浙江理工大学学报,第 28 卷,第 4 期,2011 年 7 月
Journal of Zhejiang Sci-Tech University
Vol. 28, No. 4, Jul. 2011

**文章编号**: 1673-3851 (2011) 04-0631-07

# 基于 SAML 面向服务架构安全模型研究

**谢玉开, 周　莉**
(浙江理工大学经济管理学院, 杭州 310018)

**摘　要**: 为了解决目前主流的基于 WS-security 的面向服务安全框架中的安全脆弱性问题,保证面向服务架构中 Web 服务的安全,通过采用将安全语句封装在 SAML 断言语句块中,创建 SAML 认证声明及进行 SAML 授权等为服务响应模块提供安全断言,并通过网络层和服务层的安全实现来保证 Web 服务的安全和实现用户的单点登录等。

**关键词**: 面向服务架构模型; 安全断言标记; 单点登录
**中图分类号**: F490.6;TP393.08　　**文献标识码**: A

## 0　引　言

在信息技术发展过程中,为满足信息化建设不断增加的复杂程度、提升软件系统的快速构建和响应业务变化能力、充分利用用户原有 IT 资源、实现跨平台的数据共享和业务协同,面向服务架构(service oriented architecture,SOA)作为一种新的集成方式以其可重用性、松散耦合、粗粒度及互操作性等优点,已经成为目前企业应用集成的主要方法,得到了日益广泛的运用。面向服务架构模式能够更加容易实现跨越企业边界的业务系统自动化和信息共享,但开放的数据访问和 Web 服务调用给商业运作带来便利的同时,也更加容易受到攻击,如果没有提供良好的安全防护机制,开放 Web 服务无疑等于打开了潘多拉宝盒。在未受保护的 SOA 应用中,想要阻止 Web 服务的未授权使用实际上是不可能的;未授权用户可以非常轻松地访问 Web 服务,很容易出现非法用户过多而导致的合法用户的服务拒绝访问 DoS(denial of service)。笔者在简要分析了目前主流的基于 WS-security 的面向服务安全框架及其安全脆弱性的基础上,提出了基于安全断言标记 SAML 的 SOA 安全框架模型,通过实现网络层及服务层的安全来具体构建 SOA 安全性解决方案。

## 1　面向服务安全研究现状

面向服务作为一种新的粗粒度、松耦合的系统架构方式,能够支持动态的企业应用集成。但面向服务架构行业标准的缺乏,面向服务应用中的安全问题成为阻碍 SOA 广泛应用的一大瓶颈。目前面向服务安全的研究重点主要运用 WS-security(Web 服务安全,Web services security)和其它规范结合 XML 安全技术保障 SOAP 通信的安全,但 WS-security 安全规范作为一种安全性构件,本身并不能保证 Web 服务安全性,也不能提供完整的面向服务架构安全性解决方案。

### 1.1　基于 WS-security 的面向服务安全框架

WS-security 协议是一种提供在 Web 服务上应用安全方法的网络传输协议,最初由 IBM、微软、VeriSign 和 Forum Systems 开发,官方名称为 WSS[1]。WS-security 协议包含了关于如何在 Web 服务消息上保证完整性和机密性的规约。在 WS-security 协议中定义了 SOAP(简单对象访问协议,simple object access

收稿日期: 2010－06－21
作者简介: 谢玉开(1985－),男,湖南隆回人,硕士研究生,主要从事面向服务架构、Web 服务安全、企业信息化的研究。

protocol)消息的安全标准和途径,其目标是通过不依赖于传输层的安全来保障服务的安全性。在基于 WS-security 协议的安全框架中主要通过将各种 Web 服务协议、应用层协议与安全传输层协议及各种加密技术结合起来,通过在 SOAP 消息中嵌入安全性机制和安全令牌,实现 Web 服务环境下的消息完整性、数据保密性和对消息及用户身份认证。其安全框架如图 1 所示。

