基于 SAML 的数字资源统一访问控制机制

SAML - Based Unified Access Control Mechanism for Digital Resources

袁亮环

(安徽中医学院图书馆 合肥 230038)

摘 要 针对目前图书馆各数字资源系统访问控制机制存在的缺点,提出一种利用 SAML 的虚拟身份认证方式,通过应用系统间的访问控制信息的交换,实现数字资源的统一访问控制,方便用户对数字资源的访问,减少数字图书馆管理机构的管理成本。

关键词 SAML 单点登录 虚拟身份 访问控制

中图分类号 TP309

随着图书馆自动化、数字化水平的进一步提高,各高等院校和科研机构的图书馆购买或自建了大量的数字化信息资源,并采用 Web 方式来提供服务,这些资源由于版权限制、费用约束或管理要求,需要对用户进行身份认证和使用授权后才能使用。目前,图书馆数字资源的访问控制方法主要有以下几种:基于 IP 限制的访问控制机制、基于个体用户名/密码的访问控制机制、基于单一用户名/密码的访问控制机制。

由于各个应用系统开发时缺乏统一的规范,各系统由不同的机构开发,造成了应用系统的平台、技术水平、结构各不相同,各应用系统都有相互独立的身份认证和访问控制策略。每次读者使用数字资源时都要先认证自己,用户进入不同应用系统,需要分别输入不同的账号和密码。同时用户也必须记住许多用户名和密码,非常不便;对管理机构来说,需要管理大量用户的用户名和密码等个人信息,在某一用户信息改变时需同步修改大量应用服务中的同一用户信息,增加了管理成本。

针对这类问题,迫切需要一种方式能够跨系统透明地访问受保护的图书馆资源,结构化信息标准促进组(Organization for the Advancement of Structured Information Standards,OASIS)的安全服务技术委员会提出了安全声明标记语言(Security Assertions Markup Language,SAML),为在线合作伙伴安全信息的创建和交流,定义并维护一种标准的、基于 XML 的架构,该标准为实现不同系统的安全信息交换提供了统一规范和解决框架,使得透明地访问多个需授权访问的资源成为可能。本文提出一种基于安全声明标记语言的虚拟身份认证的数字资源访问控制机制。通过虚拟身份认证的单点登录(Single Sign - On,SSO)系统可以满足用户和管理员的需求,使用者只需要记忆一组用户名和密码,在一个认证系统进行认证后,就可以实现全局登录,即用户再访问其他数据库资源时,不需要再次登录就能够被认证进行需要授权的访问[1~2]。

1 安全声明标记语言(SAML)

安全声明标记语言 SAML 是一种为交换安全信息而设计的基于 XML 的框架性语言,它提供了一种标准的格式对身份证明进行 XML 编码,因此具有跨平台的交互能力,用来在多个信任合作者之间交换安全信息。SAML V2.0 标准主要包括以下几个方面的内容[3]:

SAML V2.0 的一致性需求(Conformance Requirements for the OASIS Security Assertion Markup Language(SAML) V2.0)。

SAML V2.0 声明和协议(Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0)。定义了 SAML 认证、属性、授权以及认证授权的请求、应答消息格式。

SAML 绑定(Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0)。描述了传输时 SAML 声明及请求回复消息如何与具体协议绑定。

SAML 说明(Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0)。描述了 SAML 实现 Web SSO 的两种方式及其消息传输过程。

SAML 元数据(Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0)。

SAML 授权上下文(Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0)。

SAML 的元数据规范(SAML metadata schema)。

SAML 的安全性和策略考虑(Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0)。从信息安全角度描述了保证 SAML 声明安全性、完整性和真实性的相应策略。

SAML 术语表(Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0)。解释了 SAML 系统中使用的术语定义。

SAML 的主体是声明和协议,SAML 定义了 3 种声明:a. 认证声明(Authentication Assertion),是 SAML 认证机构对主体进行身份描述和鉴别的相关信息的描述,如被认证主体的域,IP 地址,认证的机构、方法、时间等信息。b. 属性声明(Attribute Assertion),描述与授权相关的信息,如主体用户的标识,所属用户组,角色,以及可访问的资源和权限。c. 授权决策声明(Authorization Decision Assertion),描述根据指定的证据,对一个请求者对特定资源的授权行为的结果(允许、拒绝、无法确定),如请求被允许或拒绝的信息。

作者简介:袁亮环,男,1973 年生,硕士,馆员,研究方向为数字资源管理、数据安全。

SAML 作为一种基于 XML 的安全信息交换、共享语言，具有如下特点：支持 SSO，通过 SAML，用户只需登录一次通过身份认证后，就可以在所有信任站点中访问；灵活性，支持可扩展机制，允许开发人员对现有元素进行扩展和选择；平台无关性，支持异构平台的信息交换，实现不同系统的统一认证。

2 基于 SAML 的单点登录系统

基于 SAML 的 SSO 服务模式包括三个实体，它们分别是：a. 用户代理(User Agent)，用户访问资源的实体，在 Web 访问方式下即为用户浏览器。b. 服务提供者(Service Provider，SP)，是指为用户提供某种服务的应用系统。c. 身份提供者(Identity Providers，IDP)，是一种特殊的服务提供者，它为其他的实体提供身份认证、实体信息访问控制等服务，即身份认证服务器[4~5]。

系统基本认证工作过程如下：a. 用户通过浏览器向 SP 发送访问请求，要求访问须授权访问的资源。b. SP 检查到用户是否登录，如没有授权信息，则确定进行认证的 IDP 并把该用户重定向到选定的 IDP。c. 用户根据 SP 确定的身份认证服务器发送认证请求。d. 身份认证服务器对用户进行身份鉴别。e. 身份认证服务器对用户进行身份鉴别后，向用户发送鉴别结果，用户根据响应消息向服务提供者请求访问。即用户浏览器被重定向回服务提供者网站，此时重定向消息中包含着认证信息。f. SP 根据认证信息决定允许或拒绝提供服务(如图 1 所示)。

