角色关联：相等、包含、相交和无关。然而，Ajith Kamath 注意到这种策略集成方法仍然会在构造全局规则时引起冲突，这些冲突是由于角色间的层次结构和 DoS 所引起的。因此，在映射用户证书时添加了适当的用户介入。

3.4　优化策略和评估标准

多域安全互操作的一项重要前提是必须尽可能保持所有协同域的自治性，即在高度集成的同时保持各域自治性的最大化，因此在集成性和自治性之间存在着一种动态的平衡。尽管在大多数集成环境中是不允许违背任一协同域的安全策略的，然而各个协同域有时也会自愿地牺牲一定的自治性来建立更强大的多域互操作策略，当然这种自治性的损耗必须保持在一个可以接受的范围之内。Basit Shafiq 等人[10]给出了计算这种“损耗”的方法：

假设 L_A 表示所有影响域 A 自治性的跨域映射的集合，那么对于域 A 而言，由 L_A 所引起的自治性损耗 $AL(L_A)$ 可以表示如下：

$$AL(L_A)=\frac{\left(\begin{matrix}Total\ number\ of\ local\ accesses\ without\\ any\ cross\text{-}domain\ role\ mapping\ link\end{matrix}\right)-\left(\begin{matrix}Total\ number\ of\ local\ accesses\ in\\ presence\ of\ all\ role\text{-}mapping\ links\ in\ L_A\end{matrix}\right)}{\left(\begin{matrix}Total\ number\ of\ local\ accesses\ without\\ any\ cross\text{-}domain\ role\ mapping\ link\end{matrix}\right)} \tag{5}$$

以上表达式也可以用于计算域的整体自治性损耗，并且仅由跨域映射产生的损耗可能会大于域中所有映射产生的损耗，即 $AL(L_A)\leqslant\sum_{l\in L_A}AL(\{l\})$。这个矛盾的产生是因为大量跨域角色映射产生可能会降低许多共性本地访问数量。假设为域 A 中每一个跨域角色映射 l_i 定义一个集合 S_i（$S_i\subseteq L_A$），域 A 中所有受到 l_i 影响的本地访问也将受到跨域映射 $l_k in S_i$ 的影响，那么使得域 A 的自治性损耗保持在临界值 α 以内的表达式，可以表示成如下形式：

$$\sum_{l_i\in L_A}\left(\prod_{l_k\in S_i}(1-u_{rk})\right)AL(\{l_i\})u_{ri}+\sum_{(l_p,l_q\in L_A)\wedge ind\_sod(l_p,l_q)}AL(\{l_p,l_q\})u_{rp}u_{rq}\leqslant\alpha \tag{6}$$

其中，u_{ri}，u_{rk}，u_{rp}，u_{rq} 分别表示用户 u 是否获得角色 r_i，r_k，r_p，r_q，当用户 u 获得相应角色时其值为 1。

4　多域安全互操作系统及其应用

由于网格与移动网络的大规模分布性和实时动态性，其安全访问控制机制往往采用了多域安全互操作的管理机制。

Linda A. 等人[49]以解决大型网格项目 European DataGrid（EDG）[50]中认证和授权的安全问题为应用背景定义了 113 条安全需求，将大规模网格环境看作是由分布在多个不同安全域上的多个大型虚拟组织（Virtual Organization）组成，网格中的访问控制策略则根据用户是否具备虚拟组织的成员资格而定。虚拟组织成员服务（VOMS；Virtual Organization Membership Service）是虚拟组织成员的核心数据库，它支持多个虚拟组织的成员资格，因此一个 VOMS 代理证书可以包含多个虚拟组织的信息。EDG 中已经实现的安全策略如下：

- 认证和指派　通过 GSI/PKI/X509、CA 中心等实现；
- 全局授权　通过虚拟组织成员服务实现；
- 本地授权　通过被禁用户、本地策略和 Java 安全机制实现；
- 网络安全　通过防火墙、访问控制列表和网格协议使

用的端口实现；

·计费机制　通过使用服务器/客户端 GSI 认证消息的计费模型实现；

·机密性　通过严格访问控制、加密算法保护机密信息；

·数据完整性　通过数据传输的可信层安全机制实现。

Distributed Coalitions Infrastructure(DisCo)[51]基于 Java SDK 1.3 开发而成，主要利用的是 Java 支持的远程进程调用(java.rmi 类)，主要适用于动态结盟环境，即具有不对等且动态变化的信任关系的多个网络主机分布在多个安全域上，提供了与认证和访问控制、安全通信、代码释放、进程权限管理等应用无关的特性支持，因此 DisCo 将应用开发者从管理这些特性中解脱出来，为多域环境下的分布式应用提供了一种简洁、统一的接口。此外，DisCo 还可以持续监控建立的连接、保持正确的应用操作从而应对不断变化的信任关系。