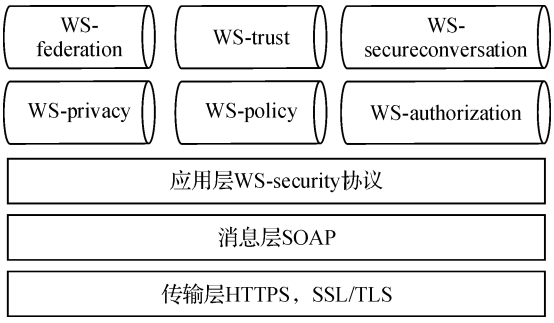


图 1 基于 WS-security 的面向服务安全框架

其中,各种 Web 服务层协议包括 WS-policy(Web 服务策略,Web services policy)、WS-trust(Web 服务信任模型,Web services trust)、WS-privacy(Web 服务隐私策略,Web services privacy)、WS-secureconversation(Web 服务安全会话,Web services secure conversation)、WS-federation(Web 服务联邦信任,Web services federation)、WS-authorisation(Web 服务安全授权,Web services authorisation)等,形成了一个庞大 WS-security 协议规范。a)WS-policy 端点策略:主要描述中间节点和端点上的安全性及其它业务策略上的能力和限制,如所需的安全性令牌、所支持的加密算法和隐私权规则等;b)WS-trust 信任模型:描述如何使 Web 服务能够安全地进行互操作的信任模型的框架,负责处理内部认证和标识的发放;c)WS-privacy 隐私权模型:描述 Web 服务和请求者如何声明主题隐私权首选项和组织隐私权实践声明的模型;d)WS-secureconversation 安全会话:描述如何管理和认证各方之间的消息交换,包括安全性上下文的交换以及会话密钥的建立;e)WS-federation 联邦信任:描述如何管理和代理异类联合的环境中的信任关系,包括支持联邦身份;f)WS-authorization 授权:描述如何管理授权数据和授权策略,定义对访问和交换数据的授权[1]等。

在应用层中,安全性信息作为附加的控制信息以 SOAP 消息的形式进行传递,不依赖任何传输协议。因而,WS-security 规范具有传输独立性,能保证端到端的安全性。这种基于消息级的安全模式相对于传输级(点到点)的安全模式而言,更适合用于分布式异构环境中,还能有效地防止消息在经过中间节点时遭到第三方的破坏。

在消息层中,SOAP 安全扩展定义 XML 加密和 XML 签名如何应用到 SOAP 的标准,这样 SOAP 信息就可以被加密或者签名。SOAP 安全扩展主要用于进行 SOAP 消息控制,由 SOAP 消息拦截器、SOAP 消息拦截网关、SOAP 消息路由器、契约服务管理等模块组成。SOAP 安全规范在 SOAP 的头元素里定义了 XML 数字签名的使用,数字签名经过加密算法计算后的值附加在数据对象后面,数据接受对象从签名中验证数据的来源和完整性。

### 1.2 WS-security 安全框架脆弱性分析

WS-security 安全框架作为一种安全性构件,本身并不能保证 Web 服务安全性,也不提供完整的面向服务架构安全性解决方案。实现 WS-security 并不意味着应用程序不会受到攻击或者安全性不会受到威胁。因此,它需要与其它 Web 服务扩展和更高级的特定应用程序的协议联合使用,以适应多种安全性模型和加密技术。WS-security 安全框架的实质是运用 WS-security 和其它 Web 服务规范结合 XML 安全技术保障 SOAP 通信的安全。虽然制定了许多标准的安全规范,提供了进一步解决 Web 服务安全性问题的诸多方案,但这并不代表它具有很好的通用性和适应性,甚至它提供的有些规范、方案也仅限于理论范畴[6]。

