一个 Web 服务访问控制模型*)

韩 涛 郭荷清 高 英 李 冬 刘 壮
(华南理工大学计算机科学与工程学院 广州 510640)

摘 要 本文设计了一种 Web 服务的通信机制用来解决应用层 SOAP 消息的安全传输,通过扩展 SAML 的语法与 XACML 结合来实现其应用,以解决访问控制的问题,并在此基础上提出了一个完整的 Web 服务的访问控制模型,保证对 Web 服务安全的、细粒度的访问控制。最后,以一个应用的实例来具体地实现此访问控制模型。

关键词 Web 服务,访问控制,XACML,SAML

An Access Control Model for Web Services

HAN Tao GUO He-Qin GAO Ying LI Dong LIU Zhuang
(Dept. of Computer Science and Engineering, South China of Tech., Guangzhou 510640)

Abstract This paper proposes a mechanism for Web services secure communication to assure secure transport of SOAP message at application layer; SAML's syntax is extended to be implemented in XACML application, which solves the problem of access control. Finally, an entire access control model for Web services is presented to assure secure 'fine-grained' access control. Finally the model is explained in detail by an application example.

Keywords Web services, Access control, XACML, SAML

随着互联网技术与应用的发展,基于 Web 服务的分布式应用(如电子商务和电子政务等)已成为十分重要的发展方向。为保证 Web 服务能够在 Internet 上得到广泛的应用,必须保证 Web 服务的安全。目前,典型的 Web 服务正面临着各种新的挑战,其中 Web 服务的安全通信和访问控制成为 Web 服务进一步应用和发展所必须解决的关键问题。

Web 服务的通信是以 SOAP 的消息传输为基础,而 SOAP 协议是应用层协议,因此,Web 服务的安全通信必须保证应用层 SOAP 消息的安全传输。目前,对这一问题国内外一些研究机构做了一定的研究工作,特别是韩国信息安全研究中心。2003 年,此研究中心的 Kiyoung 等人提出了 Web 服务安全通信的重要性,并给出了基于 XKMS(XML Key Management Specification,XML 密钥管理规范)实现的架构[1];2004 年,此研究中心的 Namje 等人提出了基于 XKMS 的密钥管理模型 E-XKM,在一定程度上解决了 SOAP 消息传送的机密性,但却忽略了消息的传输效率[2]。文本在 XKMS 的基础上,提出了一种高效的安全通信机制,保证了应用层 SOAP 消息传输的机密性、可用性、完整性和不可否认性。

Web 服务的访问控制是 Web 服务研究的一个重要领域。有两个基本的访问控制模型可以应用于 Internet 上的系统:ACL(Access Control Lists,访问控制列表)和 RBAC(Role-Based Access Control,基于角色的访问控制)。在 ACL 中,每个用户名都被映射为特殊资源的一个单独的权限集,这个权限集包括 Read、Write、Execute 和 Change 权限,将这个排列称为"访问矩阵";RBAC 这几年得到了快速的发展,主要是因为它允许考虑用户的上下文来执行访问控制,用户可以划分到组中,并为其分配"角色",这些角色能够反映组织结构,但遗憾的是,在应用于 SOAP 时,RBAC 注重的是用户的角色,而不是处理消息的服务的角色,因此造成了很大的迷惑。

XACML(eXtensible Access Control Markup Language,可扩展访问标记性语言)是一个 OASIS 标准,该标准是一个通用的访问策略定义语言,提供一套语法来管理对系统资源的访问。在特定的 XML 的文档环境中,XACML 将 ACL 扩展为〈对象,主体,动作,条件〉的策略。近几年关于 Web 服务的访问控制的技术研究引起了研究人员的广泛关注:2003 年,弗吉尼亚大学的 Lorch 等人提出了 Carder Architecture,第一次用 XACML 解决访问控制问题[3];2004 年,Sun 实验室的 Anderson 深入分析了 XACML 的策略定义[4];2005 年,慕尼黑大学的 Matheus 等人提出了 XACML 中产生冲突的解决方案[5]。然而,以上的研究成果并没有解决下面的重要问题:XACML 没有标准化一个完整的认证解决方案,它没有明确定义 PEP(Policy Enforcement Point, 策略执行点)和 PDP(Policy Decision Point, 策略决策点)之间的通信协议,所以需要一个强大的标准来支持。SAML(Security Assertion Markup Language,安全性断言标记语言)无疑是目前最好的选择,SAML 是一个基于 XML 的架构,用于交换安全信息,该安全信息以断言或者有关主体的事实的形式来交换。本文将扩展 SAML2.0 语法,定义 XACML 之间通信的协议,来真正实现 XACML 的访问控制策略。