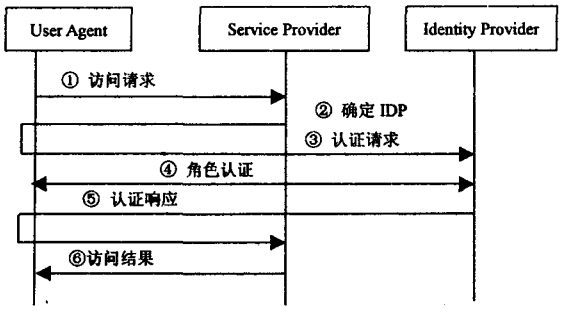

图 1

3 基于 SAML 的 Web SSO 在数字图书馆中的应用

数字图书馆目前提供的服务基本上建立在 B/S 模式上的，因此本文采用的是一种基于 SAML 的 Web SSO 体系结构。在这种 Web SSO 体系结构中，所有的安全算法都在 IDP 中实现，读者通过浏览器即可完成所有认证，并且可以存在多个独立的身份提供者，各服务提供者决定由哪个 IDP 进行身份认证，认证声明可以在信任域或站点中通用。

用户在使用服务提供者的服务时，可以直接发送自己的虚拟身份给身份提供者，身份提供者验证通过后，给用户颁发一个全局登录的信任状。此信任状包含用户的虚拟身份、访问权限、有效期以及身份提供者的签名和认证时间等信息。有效期一般根据用户所需要的安全等级来设定，安全等级越高有效期越短。当到了有效期后，此信任状就被视为无效。用户可以拿着此信任状向服务提供者申请服务；用户也可以直接向服务提供者发送服务请求，在服务提供者处通过超链接到身份提供者处进行认证。

基于 Web 的 SSO 基本模式包含 3 个参与者：检测机构、认证者、凭证库，用户采用域标识和通用标识联合表示用户的虚拟身份，域标识指示用户的身份提供机构，通用标识是用户真实身份的映射，减少用户隐私信息的过分暴露，用户首先在一个身份提供者处进行注册认证，获得域标识和通用标识表示的虚拟身份，身份提供者也同时充当认证者。系统对数字资源的访问控制流程如下：a. 若用户申请访问某个受保护数字资源，系统检测机构首先检查请求中是否提供了身份认证声明，若包括身份证明则直接转下面第 4 步，若没有提供则由应用服务选择身份认证服务器后将信息返回给用户要求进行身份鉴别。b. 用户被重定向到 IDP 的登录页面，要求用户进行登录(使用用户名和适当的用户凭证，例如密码或者证书)。IDP 查看用户名和用户凭证，并且在用户凭证库中验证它们。如果验证成功，IDP 返回用户包含认证时间、认证者、角色、权限等信息的认证声明。c. 用户携带 SAML 认证声明，重定向到应用服务，再次访问请求的数字资源。d. 应用服务根据用户提供的认证声明，通过向 IDP 发送 SAML 请求，进一步向认证服务器确认信息访问者身份。e. 认证服务器接收到应用服务的 SAML 请求，取出对应的 SAML 声明，返回 SAML 响应给应用服务。f. 应用服务系统根据身份鉴别结果，解析 SAML 认证声明，授予或拒绝信息访问者对请求数字资源的访问请求。

4 结束语

本文分析了当前数字资源访问控制机制存在的缺陷，提出了采用 SAML 描述，基于虚拟身份的 Web SSO 系统，与传统的访问控制系统相比，SAML 采用标准的格式对身份证明进行 XML 编码，SAML 声明可以与多种业界标准的传输协议或 XML 消息交换架构相绑定(如 HTTP、SMTP、FTP、MIME，以及 SOAP、Biztalk、ebXML 等)，因此很好地解决了分布式环境下异构平台的信息交换问题，SAML 的主要设计目标是解决 SSO 问题，以及分布式环境下验证/授权信息交换的问题。此系统具有：a. 平台无关性。SAML 的设计屏蔽了任何平台架构的特殊性。b. 松耦合性。SAML 不需要用户信息的同步更新等复杂的实现。c. 便捷性。终端用户只需登陆一次即可访问所有服务(即 SSO)。d. 管理方便性。应用服务提供者对用户的管理将更加方便。e. 隐私保护。采用虚拟身份认证，减少用户真实信息的过多暴露给非相关部门。f. 安全性。用户减少密码输入次数，减少密码泄露的机会，由专门的 IDP 进行认证，提高认证强度。

这种访问控制机制采用 SAML 进行用户身份认证，实现了异构应用系统间的访问控制信息交换，使用户可以方便地访问数字图书馆中数字资源，同时减少了数字图书馆管理机构的管理成本。

参 考 文 献

1 刘 利. Web 服务环境下基于 SAML 的联合单点登录系统设计[J]. 广西科学院学报，2003，19(4)：185－188

2 杨 青，怀进鹏，徐枞巍. 基于 SAML 的协同电子商务安全服务系统[J]. 计算机工程与应用，2002(14)：228－232

3 Prateek. Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0[EB]. [2008－03－07]. http://docs.oasis－open.org/security/saml/v2.0/saml－conformance－2.0－os.pdf

4 John Hughes. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0[EB]. [2008－03－06]. http://docs.oasis－open.org/security/saml/v2.0/saml－profiles－2.0－os.pdf

5 Scott Cantor. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0[EB]. [2008－03－06]. http://docs.oasis－open.org/security/saml/v2.0/saml－core－2.0－os.pdf

(责编：王平军)