尽管 WS-security 标准有助于 SOAP 消息的加密和签名,但该标准并未涉及任何有关认证、授权和安全策略的内容,且 WS-security 只能提供基本的安全保障,大部分安全标准都是在假定双方已经建立信任的基础上进行操作,而且它们的目的主要是保护单个 Web 服务的安全,对服务组合中的安全问题缺乏考虑。因此,为解决服务组合中存在的安全问题,对各参与方安全能力和安全需求的描述,以及如何在 Web 服务组合流程中实现安全能力与安全需求的自动匹配是目前研究的重点。而安全断言标记 SAML[2](security assertion markup language,SAML)与 WS-security 规范的最大区别在于它以有关多个主体的断言的形式来表述安全性。SAML 安全断言通过定义用来交换身份认证、属性和授权断言的认证、属性和授权决策信息的集合,直接使用 XML 加密和 XML 签名,利用 SAML,网络中的任何点都可以断言它知道用户或数据块的身份,然后由接收应用程序作出决定,如果它信任该断言,则接受该用户或数据块,任何符合 SAML 安全断言

的模块都可以断言对用户或数据的认证,通过使用安全身份断言标记,成功应用 REST 模式,提供 RESTful 安全服务,将认证与被访问的资源分隔开来,实现用户统一单点登录。

## 2　基于 SAML 的 SOA 安全模型及其实现

面向服务技术是最近几年迅速兴起的一种新的系统设计模式,它是一种崭新的分布式服务模型,是 Web 上数据和信息共享和数据集成的有效机制。面向服务架构 SOA 作为构建 IT 系统的一种新的架构模式,能够通过重用现有 IT 资产来构建新的业务应用,并且具有灵活改变的能力以支持未来业务的发展。目前主流的面向服务安全技术主要集中于对网络传输加密,通过运用 XML 相关技术及相关安全规范来保障数据通信的安全,但在面向服务架构中,服务之间跨域操作及异构平台下的松耦合性不是靠简单的几个安全规范和WS-security安全所能保证的。要构建全面的 SOA 安全性解决方案必须集成当前可用的安全技术,具体通过网络层和服务层的安全来保证 Web 服务的安全,采用将安全语句封装在 SAML 断言语句块中,创建 SAML 认证声明及进行 SAML 授权等为服务响应模块提供安全断言,并通过 Web 服务信任和 Web 服务安全策略实现用户的联邦身份认证,实现用户的单点登录等,其安全模型如图 2 所示,模型主要分两部分,即服务层安全和网络层安全等。

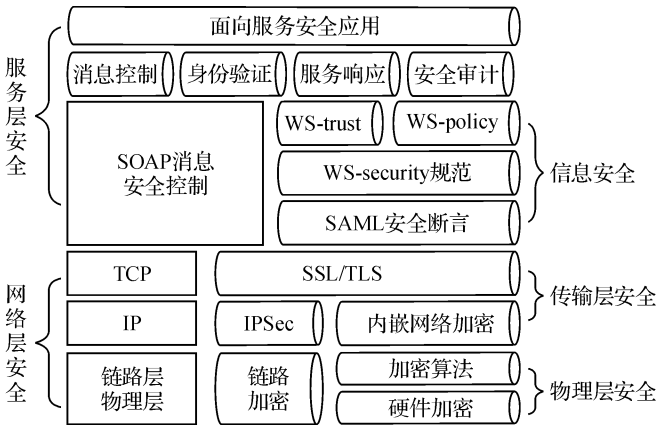


图 2　基于 SAML 的 SOA 安全模型

a)网络层安全可按传输层和物理层分层实现。其中传输层安全主要通过安全套接字层(secure sockets layer,SSL)协议和传输层安全(transport layer security, TLS)协议,结合相应的 IPSec 安全协议来实现。其中,SSL 是一个用来保证安全传输文件的协议,它基于强公钥加密以及 RSA 私钥密码的公开密钥体制和X.509数字证书技术来保护信息传输的机密性和完整性,主要提供三方面的安全服务:用户和服务的合法性认证、加密数据及隐藏传输数据、维护数据的完整性等。而 TLS 则是用于在两个通信应用程序之间提供保密性和数据完整性的安全传输协议,由于 TLS 是独立于应用协议的,所以高层协议可以透明地分布在 TLS 协议上面。TLS 记录协议是一种分层协议,主要由两层组成:TLS 记录协议和 TLS 握手协议。TLS 记录协议支持信息传输、将数据分段到可处理块、压缩数据、应用 MAC、加密以及传输结果等。而 TLS 握手协议通过对等双方在记录层的安全参数上的一致性自我认证,用于管理密钥交换、报警以及密码的修改等。

