第 36 卷 第 3 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.3 Computer Engineering February 2010
·博士论文· 文章编号：1000—3428(2010)03—0010—03 文献标识码：A 中图分类号：TP309

Web 服务中基于信任的访问控制

马晓宁，冯志勇，徐 超
(天津大学计算机科学与技术学院，天津 300072)

摘 要：将安全断言标记语言和可扩展的访问控制高标识语言相结合，设计一种 Web 服务下的基于信任的访问控制模型。在信任域内，服务提供方利用与请求方的直接交互经验和域内其他证人的推荐信任信息，进行信任评估和授权，该模型包括认证模块和访问控制模块。认证模块实现单点登录的功能，访问控制模型实现基于信任的访问控制和授权功能。

关键词：Web 服务；信任；访问控制；安全断言标记语言

Trust-Based Access Control in Web Service

MA Xiao-ning, FENG Zhi-yong, XU Chao
(School of Computer Science and Technology, Tianjin University, Tianjin 300072)

【Abstract】This paper designs a WS-TBAC(Trust-Based Access Control for Web Service) model by using Security Assertion Markup Language(SAML) and eXtensible Access Control Markup Language(XACML). In trust region, providers use direct interactive experience and recommended trust information from other witness in the region, to evaluate requestors' trust and decide whether to give authorization or not. This model includes authentication module and access control module. Authentication module realizes single sign on, and access control module realizes access control and authorization based on trust.

【Key words】Web service; trust; access control; Security Assertion Markup Language(SAML)

1 概述

Web 服务凭借其标准化、松散耦合、语言与平台的无关性以及开放性等特点，迅速地成为了企业跨平台应用集成的首选。安全和信任是 Web 服务最重要的需求之一。当前，OASIS 已经发布了一系列的 Web 服务安全规范，主要有 WS-Security 系列规范、安全断言标记语言 Security Assertion Markup Language(SAML)[1]规范、可扩展的访问控制高标识语言 eXtensible Access Control Markup Language(XACML)[2]规范，并提出 WS-Trust 规范和 WS-Federation 规范提供对信任的支持，通过交换安全令牌在不同的信任域之间发布和分发信任状(credential)，但该模型主要针对 Web 服务安全的认证方面，并不提供信任评价和信任决策的支持。

本文针对 OASIS 发布的诸多关于 Web 服务安全的规范不能满足服务提供者利用对服务请求方的信任信息进行信任评估并根据信任评估结果进行授权和访问控制的问题，将信任机制引入访问控制中，提出了一种 Web 服务下的基于信任的访问控制模型(Trust-Based Access Control for Web Service, WS-TBAC)。

该模型将 SAML 和 XACML 相结合，在固定的信任域之内，服务提供方利用与请求方的直接交互经验和域内其他证人的推荐信任信息，计算对请求方的信任度，与自身预先设定的授权的信任标准进行比较，然后根据比较结果进行决策和授权。该模型包括使用 SAML 的认证模块和使用 XACML 的访问控制模块 2 个部分。

2 模型整体架构和流程

在域内存在 4 种实体：服务请求方，服务提供方，中心认证服务器和提供信任信息的证人。模型整体的架构和流程如图 1 所示。首先，服务请求方在域内的中心认证服务器进行注册，这样才能够在以后的交互过程中对服务请求方进行认证。中心认证服务器使用 SAML。域内其他实体均已在中心认证服务器处完成注册。

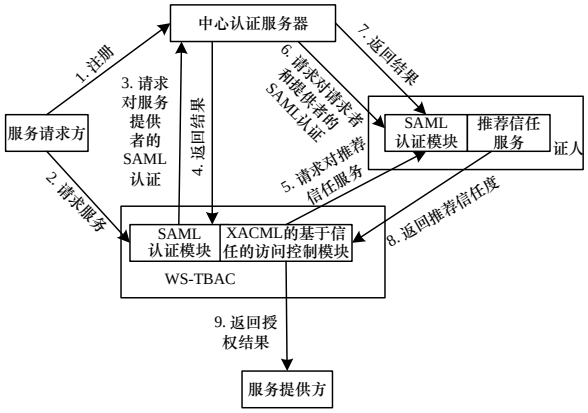

图 1 模型架构和流程

服务提供方在获得请求方的服务请求之后，其 SAML 认证模块要完成认证的功能，向中心认证服务器发送 SAML 请求，中心认证服务器返回验证结果。在验证成立后，XACML 的基于信任的访问控制模块要对服务请求进行授权决策，在决策过程中，需要向域内其他证人请求推荐信任。

