第 32 卷 第 16 期 计 算 机 工 程 2006 年 8 月
Vol.32 № 16 Computer Engineering August 2006
·安全技术· 文章编号：1000—3428(2006)16—0136—03 文献标识码：A 中图分类号：TP393

基于属性证书的 Web Services 访问控制模型

金丽娜，蒋兴浩，李建华
（上海交通大学电子信息与电气工程学院，上海 200030）

摘 要：Web Services 的安全性已成为 Web Services 广泛应用的主要障碍，Web Services 需要解决的安全问题包括：机密性，完整性，抗抵赖性，身份认证，授权和访问控制等。该文针对 Web Services 的授权和访问控制中存在的问题，提出了一种基于属性证书的 Web Services 授权机制并分析了利用属性证书实现 Web Services 角色访问控制的特点。

关键词：Web Services；属性证书；访问控制；PMI

Access Control Model for Web Services Based on Attribute Certificate

JIN Li'na, JIANG Xinghao, LI Jianhua
(School of Electronic Engineering and Information Technology, Shanghai Jiaotong University, Shanghai 200030)

【Abstract】 The security problem including confidentiality, integrity, nonrepudiation, authentication, authorization and access control has become the main obstacle for WS before its large scale application. This paper presents an attribute certificate based authorization mechanism for WS and analyzes the characteristics of access control model for WS aiming at the authorization and access control problem WS faces.

【Key words】 Web Services; Attribute certificate; Access control; PMI

Web Services 作为开放技术架构将是未来应用架构的一个极为重要的模式，与传统的分布式应用模型如：DCOM，CORBA，RMI 相比，有完好的封装性、松散耦合、使用协约的规范性、使用标准协议规范、高度可集成等特性，从而确定了 Web Services 日益主流的地位，但是在被大规模应用之前，Web Services 仍然要解决以下的安全问题：

(1)数据的机密性。如何保证传送消息不被未经许可的第三方看到。

(2)数据的完整性。如何保证收到的消息没有被篡改过。

(3)身份认证。如何鉴别通信双方的身份。

(4)授权和访问控制。如何保证用户的操作没有超越他的权限。

当前 Web Services 所采用的访问控制方法和应用于 Web 页面的方法没什么不同。如在 Web 服务器(比如 apache,IIS)上普遍使用的 IP 阻塞(IP blocking)，通过识别特定 IP 地址，服务器通常保存一个禁止访问的 IP 地址列表。这样的安全措施显然是粗糙的，让那些潜在的客户无法访问，Web 服务的接口描述 WSDL 文件也无法获得，更为全面的安全策略也无法实现。Web Services 对安全性的要求高得多，而且其安全性需求是多样化的。因此，需要为相异的 Web Services 设计一种具备通用性的访问控制模型。

本文针对 Web Services 的授权和访问控制中存在的问题，提出了一种基于属性证书的 Web Services 授权机制，通过在属性证书的 attributes 字段加入持有者拥有的角色信息来实现授权。另外本文采用基于 XML 的属性证书，使属性证书在 Web Services 中的应用更为简便。最后分析了利用属性证书实现 Web Services 角色访问控制的特点。

1 相关技术

1.1 Web Services[1]及其关键技术

W3C 将 Web Services 定义为一种通过 URL 标识的软件应用，其接口及绑定形式可以通过 XML 标准定义、描述和检索，并能通过 XML 消息和互联网协议完成与其它应用的直接交互。简单地理解，Web Services 是一种应用程序，它可以使用标准的互联网协议，如超文本传输协议(HTTP)和 XML，将功能纲领性地体现在互联网和企业内部网上。

Web Services 面向服务的架构(SOA)如图 1 所示。Web Services 系统结构是基于 Services Provider(服务提供者)、Services Requestor(服务请求者)、Services Registry(服务注册中心)3 个角色和 Publish(发布)、Find(发现)、Bind(绑定)3 个动作构建的。服务提供者利用 WSDL 描述自己的 Web Services，并将服务发布到 UDDI；服务请求者利用 SOAP 消息向服务提供者发送使用服务的请求；服务注册中心的作用是通过在 UDDI 中查找满足服务请求者要求的服务。