本文从研究 Web 服务的安全通信和访问控制入手,提出了一个 Web 服务访问控制模型,保证了客户端到服务器端的安全通信,并通过结合 SAML 与 XACML 来实现细粒度的访问控制策略。最后,在具体的实现中给出一个应用的实例。

*)国家 973 高技术研究发展计划基金资助项目(G20000263)。**韩 涛** 博士研究生,主要研究方向为网络信息系统的安全、信息系统建模;**高 英** 博士研究生,主要研究方向为网络信息系统的集成;**李 冬** 博士研究生,主要研究方向为电子商务与网络安全;**刘 壮** 博士研究生,主要研究方向为并行处理技术和分布式系统。

1 Web服务的安全通信

安全通信是Web服务安全的基础，由于Web服务通信以应用层SOAP消息的传输为基础，因此，Web服务的安全通信机制必须提供一个安全的SOAP信道。然而常用的安全通信机制(如SSL、IPsec等)只适用于传输层/网络层的数据安全保护，所以本文设计了一种Web服务的通信机制，完成了应用层SOAP消息的安全传输，实现了实体的身份验证，保证了所传递消息的机密性、完整性、不可否认性。

表1 Web服务的通信机制的符号描述表

符 号	说 明
C	客户端
S	服务器端
K_A, K_A^{-1}	A的公钥，A的私钥
$\{M\}_{K_A}, \{M\}_{K_A^{-1}}$	用A的公钥、私钥对M进行加密
$Sig_A(M)$	用A的私钥对M进行签名
SessionID	会话标示符
T_{i1}, T_{i2}	第i个消息请求、应答所使用的时间戳

如图1所示，安全的通信过程如下：

① C→S: $\{Request1\}_k$, $Sig_C\{Request1\}$, $\{k\}_{K_S}$, T_{11}

② S→C: SessionID, $\{Response1\}_k$, $Sig_S\{Response1\}$, T_{12}

③ C→S: SessionID, $\{Request2\}_k$, $Sig_C\{Request2\}$, T_{21}

④ S→C: SessionID, $\{Response2\}_k$, $Sig_S\{Response2\}$, T_{22}

说明：

(1)首先，客户端利用XKMS的信任服务实现的注册服务来完成密钥对和相关绑定信息的注册，然后选取此次对话的加密算法，生成会话密钥，对请求的消息进行加密，并且用私钥对消息签名，同时用服务器的公钥加密会话密钥，最后附加时间戳，把安全处理的结果发送给服务器端。

(2)服务器端收到消息后，首先用自己的私钥解密会话密钥，然后用会话密钥解密请求消息，根据请求消息中客户端传递的密钥信息，利用XKMS信任服务实现的定位服务，来获取客户端的公钥，进而验证签名的有效性。随后，在访问控制模型中完成其身份验证和决策请求(详见第四部分)，若通过，则建立会话，调用客户端请求的服务，并对响应消息进行加密、签名处理，然后附加时间戳，发送给客户端[5,6]。

(3)，(4)客户端收到响应消息后，解密、验证签名的有效性，进行与服务端安全的通信。

上述会话有超时机制，根据时间戳来判断，如果超时，则中断会话；若在通信中发生致命错误，如认证、解密、身份验证错误等，则导致会话终止、通信失败、发送出错信息。

2 XACML与SAML

这一部分定义了如何通过扩展SAML2.0语法来保护、传输和请求XACML的语法实例[7]，这里定义了6种查询和陈述类型：

(1)AttributeQuery：SAML的标准的属性请求，用来向AA(Attribute Authority，属性机构)查询一个或多个属性值。

(2)AttributeStatement：包含一个或多个属性值的标准的SAML属性陈述，用于AA的SAML属性查询响应，或者作为一个SAML断言存储在属性仓库中。