在底层 TCP/IP 分层结构中,物理层安全主要通过 Web 链路加密及配套的加密算法或硬件加密来保证数据的机密传输和防止未授权用户的非法访问。而网络层安全保障技术主要是 IPSec 安全协议,通过该协议使用两种通信安全协议,即 AH(authentication)和 ESP(encapsulating security payload)为上层提供可互操作的、高质量的且基于密码学的安全性服务。其中,AH 主要负责提供无连接的完整性、数据发起验证和重放保护,结合发送方的数字签名,实现发送方的身份验证和防止第三方的攻击。而 ESP 则提供了一种对 IP 负载进行加密的机制,对数据报中的数据进行加密,防止诸如 Sniffer 之类的网络监听,保证机密信息安全。

b)服务层安全则主要通过 SOAP 消息控制、用户身份验证、SAML 安全断言和安全审计系统,结合 Web 服务模型中相关安全技术如契约管理等来具体实现。在 SOA 安全模型中,用户身份验证和授权发生在基于服务的授权用户数据库检查用户证书的时候。通过侦听 SOAP 消息,并把消息标题头中列出的用户信息与保存在现有安全性基础架构中的用户信息进行比较,便可实现用户身份验证和授权。身份认证保证授权的用户能够进行被授权的资源访问。企业级 SOA 中身份认证不局限于单一安全控制域,往往需要实现跨企业安全控制域的认证活动,安全断言标记语言标准提供了不同安全域之间认证的交互,通过一个标准的认证过程,多方达成一致,使用一组给定的标准来对一组指定的用户进行身份验证,参加这个过程的安全域组成一个身份联邦(identity federation)。联邦身份认证结果以断言方式封装在 SOAP 消息中,各个安全域都

承认认证结果的合法性，所以安全断言也实现了单点登录，SOAP 消息获得的安全断言在整个身份联邦中都是有效的，无需重复认证。

## 3 安全断言模块的实现

在身份验证过程中必须创建 SAML 安全断言，为用户调用的 Web 服务提供用户的真实性安全断言服务。其中，SAML 是一项基于 XML 的交换安全性信息的框架，实现用户的单点登录和保证 Web 服务安全性是 SAML 最重要的用途[3]。SAML 标准中包括了如何在通信协议和框架中使用 SAML 断言描述，即基于 SAML 应用协议消息流和安全机制。在 SOA 安全模型框架中(图 3)，身份认证模块主要通过把 SOAP 消息标题头中包含的用户身份与联合身份验证数据库中列出的用户信息进行匹配，再通过身份验证模块为用户创建代表用户身份的 SAML 断言，并创建唯一指向这个断言的凭证，而服务提供者则使用该凭证来获取 SAML 身份验证断言[4]。因为 SAML 身份验证断言并不随主体一起传输，通过 SAML 身份验证断言，用户访问联邦安全域内的所有 Web 服务时，就只需要一次登录，能够实现在不同的实体间交换有关主体的安全断言信息，实现分布式环境下不同安全服务的互操作性，并保证 Web 服务的安全性[5]。

