基于 SAML 的单点登录模型的改进 *

尹 星[1,2],吴国新[2]

(1.江苏大学 电气信息工程学院,江苏 镇江 212013;
2.东南大学 计算机科学与工程学院,江苏 南京 210096;

摘 要:分析了两种典型的基于 SAML 的单点登录模型,针对流程复杂的缺陷进行简化,提出改进的单点登录模型,对三种模型进行比较,分析出改进模型所具有的性能优势。

关键词:SAML;单点登录(SSO);Web 服务

中图分类号:TP393.09 **文献标识码**:A

An improved SAML-based single sign on model

YIN Xing[1,2], WU Guo Xin[2]

(1.School of Electrical and Information Engineering, Jiangsu University, Zhenjiang 212013, China;
2.School of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: After analyzing the current two SAML based SSO models, an improved SSO model was brought up to simplify the process of SSO. Finally, the three models were compared and the efficiency advantage of the improved SSO model was analyzed.

Key words: SAML; SSO; Web service

Web 服务的出现使得企业与它的合作伙伴、客户以及员工之间的关系变得更加紧密[1]。虽然 Web 服务的真正价值更多地体现在企业之间,但是目前许多企业仍然首先把 Web 服务的应用限制在企业内部,这是因为当前跨域的应用面临着这样一个严重问题:当用户登录到多个系统上请求服务时,用户可能需要预先分别在这些站点注册,然后在每次使用站点服务时都要进行认证。大量的用户名和密码不仅使得用户难以记忆和区分,而且安全风险很大;此外企业需要花费较大的开销来管理大量用户信息。因此,Web 服务要想取得成功必须首先解决安全问题[2],而安全问题的关键在于如何以一种灵活、简便、可互操作的方式来实现跨多域、跨异构系统的安全的服务访问。

1 传统单点登录技术及 SAML 规范

对于如何实现只需进行一次身份认证就能访问多个服务,当前较好的解决方案就是使用单点登录 SSO (Single Sign On)技术。使用单点登录技术,用户只需在初次登录时进行一次性认证,即可获得所需访问系统和应用软件的授权。

虽然传统的单点登录技术能在某种程度上实现“一次登录,任意访问”,但是由于不具备开放性和标准性,因此仍不能跨域实施。这就需要一个能跨域传递符合通用标准的安全令牌的单点登录机制,让所有的安全组件在分布式异构环境中联合工作。当前与单点登录的相关 Web 服务安全规范是安全性断言标记语言 SAML (Security Assertion Markup Language)[3]。作为 XML 的一个子集,SAML 最主要的目的就是实现 Web SSO,它解决了 Web 服务安全体系中的身份认证多次使用的问题。此外,SAML 并不定义任何新的认证和授权机制或方法,只定义用于不同域的服务间安全信息传输的文档结构[4]。

2 典型的基于 SAML 的单点登录模型的分析

典型的基于 SAML 的单点登录模型有两种,即 Pull 模型和 Push 模型[5]。这两种模型的框架都是由如下三个部分组成:

* 基金项目:国家 863 项目(项目编号:2007AA01Z422);江苏大学高级人才项目(项目编号:06JDG032)

(1)主体:请求访问某种资源的实体,可以是用户或者程序。

(2)源站点:在本文中也称作 SAML 权威机构或者安全认证机构,负责验证主体身份的合法性,并向主体提供其所需的安全信息以作为凭证(本文中即为 SAML 令牌)。由于该站点是主体身份信息提供者,所以称为源站点。

(3)目标站点:受保护的网络资源的持有者,能向合法主体提供其所需资源。

下面分别对 Pull 模型和 Push 模型进行分析。

2.1 Pull 模型

Pull 模型是指目标站点从源站点那里把身份验证声明拉过来,如图 1 所示,对该模型的登录流程描述如下:

(1)主体登录到源站点进行身份认证。

(2)若主体通过了认证,则源站点返回包含用户身份信息的 SAML 身份认证令牌。

(3)主体使用令牌向目标站点请求使用受安全保护的资源。

(4)目标站点接收到用户身份验证令牌后,持该令牌到源站点请求 SAML 身份验证声明。

(5)源站点返回 SAML 身份验证声明。

(6)目标站点收到 SAML 身份验证声明后,为主体提供资源。

在 Pull 模型中,身份验证令牌是由源站点产生和维护,仅在主体被重定向到新的目标站点时,该目标站点才获取该令牌。

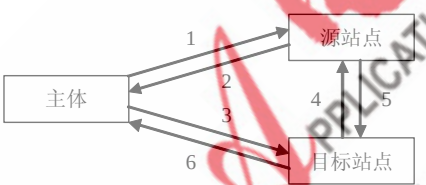

图 1 Pull 模型登录流程

2.2 Push 模型

Push 模型是指目标站点把授权令牌推给源站点,如图 2 所示,对该模型的登录流程描述如下:

(1)主体登录到源站点进行身份认证。

(2)若主体通过了认证,则源站点向目标站点请求 SAML 授权令牌。

(3)目标站点根据源站点提供的用户信息为该用户提供 SAML 授权令牌。

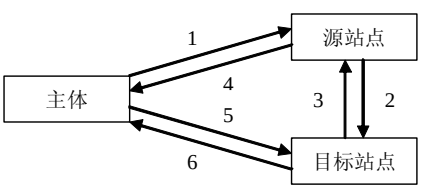

图 2 Push 模型登录流程

(4)源站点接收到目标站点生成的 SAML 授权令牌后将其转发给主体。

(5)主体使用授权令牌向目标站点请求受安全保护的资源。

(6)目标站点收到主体发送过来的 SAML 授权令牌后为主体提供资源。

在 Push 模型中,目标站点生成并维护授权令牌,而源站点则将使用该令牌将主体重定向到目标站点。

当前基于 SAML 的单点登录系统都是以上述两种模型为基础的,具体采用哪种取决于应用环境。当源站点链接有大量目标站点时,Push 模型可能更适合,因为这种情况下,源站点就无需在目标站点接受由其生成的令牌或与之相关的声明之前维护这些令牌或声明。但是当目标站点处理能力有限或者不宜保存用户身份信息时,就应该采用 Pull 模型,让维护令牌或声明的工作由源站点来处理。

2.3 典型 SAML 单点登录模型的不足

通过对 Pull 模型和 Push 模型的分析和比较可以看出,尽管在这两种单点登录模型中用户也只进行了一次身份认证,但每次申请新的服务时,Pull 模型都要目标站点向源站点发出请求以使用户令牌生效,而 Push 模型都需要源站点向目标站点发出请求以获取用户令牌。这两种模型的结构是相似的,只是运行流程有所不同。从上面的分析可以看出,基于这两种模型的单点登录系统面临如下三个问题:

(1)在用户每次访问一个新的目标服务站点时,都需要在源站点与新的目标站点之间交换安全信息,因此整个实现过程比较复杂。此外,当某个时刻有很多用户需要同时访问多个服务,则网络中的数据流量会明显增大。

(2)由于源站点与目标站点之间具有较强的依赖关系,因此系统的灵活性不足。

(3)如果使用这两种模型,就需要在源站点或者目标站点上维护用户的令牌,当一个站点同时需要维护的用户令牌过多,或者当一个站点同时接收到过多的令牌请求时,可能会导致该站点发生服务阻塞,这不仅会使安全服务得不到响应,甚至还有造成服务器崩溃的隐患。因此,上述两种模式都不适用于大量用户在相同时间调用很多服务,并且源站点处理能力又很有限的场合。

鉴于 Pull 模型和 Push 模型的不足,就需要寻求一种新的基于 SAML 的单点登录模型,以简化单点登录系统的登录过程。本文在这两种模型的基础上进行改进,提出一种新的基于 SAML 的单点登录模型。改进的目标是解决上述三点不足,使得包含 SAML 声明的令牌仅在主体与源站点、以及主体与目标站点之间进行传递,而源站点和目标站点之间无需进行安全信息的互传,并且使令牌的维护工作由代表主体的客户端来完成。

3 基于 SAML 的单点登录模型的改进

对单点登录模型进行改进的思想是：源站点采用 SAML 断言作为会话令牌，令牌中包含的用户身份和属性信息通常由安全机构进行加密和数字签名，形成安全的 SAML 令牌。这样收到此令牌的目标站点通过对签名进行验证就可以知道令牌发行者的身份，从而间接认证了申请服务的主体的身份。当目标站点解析该令牌之后便可看到主体身份和属性信息，然后根据这些信息做出对该用户的访问控制决策。在这种情况下，如果主体需要向别的目标站点申请新的网络服务，它只需将已经获得的 SAML 权威机构颁布给他的安全的 SAML 令牌出示给目标站点即可。改进模型如图 3 所示。