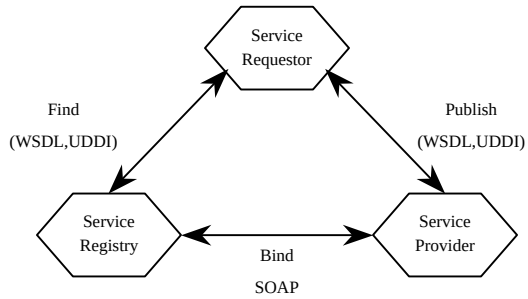

图 1 Web Service 系统结构

Web Service 完全基于 XML 技术。服务提供者和服务请求者均使用 XML 传递消息和数据流。当然，Web Services 还需要标准的格式和协议用以对 XML 进行合理的解释。这

基金项目：上海市科委重点课题支持项目(035115013)
作者简介：金丽娜(1981—)，女，硕士，主研方向：信息安全；蒋兴浩，博士；李建华，教授、博导
收稿日期：2005-08-25 **E-mail：**snoopyjlna@sjtu.edu.cn

些标准的格式和协议就是 Web Services 所基于的 XML 的三大关键技术：SOAP，UDDI 和 WSDL。

(1)XML：可扩充的标记语言，是一个基于文本的 W3C 规范的标记语言，是 SGML 针对特定应用领域的一个子集。XML 严格地定义可移植的结构化数据，并对数据赋予上下文相关功能。

(2)SOAP：简单对象访问协议，是一种用于在分布式环境中交换信息的轻量级协议，是关于 SOAP 消息的格式和处理规则，为沿着 SOAP 消息路径交换信息而需要的、不同应用程序之间生成和接收 SOAP 消息的、交互过程的简单控制机制等的一整套规范和约定。

(3)UDDI：统一描述、发现和集成协议，是一套基于 Web 的、分布式的、为 Web Services 提供信息注册中心的实现标准，同时包含一组使企业能将自身提供的 Web Services 注册使得别的企业能够发现的访问协议。

(4)WSDL：Web Services 描述语言，是一套基于 XML 的语法，用以将 Web Services 描述为能够进行消息交换的 Services 访问点的集合。

1.2 权限管理基础设施

PMI 是由属性证书、属性权威、属性证书库等部件构成的综合系统，用来实现权限和证书的产生、管理、存储、分发和撤销等功能。PMI 的授权模型如图 2 所示。

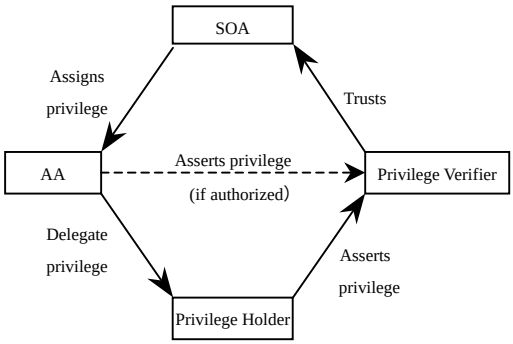

图 2　PMI 授权模型

其组成实体为：

(1)SOA(Source of Authority)：整个 PMI 系统的最终信任源和最高管理机构，主要职责是授权策略的管理与应用、AA 的设立审核及管理、属性证书的颁发、更新、废除等。

(2)AA(Attribute Authority)：授权管理体系的核心服务节点，职责主要包括属性证书颁发、更新、废除等。

(3)Privilege Holder(特权持有者) :即拥有并使用属性证书的实体或人。

(4)Privilege Verifier(特权验证者：检验 AC 的合法性并使用其结果的实体。

属性证书AC[3](Attribute Certificate)是由属性权威机构 AA(Attribute Authority) 签发的用来将实体和其权力等信息绑定在一起的数据结构。属性证书由签发它的AA签名，以此来实现数据的一致性和证书的有效性。属性证书的格式由ITU标注X.509v4 标准和推荐的模板格式[rfc3281.txt]及其它相关标准定义。其组成部分为版本号(version，当前版本是v2)、持有者(holder)、签发者(issuer)、签名(signature)、序列号(serialNumber)、有效期(validPeriod)、属性(attributes)、颁发者唯一标识符(issuerUniqueID)和可选的扩展(extentions)。其中前 7 项为必需项，是构成属性证书的基本信息，后 2 项是可选项。利用属性证书中指定的签名算法，将证书 9 项内容作为输入得到签名值，并把签名值附在证书的最后构成一个完整的属性证书。