(3)XACMLPolicyQuery：通过扩展SAML语法来表示的一种XACML策略请求，用来向PAP(Policy Administration Point，策略管理点)请求一个或多个策略，为了在XACML请求上下文中可用，在SAML属性中一定要加上命名空间，即"xs=urn:oasis:names:tc:saml:2.0:profiles:attribute:xacml"，一个策略请求可以这样表示：

```
〈xs:element name="XACMLPolicyQuery"
          type="XACMLPolicyQueryType"/〉
〈xs:complexType
name="XACMLPolicyQueryType"〉
 〈complexContent〉
  〈xs:extension
base="samlp:RequestAbstractType"〉
   〈xs:choice minOccurs="0"
maxOccurs="unbounded"〉
    〈xs:element
ref="xacml-context:Request"/〉
     〈xs:element ref="xacml:Target"/〉
     〈xs:element
ref="xacml:PolicySetIdReference"/〉
     〈xs:element
ref="xacml:PolicyIdReference"/〉
    〈/xs:choice〉
   〈/xs:extension〉
  〈/xs:complexContent〉
〈/xs:complexType〉
```

(4)XACMLPolicyStatement：通过扩展SAML语法来表示的一种XACML策略陈述，用于PAP的XACML查询响应，或者作为一个SAML断言存储在策略仓库中。相应的请求响应可以这样表示：

```
〈xs:element name="XACMLPolicyStatement"
          type="xacml-saml:XACMLPolicyStatementType"/〉
〈xs:complexType name="XACMLPolicyStatementType"〉
 〈xs:complexContent〉
  〈xs:extension
base="saml:StatementAbstractType"〉
   〈xs:choice minOccurs="0"
maxOccurs="unbounded"〉
    〈xs:element ref="xacml:Policy"/〉
    〈xs:element ref="xacmlPolicySet"/〉
   〈/xs:choice〉
  〈/xs:extension〉
 〈/xs:complexContent〉
〈/xs:complexType〉
```

(5)XACMLAuthzDecisionQuery：通过扩展SAML语法来表示的一种授权决策的请求，用于向XACML PDP请求授权决策。

(6)XACMLAuthzDecisionStatement：通过扩展SAML语法来表示的一种授权决策的陈述，用于表示XACML PDP的授权决策响应(详见第5部分)。

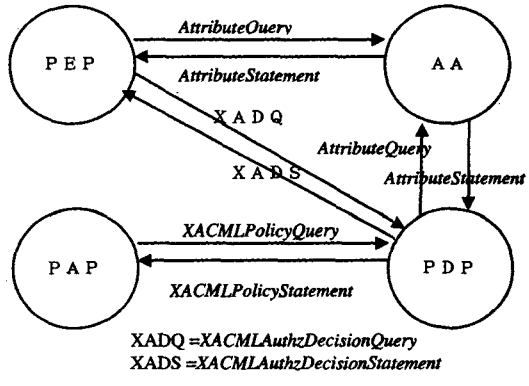

图1 XACML应用模型

图1所示的XACML应用模型解释了不同组件之间消息的传递，在这里不需要XACML作任何语法上的扩展，而SAML则必须定义语法上的扩展来支持相应的属性的查询和陈述，即扩展后的SAML定义了XACML的组件之间的通

信协议。

3 Web服务访问控制模型

基于对以上两个问题的分析与解决，提出了一个Web服务访问控制模型，如图2所示，首先保证从客户端到SAML PEP(SAML策略执行点)之间的信息的安全传输，提供了一个安全的SOAP信道，而一旦SAML PEP收到访问请求，将生成授权决策请求发送给SAML PDP(SAML策略决策点)，SAML PEP根据得到授权决策的结果决定是否允许客户端调用相应的Web服务。