5　多域安全互操作发展趋势的展望

近年来，多域安全领域的研究已取得较大的成果，特别是基于信任管理的自动信任协商机制的提出[52,53]，掀起了该领域的一个研究高潮，但是仍然存在以下几个值得关注的研究方向：

(1)基于真正意义的多域(至少三个域)安全互操作研究初现端倪，但对安全约束和冲突解决的研究还有待深入。Eric Freudenthal 等人所提出的动态结盟环境下的访问控制模型 dRBAC 考虑到了多域分布协同工作的情况，采取了“指派钱包”和“发现标记”的方法来追踪跨域指派的有效性。Mohamed Shehab 等人则直言不讳地将研究重点置于三个域的应用环境之下，引入访问路径和访问路径约束的概念，提出了分布式 SERAT 协议来解决跨域角色的映射和传递问题，并卓有成效地解决了角色传递中产生的角色层次冲突问题。然而，dRBAC 对“域”的概念过于淡化，几乎尚未考虑域自治性对互操作安全性的影响；SERAT 则只考虑了角色层次冲突，而恰恰忽略了对多域互操作影响较大的 SoD 冲突问题。因此，多域互操作对于真正意义的“安全”而言才刚起步，对多域策略中安全约束和冲突解决的研究纵然复杂，但值得深入。

(2)基于信任管理多域互操作研究普遍存在第三方信任失效、伪造信任证等共性的安全弊端。首先，由于信任管理的基本思想就是借助可信第三方来定义映射关系，那么对于第三方的依赖使得第三方的可信度对于系统而言至关重要。对第三方可信与否的判定失效对于整个系统安全的打击是致命的；其次，信任管理基于信任证来表示信任关系，信任证所反映实体的可信度必须具有较高的真实性和客观性。文献[39]和文献[40]在构造信任管理模型时都分别考虑到了实体的历史经验、实体间的相对信任度和反馈评价意见的可信度，在一定程度上降低了实体伪造信任证的机率，但是对历史经验、相对信任度和反馈评价意见可信度这一整套系统化的度量方法以及三者间潜在的关联还尚未见形式化的表述。因此，对于多域环境下的信任管理研究可以参考 PeerTrust 中对节点可信度评估方法来实现对实体可信度的评估。

(3)多域策略集成时对集成算法复杂度的考虑和优化。在构造多域环境下的互操作集成策略时，通常使用两两集成的办法，最终实现所有域策略的集成，因此构造的全局策略可能会比较复杂。Bo Lang 等人虽然提出元策略的架构来添加、删除策略，从而实现大规模分布式协同环境下的策略集成，但是元策略本身就是集成了三类访问控制模型的集合体，已经具有较高的复杂度，那么如果继续添加新的策略将直接导致集成策略复杂度的攀升，因此在策略集成过程中必须考虑到对算法复杂度的降低和优化。

结束语　多域环境下的安全互操作问题是近年来分布式环境下安全问题研究的一个新的发展方向。在多个高度自治的安全域间，如何以最小的安全风险为代价来实现最大化的资源共享是多域环境下安全互操作需要解决的首要问题。RBAC 模型是具有较强表达能力和较大灵活性的经典访问控制模型，为多域环境下访问控制策略的集成提供了强大的技术支持，未来多域安全互操作中策略集成方面的研究方向可以继续深入扩展 RBAC 的层次结构和诸如 DoS 等各种约束条件来拓展新的研究领域。

参 考 文 献

[1] V-Gomez J. Multidomain Security. Computer & Security, 1994, 13:161-184

[2] Bonatti P, Vimercati S D C, Samarati P. An Algebra for Composing Access Control Policies. ACM Transactions on Information and System Security, 2002, 5(1)

[3] Dawson S, Qian S, Samarati P. Providing Security and Interoperation of Heterogeneous Systems, Distributed and Parallel Databases, August 2000, 8:119-145

[4] Qian X, Lunt T F. A MAC Policy Framework for Multilevel Relational Databases. IEEE Transactions on Knowledge and Data Engineering, 1996, 8(1):3-15