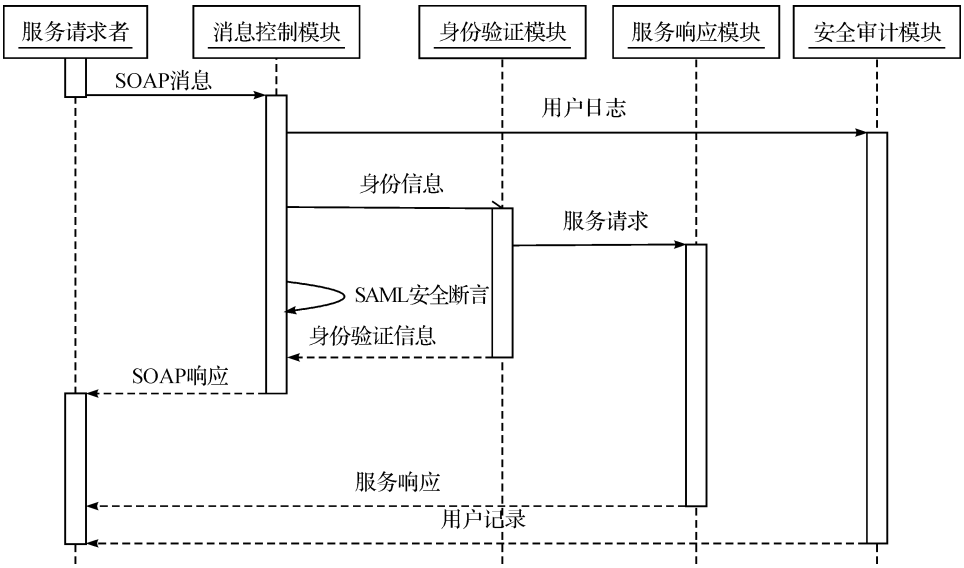


图 3 SOA 安全断言模块实现序列

在 SAML 中，安全语句被封装在断言语句块中。通过创建 SAML 认证声明、SAML 授权决策声明和属性声明，为服务响应模块提供安全断言，包括时间戳、断言 ID 和断言主题等，其中的＜saml：Condition＞元素用来描述断言的有效时间、特定接收者；＜saml：Subject＞元素用来描述认证对象的相关信息；＜saml：AuthenticationStatement＞记录了认证方式、认证时间、安全域等内容；＜saml：AuthnContext＞则记录了授权的依据、权限等信息[7]。

其部分实现示例如下：

```
＜saml：Assertion xmlns：saml= urn：oasis：names：tc：SAML：2.0：assertion
Version＝"2.0" IssueInstant＝"2010－05－20 T 12：00：00Z"＞
＜saml：Conditions NotBefore＝"2010－05－15 T 12：00：00Z"
NotOnOrAfter＝"2010－22－15 T 12：10：00Z"＞
＜/saml：Conditions＞
＜saml：AuthenticationStatement AuthenticationMethod＝"password"
AuthenticationInstant＝"2010－05－20 T 12：00：00＋01：00"＞
＜saml：Subject＞
＜saml：NameID Format＝"urn：oasis：names：tc：SAML：1.1：nameid－format：emailAddress"＞ j.smith@acme.org
```

```
</saml:NameID>
<saml:SubjectConfirmation>
<saml:NameIdentifier>
<SecurityDomain>
"www.vtest.com"
</SecurityDomain>
<saml:NameID format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
JYGH5F901
</saml:NameID>
<saml:SubjectConfirmationDate>
Securitykeyword =X.509 V3
</saml:SubjectConfirmationDate>
<saml:RequesteAuthnContext>
<saml:AuthnContext>
<saml:AuthnStatement AuthnInstant="2010-05-20 T12:00:00Z"
SessionIndex="67775277772">
</saml:AuthnStatement>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:RequesteAuthnContext>
</saml:NameIdentifier>
</saml:SubjectConfirmation>
</saml:Subject>
</saml:AuthenticationStatement>
</saml:Assertion>
```

