基于策略的 Web 服务访问控制研究*)

沈海波　洪　帆
(华中科技大学计算机学院　武汉 430074)

摘　要　资源的访问控制是开放、异构 Web 服务环境必须满足的重要安全需求之一。提出了基于策略的访问控制(PBAC)模型,比较了 PBAC 与基于角色的访问控制(RBAC),分析了 PBAC 对策略语言和策略管理架构的需求;基于扩展访问控制语言(XACML)和基于属性的访问控制(ABAC)模型,提出了一种基于策略的访问控制方法。这种方法满足了 Web 服务对互操作性、管理灵活性和系统规模性的需求。最后,对语义策略语言进行了展望。

关键词　Web 服务,基于属性的访问控制,策略,XACML

Study on Policy-based Access Control for Web Services

SHEN Hai-Bo　HONG Fan
(School of Computer, Huazhong University of Science and Technology, Wuhan 430074)

Abstract　Access control to resources is one of the most important requirements to be satisfied in open, heterogeneous Web service environment. A Policy-Based Access Control (PABC) model is proposed, and PBAC is compared with Role-Based Access Control (RABC). The requeirements for policy language and policy management architecture in PBAC are analyzed. Based on eXtensible access control language (XACML) and attribute-based access control (ABAC) model, a policy-based access control approach is proposed in this paper. This approach satisfies the requirements of the interoperability, flexibility and scalability to the Web service environment. In the end, senmantic policy language is prospected.

Keywords　Web service, Attribute-based access control, Policy, XACML

1　引言

Web 服务是一种崭新的分布式计算模式,基于一系列开放的标准协议,如服务调用协议 SOAP、服务描述协议 WSDL 和服务发现/集成协议 UDDI 等。其松散耦合、语言中立、平台无关性、开放性使得它将成为现代企业的服务框架。在 Web 服务环境,访问控制需要跨越管理域的边界,能够在异构的系统之间实现;并且,由于 Web 服务的无处不在性,服务提供者通常事先无法知晓请求者的身份。与传统的集中式系统和客户-服务器环境相比,Web 服务环境更具动态性和分布性,它带来了传统的安全模型不能处理的许多新的安全挑战[1],如规模性、灵活性和互操作性等。目前使用的几种访问控制方法,如基于身份的访问控制、基于角色的访问控制等均不能较好地应用于这种环境,因为它们采用集中式的控制方式,并且存在如下几方面的缺点:(1)只能提供有限的、粗粒度的策略定义功能;(2)仅仅只根据请求者的身份或角色进行授权决策;(3)通常没有利用开放的、标准的格式来表达访问控制策略[2]。而基于策略的访问控制 (Policy Based Access Control, PBAC)[3]是近年来比较流行的访问控制模型,它通过预先定义的策略和规则,灵活地控制用户对资源的访问 。其灵活性和多样性可弥补目前存在的访问控制机制的缺陷,满足现代企业在访问控制上日益变化的需求 。

为了解决 Web 服务环境对访问控制的规模性、灵活性和互操作性的需求,我们在分析基于策略访问控制模型的基础上,提出了一种基于策略的 Web 服务访问控制方法(称为 WS-PBAC 方法)。在 WS-PBAC 方法中,采用特别适合于 Web 服务环境的基于属性的访问控制(Attribute-Based Access Control, ABAC)[4]来定义,利用 XACML(eXtensible Access Control Language)[5]来编码和执行,它们可以提供统一的、互操作的策略表示和执行。我们还给出了实现框架,讨论了策略评估过程、安全机制等相关问题。

2　基于策略的访问控制模型及相关问题

2.1　PBAC 策略模型

PBAC 通过预先定义的策略和规则,控制用户对资源的访问 。PBAC 策略模型如图 1 所示[3]。

该模型包括 5 种组件:

(1)规则(Rule)。Rule 是定义 Policy 的基本构件,Rule 提供了在一个 Policy 中测试相关属性的条件,该条件由用户属性、环境属性的名/值对构成,可根据各种属性的值判断 Rule 的真假 。规则可以有复杂的逻辑 。

