中国图书馆学报(双月刊)2008 年第 5 期
ZHONGGUO TUSHUGUANXUEBAO

●郭秋萍　焦　允　周九常

一种面向 Web 图书馆的读者认证信息单点登录模型研究*

摘　要　目前 Web 图书馆电子资源传统访问方式存在着缺陷。对读者认证信息的单点登录模型进行了研究,提出并验证了 Web 环境下的联合 SSO 模型。该模型利用用户首次的登录信息,将其在分布式 Web 图书馆站点之间进行传递,从而在整个数字图书馆联盟内实现“一次登录,多站点访问”。图 4。参考文献 4。

关键词　Web 图书馆　读者登录　读者信息认证　单点登录模型　数字图书馆联盟

分类号　G250.76

ABSTRACT　At present, there are shortcomings in traditional access methods for electronic resources in Web libraries. In this paper, the authors make a study of a model of user information authentication Single Sign-On, and propose and test a united SSO model in the Web environment. The model utilizes user's first-time sign-on information, delivers it among distributed Web library sites, and realizes “one-time sign-on and multiple-site access in the whole digital library alliance. 4 figs. 4 refs.

KEY WORDS　Web library.　User sign-on.　User information authentication.　Single Sign-On model.　Digital Library Alliance.

CLASS NUMBER　G250.76

1　引言

当前基于 Web 构建数字图书馆联盟的研究主要集中于系统集成与资源整合,如对图书馆信息系统进行 Web 服务和数据的整合等。数字图书馆联盟作为一个跨域分布式 Web 系统,对外部用户提供跨越不同可信域的无缝链接十分重要。现有的图书馆信息系统普遍采用用户认证机制,只有登录成功的用户才具有访问该站点提供服务的权限,这种情况导致用户在访问某一联盟成员馆站点时,必须重新登录,严重影响了整个系统在逻辑上的统一性,不利于数字图书馆联盟的真正实现。尤其是在基于 Web 平台的图书馆联盟中,各成员之间的松耦合性更加明显,所采用的认证技术可能完全异构,使得登录问题更加突出。单点登录(Single Sign-On,SSO)技术利用用户首次的登录信息,将其在分布式 Web 图书馆站点之间进行传递,从而在整个联盟域内实现“一次登录,多站点访问”,是解决该问题的有效途径之一[1]。

2　主流单点登录模型

2.1　Kerberos 模型

Kerberos 是一种基于密钥分发模型的网络身份验证方法,其验证原理是:若用某个用户的密钥加密某一信息,那么只有该用户才能解密[2]。因此,通过解密即可证明该用户的合法性。Kerberos 模型包括三个参与方,即需要进行身份认证的双方和一个双方都信任的第三方。其中,发起方称为客户方,响应方称为服务器方,进行统一用户验证和票据发放的一方称为密钥分发中心(KDC)。客户方通过向服务器方递交自己的“票据”(Ticket)以验证身份,票据中封装了加密密钥和其它信息,是 Kerberos 模型的核心。KDC 能够发放的票据有两种:票据授权票据(TGT)和服务票据(ST)。单点登录时,KDC 首先向合法用户发放 TGT,合法用户在访问某一服务时,利用 TGT 向 KDC 申请该服务的 ST,经过客户方和服务器方双端认证后,建立双方会话(Session)。

Kerberos 模型是目前实现身份认证及单点登录的一个主要且相对成熟的模型,但由于 Kerberos 模型无法在异构环境下实现站点间的单点登录,因此,不能将其直接应用到数字图书馆联盟这样的分布式系统中。

2.2　SAML 模型

SAML(安全声明标记语言)定义了一个基于声

* 本文系国家社会科学基金项目“我国图书馆知识转移与共享体系和策略研究”(项目批准号:06BTQ009)的研究成果之一。

明(Assertion)的安全信息交换框架,单点登录是其中一个主要的设计目标[3]。其基本原理是:通过在不同站点之间交换用户声明,实现用户一站式的 Web 访问。当用户第一次登录一个支持 SAML 的系统后,其授权信息便以声明的形式被存放。一个声明可由多个域组成,分别用来存储声明 ID、主体名字、主体安全域、声明生效条件、允许对哪些资源进行访问等信息。在用户访问其它站点时,仅交换声明即可,无需重复认证。