证人在获得提供方的推荐信任服务请求之后，需要对服

基金项目：国家“863”计划基金资助项目“面向解决方案的服务架构及支撑环境”(2007AA01Z130)

作者简介：马晓宁(1979－)，男，博士研究生，主研方向：面向 Web 服务和 SOA 环境下的安全与信任；冯志勇，教授；徐 超，博士研究生

收稿日期：2009-08-06 **E-mail：**mxn@tju.edu.cn

务提供方和请求方进行认证，由 SAML 认证模块完成，然后将对请求方的推荐信任度发送给服务提供方。

最后，提供方利用自身的访问控制策略对请求方进行信任评估和决策，返回授权结果。

3 认证

服务提供方和证人的 SAML 认证模块具有相同的结构。图 2 显示了 SAML 认证模块的结构和与中心认证服务器的交互。

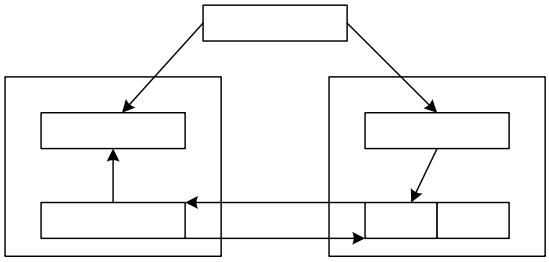

图 2 SAML 认证过程

当认证过程的客体是服务请求方时，认证主体是服务提供方，认证的对象是服务提供方；而当认证过程的客体是服务提供方时，认证主体是提供推荐信任信息的证人，认证的对象是服务提供方和服务请求方。认证过程如下：

(1)认证客体(服务请求方或者是服务提供方)在中心认证服务器上进行注册。

(2)认证客体向认证主体发送服务请求(请求获得服务，或请求获得推荐信任的信息)。

(3)认证主体的拦截器拦截客体的请求，重定向到 SAML 响应器。

(4)SAML 响应器向中心认证服务器发送 SAML 认证断言请求。

(5)中心认证服务器在信息库中查询认证客体的信息。

(6)中心认证服务器将结果以认证断言的形式返回。

4 访问控制

服务提供方在完成认证之后，其认证模块将服务请求转发到访问控制模块，对服务请求方进行信任评估和决策。

图 3 示出了访问控制的架构。该模块由策略管理、信任度计算和决策授权 3 个部分组成。

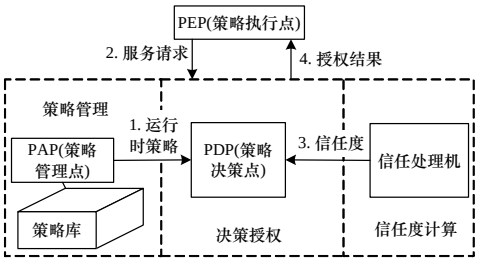

图 3 访问控制模块架构

4.1 策略管理

策略是 XACML 的核心，包含了大量的标签[3]。在 WS-TBAC 的策略模型中，<target>标签是该策略集(策略、规则)的索引，用于查找某个访问控制请求所适用的策略集(策略、规则)，其中，<subject>定义了适用的访问请求主体，例如，<subject>anysubject</subject>表示适用于任何主体；<resource>标签定义了适用的客体，如某个 Web 服务的 wsdl 文件；<action>标签定义了主体请求获得的行为，如 Web 服务的执行(execute)。而<condition>标签是 Web 服务下 TBAC 策略模型中最重要的标签之一，它定义了被授权所必须满足的信任条件，其中包括 2 个主要的部分：信任度标准(trust_standard)和信任度比较函数(function: trust_compare)。在获得该服务提供方对该访问请求方的信任度之后，利用信任度比较函数比较信任度标准和该请求方的信任度，相应地返回 true 或 false。WS-TBAC 策略模型如图 4 所示。

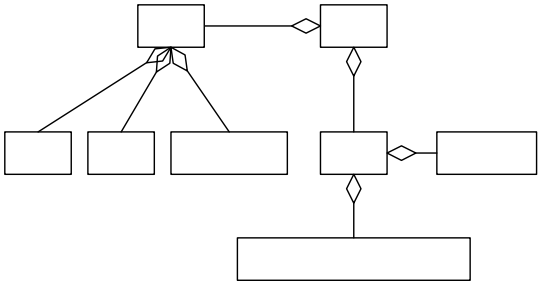

图 4 WS-TBAC 策略模型

4.2 信任度计算

本文选择 regret[4]系统中的算法计算信任度，包括：双方直接交互信息，称为个体纬度；来自于域中其他证人的信息，称为社会纬度。最后将两者进行综合。

个体纬度的信任度有如下的公式：

$$T_{\ p}(\varphi)=\sum_{o_i\in ODB_{\varphi}^{p,r}}\rho(t,t_i)\times Imp(o_i,\varphi)$$

