Web 服务访问控制规范及其实现 *

张赛男
(中国人民解放军理工大学 理学院,江苏 南京 211100)

摘 要:提出了一种用于 Web 服务的访问控制模型,这种模型和 Web 服务相结合,能够实现 Web 服务下安全访问控制权限的动态改变,改善目前静态访问控制问题。新的模型提供的视图策略语言 VPL 用于描述 Web 服务的访问控制策略。给出了新的安全模型和 Web 服务集成的结构,用于执行 Web 服务访问控制策略。

关键词:Web 服务;访问控制;视图策略语言;访问控制策略
中图分类号:TP311.5;TP309 文献标识码:A 文章编号:1674-7720(2011)19-0011-03

Specification and realization of access control of Web services

Zhang Sainan
(Institute of Science, PLA University of Science and Technology, Nanjing 211100, China)

Abstract: This paper proposes an access control model for Web services. The integration of the security model into Web services can realize dynamic right changes of security access control on Web services for improving static access control at present. The new model provides view policy language to describe access control policy of Web services. At the end of the paper we describe an infrastructure of integration of the security model into Web services to enforce access control polices of Web services.

Key words: Web services; access control; view policy language; access control policy

随着 Web 服务的广泛应用,Web 服务中的访问控制策略描述及实现显得尤为重要。目前,Web 服务安全标准以及其实现并不完善,Web 服务安全多数交由作为应用程序服务器的 Web 服务器的安全机制管理。例如,Tomcat 服务器为用户、组、角色的管理和为访问 Java-Web 应用程序的权限提供了安全管理。但是,Tomcat 中的授权是粗粒度的,也就是说,Tomcat 不可能限制对 Web 服务的单个的访问操作。

本文通过示例,探讨如何把一种新的安全模型应用到 Web 服务中。这种新的安全模型提供了一种规范语言——视图策略语言,其授权可以在 Web 服务单个的操作层次上细粒度地指定,同时授权还可以通过操作的调用动态地改变。这种模型和 Web 服务相结合,能够实现 Web 服务下安全访问控制权限的动态改变,改善目前静态访问控制的问题。

1 Web 服务访问控制规范

1.1 图书中心系统

图书中心系统是一个 Web 服务的简单应用,其结构如图 1 所示。

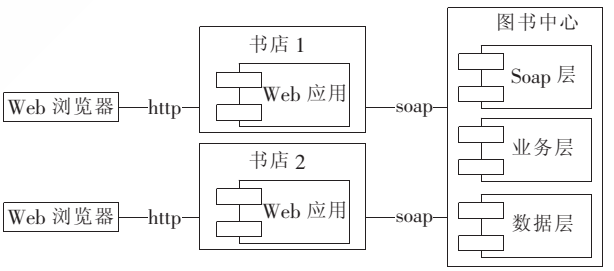

图 1 影视中心结构图

图书中心系统主要提供书店注册服务、书店客户注册服务、书店处理客户注册请求服务、书店管理客户借阅图书信息服务和为所有的用户查询图书信息的服务。其中书店注册是其他所有服务的前提条件。

1.2 系统中的访问控制需求

图书中心系统的访问控制需求描述如下:

BusinessRegistration:书店经理注册自己的书店。这个注册是其他所有服务的前提条件。

CustomerRegistration:书店的客户向书店提交注册申请。

* 基金项目:解放军理工大学理学院青年基金(QN-DZ-2010-03)

CustomerRegistrationProcess：书店处理客户的注册申请。

CustomerBookList：书店仅能为自己的客户使用此服务。客户可以查询己借阅清单，但不能在此清单上添加新的请求，只有店员可以添加客户的借阅清单。

BookSearch：店员和客户都能使用此服务查询图书信息。

1.3 系统中的访问控制

基于视图的访问控制 VBAC (View-Based Access Control) 模型是专门用于支持分布式访问控制策略的设计和管理的模型[1]，图 2 是 VBAC 的简易模型。VBAC 模型可以看成是基于角色的访问控制 RBAC (Role-Based Access Control)模型的扩展，VBAC 增加了视图以及模式的概念。视图描述的是对访问对象的授权，视图被分配给角色。如果一个主体所扮演的角色拥有对某个对象访问的视图，则这个主体就可以访问此对象。如果这个角色没有这个视图，则这个主体就不能访问此对象。模式描述的是视图和角色动态的分配以及删除。

