第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0144—03 文献标识码：A 中图分类号：TP309

结合协商机制的 Web 服务属性访问控制模型

傅鹤岗，王 建
(重庆大学计算机学院，重庆 400044)

摘 要：针对实现有效 Web 服务访问控制的问题，提出一种结合协商机制的 Web 服务属性访问控制模型。该模型基于安全断言标记语言和可扩展访问控制标识语言，利用主体属性和上下文属性的组合限制条件，提供细粒度的访问控制。通过加入协商机制，服务请求者可以与服务提供者相互沟通，在访问请求中动态地调整参数信息以获得访问授权。

关键词：Web 服务；访问控制；协商

Attribute Access Control Model for Web Services with Negotiation Mechanism

FU He-gang, WANG Jian
(College of Computer, Chongqing University, Chongqing 400044)

【Abstract】 This paper proposes an attribute-based access control model for Web services with negotiation to provide an effective access control mechanism. The model is based on SAML and XACML and takes the restrictive condition composed of identity attributes and context attributes to provide fine-grained access control. The negotiation ability in the model can make service requester communicate with the service provider and change the parameters in the request to get access to the services.

【Key words】 Web services; access control; negotiation

在当前的网络环境中，将企业应用移植到 Web 服务平台来增强应用系统的性能，为客户提供多元化的服务已成为一种趋势。Web 服务是一种松散耦合的 Web 应用，同以往的应用系统相比，Web 服务所处的环境更灵活多变，各种不确定因素更多。因此，如何保证有效的 Web 服务访问控制成了严峻的挑战。本文提出一种 Web 服务访问控制模型，采用基于属性的限制方式，结合协商机制，大大加强了访问控制机制的灵活性。

1 相关工作

目前，国内外很多学者和机构对 Web 服务的访问控制做了有益的研究和探索。文献[1]提出基于可扩展访问控制标识语言(XACML)的访问控制与 RBAC 限制，对基于 XACML 的 RBAC 框架进行了扩充，使 RBAC 模型可以在 XACML 中实现动态职责分离和动态基数限制，但模型中没有考虑上下文信息，不能有效地实现动态的访问控制。文献[2]提出了计算系统中基于上下文和角色的访问控制模型，在基于角色的访问控制模型中加入了上下文信息，为 Web 服务提供了更灵活的访问控制，但这些模型没有采用基于属性的访问控制方式，不能解决 Web 服务跨越安全域访问的问题。文献[3]提出了信任和上下文可识的 Web 服务会话访问控制模型，通过属性限制的方式对 Web 服务进行访问控制，但这些模型均不具备对服务参数进行协商的能力。文献[4]提出的 Ws-AC 模型能够对服务参数进行协商，但对于每一类服务参数，最多只能定义 3 个协商策略，并且这 3 个策略的使用顺序是固定的，因此，协商方式不够灵活、效率不高。此外，该模型主要基于 WS-Policy 规范，没有考虑安全断言标记语言(SAML)和 XACML 规范。文献[5]提出了关于 Web 服务的协商机制，但未运用到访问控制领域中。

2 模型设计

基于属性的 Web 服务访问控制模型通过参与决策的相关实体的属性进行授权决策。实体可以是主体(subject)、客体(object)或环境(environment)。

主体属性分为静态属性和动态属性。静态属性包括主体的身份、职位等，动态属性包括主体的年龄、信用度等。

客体属性主要包括资源的标识、创建者、创建日期等。

环境属性通常描述事务处理时的上下文，包括时间、日期、系统状态、安全级别等。

在访问控制模型中加入协商机制可以使服务提供者对其信任的服务请求者动态地提供协商建议，服务请求者根据服务提供方所提供的建议改变服务访问请求来获得访问授权，这使得整个过程在保证安全的前提下，有效地提高了服务的访问效率。

2.1 模型元素及其定义

定义 1 设 SUC(Simple User Condition)为原子主体属性限制条件；CUC(Composite User Condition)为组合主体属性限制条件；SCC 为(Simple Context Condition)为原子上下文环境属性限制条件；CCC(Composite Context Condition)为组合上下文环境属性限制条件。

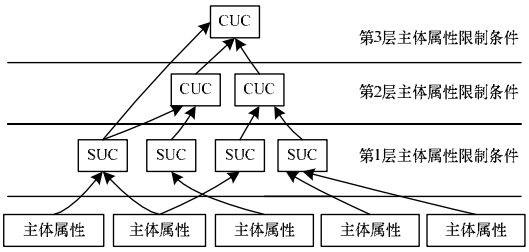
SUC 和 SCC 的结构为：<at, op, value>。其中，at 为属性名称，对于 SUC 来说属性为主体属性，对于 SCC 来说属

