一种基于 SAML 的 Web 服务单点登录模型研究与实现①

Research and Realization of an SAML – Based Web Services Single Sign on Model

张 慧 李建华 马 华 (中南大学 信息科学与工程学院 湖南长沙 410075)

摘 要：由于 Web 服务具有异构性和松耦合性等特点,而现有的跨域单点登录方案主要针对基于 Web 站点的应用,不能较好的适用于 Web 服务环境。提出了一种基于 SAML 的 Web 服务单点登录模型,介绍了该模型的两种实现模式,并给出了组合服务的单点登录方法。基于 OpenSAML 和 WSS4J 等开源项目,给出了该模型的原型实现,并分析了模型的安全性。该模型使得跨域的 Web 服务单点登录变的简单,可适用于各种跨域的基于 Web 服务的应用场景中。

关键词：SAML Web 服务 单点登录 身份认证 安全

1 引言

随着 Web 服务技术规范和标准的不断发展,Web 服务已经逐渐从理论研究转向实际应用。很多跨域的系统集成都是使用 Web 服务来实现的。但用户在访问这些系统时,需要多次输入口令或者其它身份凭证。这有两个缺陷:1) 每个系统都必须要维护用户的信息,加大了系统的管理任务,同时造成用户的不便; 2) 用户的信息可能是敏感的,不能被协作的系统所共享。所以,在跨域的环境下使用单点登录技术变得非常的重要。

传统的单点登录技术[1] 主要是针对单域环境下的,一般是用统一身份认证技术来实现的,如 LDAP,所有的系统都到一个集中的地方去认证。但对于跨域的系统,由于各系统用户是不一致的,且互相是不可知的。所以传统的单点登录技术在跨域环境下是不可行的。

目前,针对跨域环境下的单点登录解决方案主要有:微软的. NET Passport、Sun Microsystems 等建立的自由联盟计划 (liberty alliance project) 以及 Microsoft 和 IBM 联合开发的 Web 服务联邦语言 (WS – Federation)。. NET Passport 技术是通过其 Passport 来实现单点登录的,只要用户通过微软的 Passport 服务器的验证,就可以访问所有与 Passport 服务器合作的站点。但由于微软在 Passport 验证技术方面不公开,使得在安全性方面有一定的隐患。目前,Passport 还不支持 Web 服务。自由联盟计划和 Web 服务联邦语言都是通过建立联盟身份,来访问联盟中的其它系统的。但由于 Web 服务是松耦合的,所以建立联盟身份并不是每个 Web 服务场景所必须的。

安全声明标记语言 (Security Assertion Markup Language,SAML) 是由结构化信息标准促进组织 (OASIS) 的安全服务委员会 (SSTC) 提出的,用来在不同信任域之间交换安全信息。SAML 为认证和授权服务提供了标准的描述,基于 XML 具有跨平台性,提供了强大的断言 (Assertion) 机制,使得跨域的系统可以通过断言来进行验证,适用于 Web 服务的松耦合环境。本文设计了一种基于 SAML 的 Web 服务单点登录模型,借助于 SSL 和 PKI 技术,实现了跨域的 Web 服务单点登录。同时给出了模型的两种实现模式,并基于其中一种模式实现了组合服务的单点登录。最后基于开源项目,给出了该模型的原型实现,并对模型的安全性做了分析。

① 基金项目:湖南省教育厅科学研究项目(07C425)

2 相关工作

目前对基于 SAML 的 Web 服务单点登录模型学术界和工业界都有了一定的研究。SAML 规范中的 Bindings 部分定义了 SAML 如何与 SOAP 协议进行绑定,为 SAML 与 Web 服务的结合提供了标准。文献[2]提出了一种基于 Systinet 公司的 WASP Card 产品来构建 Web 服务单点登录应用,虽然这个产品可以对 SAML 请求进行响应并发布断言等,但这种方法依赖于特定的产品,通用性不强。文献[3]提出了一种基于 SAML 的 Web 服务单点登录设计方案,但没有给出方案的实现架构。文献[4]对基于 SAML 的单点登录系统进行了分析,但没有给出在 Web 服务环境下如何实现单点登录。相比之下,本文给出了一种较完善的基于 SAML 的跨域的 Web 服务单点登录模型,可以较好的适应跨域的 Web 服务单点登录。