(2)策略(Policy)。由多个规则通过简单的逻辑关系连接而成 。

(3)资源(Resource)。系统中被保护的对象,也是用户需要访问的对象 。

(4)策略关联(Association)。表示该策略应用在哪类资源上,它是资源到保护资源的策略之间的映射。

(5)属性(Attributes)。属性与用户的会话相关联,包括,

*)湖北省自然科学基金项目(NO:2004ABA055)和湖北省教育厅重点项目(NO:D200531005)资助。沈海波　教授,博士生,主要研究领域为访问控制和网络安全;洪　帆　教授,博导,主要研究方向为密码学和信息安全。

环境属性（如当前时间、服务器地址、网络连接的安全力度）和用户属性（如用户名、组和角色用用户自定义的属性等）。

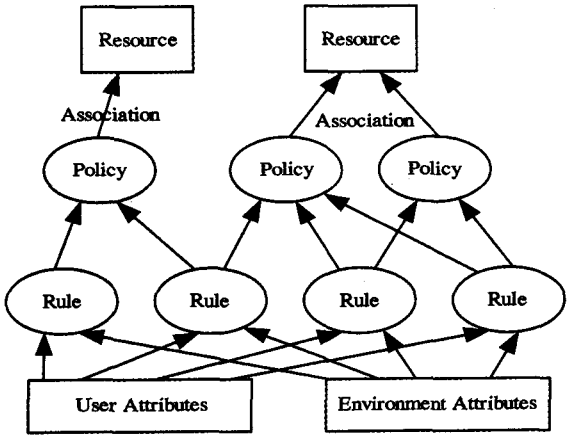

图 1　PBAC 策略模型

2.2　PBAC 与 RBAC 的比较

基于角色的访问控制（Role-Based Access Control，RBAC）[6]减少了管理费用，增强了管理灵活性，因此近来被广泛重视。但由于角色是静态的，角色通常与用户身份相关联，角色分配由人工实施，当用户数量较大时，管理工作量仍然很大；特别是当服务请求者和资源在不同的安全域时，管理规模是一个严重的问题。另外，在 Web 服务环境中用户身份通常是事先不可知晓的，且是动态变化的，基于用户身份或基于用户角色的访问控制，不太适合于 Web 服务的动态异构环境，至少需要进行适当的扩展。与 RBAC 相比，PBAC 有更多优点。下面我们从如下几方面，对 PBAC 与 RBAC 进行了比较。

(1)PBAC 是 RBAC 的超集。PBAC 能提供基于各种属性的授权决策，能够完全支持所有的角色，一个角色仅仅是一种属性。因此，RBAC 可看作是 PBAC 的特例，PBAC 可看作是 RBAC 的扩展。

(2)PBAC 的应用范围更广。RBAC 完全依据用户的角色（属性）对用户授权，而没有考虑用户的其他特性、环境属性（如当前时间、系统负荷等）和当前的资源状态，因而不能解决诸如“限制职员在上班时间访问资源”的问题。而 PBAC 支持用户属性、资源属性和环境属性，适用范围更广。

(3)PBAC 支持基于动态属性的授权决策。RBAC 是基于静态信息进行授权决策的（因为角色是静态的），而 PBAC 在授权决策中使用的属性可以是静态的，也可以是动态的（如当前位置、系统时间等）。

(4)PBAC 能为企业、组织建立更强大的访问控制规则。许多企业、组织需要更强大、更灵活的访问规则，RBAC 难于满足，而 PBAC 利用组合逻辑来组合规则和策略，从而可定义更复杂的策略，满足企业、组织的需要。

2.3　对策略语言及管理架构的需求

策略是 PBAC 中最基本的元素，因此，策略管理就显得尤为重要。策略管理包括策略的定义、存储、基于策略的推理、更新与维护、执行等。策略由策略语言来定义和编码，策略语言应满足如下的需求：