2 系统方案

2.1 属性证书的设计

由于属性证书不包括公钥，因此属性证书需要同认证服务一起验证属性证书持有者的身份。虽然 X.509 证书的最新版本允许在其扩展项中加入属性信息，但是证书中最不稳定的内容往往就是属性信息，用户名称改变的频率远远低于属性信息的变化，这样频繁地更新和撤销将给系统带来非常大的负担，另外 PKI 的证书权威和 PMI 的属性权威也往往并不相同，因此这也给证书的签发和撤销带来一定的困难。同时考虑到 Web Services 使用 XML 和基于 XML 的标准的特点，本文采用了基于 XML 格式的属性证书，其格式如下。

```
<?xml version='1.0' encoding='utf-8'?>
<AttributeCertivicate>
<AttributeCertificateInfo>
  <vrsion></version>
  <holder>
        <baseCertificateID>
              <issuer>…</issuer>
              <serialNumber>…</serialNumber>
        </baseCertificateID>
  </holder>
  <issuer>…</issuer>
  <signature>
http://www.w3.org/2000/09/xmldisg#rsa-sha1
</ signature >
  <serialNumber>…</serialNumber>
  <attCertValidity>
        <notBefore>2005-05-01T10.00.00</notBefore>
`       <notAfter>2005-10-01T10.00.00</notAfter>
  </attCertValidity>
  <attributes>
        <attribute>
          <role>
              <roleAuthority>…</roleAuthority>
              <roleName>…</roleName>
          </role>
          <clearance>…</clearance>
        <attribute>
  </atttibutes>
</AttributeCertificateInfo>
<SignatureAlgorithm>
http://www.w3.org/2000/09/xmldisg#rsa-sha1
</SignatureAlgorithm>
<SignatureValue>……</SignatureValue>
</AttributeCertivicate>
```

holder 字段包含连接身份证书 PKC 的信息，用它来指示与属性证书持有者对应的身份证书 PKC。holder 字段可以采用 3 种信息来实现和身份证书的绑定：对应 PKC 的序列号和签发者信息，对应 PKC 的主体信息或者某个对象的序列值。本文定义的基于 XML 的属性证书的 holder 项通过对应的签发者信息和身份证书的序列号来实现绑定，分别用 issuer 和 serialNumber 字段表示。attributes 字段可以包含标准的属性信息，如 Service Authentication Information、Access Identity、Role、Clearance 等，也可以包含应用程序自己定义的属性信息。本文属性证书的 attributes 字段包含 role 字段和 clearance 字段。role 字段包含 roleAuthority 和 roleName 字段，分别表示角色授权者和角色名称。clearance 表示机密等级。

根据WS-Security[4]中对SOAP头部的扩展机制，可以把基于XML的属性证书作为一种基于XML的安全令牌嵌入SOAP报头的<wsse:Security></wsse:Security >元素中。如下所示：

```
<?xml version='1.0'?>
<env:Envelope
xmlns:env="http://www.w3.org/2001/12/soap-envelope">
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
<env:Header>
<wsse:Security>
  <AttirbuteCertificate>
        …
  </AttributeCertificate>
</wsse:Security>
</env:Header>
<env:Body>
. . .
</env:Body>
</env:Envelope>
```