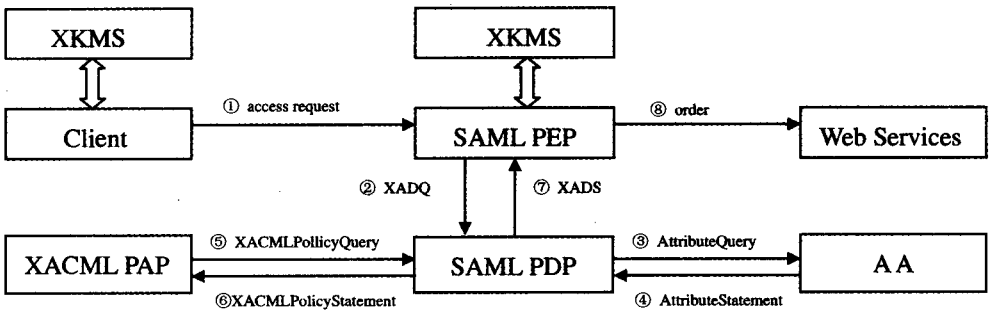

图2 Web服务访问控制模型

(1)客户端发送访问请求给SAML PEP。

(2)SAML PEP收到请求后，利用XKMS的定位服务，来获取客户端的公钥，验证签名的有效性，以及消息的完整性。然后，将请求信息从SOAP消息中取出，生成〈XACMLAuthzDecisionQuery〉格式的授权决策请求，发送给SAML PDP。

(3)，(4)SAML PDP都到请求后，向一个或多个AA查询相关的属性值，包括目标中的三类属性(主体、资源、动作)。

(5)，(6)SAML PDP把属性值写入〈XACMLPollicyQuery〉，发送给XACML PAP，XACML PAP根据目标的限制条件对存储的策略进行检索，把匹配目标的访问控制策略发送给SAML PDP。

(7)SAML PDP将对得到的访问控制策略进行评估，然后做出授权决策〈 XACMLAuthzDecisionStatement 〉发送给SAML PEP。

(8)根据〈 XACMLAuthzDecisionStatement 〉，SAML PEP决定允许或拒绝客户端的请求。

XACML提供了创建策略和规则来控制信息访问的机制，是一种比简单的拒绝访问或授权访问更细粒度的访问控制，该策略描述语言用于定义通用的访问控制需求，包括若干标准扩展点来定义新的功能、数据类型、组合逻辑等。然而，XACML并没有定义协议本身的传输机制，与SAML的无缝结合才使得XACML的访问控制策略得以真正实现。

4 应用实例

为了进一步解释该访问控制模型，将其应用到一个实际的环境中：Computerclub俱乐部在其服务器上提供了很多资源，而只有俱乐部的VIP会员才可以访问其内部资源。所以，当SAML PDP得到SAML PEP的一个授权请求时，使用布尔判断来比较一个请求中的参数值和目标里面的条件值，将请求关联到相应的策略上。

例如，属于Computerclub俱乐部的会员Bob，想读取内部资源 www. ComputerClub. com/inside_resource/private. txt，相应的〈XACMLAuthzDecisionQuery〉提供与用户请求相关的主体、资源等属性值，作为授权决策请求发送给SAML PDP，授权请求可以这样表示：

```
〈XACMLAuthzDecisionQuery〉
 〈Request〉
  〈Subject〉
   〈Attribute AttributeId="urn:oasis: names: tc: xacml: 1.0: subject: subject-id" DataType="urn: oasis: names: tc: xacml: 1.0: data-type: rfc822Name"〉
   〈AttributeValue〉Bob@ComputerClub. com〈/AttributeValue〉
   〈/Attribute〉
   〈Attribute AttributeId="group" DataType="http://www. w3. org/2001/XMLSchema#string"〉
   〈AttributeValue〉VIP〈/AttributeValue〉
   〈/Attribute〉
  〈/Subject〉
  〈Resource〉
   〈Attribute AttributeId="urn:oasis: names: tc: xacml: 1.0: resource: resource -id" DataType="http://www. w3. org/2001/XMLSchema#anyURI"〉
   〈AttributeValue〉http://www. ComputerClub. com/inside_resource/private. txt〈/AttributeValue〉
   〈/Attribute〉
  〈/Resource〉
  〈Action〉
   〈Attribute AttributeId="urn: oasis: names: tc: xacml: 1.0: action: action-id"
   DataType="http://www. w3. org/2001/XMLSchema#string"〉
   〈AttributeValue〉read〈/AttributeValue〉〈/Attribute〉
  〈/Action〉
  〈/Request〉
  〈ReturnContext〉
   〈AttributeValue DataType="http://www. w3. org/2001/XMLSchema#Boolean"〉read〈/AttributeValue〉
  〈/ReturnContext〉
〈/XACMLAuthzDecisionQuery〉
```