(1)具有良好的定义，即策略语言的语法和结构是清晰的、无歧义性，以此语言编码的策略的意义应独立于它的具体实现。

(2)具有灵活性和可扩展性。策略语言的灵活性是指能允许表达新的策略信息，可扩展性是指允许在新的版本中增加新的策略类型。

(3)具有互操作性。通常有几种语言能用于不同的管理域中表达类似的策略，为了使来自这些不同管理域的不同服务或应用能根据在策略中陈述的表现进行互相通信，策略语言必须具备互操作性。

一旦策略在给定的管理域中被定义，则需要策略管理架构来转换、存储和执行这些策略。因此，对策略管理架构的主要需求有：

(1)具有良好定义的界面。策略管理架构必须具有良好定义的界面，它独立于应用中的具体实现。在此策略管理架构中，各构件之间的界面必须是清晰的、无歧义的。

(2)具有互操作性。系统应能够与存在在其他管理域中的策略架构进行互操作。

(3)具有冲突解决能力。策略架构能够检测一个给定的策略是否与存在的其他策略相冲突，并提供解决方案。

(4)具有规模性。策略架构能够满足来自不同组织的异构资源、用户和访问控制需求的要求，在系统负载增加的情况下，保持高质量的执行效率。

(5)具有管理简单性。策略架构应有策略管理工具，实现策略的定义和其他管理，减轻管理负担。

策略语言 XACML 及其管理架构，可以满足上述的多种需求。

2.4　面向 Web 服务的策略规则

在 Web 服务访问控制上下文中，策略规则表达了谁在什么条件约束下能访问哪个服务（资源）。策略规则是 PBAC 的核心，根据策略决策过程，我们可根据用户属性、环境属性、资源属性和用户对资源的访问方式等设定规则，但应综合考虑各种影响授权的因素，避免以用户为中心进行授权所带来的局限性。多个规则可任意组合形成策略，策略与资源关联后，系统就可以对该资源进行访问控制。根据 Web 服务环境对访问控制的需求，可总结出下面几类规则：

(1)基于请求者属性的规则。该类规则检查用户的安全属性。安全属性中常见的有用户的 ID、所属的用户组、角色等，还包含用户帐号、档案号、许可级别等一些比较特殊的属性。

(2)基于目标服务属性的规则。该类规则检查被访问服务的属性。目标服务的属性包括资源的名称、存放位置、创建时间、安全级别等。

(3)客户规则。用户自定义的规则，此类规则一般都有比较复杂的逻辑，也可能与应用密切相关。

(4)基于环境属性的规则。环境属性包括时间、网络拓扑、连接状况、用户认证状况等，因此可构成时间规则、拓扑规则、连接规则、身份验证规则等。时间规则用于判断当前时间是否在一个指定的时间范围内；拓扑规则应用于网络环境下的访问控制，它检查服务器和客户端的地址和名称，看它们是否属于某个指定的网络地址段；连接规则以服务器/客户端之间的连接属性为检查的依据，判断该连接是否安全，例如密码强度是否足够等；身份验证规则以用户通过身份验证的方式作为检查的依据。

3　基于 XACML 的 PBAC 实现

PBAC 能综合考虑影响授权的各种因素，具有很强的实

用性，被广泛应用在企业级信息系统的访问控制中。例如Bea公司的应用服务器WebLogic，Entegrity公司的权限管理系统AssureAccess等，它们的访问控制功能非常齐全，但它们的实现都采用自己的方式来描述访问控制策略，这将不利于策略的共享，难于实现系统间的互操作。策略描述标准化必将是PBAC未来发展的趋势，也是系统间互操作的基本要求。为此，根据PBAC对策略管理的需求，我们采用OASIS标准XACML和基于属性的访问控制(ABAC)方法，设计了一个具有良好可扩展性、互操作性的PBAC实现框架。