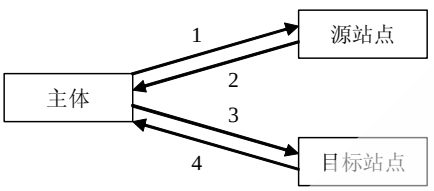

图 3 基于 SAML 的单点登录改进模型

改进的基于 SAML 的单点登录模型消息交换和处理流程描述如下：

(1)主体将自己的登录信息发送至源站点以请求身份认证。

(2)源站点的认证模块对用户登录信息进行验证，并为合法的用户生成 SAML 断言信息，然后使用源站点与目标站点事先协商好的密钥进行加密和数字签名，形成了安全的 SAML 令牌，最后将该令牌返回给主体。

(3)主体使用该令牌访问目标站点。

(4)目标站点对该令牌进行签名验证，以确认令牌的颁布者就是源站点，从而无需再与源站点进行交互，同时也间接验证了服务请求的发起者是合法的。接着，目标站点根据解密后所获得的 SAML 断言信息以决策是否以及如何为用户提供相应的服务。

4 三种模型的比较与分析

与 Pull 模型和 Push 模型相比，改进后的单点登录模型具备如下一些突出的优点：

(1)主体向源站点进行请求验证时，源站点无需向目标站点请求授权决策；主体访问目标站点时，众多目标站点无需频繁地对源站点进行安全性验证请求。为了证明改进模型确实简化了单点登录系统的复杂性，本文对三种模型进行了具体的性能分析，通过表 1 对三种模型在四种不同应用场景下源站点被访问的次数进行了统计。从表中可以看出，无论主体和目标站点的数量是多少，改进模型源站点被访问次数均少于另外两种模型，特别是当每个主体需要访问的目标站点的数目 m 的取值很大时，应用改进模型能明显减轻源站点的负载，同时也简化了单点登录系统的运行流程，并降低了网络中数据的流量。

表 1 三种模型在不同应用场景下源站点被访问次数的统计

模型	场景			
	1 个主体访问 1 个目标站点	1 个主体访问 m 个目标站点	n 个主体访问一个目标站点	n 个主体，每个主体访问 m 个目标站点
Pull 模型	2	$1+m$	$2\times n$	$(1+m)\times n$
Push 模型	2	$2m$	$2\times n$	$2m\times n$
改进模型	1	1	n	n

(2)从源站点发出的安全令牌能被所有源站点信任的目标站点查看，无需在源站点和指定的目标站点之间事先建立安全通道，而只需事先协商好加密和数字签名处理的密钥。这样，这两类站点间的独立性就得到增强，提高了系统的灵活性和可配置性。

(3)大量的用户令牌由各个主体自己维护，这就减轻源站点或目标站点用于维护令牌的开销。

改进的基于 SAML 的单点登录模型具备了上述三点独特的优势，说明了这样的改进确实能简化单点登录的运行流程，并提高单点登录系统的效率和灵活性。改进后的模型比上述两种典型模型更适用于大量用户同时访问很多服务，并且源站点处理能力又很有限的场合。

本文首先介绍了传统单点登录技术以及 SAML 规范，然后对两种典型的基于 SAML 的单点登录模型进行了分析，并指出了这两种模型存在的缺陷。在此基础上提出了改进型的 SAML 单点登录模型，并通过对三种的比较，验证了这样的改进确实能简化单点登录的流程，改进的 SSO 模型能更好地应用于 Web 服务中很多用户同时跨域访问多服务的应用场景。

参考文献

[1] FOSTER I, KESSELMAN C, NICK J M, et al. The Physiology of the Grid－: An Open Grid Services Architecture for Distributed Systems Integration. http://www.globus.org/research/papers/ogsa.pdf.

[2] IBM.com. Web Services 的安全性. http://www.cit.fudan.edu.cn/webservices/0004/Course_pdf/chapter07.pdf.

[3] Martijn de Boer. Single sign on for web service. Apr 18, 2005. https://forums.sdn.sap.com/thread.jspa?threadID=35990&messageID=343047.

[4] OASIS Security Services (SAML) TC. http://www.oasis－open.org/committees/security.

[5] GALBRAITH B, HANKISON W. Web 服务安全性高级编程[M]. 吴旭超，王黎，译. 北京：清华大学出版社，2002.

(收稿日期：2008－12－19)