该式利用双方以往的直接交互结果计算服务提供方对服务请求方的信任度，是对所有参考事件的信任评价的综合。其中，φ 是用于计算直接信任度的不同事件的类型，不同类型的事件对直接信任度计算的影响是不同的；$ODB_{\varphi}^{p,r}$ 被定义为服务提供方 p 与服务请求方 r 之间发生的、对应于事件类型 φ 的所有结果的集合；$T_{\ p}(\varphi)$ 被定义为服务提供方 p 与服务请求方 r 之间的对应于事件类型 φ 的直接信任度；t 为当前时间，t_i 是事件发生的时间，$\rho(t,t_i)$ 表示该事件随着时间的推移对直接信任计算的衰减，$\rho(t,t_i)$ 是时间的函数，其中，$\frac{f(t_i,t)}{\sum_{o_j\in ODB_{\varphi}^{p,r}}f(t_j,t)}$ 的形式由服务提供方选择，文献[4]给出的比较简单的形式是 $f(t_i,t)=\frac{t_i}{t}$；$Imp(o_i,\varphi)$ 表示在事件 i 中，提供方 p 对请求方 r 的信任评价；$Imp(o_i,\varphi)=g(X_i^S-X^C(\varphi_i))$，$X^C(\varphi)$ 表示提供方对事件类型为 φ 的事件的预期收益；X_i^S 表示事件 i 的实际收益，函数 g 表示服务提供方根据事件 i 实际收益与预期收益的差值而做的信任评估，g 的具体形式由服务提供方选择，文献[4]给出的是 $g(x)=\sin(\frac{\pi}{2}x)$。令 $a(\varphi)$ 表示事件类型为 φ 的信任度在总信任度中占的权重，$\sum_{\varphi}a(\varphi)=1$，则总的直接信任度 $T_{\ p\to r}^{\ D}=\sum_{\varphi}[a(\varphi)\times T_{\ p\to r}^{\ D}(\varphi)]$。信任度的取值区间为[-1, 1]。

社会纬度的信任度是域内所有证人提供的推荐信任度的平均值。有如下的公式：$T_{\ p\to r}^{\ w}=\frac{1}{n}\sum_{w}T_{p\to w}\times T_{w\to r}$。其中，$T_{p\to w}$ 是服务提供方对域内证人的信任度；$T_{w\to r}$ 是证人对服务请求方的信任。在服务提供方计算请求方的信任度时，需要使用域内其他证人的推荐信任度，此时，该服务提供方向域内其

他的证人发送推荐信任请求，在证人对服务提供方和请求方进行认证之后，返回响应的推荐信任度。

最后，信任度的计算式是 $T_{p\to r} = \varepsilon \times T_{p\to r}^{D} + (1-\varepsilon)\times T_{p\to r}^{w}$。其中，$\varepsilon$ 是来自于直接交互经验的个人纬度的信任度的权重。图 5 示出了信任计算部分的结构。首先，对信任处理机进行初始化，输入相应的计算公式，公式采用 XML 格式表示。然后，信任度计算所需的数据，同样采用 XML 格式表示，经过解析器的解析存入数据库中，信任处理机利用数据库中的数据计算信任度并将结果发送给策略决策点(PDP)。

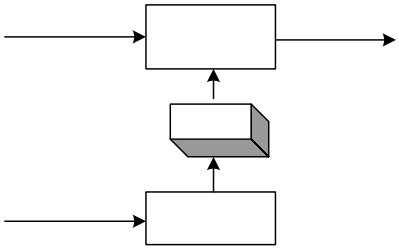

图 5　信任计算结构

4.3　决策和授权

决策和授权由 PDP 完成。策略决策点通过比较服务请求方的信任度和策略文件中<condition>标签中的信任标准进行决策。当比较的结果返回为 true 且 effect 的值为 permit 时，返回结果为授权；反之，则为拒绝授权。