3.1 实现框架

基于Web服务的特性，我们提出了一种基于XACML和ABAC的保护Web服务的PBAC实现框架，如图2所示。

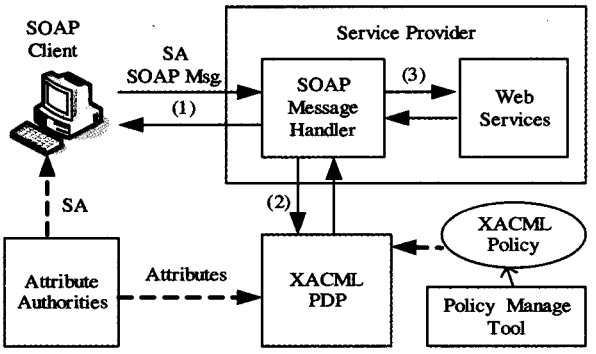

图2 PBAC实现框架

图中描述的主要访问控制工作流程如下：

(1)为了访问Web服务，Web服务(SOAP)客户端首先从主体属性中心获取需要的主体属性，然后向服务提供商发出SOAP请求信息，其中主体属性包含在SOAP头部。主体属性一般以SAML(Security Assertion Markup Language)[7]属性声明方式表示。

(2)扮演PEP角色的SOAP Message Handler收取SOAP请求信息，并前传到PDP请求授权决策。为了进行授权决策，PDP还可以向相关的Attribute Authorities获取资源属性和环境属性。有了主体属性、资源属性和环境属性，PDP与XACML Policy中的属性值进行比较评估，作出许可(permit)或拒绝(deny)的授权决策，并将决策结果返回给SOAP Message Handler。

(3)如果允许访问，则SOAP Message Handler将原始有SOAP请求传递给实际的Web Service端点。

3.2 访问控制策略表示

每个机构可以有自己的策略库，它以符合ABAC模型的结构化形式存储。在ABAC中，策略与属性关联，授权实体被分配以适当的属性。ABAC机制利用相关实体(如主体、资源、环境)的属性作为授权决策的基础，尤其适合于开放和分布式系统中的授权和访问控制。在WS-PBAC方法中，采用ABAC策略来表示。ABAC策略通常定义了服务请求者为了访问某服务，必须拥有哪些属性。而ABAC策略则用XACML语言格式来编码。XACML语言的访问控制策略能让用户定义相关的规则，以说明谁在什么时候什么条件下能做什么。具体策略形式见文[5]。

3.3 PDP策略评估

PDP是负责对XACML请求进行评估、判断的服务程序，是独立于PEP结点而设计的模块。一个PDP具有双重角色：一方面专门负责处理由SOAP Message Handler发来的请求，并返回服务决策；另一方面它存储的策略又作为其他PDP或者属性授权的引用点。如图3所示，在一个请求决策的过程中，PDP完成四个步骤：①PDP收到SOAP Message Handler签名的SAML请求，根据签名判断请求是否有效；②PDP从有效的请求中提取出XACML属性，把这些属性分类，从而重构XACML请求；③根据本地的策略以及由SOAP Message Handler发来的属性，将消息中的属性与策略中的属性值进行匹配比较，PDP对请求进行授权评估，而且也可以引用其他参考节点(属性授权结点)联合授权；④PDP形成一个SAML XACMLDecisionStatment，包含XACML授权结果，封装成一个声明后，进行签名返回给SOAP Message Handler，并关闭此次连接。

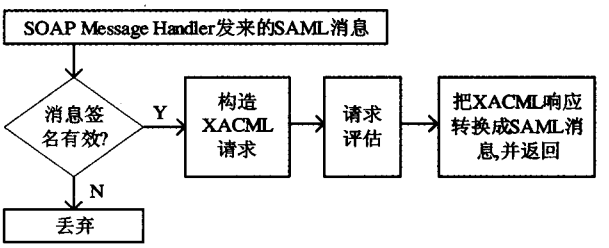

图3 PDP评估过程

目前，美国SUN公司已开发出开放的源代码XACML PDP[8]。

3.4 策略冲突解决

在Web服务环境，可能有多个策略(如安全策略、隐私策略、企业协议等)与单个服务关联，几个规则、策略、策略集可能用于定义单个访问请求，这些规则或策略可能存在冲突或不一致性。因此，PDP在进行授权决策过程中，可能会给出不同的评估结果。为此，XACML提供了一种称之为组合算法(Combining Algorithms，包括规则组合算法和策略组合算法)的机制，来解决上述问题。一种组合算法是一个优先规则，它说明了PDP应返回哪种唯一的、最终的决策结果。XACML共提供了如下五种标准组合算法：