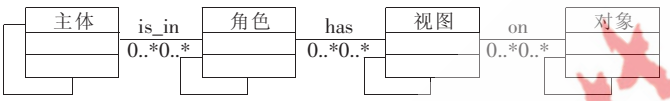

图 2 VBAC 模型

视图策略语言 VPL(View Policy Language)是一种说明性的语言，用于描述 VBAC 策略。VPL 用于描述角色、视图以及模式。角色在角色声明 roles 之后，视图以及模式声明使用关键字 view 和 schema。

角色声明描述了策略中的角色以及这些角色初始拥有的视图。图 3 是图书中心的角色声明。这个例子中有 customer 和 staff 两个角色。staff 继承了 customer，customer 能够调用的操作，staff 也可以调用。staff 拥有初始视图 BusinessRegistratoin，关键字 holds 来说明角色拥有视图，而 customer 没有初始视图。

```
roles
customer
staff extends customer
holds BusinessRegistration
```

图 3 VPL 角色声明

图 4 是图书中心的访问控制需求的 VPL 视图声明，关键字 controls 引导的是一个类或者接口。例如，视图 BusinessRegistration 允许调用类 BusinessRegistration 的操作 processRegisterRequest。VPL 视图可以静态地被限制给特定的角色，这些角色罗列在关键字 restricted to 后面。例如，视图 BusinessRegistration 只能被赋给角色 staff 而不能赋给 customer。

VPL 对被描述的授权操作的参数没有限制，即不需要全部参数才能调用某个操作。例如，调用操作 getCustomerGUID 仅需要书店的 loginBusinessID 就能获取到自己书店的所有客户的信息。因为，书店在注册以后有对应的 loginBusinessID。由于基于 CORBA 的应用程序，都会采取为每个客户端在服务器端创建一个对象的设计模式。因此，客户端与创建的对象进行通信无需身份

```
view BusinessRegistration controls BusinessRegistration restricted to staff
{processRegisterRequest}
view CustomerRegistration controls CustomerRegistration restricted to customer
{processRegisterRequest}
view CustomerRegistrationProcess controls CustomerRegistrationProcess
                                                    restricted to staff
 {getCustomerGUID(loginBusinessID,-,-,-) if caller=loginBusinessID
  processRegisterRequest(loginBusinessID,-,-,-) if caller=loginBusinessID
 }
view CustomerBookListFull controls CustomerBookList restricted to staff
{processAddRequest(loginBusinessID,-,-,-) if caller=loginBusinessID
 processQueryRequest(loginBusinessID,-,-) if caller=loginBusinessID
}
view CustomerBookListRestricted controls CustomerBookList
{processQueryRequest(-,-,customerGUID) if caller=customerID}
view BookSearch controls BookSearch
{processRequest}
```

图 4 VPL 视图定义

验证。例如，在这个例子中，每个客户端在服务器端都有一个 CustomerRegistrationProcess 对象，由于 SOAP 对面向对象支持的局限性，将 loginBusinessID 作为一个参数给出。

因此，研究扩展 VPL 来说明操作被调用的时候所必须具备的条件是在操作后添加 if caller=param 来指定必备条件。这个表达式中，关键字 caller 表示此操作调用者的 ID，param 表示操作的实参。调用者由一个整数表示其身份。如果操作的某个参数不是必须的，用"-"表示；如果视图中操作参数没有任何条件限制，则 VPL 视图中仅有操作名称的标识符，而没有参数列表。例如，视图 BusinessRegistration 中的操作 processRegisterProcess 就属于这一类型。

依据服务 CustomerBookList，角色 staff 和 customer 有不同的访问需求。staff 可以调用 processAddRequest 以及 processQueryRequest 两个操作，但是 customer 仅能调用 processQueryRequest。视图 CustomerBookListFull 确定其使用角色是 staff，可以拥有两个操作，而CustomerBookListRestricted 没有角色的限制。如果视图被调用，customer 仅能查询自己借阅的书。

VPL 模式(VPL Schema)为动态访问控制建立模型。它描述给定的操作被调用后带来角色授权的改变，而角色不能拥有某个视图，用 assign 视图 from 角色表示；反之，用 assign 视图 to 角色表示。图 5 表示调用完操作 processRegisterRequest 后，将 CustomerRegistrationProcess 等视图授权给角色 staff，而将 CustomerBookListRestricted 等视图授权给角色 customer，即表示了访问控制权限动态地改变。

```
schema BusinsessRegistration controls BusinessRegistration
{processRegisterRequest}
assigns CustomerRegistrationProcess, CustomerBookListFull,
                                                    BookSearch to staff
assigns CustomerRegistration,CustomerBookListRestricted,
                                                    BookSearch to customer
```