SAML 安全信息主要包括验证断言、授权决策和主体属性组成,都以称为“断言”的 XML 结构进行描述,SAML 规范通过定义交换断言的协议、传输绑定和使用方案,通过将 SAML 安全断言信息封装到 SOAP 消息中,从而无缝集成到 SOAP 传输中,弥补 WS-security 规范的不足。其部分实现如下所示:

```
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope"
xmlns:S="http://www.w3.org/2001/12/soap-envolope"
xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/07/secext">
<SOAP-ENV:Header>
<Security actor="http://www.vtest.com" mustUnderstand="1">
<BinarySecurityToken Id="X.509 V3" EncodingType="UTF-8"
ValueType="wsse:X.509 V3">
<auth-constraint>
<description>Roles who have access.</description>
<role-name> atlantis </role-name>
</auth-constraint>
<Security-constraint>
<login-config>
```

```
<auth-method>CLIENT-CERT</auth-method>
<realm-name>myrealm</realm-name>
</login-config>
<security-role>
<description>These are the roles who have access</description>
<role-name> atlantis </role-name>
</security-role>
<wsse:Security>
<saml:Assertion MajorVersion="1" MinorVersion="0"
AssertionID="SecurityToken-ef375268"
Issuer="CompanyX"
IssueInstant="2010-05-20 T 12:00:00+01:00"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
    ...
</saml:Assertion>
<wsse:UsernameToken>vtest</wsse:UsernameToken>
<wsse:Password Type="wsse:PasswordDigest">vtest
</wsse:Password>
<wsse:Nonce>JYGH5F901</wsse:Nonce>
</wsse:Security>
</ BinarySecurityToken>
</ Security-constraint >
</SOAP-ENV:Header>
</SOAP-ENV:Envelope>
```

通过在 SOAP 消息中嵌入 SAML 安全断言，可以有效防止使用安全性令牌中可能产生的各种如安全性令牌无法被验证或授权、引用的安全性令牌无法检索和无效的安全性令牌等问题。SAML 安全断言还解决了联邦环境中如何识别身份信息共享的标准化问题，通过 SAML 断言创建身份联邦，用户就能够通过一个单点身份验证关键字进行登录[6]，并且能够在所有类型的 Web 服务项目之间无障碍使用，认证授权用户可以直接使用诸如博客、Wiki 百科等 Web 服务以及其他 Web 协作应用程序，而不需要事先与该应用程序建立关联关系。

## 4 结 语

随着 SOA 应用的日益广泛，对 SOA 增加安全性的需要就变得更加明了，笔者提出了从 SOAP 消息控制、联邦身份验证、契约管理、SAML 安全断言以及安全审计等方面，结合 TCP/IP 模型，在保证底层数据安全传输的基础上来构建 SOA 安全框架模型，实现服务层及网络层安全。具体通过 WS-trust 负责处理内部认证和标识的发放，WS-policy 描述中间节点和端点上的安全性及其它业务策略上的能力和限制，WS-security 规范实现对 SOAP 的消息控制，通过安全断言标记 SAML 提供在不同的实体间交换有关主体的安全断言信息，实现分布式环境下不同安全服务的互操作性，保证 SOA 服务的安全性。

**参考文献：**

[1] OASIS Standard 1.1 WS-Security Version 1.1[S].

[2] OASIS Standard 2.0 Secutiry Assertion Markup Language(SAML)v2.0[S].

[3] Gustavo Alonso. Securing Web Services (WS-Security, SAML)[C]. Swiss Federal Institute of Technology (ETHZ), 2007.

[4] 李　瑞, 陶　明. 基于 WS-security 的 Web 服务安全的实现[J]. 计算机与现代化, 2008(12): 131-133.
[5] Thoma Grob. Security analysis of the SAML single sign-on brower[D]. IBM Zurich Research Laboratory, 2003.
[6] 韩　伟, 范植华. 基于 SAML 的单点登录技术在 Web 服务中的应用研究[J]. 计算机工程与设计, 2005, 26(3): 634-636.

# Research on the Secure Model of Service-Oriented Archtecture Based on SAML

*XIE Yu-kai*, *ZHOU Li*
(School of Economics and Management, Zhejing Sci-Tech University, Hangzhou 310018, China)

**Abstract**: In order to solve the safety vulnerability problems of the mainstream SOA Security framework based on the WS-security, ensure the security of service in the service oriented architecture, the author put forward the secure model of service oriented archtecture framework based on the security assertion markup language, mainly focusing on the network layer and service layer security to build the SOA security solution, specifically through encapsulating the secutiry assertion into the SAML assertion statement, creating SAML secure statement and promising the secure of SAML authentication for the service provider to ensure the security of web services in SOA and achieve the user's single sign on. etc.

**Key words**: service-oriented architecture model of security; security assertion markup language; single sign on

**(责任编辑: 马春晓)**