Web 服务中基于信任的跨域安全认证模型

卢晓霞，韩坚华
（广东工业大学 计算机学院，广东 广州 510006）

摘 要：在分析 XCAML 和 WS-Security 安全规范的基础上，设计出一种基于信任的跨域安全认证模型 TB-WSCDSA。该模型解决了跨域服务双方身份认证的问题，并依据各自安全域的访问控制策略和信任计算所需的数据和算法，计算双方的信任度，根据信任度阈值比较结果对双方进行信任评估和授权，并将结果以信任证书的方式发送给服务双方以保证安全通信。

关键词：Web 服务；信任；身份认证；数字证书
中图分类号：TP393.4 **文献标识码**：A **文章编号**：1674-7720(2012)03-0050-03

Trust-based cross-domain security authentication of Web service

Lu Xiaoxia, Han Jianhua
(College of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: This paper designs a trust-based cross-domain security authentication of Web service(TB-WSCDSA)based on XCAML and WS-Security. This model resolves the problem of cross-domain authentication, and computes trust value of both sides according to algorithm and datum about trust computation and policy from providers and requestors. Finally, TB-WSCDSA decides whether to give both sides authorization based on policy, and gives trust certificate that containes the result of authorization to make sure communication security.

Key words: Web service; trust; identity authentication; digital certificate

Web 服务凭借其松散耦合、语言与平台无关以及开放、标准化等优点，已经成为企业跨平台应用集成的首选[1]。但是，Web 服务的安全及信任仍然是制约其发展的最大阻碍。当前，OASIS 已经发布了一系列的安全规范，主要有 WS-Security 规范、安全断言标记语言 SAML 规范、可扩展的访问控制高标识语言 XCAML 规范，而且又提出 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安全域通信双方建立信任[2]，但是这主要还是针对 Web 服务安全的身份认证，并没有提供如何进行信任评价和信任决策。

本文针对 OASIS 发布的关于 Web 服务安全规范不能满足服务双方利用信任信息进行信任评估和决策授权的问题，将信任机制引入身份认证及访问控制中，提出了一种 Web 服务中基于信任的跨域安全认证模型 TB-WSCDSA (Trust-Based Cross-Domain Security Authentication of Web Service)。该模型能够解决服务提供方与请求方跨域认证的问题。它将 PKI 数字证书与 XCAML 相结合，通过一个可信的第三方机构对不同安全域的服务双方进行认证，利用双方的直接交互经验及各自域内其他证人的推荐信任信息，计算信任度，并与自身预先设定好的信任标准或信任度阈值进行比较，然后根据比较结果进行决策和授权。决策结果保存在信任证书中，发送给服务请求方和提供方，作为双方信任并进行通信的依据。

1 模型框架

TB-WSCDSA 模型是基于 XCAML 和 PKI 数字证书的。图 1 是 TB-WSCDSA 模型图。首先，服务请求方及提供方都从本域内的 CA 认证机构获取自己的数字证书，这样才能在交互过程中进行彼此认证。可信的第三方认证机构使用 PKI 的 CA 认证。这里认定，可信的第三方认证机构已经与双方的根 CA(信任锚)建立信任关系[3]。

服务双方认证完成后，将各自的数字证书以及第三方认证结果发送到模型中的认证模块进行验证。在确认服务双方的身份后，模型的 XACML 的访问控制模块通过计算信任度决定是否发送信任证书给请求方或提供