作者简介：傅鹤岗(1950－)，男，副教授，主研方向：电子商务，软件工程；王 建，硕士

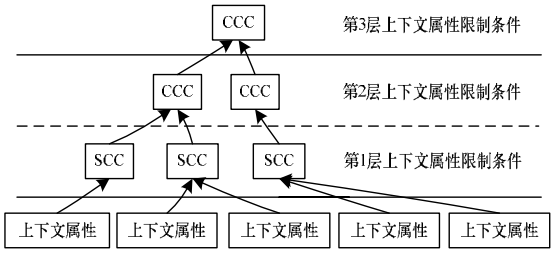
收稿日期：2009-08-28 **E-mail：**bournewang2008@gmail.com

性为上下文环境属性；op 为操作符，其取值范围为{≤, ≥,<,>,=, ≠}，此外，用户还可以自定义操作符；value 为属性值。属性限制条件可以通过组合形成更高一级的组合属性限制条件。

CUC 由多个主体属性通过组合形成，CCC 由多个上下文环境属性通过组合形成。如图 1 所示，CUC 和 CCC 分别形成一个多级的属性信息访问限制条件。



(a)多层主体属性信息限制模型



(b)多层上下文属性信息限制模型

图 1　多层属性信息限制模型

限制条件的组合形式分为 and 模式和 or 模式。and 模式要求属性条件必须满足参加计算的每一个限制条件，整个表达式限制条件结果为真。例如，age>18 and position=“IT Manager”，指当属性条件满足年龄大于 18 岁并且职位为 IT 经理时，整个限制条件为真。or 模式要求属性条件只需要满足参加计算的任何一个限制条件，整个表达式限制条件结果为真。例如：age=22 or age=23，指年龄为 22 或者 23 岁时，整个限制条件为真。

定义 2 设 ParSet 为参数集合，其结构为：ParSet={<par_1, D_{par_1}>,<par_2, D_{par_2}>,⋯,<par_n, D_{par_n}>}。其中，$par_i(i \in [1,n])$为参数名称，D_{par_i} 为参数par_i的阈值空间。

定义 3 设 Cluster 为 Web 服务参数簇集，且 $Cluster_i \subseteq$ ParSet。由定义 2 知，$Cluster_i$ 的结构为

$Cluster_i$={< par_{i1} , $D_{par_{i1}}$ >,< par_{i2} , $D_{par_{i2}}$ >,⋯,< par_{ij} , $D_{par_{ij}}$ >}

其中，$i \in [1, n]$, $j \leq n$。

定义 4 设 WSParSet 为 Web 服务的标准输入参数集合，其结构为

WSParSet={<$Cluster_1$， $D_{Cluster_1}$ >,<$Cluster_{12}$， $D_{Cluster_2}$ >,⋯, <$Cluster_n$, $D_{Cluster_n}$ >}

其中，$D_{Cluster_i}$ $(i \in [1,n])$为 $Cluster_i$ 的阈值空间，并且 $D_{Cluster_n} \subseteq D_{par_{i1}} \times D_{par_{i2}} \times \cdots \times D_{par_{ij}}$, $i \in [1,n]$; $j \leq n$。

定义 5 设 nap 为协商建议，且 nap ∈ WSParSet。

由定义 4 知，nap 的结构为

nap= {<*Cluster*, $D_{Cluster_n}$ >}

定义 6 设 neq 为协商建议触发器，其结构为：neq=<nap, CUC,CCC,U>。其中，

(1)nap 定义了 neq 包含的协商建议。

(2)CUC 和 CCC 定义了触发协商建议 neq 所必需的主体属性限制条件和上下文环境属性限制条件。

(3)U 为 neq 所对应的效用函数。每一个 neq 的效用评估值都由 U 表示，其计算方法如下：

对于 Cluster 中任意的参数 par_i 和参数的阈值空间 D_{par_i}，U_{par_i} 表示参数效用值，$U_{D_{par_i}}$ 表示参数阈值空间效用值，并且 $U_{par_i} \in [0,1], U_{D_{par_i}} \in [0,1]$。参数效用值通过归一化处理，满足条件：