(1)Deny-overrides(拒绝覆盖)：只要有一条规则的评估为Deny，那么最终授权决策也是Deny。

(2)Ordered-deny-overrides(有序拒绝覆盖)：与拒绝覆盖相同，只不过评估相关规则的顺序与将规则添加到策略中的顺序相同。

(3)Permit-overrides(允许覆盖)：只要有一条规则计算的评估为Permit，则最终授权决策也是Permit。

(4)Ordered-permit-overrides(允许按顺序覆盖)：与允许覆盖相同，只不过评估相关规则的顺序与规则添加到策略中的顺序相同。

(5)First-applicable(最先应用)：遇到的第一条相关规则的评估结果作为最终授权决策的评估结果。

3.5 安全性问题

尽管XACML提供了一个标准化的访问控制决策模型和请求/响应消息格式，但它没有定义这些构件之间的通信协议和安全机制，来保护消息的真实性、完整性和机密性。这就需要SAML来定义声明、协议和传输机制了。在我们的模型中，SAML声明在任意两个节点间在SSL[9]的保护下进行传递，包括SOAP client与SOAP Message HandlerPEP，SOAP Message Handler与XACML PDP。SSL能够完成客户端与服务端的双向认证，并提供健壮的数据加密，保证数据在发送

者与接受者之间信息的私密性。数字签名技术提供了信息的不可抵赖性与完整性。SAML 声明包括 XML 签名，利用发送方的私钥对声明的所有内容进行数字签名。接受方获得一个声明，服务程序就会验证该声明：①声明是否被签名；②签名是否正确；③验证声明的时间戳是否有效；④签名者的身份是否可信。

4 语义策略规则的需求

在 Web 服务环境中，不可能准确地预测到何种用户在何时要访问服务，以及访问何种服务，基于策略的控制很难利用关于主体、行为、事件的精确知识。为了解决这样环境对访问控制的需求，最近的研究提出采用丰富的语义来表达策略和域知识，即利用语义 Web 语言来定义和管理策略[10]，这种方法也称为基于 Ontology 的策略定义方法。基于 Ontology 的策略定义方法能带来诸多好处，事实上，基于规则的策略定义方法，是将策略编码成逻辑编程(Logic Programming)规则。基于规则的策略语言有非常强的表达能力和较高的执行效率，但会造成推理的不可判定性(可判定性是指所有的计算都在有限的时间内完成)。基于 Ontology 的策略定义方法，主要依靠描述逻辑(Description Logic)语言的表达特点。描述逻辑是一种知识表示工具，它首先定义应用领域的相关概念，然后利用这些概念去表示应用领域中的关系或属性，达到表示出应用领域中个体和对象的目的。描述逻辑有着形式化的、基于逻辑的语义规范，可以从明显的表达推理出隐含的内容。另外，语义 Web 语言能够保证在事先互不知晓的实体之间对彼此的概念、能力、行为等有共同的理解，保证了互操作性；在抽象的高层建模的策略，可简化它们的描述，改进系统的分析能力；语义 Web 语言也包括表达力较强的查询和自动推理能力。

目前，已设计了几种基于 Ontology 的语义策略规范语言，如 KAoS[11]，Rei[12]、SWSL[13]等，但由于它们是专有的，不是通用标准语言，在实际应用中会存在互操作问题。XACML 是一个基于属性的策略语言，但并不支持语义。如何在 XACML 中注入语义，是一个值得研究的问题，也是我们今后研究的一个方向。

结束语 基于策略的访问控制 PBAC 已受到广泛的重视，并逐步应用到实际中。但在目前的实际应用中，PBAC 系统大多采用自己的方式来描述访问控制策略，这不利于策略的共享和系统间的互操作。在本文中，我们基于标准的访问控制语言 XACML 和特别适用于 Web 服务环境的访问控制模型 ABAC，提出了一种基于策略的 Web 服务访问控制框架，具有较好的互操作性、灵活性和规模性。为了更好地应用 PBAC，增加策略的语义性，提高语义互操作性，我们将在这方面做进一步的研究。