方。最后,请求方使用该信任证书向提供方请求服务,提供方使用该信任证书决定是否提供服务。

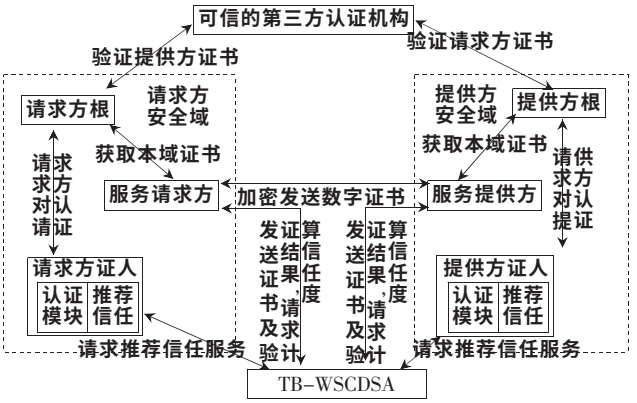

图 1 TB-WSCDSA 模型图

2 框架流程图

TB-WSCDSA 主要由认证、策略管理、信任度计算和决策授权四部分组成。图 2 显示了 TB-WSCDSA 的架构和流程。

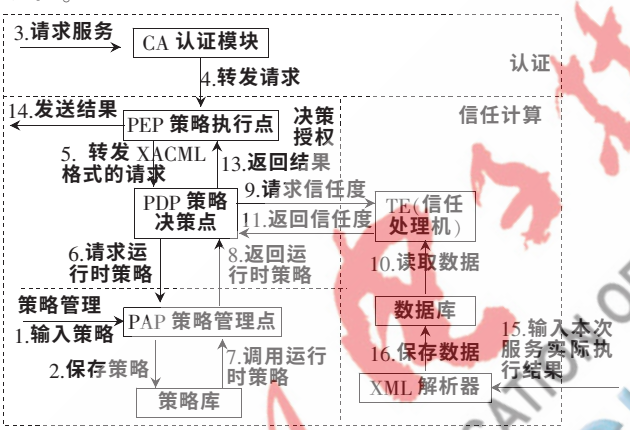

图 2 TB-WSCDSA 架构和流程图

2.1 认证

身份认证是 TB-WSCDSA 模型的基础,只有确定了服务双方的身份以后,才能够根据相关信任信息进行信任评估和授权决策。该认证过程是跨安全域的,包括服务请求方、请求方所在域的根 CA 机构(信任锚)、服务提供方、提供方所在域的根 CA 机构(信任锚)[3]、已经与双方根 CA 建立信任关系的可信的第三方信任机构以及 TB-WSCDSA。图 3 显示了认证过程。认证过程如下:

(1)服务请求方及提供方从各自所在安全域的根CA 机构获得本域数字证书。

(2)取得本域数字证书后,请求方加密发送数字证书给提供方,提供方收到后用自己的私钥解密,并通过本域的根 CA 发送到可信第三方机构进行认证,提供方同样将自己的数字证书发送给请求方进行认证。

(3) 可信的第三方 CA 机构对服务双方认证完成后,返回认证结果。

(4)服务请求方和提供方从第三方接收到认证结果

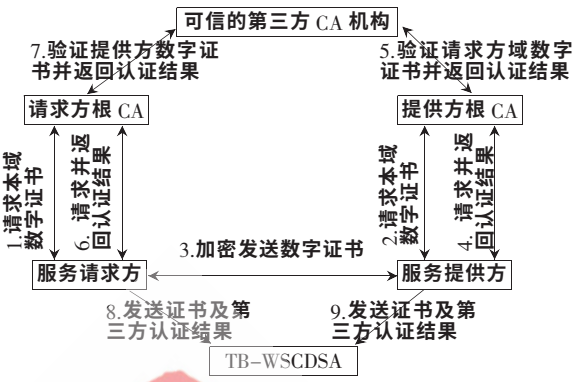

图 3 认证过程示意图

后,将对方的数字证书及第三方认证结果打包加密发送到 TB-WSCDSA 模型的认证模块;认证模块验证服务双方提供的证书及结果,完成认证。

2.2 访问控制策略管理

服务双方在完成认证后将结果发送到 TB-WSCDSA 模型的认证模块,认证模块通过请求方域及提供方域证人的请求推荐信任、双方的数字证书以及第三方认证结果后,将服务请求转发到访问控制模块,再对双方进行信任评估和决策。访问控制模块包括策略管理、信任度计算和决策授权 3 个部分。

策略是 XACML 的核心,XACML 定义了标准的策略语言模型[1]。在 TB-WSCDSA 的策略模型中,<target>标签是该策略集(策略、规则)的索引,用来查找某个访问控制请求所适用的策略集或策略规则;<subject>标签定义了适用的访问请求主体,如<subject>any subject</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);<condition>标签是 TB-WSCDSA 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,其中包括信任度阈值(trust_ threshold)和信任度比较函数(function:trust_comparison)两个主要部分。在获得服务双方的信任度之后,利用信任度比较函数来比较该信任度是否满足信任度阈值(trust_threshold)的要求,相应地返回 true 或 false。

2.3 信任度计算

TB-WSCDSA 中的信任计算部分由 XML 解析器、数据库和信任处理机三部分组成。TB-WSCDSA 计算直接信任度的信息来自于服务双方。首先,服务双方初始化各自的信任处理机,得到了信任度的计算方法。信任度计算所必需的数据用 XML 文件发送到 XML 解析器中,解析后保存在数据库相应的表格之内。在计算信任度时候,信任处理机从数据库中读取相应的数据进行计算。本文计算的信任度包括双方直接交互信息(称为个体纬度)和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[4]。