由以上可知,SAML 模型中的声明包含的只是用户首次认证成功后的结果信息,其本身并不提供具体的认证机制,若把 SAML 模型直接应用到分布式系统来实现单点登录,则存在安全性薄弱的问题。

3　基于 Web 的联合单点登录模型

Kerberos 模型具有比较安全的身份认证机制,但不能实现 Web 环境中异构系统之间的相互认证。SAML 模型虽然具有较好的跨平台无缝链接能力,但缺乏有效的认证机制,安全性比较薄弱。本文将两种模型进行融合,取长补短,提出一种新的基于 Web 的联合单点登录模型,如图 1 所示。

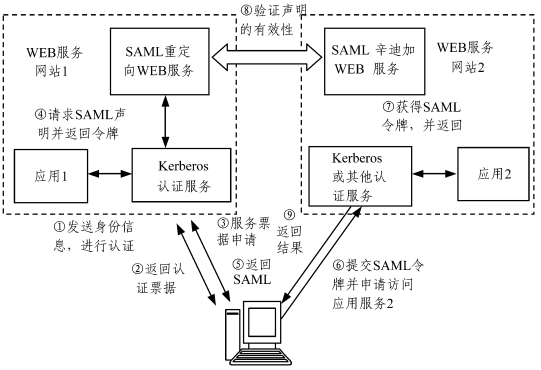

图 1　基于 Web 的联合单点登录模型

联合单点登录模型以 Kerberos 模型为基本认证机制,以保证安全性,对于联盟图书馆中未采用 Kerberos 模型的站点,则使用 SAML 声明在域间交换认证信息,以实现异构系统之间的相互认证。

4　数字图书馆联盟的单点登录过程

数字图书馆联盟是一种建立在多个独立图书馆之上的虚拟联合或逻辑联盟,它以网络为运行平台,表现为不同站点所提供的 Web 服务的集合[4]。用户在访问数字图书馆联盟的不同站点时,单点登录过程包括未登录用户登录某一站点的过程和已登录用户在不同站点间透明跳转的过程。下面分别以这两种情况为例论证本文提出的联合单点登录模型的认证过程。

4.1　基本数据结构

联合单点登录模型需要用到的基本数据结构有:票据模型与 SAML 令牌模型。其中,票据模型又包括票据(Ticket)和票据存根(Stub)两部分。票据存根记录用户的登录信息,而票据只是对票据存根的引用。

票据存根(Stub)可用数据结构表示为:Use_Stub(StubId, UserId, Site, UserIp, BeginTime, EndTime, Interval, SessionId)。其中 StubId 表示票据存根编号,UserId 是用户编号,Site 为当前访问站点,UserIp 为用户浏览器 IP,BeginTime 、EndTime 分别是票据存根创建时间和撤销时间,Interval 为最长访问时间间隔,SessionId 是用户浏览器与需访问 Web 服务器之间的会话密钥,每次重建会话时 SessionId 也随之重新生成。

票据用表达式(Sid, Sign(Sid, K_{SSOS}^{-1})) K_S 表示,其中 Sid 表示会话密钥,S 表示用户需要访问的 Web 服务器,SSOS 表示 Kerberos 认证服务器,Kx 表示 x 的公钥(x 为变元,可代表 S 或 SSOS,下同),$K^{-1}x$ 表示 x 的私钥,(…)K 表示使用密钥 K 对括号中的内容进行加密,Sign(…, $K^{-1}x$)表示对括号中的内容使用 x 的私钥进行签名。

SAML 令牌的数据结构表示为 Token(SAML_TokenId, Signed_Assertion)。其中,SAML_TokenId 代表 SAML 令牌编号,用来唯一标识用户令牌;Signed_Assertion 代表已签名的用户 SAML 声明,包含用户认证信息。由于 XML 具有良好的数据结构定义能力和跨平台性,因此,以 SAML 令牌形式可很好实现认证信息在异构站点之间的传递。

4.2　未登录用户的登录过程

未登录用户登录数字图书馆联盟某一 Web 站点 1 的过程如图 2 所示。

各方之间的信息传递和执行操作表示如下:

(1) User_Browse →Web_Server:http_request(page_url)