3 模型设计

SAML2.0 规范中定义了两个角色,分别为身份提供者(Identity provider)和服务提供者(Service provider)。身份的提供者即断言方,它用来对用户进行身份认证,并发放断言。由于身份提供者和服务提供者是基于 PKI 互相信任的,所以用户可以用获得的断言来对服务进行访问。服务提供者提供的服务既可能是单个服务,也可能是多个服务的组合。每个服务需要对断言进行检验,以确定用户的身份,然后通过访问控制系统,来决定该用户是否有权限来访问目标资源。

3.1 总体框架

如图1,该模型主要分为三个部分:身份提供者、服务提供者、终端用户。身份提供者和服务提供者之间的通信是双向安全通道,因为他们各自都拥有数字证书。而用户与身份提供者和服务提供者的通信是单向的安全通道,因为用户可能是没有数字证书。

身份提供者中包括身份验证模块、断言及助诊文件生成模块、数字签名模块、助诊响应模块。

(1) 身份验证模块主要是对用户提供的身份信息,比如用户名密码或数字证书等进行验证,判断其是否为合法用户。

(2) 断言及助诊文件生成模块是用来构造断言或断言助诊(Artifact,对断言的一个引用)。

(3) 数字签名模块是用身份提供者的私钥对整个断言或助诊文件进行签名。

(4) 助诊响应模块是根据服务提供者的助诊文件找到相应的断言文件,并返回给服务提供者。

服务提供者中包括断言处理、助诊处理、访问控制、签名确认等模块。

(1) 断言处理模块主要是通过对断言的解析来认定用户的身份,并把相关的属性传递给访问控制模块。

(2) 助诊处理模块是把客户端用户发送过来的助诊文件传递给身份提供者,并获取对应的断言文件。

(3) 访问控制模块是根据用户的相关属性来判断该用户有无访问资源的权限。

(4) 签名确认是用身份提供者的公钥对断言或助诊文件进行确认,判断是否是由身份提供者发布的。

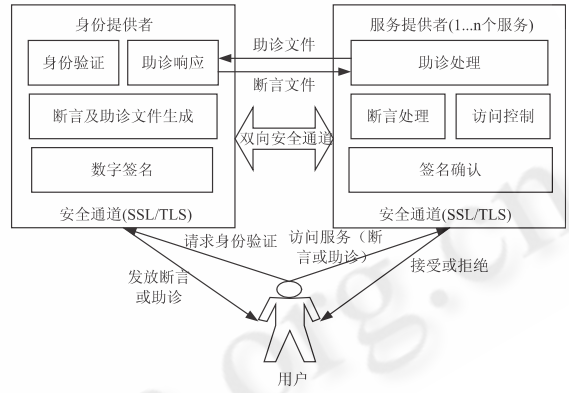

图1 Web 服务单点登录模型

3.2 执行机制

整个模型的运转情况如下:

(1) 终端用户向身份提供者发出身份验证请求。

(2) 身份提供者通过身份验证模块对用户进行验证。

(3) 如果是合法用户,则调用断言构造模块去构造相应的断言;如果非法,则拒绝请求。

(4) 身份提供者对断言进行数字签名。

(5) 用户访问目标服务,并在请求信息中添加该断言信息。

(6) 服务提供者在接收到用户请求时,首先对断言的签名信息进行确认。

(7) 如果是身份提供者发放的断言,则进行解析,否则拒绝请求。

（8）解析该断言，对该用户的身份进行确认。

（9）调用访问控制模块来查询该用户有没有权限访问目标资源，并给出最后给出响应。

上述是直接发放断言情形的执行机制，对于发放助诊文件的情形，总体上是类似的，在后面的内容中对此情况将做详细的论述。

4 模型的两种实现模式

本文给出了以下两种 Web 服务单点登录模式：Push 和 Pull。

4.1 Push 模式

Push 模式是指把断言推给服务提供者，这种模式较为简单，具体的执行步骤如图 2：

（1）用户先请求身份提供者，输入自己的身份信息；

（2）身份提供者给用户返回一个 SAML 断言；

（3）用户请求服务提供者，并把上一步骤得到的 SAML 断言作为 SAML Token 放在 SOAP 消息头中。

（4）服务提供者根据获得的 SAML 断言，进行验证，以判断是否是接受请求还是拒绝请求。

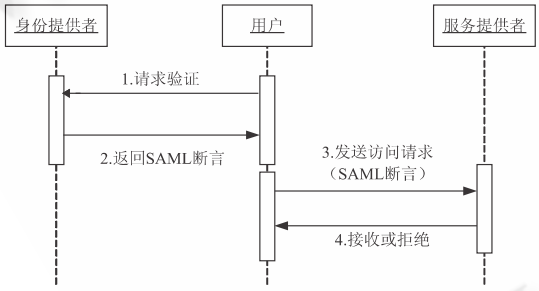

图 2 单点登录 Push 模式

4.2 Pull 模式

Pull 模式是指服务提供者从身份提供者那把断言拉过来，所以相对复杂一些，具体的执行步骤如图 3：

（1）用户先请求身份提供者，输入自己的身份信息；

（2）身份提供者给用户返回一个 SAML 助诊文件；

（3）用户请求服务提供者（请求中含助诊文件）；

（4）服务提供者向身份提供者验证（验证消息中含助诊文件）；

（5）如助诊是合法的，则返回 SAML 断言；否则拒绝请求；

（6）服务提供者根据 SAML 来决定是否接受用户的请求。

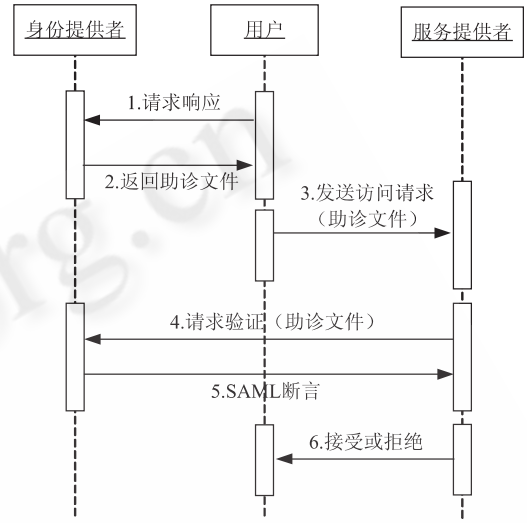

图 3 单点登录 Pull 模式

4.3 Push 与 Pull 的比较

Push 模式相对 Pull 模式较为简单，但断言部分是从客户端传向服务提供者的，所以安全性有一定的限制。而 Pull 模式中客户端只有助诊文件，助诊文件只是对验证断言的一个引用，真正验证是发生在身份提供者和服务提供者之间。而且身份提供者在向服务提供者提供断言的同时，会把助诊文件与断言的映射关系删除，也就是说助诊文件只能使用一次，防止了重放攻击。所以说 Pull 模式安全性更好一些，具体使用哪一种模式，要根据具体的环境来确定。

4.4 基于 Push 模式实现组合服务单点登录

服务提供者提供的服务既可以是单个服务，也可以是多个服务的组合。当是单个服务时，使用 Push 和 Pull 模式都是可以的。当为组合服务时，上述模型需要用 Push 模式来实现。因为在 Pull 模式中，助诊文件只能使用一次，但组合服务中每个服务都需要对用户身份进行验证。当采用此模式时，如果组合服务中有 n 个服务，则需要在身份提供者模块中相应的验证 n 次。所以，使用 Push 模式来实现组合服务的单点登录更恰当一些。当然，采用 Push 和 Pull 的组合模式也可以实现组合服务的单点登录，但比较复杂，本文对此种

情形不做研究。

组合服务中的单点登录过程如图 4：用户从服务提供者获得断言后，依次调用组合服务中的各服务。

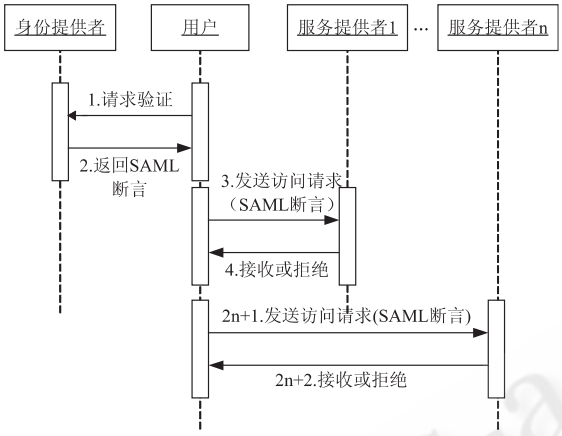

图 4　组合服务中的单点登录

5　原型系统实现

原型实现中 Web 服务支撑平台采用的是 AXIS + Tomcat，断言及助诊文件的构造与解析采用的是开源 Opensaml1.1API，并使用了 WSS4J 提供的一些类来对 SOAP 消息进行加密、签名、把 SAML Token 添加到 SOAP 消息头中。