5　结束语

本文提出了一种 Web 服务下基于信任的访问控制模型 WS-TBAC。该模型的优点是能够和 OASIS 发布的诸多 Web 服务安全规范兼容。WS-TBAC 与认证代理类似，是存在于服务请求方与服务提供者之间的中间件系统，WS-TBAC 代替所有的服务提供者完成信任计算和评估工作，而信任计算的算法和信任信息及策略又来自于服务提供者，所以，计算得到的信任度和授权决策结果是服务提供者可信赖的。服务提供者只需要验证请求方提供的信任令牌，就可以实现基于信任的授权和访问控制。认证模块实现了单点登录的功能，在认证过程中，认证的客体只要提供一次认证信息，大大简化了请求服务和推荐信任信息分享过程中的认证复杂度。

参考文献

[1] OASIS. Profiles for the OASIS Security Assertion Markup Language(SAML) Version 2.0[Z]. (2005-03-15). http://docs.oasis-open.org/security/SAML/v2.0/SAML-profiles-2.0-os.pdf.

[2] OASIS. eXtensible Access Control Markup Language(XACML) Version 2.0. Working Draft 09[Z]. (2004-04-16). http://www.oasis-open.org/ committees/download.php/6433/oasis-XACML-2.0-core-wd-09.zip.

[3] Christopher S, Ramesh N, Ray L. 安全模式：J2EE、Web 服务和身份管理最佳时间与策略[M]. 北京：机械工业出版社, 2006.

[4] Sabater J, Sierra C. Reputation and Social Network Analysis in Multi-Agent Systems[C]//Proceedings of the 1st International Joint Conference on Autonomous Agents and Multi-Agent Systems. Bologna, Italy: [s. n.], 2002: 475-482.

编辑　张正兴

（上接第 9 页）

参考文献

[1] Pagnia H, Vogt H, Gartner F. Fair Exchange[J]. The Computer Journal, 2003, 8(2): 55-75.

[2] Kremer S, Markowitch O. An Intensive Survey of Fair Non-repudiation Protocols[J]. Computer Communications, 2002, 25(17): 1601-1621.

[3] Asokan N, Schunter M, Waidner M. Optimistic Protocols for Fair Exchange[C]//Proc. of the 4th ACM Conference on Computer and Communications Security. Zurich, Switzerland: ACM Press, 1997: 8-17.

[4] Kremer S, Raskin J. Game Analysis of Abuse-free Contract Signing[C]//Proc. of the 15th IEEE Computer Security Foundations Workshop. Washington D. C., USA: IEEE Computer Society Press, 2002: 206-220.

[5] Kremer S, Raskin J. A Game-based Verification of Non-repudiation and Fair Exchange Protocols[J]. Journal of Computer Security, 2003, 11(3): 399-429.

[6] Kremer S. Formal Analysis of Optimistic Fair Exchange Protocols[D]. Brussels, Belgium: Universit'e Libre de Bruxelles Facult'e des Sciences, 2004.

[7] 张　梅，文静华，张焕国. 基于 ATL 方法的电子商务协议 FONRP 分析[J]. 计算机工程, 2008, 34(3): 151-153.

[8] 刘英杰，姚正安. 一种分析安全协议的新逻辑[J]. 计算机工程, 2007, 33(03): 163-166.

[9] 沈海峰，薛　锐，黄河燕. 用串空间分析公平交换协议[J]. 小型微型计算机系统, 2006, 27(1): 62-68.

[10] 董荣胜，陈大伟，郭云川，等. 公平非否认协议的有限状态分析[J]. 计算机科学, 2005, 32(8): 83-86.

[11] Thayer F J, Herzog J C, Guttman J D. Strand Spaces: Proving Security Protocols Correct[J]. Journal of Computer Security, 1999, 7(2/3): 191-230.

[12] Guttman J. Key Compromise, Strand Spaces, and the Authentication Tests[J]. Electronic Notes in Theoretical Computer Science, 2001, 47(1): 1-21.

[13] Li Xiangdong, Wang Qingxian. An Improvement of Authentication Test for Security Protocol Analysis[C]//Proceedings of 2007 International Conference on Computational Intelligence and Security Workshops. [S. 1.]: IEEE Computer Society Press, 2007: 745-748.

[14] Asokan N, Shoup V, Waidner M. Asynchronous Protocols for Optimistic Fair Exchange[C]//Proceedings of IEEE Symposium on Research in Security and Privacy. [S. 1.]: IEEE Computer Society Press, 1998: 86-99.

[15] Kremer S, Markowitch O. Fair Multi-party Non-repudiation[J]. International Journal on Information Security, 2003, 1(4): 223-235.

编辑　索书志