2.2 访问控制模型

本文提出了一种基于属性证书的 Web Services 访问控制模型，如图 3 所示。

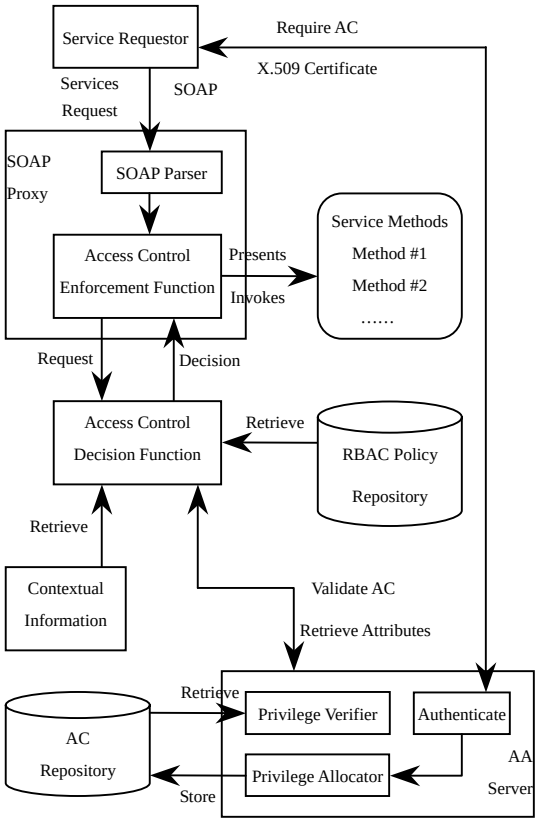

图 3 系统模型

其各部分组成如下：

(1)Service Requestor： 服务请求者，构建 SOAP 消息向服务提供者发出调用请求。

(2)SOAP Proxy：SOAP 代理服务器，截取服务用户向服务提供者的所有服务请求。主要由两个模块组成：SOAP Parser 和 AEF。

(3)SOAP Parser：SOAP 消息解析器，截取服务用户向服务提供者的所有服务请求。主要由两个模块组成：SOAP Parser 和 AEF。

(4)Access Control Enforcement Function：访问控制实施功能，简称 AEF。AEF 监控所有来自访问请求发起者的访问请求。若监测到访问请求，AEF 拦截该请求，并且以一种统一的方式向 ADF 请求判决。AEF 要求 ADF 判决时，需要向 ADF 传递判决请求信息，包括访问发起者的信息(身份信息或者属性证书)、访问目标、访问操作及参数。

(5)Access Control Decision Function：访问控制判决功能，简称 ADF。当 AEF 向 ADF 转发一个访问请求时，ADF 根据 PV 对访问发起者所持有属性证书的有效性验证结果、属性证书所包含的权限信息、环境信息以及访问策略规则，对这个请求进行判决。

(6)Service Methods：Web Services 功能模块，包含用户调用的 Service Methods。

(7)RBAC Policy Repository：角色策略库。

(8)AA Server：属性证书服务器，负责签发、查找、验证属性证书。由 Privilege Verifier，Privilege Allocator 和 Authentication 3 个模块组成。

(9)AC Repository：属性证书库，用于存储属性证书，一般情况下采用 LDAP 目录服务器。

下面以一个简单的网上书店 Web Services 为例，说明本系统模型的访问控制过程。此网上书店定义的角色授权策略如表 1 所示，一共定义了 4 种供用户调用的操作和 2 种角色。其中 getBook 和 getPrice 两种操作可以被任意用户调用，而 placeOrder 和 deleteOrder 只能被会员调用。

表 1 网上书店的角色授权策略

角色	服务操作
访问者	getBook
	getPrice
会员	getBook
	getPrice
	placeOrder
	deleteOrder

(1)用户从 UDDI 查找到此网上书店的服务并下载它的 WSDL 文件。用户客户端根据 WSDL 文件构建符合要求的 SOAP 消息向网上商店调用某种操作。

(2)网上商店的 SOAP Proxy 截获访问者的 SOAP 请求对其进行解析后经过 AEF 模块送至 ADF 模块请求判决。

(3)ADF 模块根据已制定的角色授权策略判定进行判定，若用户调用的是 getBook 或 getPrice，则允许用户调用操作，若用户调用 placeOrder 或 deleteOrder 操作，则要求用户提供相应的属性证书进行角色认证。

(4)若用户没有相应的属性证书，网上商店会要求用户向 AA Server 申请证书，若用户已有证书，则可将证书嵌入 SOAP 重新构建请求消息。

用户申请属性证书时需要对用户进行身份认证，其过程如下：(1)用户客户端向属性证书服务器提交身份证书以及申请某种角色所需要的个人信息，请求服务器为其签发相应的属性证书。(2)属性证书服务器传送给用户一个随机数 R，用户用他的私钥 SK 对 R 进行签名，形成 Signature(R，SK)，属性证书服务器根据用户的公钥 PK 验证签名是否为真，若为真，则用户通过身份认证， 服务器利用用户提交的个人信息为其签发属性证书并发送给用户。 (下转第 150 页)