[5] Osborn S L, Sandhu R, Munawer Q. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. ACM Transactions on Information and System Security, 2000, 3(2):85-106

[6] Gong L, Qian X. Computational Issues in Secure Interoperation. IEEE Transaction on Software and Engineering, 1996, 22(1):43-52

[7] Szigeti J, Ballok I, Cinkler T. Efficiency of Information Update Strategies for Automatically Switched Multi-Domain Optical Networks // IEEE ICTON 2005, 7th International Conference on Transparent Optical Networks. Barcelona, Spain, July 2005

[8] Mesko D, Viola G, Cinkler T. A Hierarchical and a Non-Hierarchical European Multi-Domain Reference network: Routing and Protection // Networks2006. NewDelhi, India, Nov. 2006

[9] Joshi J B D, Bhatti R, Bertino E, et al. An Access Control Language for Multidomain Environments. IEEE Internet Computing, 2004

[10] Shafiq B, Joshi J B D, Bertino E. Secure Interoperation in a Multi-Domain Environment Employing RBAC Policies. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(11):1557-1577

[11] Bonatti P, Vimercati S D C, Samarati P. An Algebra for Composing Access Control Policies. ACM Transaction. Information and System Security, 2002, 5(1)

[12] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based access control models. IEEE Computer, 1996, 29(2):38-47

[13] Sandhu R S, Bhamidipati V, Munawer Q. The ARBAC97 model for role-based administrator of roles. ACM Trans. on Informa-

tion and System Security (TISSEC), 1999, 2(1): 105-135

[14] Oh S, Sandhu R. A model for role administrator using organization structure// Proc. of the 6th ACM Symp. on Access Control Models and Technologies (SACMAT 2002). Monterey: ACM Press, 2002: 155-162

[15] Crampton J, Loizou G. Administrative scope: A foundation for role-based administrative models. ACM Trans. on Information and System Security(TISSEC), 2003, 6(2): 201-231

[16] Cohen E, Thhmas R K, Winsborough W, et al. Models for coalition-based access control (CBAC)[A]// Proc. 7th ACM Symposium on Access Control Models and Technologies (SACMAT 2002)[C]. 2002: 97-106

[17] Shands D, Yee R, Jacobs J, et al. Secure virtual enclaves: supporting coalition use of distributed system[A]// Proceedings of Network and Distributed System Security Symposium (NDSS 2000)[C]. 2000

[18] Bonatti P, di Vimercati S D C, Samarati P. AnAlgebra for Composing Access Control Policies. ACM Transactions on Information and System Security (TISSEC), 2002, 5(1): 1-35

[19] Joshi J B D, Ghafoor A, Aref W, et al. Digital Government Security Infrastructure Design Challenges. IEEE Computer, 2001, 34 (2): 66-72

[20] Landwehr X E. Computer Security. International Journal of Information Security, 2001, 1(1): 3-13

[21] Gong L, Qian X. Computational Issues in Secure Interoperation. IEEE Trans. Software Eng., 1996, 22(2)

[22] Quarterman J S, Hoskin J C. Notable computer networks, Communications of ACM, 1986, 29(l0): 932-971

[23] Mullender S J, Tanenbaum A S. The design of a capability based distributed operating system. Computer Journal, 1986, 29, (4): 289-299

[24] Needham R, Herbert A. The Cambridge distributed computer system. Addison-Wesley, 1982

[25] Robinson D C, Sloman M S. Domain-based access control for distributed computing system. Software Engineering Journal, 1988, 3(5): 161-170

[26] Woo Y C, Lam S S. Authorization in distributed systems: A formal approach// Proc. 13th IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, CA, 1992

[27] Theimer M M, Nichols D A, Terry D B. Delegation through Access Control Programs// Proc. 12th International Conference on Distributed Systems. IEEE Press, 1992

[28] Freudenthal E, Pesin T, Port L. dRBAC: Distributed role-based access control for dynamic coalition environments// Proc. 22nd International Conference on Distributed Computing Systems (ICDCS'02). Vienna: IEEE, 2002: 294-306

[29] Mohamed S, Elisa B, Arif G. SERAT: Secure Role Mapping Technique for Decentralized Secure Interoperability// Proc. 10th ACM Symposium on Access Control Models and Technologies. ACM Press, Stockholm, Sweden, 2005: 159-167

[30] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management // Proc. of the 1996 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 1996: 164-173

[31] Li N H, Mitchell J C, Winsborough W H. Design of a role-based trust management framework// Proc. of the 2002 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 2002: 114-130