$$\sum_{i=1}^{n} U_{par_i} = 1 \tag{1}$$

neq 的效用值评估计算公式为

$$U_{neq} = \sum_{i=1}^{n} U_{par_i} \times U_{D_{par_i}} \tag{2}$$

定义 7 设 policy 为 Web 服务访问控制策略，其结构为 policy =<ws,WSParSet,NeqSet,CUC,CCC>，其中，

(1)ws 为 Web 服务标识。

(2)WSParSet 为 Web 服务标准输入参数集合。

(3)NeqSet 为 Web 服务协商建议触发器集合，其结构为：NeqSet = {neq_1, neq_2,⋯,neq_n }。

(4)CUC 和 CCC 为满足此访问控制策略的条件。

定义 8 设 req 为一个 Web 服务访问请求，其数据结构为：req=<ws,RP,A>，其中，

(1)ws 为 Web 服务标识。

(2)RP 为 Web 服务的请求参数集合，其数据结构为：RP={<wp_1,wv_1>,<wp_2,wv_2>,⋯,<wp_n,wv_n>}，其中，$wp_i(i \in [1,n])$为 Web 服务请求参数名称，$wv_i(i \in [1,n])$为参数 wp_i 的值。

(3)A 为 Web 服务请求方的主体属性集合，其结构为：A={<a_1,v_1>,<a_2,v_2>,⋯, <a_n,v_n>}，其中，$a_i(i \in [1,n])$为 Web 服务请求方的主体属性名称；$v_i(i \in [1,n])$为 Web 服务请求方的主体属性 a_i 的值。

2.2　结合协商机制的访问控制模型

模型的协商过程如图 2 所示。首先 Web 服务请求者向 Web 服务提供者发送服务访问请求。访问请求通过属性访问控制模块进行访问控制决策。如果请求被接受，则进入系统的协商服务模块。协商服务将从访问请求中提取出服务请求参数信息，判断是否与所请求服务的标准输入参数匹配。如果不匹配，则根据协商建议触发器创建协商建议，并返回给服务请求者。服务请求者可以根据建议对请求参数信息进行相应的调整，然后再次发送服务请求。

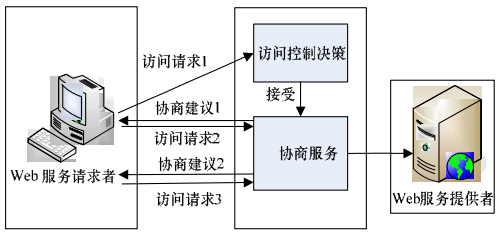


图 2　协商过程

3　模型系统结构

本文提出的访问控制模型系统结构如图 3 所示，主要包括以下 6 个模块：

(1)属性授权机构(Attribute Authorities)：属性授权机构是可信的第三方认证机构，它主要对主体的相关属性进行认证。

(2)策略执行点(PEP)：用于处理收到的 SOAP 消息，它从消息头部的 SAML 声明中提取主体属性信息，并且创建一个 XACML 请求发送到策略决策点(PDP)。

(3)策略决策点：根据接收到的 XACML 授权请求从策略库中提取对应的 XACML 策略判断访问请求是否合法，并将允许或者拒绝结果返回给 PEP。

(4)策略管理点(PAP)：用于维护和管理策略库，根据 PDP 定义策略文件。

(5)协商服务(Negotiation Service)：从接收到的 SOAP 消息中提取出请求服务的参数信息。如果参数信息与 Web 服务请求者所请求的服务参数不匹配，协商服务创建协商建议，并将结果返回给服务请求者。