图 5 VPL 模式声明

2 访问控制策略的执行

这部分描述在 Web 服务下执行 VPL 表示的访问控制策略的基础结构。这个结构中包含了执行 VPL 所描述策略的 Raccoon[2]结构。

2.1 Raccoon 结构

Raccoon 结构包含了处理 VPL 策略的开发工具以及定义角色视图的存储库(即角色、视图服务器)。视图角色服务器可以使用图形管理工具来处理,访问控制决策依据这些存储库来决定。

图 6 为 Raccoon 结构的主要部分。角色服务器包含了用户所有的角色证书,当一个客户在系统中认证时,客户得到所有属于自己的角色证书;而当客户端调用服务器端的某个操作时,相应的角色证书被传送。此调用由拦截器拦截,拦截器传送客户端信息给访问决策对象。如果客户端被准许调用此操作,访问决策对象依据给出的角色以及策略来决策。请求策略分布在服务器上,如果策略允许客户调用操作,那么拦截器给服务器发送一个请求;如果不允许,则此访问被拒绝。

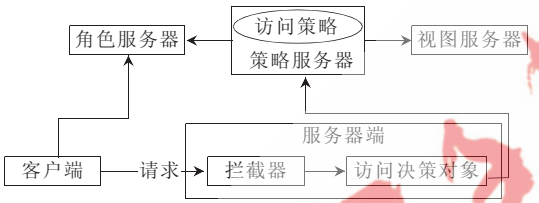

图 6 Raccoon 结构

2.2 Web 服务访问控制的实现

Web 服务访问控制的实现使用 Raccoon 来管理和执行 VPL 策略,即通过获取 SOAP 消息,让 Raccoon 做出访问控制的决策,依赖于 Raccoon 的决策,来拒绝或者发送 SOAP 消息。因为消息在服务器端加密,客户证书在服务器端传输,因此把 HTTP 作为传输协议。

2.2.1 Web 服务部署

此结构中,把 Web 服务部署在 Apache Tomcat 服务器上,同时使用 Axis 引擎。Axis 本质上是一个 SOAP 引擎,提供创建服务器端、客户端和网关 SOAP 操作的基本框架[3]。使用 Axis 是为了利用 Axis handler 概念。handler 是 SOAP 消息的特殊部分,例如,handler 可以控制消息发送方在允许消息被服务器处理之前对其执行身份验证。

2.2.2 策略部署

Web 服务的 VPL 策略部署在策略服务器中。由于 Raccoon 是基于 CORBA 的,所以部署 VPL 策略需要 CORBA 接口库。接口使用 IDL 语言描述,IDL 语言由 WSDL 演变而来。这种演变可以由 XSL 样式表转换,例如,WSDL 中 portTypes 对应了 IDL 的 interfaces,operations 对应了 IDL 的 operations,WSDL 操作中<input>元素对应了 IDL 中的参数 in,<output>对应了 IDL 中的参数 out。

2.2.3 用于访问决策的 Axis handler

Axis handler 充当 CORBA 客户端与角色以及策略服务器通信的中介。当 SOAP 消息通过 handler,handler 从 SOAP 消息中获取用户信息(如证书)以及请求的方法名以及参数。这些证书用于从 Raccoon 角色服务器中获取用户的角色证书。角色服务器中存放了用户证书和角色之间的关系。策略服务器包含了视图以及视图和角色之间的关联。基于客户角色,handler 决定是否允许访问 Web 服务操作。如果访问被拒绝,将抛出异常;否则,SOAP 消息被发送给 Web 服务。

本文使用 VPL 来描述 Web 服务的访问控制需求。VPL 以及相应的访问控制模型来源于基于 CORBA 的应用。通过扩展 VPL 来覆盖所有的 Web 服务需求。提出了一种用于实现基于 Web 应用的访问控制策略的结构,同时也为 Web 服务安全管理提供部署和管理工具。

VPL 可以用于描述 XACML 规范,可以通过样式表将 VPL 转换成 XACML。后期工作主要集中于将 Raccoon 结构转化为 XACML 模型,为其他系统提供互操作性,例如 jiffyXACML 或者 sun'sXACML。

参考文献

[1] 张赛男.软件系统 UML 建模与其安全建模的集成[J].计算机工程,2007,33(8):86-88.

[2] BROSE G. Raccoon-an infrastructure for managing access control in CORBA[C]. Proceeding Conference on Distributed Applications and Interoperable Systems (DAIS), Paris, France, 2004.

[3] PAPAZOGLOU M P.Web 服务:原理与技术[M].龚玲,张云涛,译.北京:机械工业出版社,2010.

(收稿日期:2011-01-03)

作者简介:

张赛男,女,1979 年生,讲师,硕士,主要研究方向:软件工程,分布式计算,网络安全。