[32] Li N H, Winsborough W H, Mitchell J C. Distributed credential chain discovery in trust management// Proc. of the 8th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2001: 156-165

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

[34] Winsborough W H, Seamons K E, Jones V E. Automated trust negotiation// DARPA Information Survivability Conf. and Exposition. New York: IEEE Press, 2000: 88-102

[35] Smith B, Seamons KE, Jones MD. Responding to policies at runtime in TrustBuilder// Proc. of the 5th Int'l Workshop on Policies for Distributed Systems and Networks. Washington: IEEE Computer Society Press, 2004: 149-158

[36] Nejdl W, Olmedilla D, Winslett M. PeerTrust: Automated trust negotiation for peers on the semantic Web// Proc. of the Workshop on Secure Data Management in a Connected World (SDM 2004). LNCS 3178. Springer-Verlag, 2004: 118-132

[37] 李建欣, 怀进鹏, 李先贤. 自动信任协商研究. 软件学报, 2006 (1): 124-133

[38] 张煜, 张文焱, 李先贤, 等. 多自治域协同环境中群组通信的安全访问控制. 计算机研究与发展, 2005, 49(2): 1558-1563

[39] 王远, 徐锋, 曹春, 等. 一个基于信任管理的分布式访问控制系统的设计与实现. 计算机科学, 2005, 32(8): 226-229

[40] 陈颖, 杨寿保, 郭磊涛, 等. 网格环境下的一种动态跨域访问控制策略. 计算机研究与发展, 2006, 43(11): 1863-1869

[41] 朱贤. 多域环境下基于信任管理的访问控制研究. PhD. Thesis. 2006

[42] Denker G, Millen J, Miyake Y. Cross-domain access control via PKI// Proceeding of the 3rd International Workshop on Policies for Distributed Systems and Networks (POLICY. 02)[C]. IEEE Press, 2002

[43] Piromruen S, Joshi J B D. An RBAC Framework for Time Constrained Secure. Interoperation in Multi-domain Environment// IEEE Workshop on Object-oriented Real-time. Databases (WORDS-2005). 2005: 36-45

[44] Dawson S, Qian S, Samarati P. Providing Security and Interoperation of Heterogeneous Systems// Distributed and Parallel Databases. 2000, 8: 119-145

[45] Qian X, Lunt T F. A MAC Policy Framework for Multilevel Relational Databases // IEEE Trans. Knowledge and Data Eng. 1996, 8(1): 3-15

[46] Lang Bo, Lu You, Zhang Xin, et al. A Flexible Access Control Mechanism Supporting Large Scale Distributed Collaboration// Proceedings. The 8th International Conference on Computer Supported Cooperative Work in Design. vol. 1, 2004: 500-504

[47] Hu Hualiang, Chen Deren, Huang Changqing. Secure of Role Based Distributed Collaboration Systems// 2004 IEEE International Conference on Systems, Man & Cybernetics. October 2004

[48] Kamath A, Liscano R, Saddik A E. User-Credential Based Role Mapping in Multi-domain Environment // Proceedings of the 2006 International Conference on Privacy, Security and Trust. Oshawa, Canada, 2006

[49] Cornwall L A, et al. Authentication and Authorization Mecha-

nisms for Multi-Domain Grid Environments. Journal of Grid Computing, 2004, 2: 301-311

[50] Gagliardi F, Jones B, Reale M, et al. European DataGrid Project: Experiences of Deploying a Large Scale Testbed for E-Science Applications // Performance Evaluation of Complex Systems: Techniques and Tools, Performance 2002, Tutorial Lectures, Lecture Notes in Computer Science. Vol. 2459, Springer, 2002

[51] Freudenthal E, Keenan E, Pesin T, et al. DisCo: A Distribution Infrastructure for Securely Deploying Decomposable Services in Partially Trusted Environments (TR2001-820). Technical report. Department of Computer Science, New York University, 2001

[52] Winsborough W H, Li N. Safety in automated trust negotiation // Proceedings of the 2004 IEEE Symposium on Security and Privacy(S&P2004). Oakland, CA, USA, 2004: 147-160

[53] Winsborough W H, Li N H. Towards practical automated trust negotiation // Michael JB, ed. Proc. of the 3rd Int'l Workshop on Policies for Distributed Systems and Networks. Washington: IEEE Computer Society Press, 2002: 92-103

(上接第 19 页)