(2) Web_Server→SSO_Server(联合单点登录服务器):http_request(page_url)

(3) SSO_Server→User_Browse:login_page

(4) User_Browse→SSO_Server: Use_Info(name, password)

SSO_Server→User_Browse: (Sign($Ticket_{tgs}$, $K_{User\_Browse}^{-1}$), Sid_{tgs})

User Browse→SSO_Server:($Ticket_{tgs}$)K_{Sid}

(5)SSO_Server→Ticket_Manager:(Use_Stub(StubId,UserId,
Site, UserIp, BeginTime, EndTime, Interval, SessionId),
((Sid_{tgs},Sign(Sid_{tgs},$K^{-1}_{SSO\_Server}$))K_S, SidS)

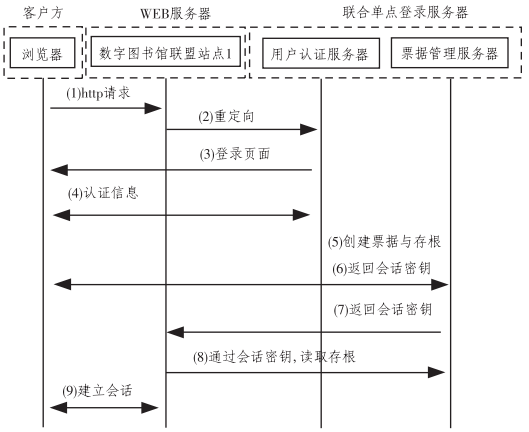

图 2　未登录用户的登录过程

(6) Ticket_Manager→User_Browse:(((Sid_{tgs}, Sign(Sid_{tgs},
$K^{-1}_{SSO\_Server}$))K_S,Sid_S)

(7)Ticket_Manager→Web_Server:Sid_S

(8) Web_Server→Ticket_Manager:(SidS, Sign(Sid_S,K^{-1}s))
K_{SSO_Server}
Ticket_Manager→Web_Server:(Use_Stub, Sign(Use_Stub,
$K^{-1}_{SSO\_Server}$)Ks)

(9)User_Browse→Web_Server:page_url

通过以上流程,图书馆 Web 站点 1 的票据管理服务器中已存储有用户认证信息,为用户接下来在站点间透明跳转提供凭据。

4.3　站点间透明跳转的过程

已登录用户在访问 Web 站点 1 时提出对 Web 站点 2 的访问,即用户在站点间进行透明跳转,其跳转过程如图 3 所示。

各方之间的信息传递和执行操作表示如下:

(1) Web_Server1→Web_Server2: http_request(page_url_2)

(2) Web_Server1→SAML_Server(重定向服务器):(http_request(page_url_2), (Sid_S, Sign(Sid_S, K^{-1}s))K_{SSO_Server})

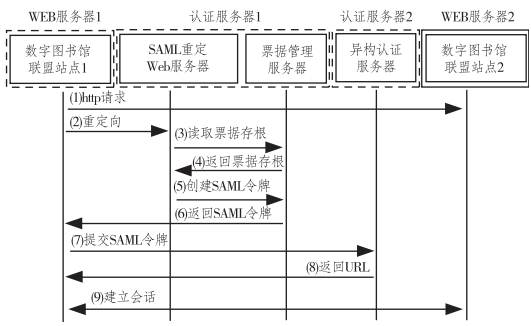

图 3　站点间透明跳转的过程

(3) SAML_Server→Ticket_Manager:(SidS, Sign(Sid_S,K^{-1}s))
K_{SSO_Server}

(4)Ticket_Manager→SAML_Server:(Use_Stub, Sign(Use_
Stub,$K^{-1}_{SSO\_Server}$) Ks)

(5)SAML_Server→Ticket_Manager:Token(SAML_TokenId, Signed_Assertion)

(6)Ticket_Manager→Web_Server1:Token(SAML_TokenId,
Signed_Assertion)

(7)Web_Server1→SSO_Server2(异构认证服务器):SOAP
(Token)

(8)SSO_Server2→Web_Server1:page_url_2

(9)Web_Server1→Web_Server2:page_url_2

5　系统的设计与验证

在系统设计与实现时,其总体架构由三部分组成:认证客户端、联合认证服务器以及应用服务器端。根据 Kerberos 模型与 SAML 模型联合认证的原理,联合认证服务器可由以下主要模块实现。