(6)访问上下文服务(Access Context Service)：通过记录用户的服务访问日志，对用户主体的动态属性信息进行调整。

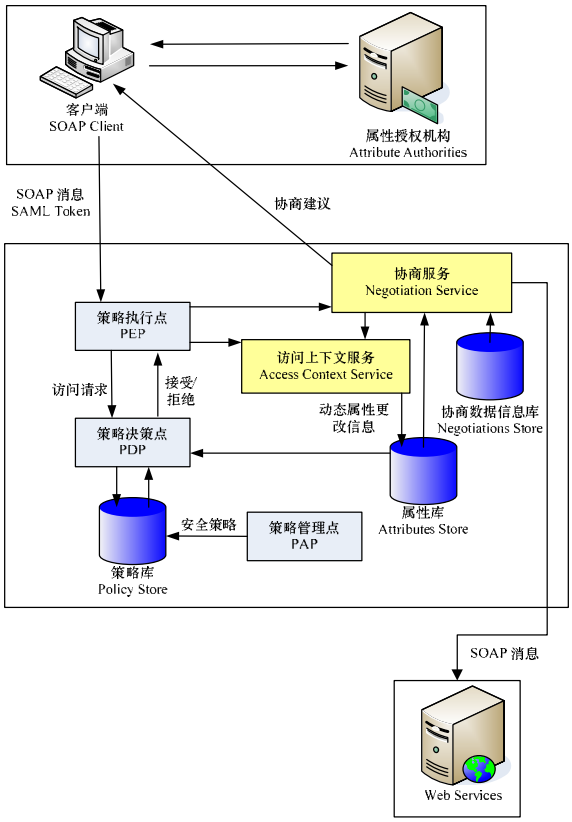


图 3　访问控制模型系统结构

4　系统应用实现

本文的系统应用实现以重庆市电力调度系统为例。重庆市电力调度系统分为市调(市级)系统和地调(区县级)系统，如南岸地调系统、璧山地调系统，各个系统相互独立。由于市调的部分应用系统需要访问地调系统的服务，因此每个调度系统都增加了访问控制模块，如图 4 所示。市调系统在访问地调系统服务时，首先从属性认证机构中获得 SAML 认证信息，然后向相应的地调系统发送访问请求。地调系统在收到服务访问请求后，根据访问控制策略，对访问请求进行访问控制。访问控制策略采用 XACML 标准。如果访问请求没有通过，而其安全参数级别达到了进行协商的要求，那么访问控制模块会向服务请求者返回适当的协商建议。

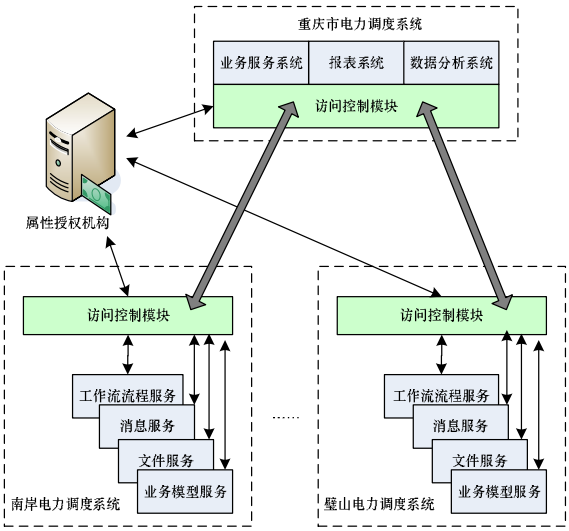


图 4　重庆市电力调度系统结构

系统访问控制模块的特性包括：支持跨越安全域的访问需求，支持将主体属性、客体属性和环境属性的访问控制策略相结合的细粒度的访问控制，支持协商服务。系统在实施后获得了较好的运行效果。

5　结束语

本文提出了一种结合协商机制的 Web 服务属性访问控制模型。该模型不仅可以灵活动态地实现主体属性及上下文相关的访问控制策略，使 Web 服务的安全体系更加灵活稳健，而且结合了协商机制，使服务提供者和服务请求者可以对服务和安全需求进行沟通，有效促进了服务访问的正常进行。此外，该模型与 SAML 和 XACML 标准结合，具有更强的互操作性。

参考文献

[1] 努尔买买提·黑力力，罗振兴. 基于XACML的访问控制与RBAC限制[J]. 计算机工程, 2008, 34(8): 19-21.

[2] Kulkarni D, Tripathi A. Context-aware Role-based Access Control in Pervasive Computing Systems[C]//Proc. of Symposium on Access Control Models and Technologies. Estes Park, CO, USA: ACM Press, 2008: 113-122.

[3] Coetzee M, Eloff J H P. A Trust and Context-aware Access Control Model for Web Services Conversations[M]. Berlin, Germany: Springer, 2007.

[4] Bertino E, Squicciarini A C, Paloscia I, et al. Ws-AC: A Fine Grained Access Control System for Web Services[C]//Proc. of Conf. on World Wide Web Internet and Web Information Systems. New York, USA: ACM Press, 2005.

[5] Raymond Y K. Lau Towards a Web Services and Intelligent Agents-based Negotiation System for B2B eCommerce[J]. Electronic Commerce Research and Applications, 2007, 6(3): 260-266.

编辑　张正兴