力(例如引入资源配置、资产配置等网络管理技术),逐步将不同的安全域和异构的网络也纳入管理范围。这些改变必将使协同变得更为复杂,对处理海量事件的能力要求更高。因此,还有许多问题亟待研究者解决。

参 考 文 献

[1] Hyland P C, Sandhu R. Concentric Supervision of Security Applications: A New Security Management Paradigm // Annual Computer Security Application Conference. Phoenix, USA, 1998

[2] Boudaoud K, McCatieNevile C. An Intelligent Agent - based Model for Security Management // The 7th IEEE International Symposium on Computers and Communications. Taormina, Italy, 2002

[3] Boudaoud K, Labiod H, et al. Network Security Management with Intelligent Agents // IEEE/IFIP Network Operations and Management Symposium. Honolulu, HI, USA, 2000

[4] Boudaoud K, Guessoum Z, et al. Policy-based Security Management Using a Multi-agent System // Workshop HPOWA. Berlin, 2001

[5] Torrellas G, Vargas L. Modeling a Flexible Network Security Systems Using Multi-agents Systems: Security Assessment Considerations // The 1st ACM International Symposium on Information and Communication Technologies. Trinity College, Dublin, Ireland, 2003

[6] Torrellas G, Cruz D. Security in a PKI-based Networking Environment: A Multi-agent Architecture for Distributed Security Management System & Control // The 2nd IEEE International Conference on Computational Cybernetics. Vienna, Austria, 2004

[7] Pilz A. Policy-Maker: a Toolkit for Policy-based Security Management // The 9th IEEE/IFIP Network Operations and Management Symposium. Seoul, Korea, 2004

[8] Distributed Management Task Force. CIM Specification 2.2 - 1999 Common Information Model

[9] Duan Haixin, Wu Jianping. Security Management for Large Computer Networks // APCC/OECC'99. Beijing, China, 1999

[10] Erfani S. Security Management System Functional Architecture for Enterprise Network // The 7th IEEE/IFIP Network Operations and Management Symposium. Honolulu, USA, 2000

[11] 黄承夏,杨林,马琳茹,等. 基于组件技术的网络安全管理架构研究. 信息安全与通信保密, 2006, 6: 61-63

[12] 陈汉章,张玉清. 一种基于插件与联动技术的复合安全网关. 计算机工程, 2006, 15(32): 143-145

[13] Xu C, Gong F, Baldine I, et al. Celestial Security Management System // DARPA Information Survivability Conference and Exposition. Hilton Head, USA, 2000

[14] Coyle J, Demerest J, McAllister R. A Proposed Security Management Framework for the Global Information Community // The 6th IEEE Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises, Cambridge, MA, 1997

[15] Damianou N, Bandara A, Sloman M, et al. A Survey of Policy Specification Approaches. Tech Rep. London: Department of Computing at Imperial College of Science Technology and Medicine, 2002

[16] Internet Engineering Task Force. RFC3060-2001 Policy Core Information Model-Version 1 Specification

[17] Hayton R J, Bacon J M, Moody K. Access Control in an Open Distributed Environment // IEEE Symposium on Security and Privacy. Oakland, USA, 1998

[18] Ribeiro C, Zuquete A, Ferreira P, et al. SPL: An access control language for security policies with complex constraints // Network and Distributed System Security Symposium. San Diego, USA, 2001

[19] Damianou N, Dulay N, Lupu E, et al. The Ponder Policy Specification Language // Workshop on Policies for Distributed Systems and Networks. Bristol, UK, 2001

[20] Corradi A, Montanari R, Lupu E, et al. A Flexible Access Control Service for Java Mobile Code // IEEE Annual Computer Security Applications Conference. New Orleans, USA, 2000

[21] Jarnhour E. Distributed Security Management Using LDA PDirectories // The 21st International Conference of the Chilean Computer Science Society. Punta Arenas, Chile, 2001

[22] Tsoumas B, Gritzalis D. Towards an Ontology - based Security Management // The 20th IEEE International Conference on Advanced Information Networking and Applications. Vienna, Austria, 2006

[23] Tsoumas B, Dritsas S, Gritzalis D. An Ontology-Based Approach to Information Systems Security Management // Computer Network Security. Heidelberg: Springer Berlin, 2005: 151-164

[24] Shin M, Moon H, Ryu K H, et al. Applying Data Mining Techniques to Analyze Alert Data // The 5th Asia-Pacific Web Conference. Xian, China, 2003

[25] Bidou R. Security Operation Center Concept & Implementation. http://www.ossim.net/docs.php