个体纬度的信任度公式如下：

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

该式利用双方以往的直接交互结果计算信任度，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 被定义为所有出现的结果的集合；$ODB_{\varphi}^{p,r}$ 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的所有结果的集合；$T_{p\xrightarrow{D}r}(\varphi)$ 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；$\rho(t,t_i)$ 中的 t 是当前时间，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度计算的衰减，$\rho(t,t_i)=\dfrac{f(t_i,t)}{\sum_{o_j\in ODB_{\varphi}^{p,r}}f(t_j,t)}$，其中 $f(t_j,t)$ 的形式由服务双方选择；$\mathrm{Im}\rho(o_i,\varphi)$ 表示在事件 i 中，服务提供方 p 对请求方 r 的信任评价或服务请求方对提供方的信任评价，$\mathrm{Im}\,\rho(o_i,\varphi)=g(X_i^s-X^C(\varphi_i))$，$X^C(\varphi)$ 表示提供方或请求方对事件的预期收益；X_i^s 表示事件的实际收益，函数 g 表示服务提供方或请求方根据事件实际收益与预期收益的差值而做的信任评估，g 的具体形式也由服务双方选择。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，$\sum_{\varphi}a(\varphi)=1$，则总的直接信任度为 $T_{p\xrightarrow{D}r}=\sum_{\varphi}[a(\varphi)\times T_{p\xrightarrow{D}r}(\varphi)]$。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。其公式为：$T_{p\xrightarrow{w}r}=\dfrac{1}{n}\sum_{w}T_{p\to w}\times T_{w\to r}$。对服务提供方来说，$T_{p\to w}$ 是提供方对请求方域内证人的信任度，$T_{w\to r}$ 是证人对服务请求方的信任；对服务请求方来说，$T_{p\to w}$ 是请求方对提供方证人的信任度，$T_{w\to r}$ 是证人对服务提供方的信任。在服务提供方计算请求方的信任度时，需要使用请求域内其他证人的推荐信任度，此时，该服务提供方向请求域内其他的证人发送推荐信任请求，在证人对请求方进行认证之后，返回相应的推荐信任度。同样地，在服务请求方计算提供方的信任度时，需要使用提供方域内其他证人的推荐信任度，此时，该服务请求方向提供方域内其他的证人发送推荐信任请求，在证人对提供方进行认证后，也返回相应的推荐信任度。

最后，信任度的计算式为：$T_{p\to r}=\varepsilon\times T_{p\xrightarrow{D}r}+(1-\varepsilon)\times T_{p\xrightarrow{w}r}$。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。信任计算的结构如图 4 所示。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。最后，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）。

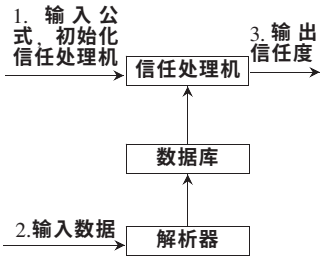

图 4 信任计算结构

2.4 决策和授权

决策和授权由 PDP 完成，就是根据访问控制策略和信任度来决定是否给予授权的过程[5]。其决策的过程如下：

（1）解析服务双方的服务请求，获取<subject><resource><action>和<environment>标签（<environment>标签可能不存在）。

（2）根据以上 4 个标签查找<target>与此相匹配的策略文件 policy.XML。

（3）如果存在相应的策略文件，则进行步骤（4）；否则，返回 not-applicable，访问控制决策失败。

（4）解析 policy.XML 中 rule 的<condition>标签，获得信任度比较函数 trust_comparison 和信任度阈值 trust_threshold，请求获取服务提供方对该服务请求方的信任度 requestor_trust 以及服务请求方对提供方的信任度 provider_trust。

（5）返回服务双方的信任度 requestor_trust 和 provider_trust。

（6）根据<condition>标签中定义的信任度比较函数 trust_comparison，比较服务双方的信任度 requestor_trust 和 provider_trust 是否大于等于各自的信任度阈值 trust_threshold，如果是，则返回 true；否则，返回 false。

（7）验证返回值是 true 还是 false，如果是 true，则返回<effect>标签值 permit；否则，返回 deny。

最后，PDP 将决策的结果发送给 PEP，PEP 将决策结果封装在信任证书中发送给服务请求方和服务提供方。服务请求方利用 TB-WSCDSA 提供的信任证书向服务提供方请求服务，而服务提供方利用信任证书授权请求方使用服务。

本文提出了一种 Web 服务下基于信任的跨域认证模型 TB-WSCDSA。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。TB-WSCDSA 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，TB-WSCDSA 代替服务提供方和请求方，完成信任计算和评估工作，而信任计算的算法、信任信息及策略又来自于服务双方。因此，计算得到的信任度和授权决策结果是服务双方可信赖的。服务双方只需要验证各自通信时提供的信任证书，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] 马晓宁，冯志勇，徐超.Web 服务中基于信任的访问控制[J].计算机工程，2010，36(3)：10-12.

[2] PAPAZOGLOU M P. Web 服务原理和技术[M].北京：机械工业出版社，2009.

[3] 俞旭.PKI 中几种信任模型的分析研究[C].江苏省电力安全论坛论文集，2004：351-356.

[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.

[5] 冯晓宁，冯志勇，徐超.Web 服务中跨安全域的基于信任的访问控制模型 [J]. 计算机应用研究，2009，26(12)：4751-4753，4767.

(收稿日期：2011-09-06)

作者简介：

卢晓霞，女，1986 年生，硕士研究生，主要研究方向：Web 安全。

韩坚华，女，1955 年生，教授，主要研究方向：互联网计算。