5.1　身份提供者方

身份提供者方拥有用户的身份信息。在本模型的实现中既可以是一个普通的应用，也可以是一个 Web 服务。下面以身份提供者是以 Web 服务形式发布的系统为例，它主要有身份验证、SAML 构造与解析、数字签名、助诊响应等模块。

（1）身份验证模块 Logon()：用户把 UsernameToken 或 X.509Token，加载在 SOAP 消息头中，供身份提供者验证。WSS4J 中提供了类 org.apache.ws.axis.security.WSDoAllSender，实现了把 Token 文件加入 SOAP 消息头中。类 org.apache.ws.axis.security.WSDoAllReceiver 解析消息头，对用户身份进行验证。

（2）断言及助诊文件生成模块 MakeAssertion() 及 MakeArtifact()：生成 Opensaml1.1API 中的 SAMLAssertion 或 SAMLArtifactType 类对象。

（3）数字签名模块 Sign()：对断言或助诊进行数字签名。

（4）助诊响应模块 ArtifactResponse()：根据助诊文件中的 SourceID 找到临时存储的断言，并返回给服务提供方。

5.2　服务提供者方

服务提供者方在接收到用户的请求消息后，将会对断言或助诊进行一系列的处理，主要有断言处理、助诊处理、访问控制、签名确认等模块。

（1）断言处理模块 DoAssertion()：对断言 SAMLAssertion 对象进行解析，取得相应得属性，进行验证，然后传给访问控制模块做访问控制决策。

（2）助诊处理模块 DoArtifact()：调用身份提供者的 ArtifactResponse() 服务，来获取对应的断言。

（3）访问控制模块 AccessControl()：根据上述得到的断言属性来构造请求，并通过策略评估，来判断用户是否有权限使用该资源。该模块基于开源项目 XACML 做访问控制。

（4）签名确认模块 SignVerify()：对断言或助诊文件进行签名确认。

6　安全性分析

在 Web 服务单点登录过程中需要考虑传输的安全性，包括保密性、完整性、不可抵赖性及重放攻击等。

1. 保密性

保密性意味着只有期望的接收方才能读取消息的内容，而在消息发送途中截取消息的其他任何人都不能读取它的内容。在上述模型当中，一方面考虑传输过程的机密性，传输过程中都使用 SSL/TLS。另一方面由于消息可以被中间结点获得，所以需要对消息本身进行加密，可以使用 XML 加密技术选择性地对这些部分进行加密。

2. 完整性和不可抵赖性

模型中对 SAML 的请求/回复消息都使用了数字签名，可以防止消息被篡改。根据安全级别的要求，可以对消息的部分内容或全部内容进行签名。

3. 重放攻击

模型中对断言和助诊文件中加了时间条件，来确保这两种文件的有效期，应该要尽可能的短，以免被恶意的第三者获取。同时 SOAP 消息中都加入了时间戳，接收方对消息头中的时间戳进行检测，从而避免重放攻击。

（下转第 38 页）

(上接第 52 页)

所以该模型的安全性较好,可以适用于跨域的 Web 服务单点登录场景。

7 结束语

基于 SAML 标准,本文设计了 Web 服务单点登录模型,给出了单点登录的 Push 和 Pull 模式的实现方法,并基于 Push 模式实现了组合服务的单点登录。最后结合开源项目给出了模型的原型实现,并对模型的安全性做了分析。这个模型较好的解决了现有的跨域的单点登录方案不能适应于 Web 服务环境的问题。

参考文献

1 林满山,郭荷清. 单点登录技术的现状及发展. 计算机应用,2004,24(6):248 – 250.

2 韩伟,范植华. 基于 SAML 的单点登陆技术在 Web 服务中的应用研究. 计算机工程与设计, 2005,26(3): 634 – 636.

3 胡剑,寇雅楠. 基于 SAML 的 Web 服务中联合单点登录的设计与实现. 制造业自动化, 2007, 29(10): 79 – 81.

4 陈科,佘□,黄迪明. 基于安全断言标记语言辅件技术的单点登录系统分析. 计算机应用, 2005, 25(11): 2574 – 2576.