参 考 文 献

1 World Wide Web Consortium. Web service. http://www.w3.org/2002/ws

2 Juliano F S, Luciano P G, Marinho P B, et al. Policy-Based Access Control in Peer-to-Peer Grid Systems. In: Proceedings of The 6th IEEE/ACM International Workshop on Grid Computing, 2005

3 Entegrity Solutions Whitepaper. AssureAccess Policy-Based Access Control: A definition, and how it extends Role-Based Access Control. http://www.entegrity.com/products/whitepaperall.shtml. 2005

4 沈海波，洪帆. 面向 Web 服务的基于属性的访问控制研究. 计算机科学，2006，33(4)：92～96

5 OASIS Standard. eXtensible Access Control Markup Language (XACML) Version 1.0. February 2003. http://www.oasis-open.org/committees/xacml

6 Ferraiolo D F, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC), 2001, 4(3)

7 OASIS Standard. Security Assertion Markup Language (SAML) V1.1, October, 2003. http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf

8 Sun's XACML Implementation Programmer's Guide. http://sunxacml.sourceforge.net/guide.html, June 2006

9 Microsoft Knowledge Base. Description of the Secure Sockets Layer (SSL) Handshake, 2003. http://support.microsoft.com/default.aspx?scid=kb.

10 Nejdl W, Olmedilla D, Winslett M, et al. Ontology-based policy specification and management. In: 2nd European Semantic Web Conference (ESWC), volume 3532 of Lecture Notes in Computer Science, Heraklion, Crete, Greece, Springer, May 2005. 290～302

11 Uszok, Bradshaw J, Jeffers R, et al. KAoS Policy and Domain Services: Toward a Description-Logic Approach to Policy Representation, Deconfliction, and Enforcement. In: Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Network, Italy, June 2003. 93～98

12 Kagai T, Finin A, Joshi A. Policy Based Approach to Security on the Semantic Web. In: Proceedings of the 2nd International Semantic Web Conference (ISWC), LNCS, Springer, 2003, 2870

13 SWRL: A Semantic Web Rule Language Combining OWL and RuleML. Draft Version 0.7, 21 December 2004. http://www.daml.org/rules/proposal/

(上接第 106 页)

参 考 文 献

1 Greengrass Ed. Information Retrieval: A Survey. http://www.nlp.org.cn/categories/default.php?cat_id=17

2 Craven M, DiPasquo D, Freitag D, et al. Learning to Construct Knowledge Bases from the World Wide Web. Artificial Intelligence Elsevier, August 1999

3 Winkels R, Bosscher D, Boer A, Hoekstra R. Extended conceptual retrieval. Legal Knowledge and Information Systems. Jurix 2000. In: The Thirteenth Annual Conference. Amesterdam: IPS Press, 2000. 85～97

4 Raghavan V V, Wong S K M. A critical analysis of vector space model for inormation retrieval. Journal of the American Society for Information Sciences, 1986, 37(5): 279～287

5 Van Rijsbergen C J. Information Retrieval. Butterworths, 1979

6 Turtle H, Croft W B. Evaluaton of an inference network-based retrieval model. ACM Transantions on Information Systems, 1991, 9(3): 187～222

7 Swoogle. Semantic Web Search Engine. http://swoogle.umbc.edu/

8 Mandala R, Tokuanga T, Tanaka H. Combining multiple evidence from different types of thesaurus for query expansion. SIGIR, 1999

9 Miller G A, et al. Introduction to WordNet: an on-line lexical database. International Journal of Lexicography, 1990, 3(4): 235～312

10 Jin Qianli, Zhao Jun, Xu Bo. Query Expantion Based on Term Similarity Tree Model. IEEE, 2003. 400～406

11 Baeza-Yates R, Ribeiro-Netod B 等著. 现代信息检索. 王知津，贾福新，等译. 机械工业出版社，2005. 165～285

12 李飞，高济，刘柏嵩，周明健. 知识管理中语义与关键字相结合的检索方法. 计算机辅助设计与图形学学报，2004，16(12)