而授权决策如下所示，在〈 XACMLAuthzDecisionStatement 〉中绑定了SAML PEP请求时提供的所有的属性，评估结果是允许Bob读取内部资源 www. ComputerClub. com/inside_resource/private. txt。

```
〈XACMLAuthzDecisionStatement〉
 〈Response〉
  〈Result〉
   〈Decision〉Permit〈/Decision〉
   〈Status〉〈StatusCode Value="urn: oasis: names: tc: xacml: 1.0: status: ok"/〉〈/Status〉
  〈/Result〉
 〈/Response〉
 〈Request〉
  …
  …
 〈/Request〉
〈/XACMLAuthzDecisionStatement〉
```

结束语 本文提出了一个Web服务访问控制模型，致力于解决Web服务的安全通信与访问控制问题，该模型保证了消息传递的安全性，并实现了细粒度的访问控制。该模型具有灵活、可扩展、跨平台、易维护等特征，能够解决典型Web服务中的访问控制问题。

XACML规范尚处于发展阶段，规范本身的细节还有待于进一步的讨论和研究，由于尚没有实现多个请求的并发处

(下转第216页)

断变化各属性的值，以确定 k 个类及每个类的记录数 i，因此最后生成的数据集的规模将是 $i \times k$。

就第 i 个类的空间形状而言，它是以 $(4 \times i, 0, 0 \cdots)$ 为中心，1 为边长的一个超立方体。类内的每一条记录，它们的层次属性分布且仅分布在概念层次树树根的一棵子树上——即对分别属于不同类的任意两条记录，它们的层次属性的公共祖先只会是概念层次树的根(如图 3 所示)。

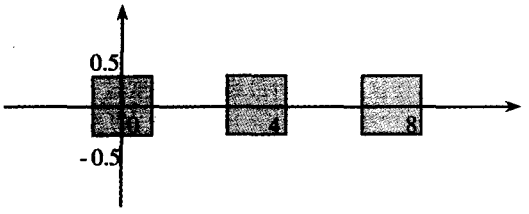

图 3　数据集分布

采用此方法合成的数据，有如下特点：数值型属性有着较小的类内距离和较大的类间距离；在同一个类内的层次型数据，概念距离更接近。综上所述，合成的类有着比较低的类内相异度，和较高的类间相异度。

我们的测试环境为 P3 866、128M 内存、4G 硬盘、Slackware Liunx 11、内核版本 2.4.33、gcc 版本 3.4.6、编译选项"-O3"。

我们应用 k-medoids 聚类算法测试我们的相异度计算方法与传统方法对于聚类准确性的影响。两种度量方法的主要区别在于层次类型变量的相异度计算，在传统方法中，只比较属性的值而不管其所在层次和位置，而我们的方法则根据定义 1 的方法进行计算。

实验 1：聚类数 $k=3$，属性数 $d=10$(其中 9 个数值属性，1 个层次属性)，结果如表 1。

表 1　$d=10$ 时实验结果的对比表

每类记录数	本文的度量方法		传统的度量方法	
	运算时间(秒)	准确度(%)	运算时间(秒)	准确度(%)
1000	1	99.3	1	89.7
2000	4	99.5	4	86.7
4000	38	99.9	18	83.9
8000	225	99.8	249	75.4
10000	278	99.7	251	79.2

实验 2：聚类数 $k=3$，属性数 $d=6$(其中 5 个数值属性，1 个层次属性)，结果如表 2。

由于这两种方法结果都不很稳定，准确度与开始时随机选择的中心点有一定关系，因此我们对每一个样本数据都进行了 5 次实验，取平均值。

与传统的相异度计算方法相比，我们的算法度量更具合理性和可解释性，所以准确度更高。当然，由于层次类型属性的相异度计算需要比较概念层次树中不同层次的值，因此通常比传统的计算方法需要更多的时间。

表 2　$d=6$ 时实验结果的对比表

每类记录数	本文的度量方法		传统的度量方法	
	运算时间(秒)	准确度(%)	运算时间(秒)	准确度(%)
1000	1	99.9	1	99.7
2000	4	99.9	4	96.7
4000	38	99.9	18	93.9
8000	225	96.9	249	95.4
10000	278	97.4	251	89.2

结束语　本文在分析传统类型变量相异度量的基础上，定义了"层次类型"的概念，提出了层次类型变量的相异度量计算方法。引入层次类型变量，并结合传统类型变量，设计了具有包括层次类型在内的混合数据类型描述的对象之间的相异度量方法，并基于此实现了此类对象的聚类分析。实验表明，对于具有层次型属性的数据集，其聚类准确度高于传统的相异度度量方法。

本文所提出的算法对于层次型和数据型的混和类型数据比较有效，而其它类型数据处理还需要采用传统的方法度量。另外，两个层次类型属性值的相异度的计算方法本身也有待于进一步改进，例如将节点的位置与节点值综合考虑进行相异度计算。因此在今后的工作中，我们将在以下两个方面进行更深入的研究。

(1) 对于层次类型属性，进一步探索更加准确、合理的相异度计算方法，包括两个层次类型变量对应的概念层次树中各节点本身的值、其祖先和子孙节点的值以及层次关系等；

(2) 研究包括层次类型属性在内的多种类型混合的数据类型所描述对象的相异度计算方法。

参 考 文 献

1　李桂林，陈云晓. 关于聚类分析中相似度的讨论[J]. 计算机工程与应用，2004，31：64～82

2　Han J，Kamber M. Data Mining：Concepts and Techniques. Higher Education Press，Morgan Kaufmann Publishers，2001，5

3　郭金华. 数据挖掘中聚类分析的研究[D]. 武汉理工大学管理学院，2003

4　Jain A K，Murty M N，Flynn P J. Data Clustering：A Review. ACM Computing Surveys，1999，31(3)：264～323

(上接第 161 页)

理，因此本文所提出的实现方案在满足多个请求时尚有一定的困难，访问控制的安全性还需进一步的认识和解决。

参 考 文 献

1　Park N，Moon K，Sohn S. XML key management system for Web-based business application. In：Network Operations and Management Symposium 2004，NOMS 2004 on April 2004，1：903～904

2　Park N，Moon K，Sohn S. A study on the XKMS-based key management system for secure global XML web services. Advanced Communication Technology，2004，1：492～495

3　Lorch M，Kafura D. An XACML-based policy management and authorization service for globus resources. In：Grid Computing 2003. Proceedings on Nov 2003. 208～210

4　Anderson. An introduction to the Web Services Policy Language (WSPL). In：Policies for Distributed Systems and Networks on June 2004. 189～192

5　Matheus A. How to Declare Access Control Policies for XML Structured Information Objects using OASIS' eXtensible Access Control Markup Language (XACML). In：System Sciences 2005. HICSS '05 on 03 Jan 2005. 168a～168a

6　Marin L G. A Network Access Control Approach Based on the AAA Architecture and Authorization Attributes. In：Parallel and Distributed Processing Symposium 2005 on April 2005. 287a～287a

7　Jeong J，Dongkyoo S，Dongil S. An XML-based single sign-on scheme supporting OSGi framework. In：Consumer Electronics 2005 on Jan. 2005. 31～32