①认证服务模块:对用户提交的认证信息进行处理,判断用户身份是否合法,并根据判断结果决定是否返回 TGT 票据。

②票据授权服务模块:对用户申请具体的应用服务票据的请求进行处理。根据用户提交的 TGT 的有效性以及用户身份的合法性决定是否返回相应服务器票据 ST。

③密钥管理模块:负责随机生成会话密钥,将用户输入的用户名及密码转换成用户的长期密钥。

④Web请求重定向服务模块:在访问有异构认证服务器的站点时,根据Kerberos认证服务器中用户首次认证的信息创建SAML声明,并生成一个相应的SAML令牌。

⑤SAML辛迪加服务模块:对用户提交的SAML令牌进行解析,提取出其中的SAML声明,验证声明的有效性并根据声明决定用户的访问权限。

⑥数据处理模块:对各种数据信息进行解包或者封装操作。模块包括有加密/解密函数,针对于票据、票据存根、SAML令牌等数据结构的解析与封装函数。

除了上述模块之外,还需要根据情况编写一些非功能性的模块,如线程控制模块、传输控制模块等。

采用WebLogic Server 9.0为服务器平台对整个联合认证过程进行了实验,其结果如下:

(1)首次访问数字图书馆联盟站点1的登录页面http://172.25.132.157:7001/login.jsp,在登录表单中输入用户名DataLibUnion_SSO和口令,登录成功后,显示欢迎页面以及用户登录成功的账号,如图4所示。

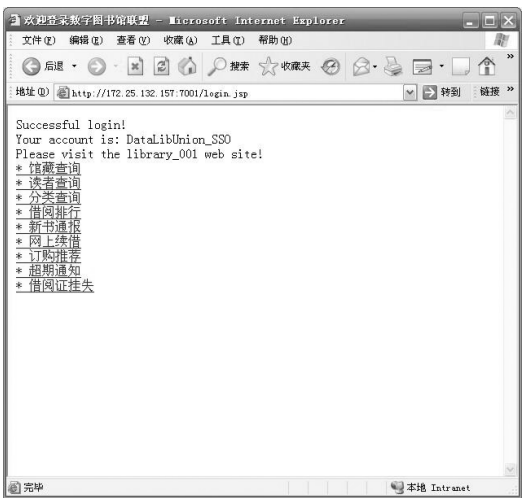

图4 首次登录成功

(2)在浏览器中手工输入地址http://172.25.132.157:7003/lib2/index.jsp(即访问另一站点2),浏览器直接显示相关页面内容,而不需要再次登录,以实现站点间的跳转。

6 结论

Kerberos模型和SAML模型是目前两种主流的单点登录模型,各有其优缺点。本文通过对它们进行分析、比较,取长补短,提出了一种新的Web环境下的联合单点登录模型。并以未登录用户登录某一站点和已登录用户在不同站点间透明跳转这两种典型情况为例,论证了该模型的认证过程。验证结果表明该模型同时具有基于密钥的安全性和跨平台无缝链接两种特点,适合用于构建数字图书馆联盟这样的分布式系统的单点登录。

参考文献:

[1] Gilmore B, Farvis K, Maddock J. Core Middleware and Shared Services Studies Single Sign-on Report[EB/OL]. http://www.jisc.ac.uk/index.cfm?name=prog_middss_studies. 2004(9).

[2] S P Miller, B C Neuman, J I Schiller. Section E.2.1: Kerberos Authentication and Authorization System[R]. M.I.T Project Athena, Cambridge, Massachusetts, 1987(12).

[3] Hallam B P, Maler E. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)[EB/OL]. http://www.oasis-open.org/committees/security/docs/. 2002(12).

[4] 任树怀,孙桂春. 信息共享空间在美国大学图书馆的发展与启示[J]. 大学图书馆学报, 2006(3):94-96.

郭秋萍 郑州航空工业管理学院教授,硕士。通讯地址:郑州。邮编450015。

焦 允 郑州航空工业管理学院讲师,硕士。通讯地址同上。

周九常 郑州航空工业管理学院副教授,博士。通讯地址同上。

(收稿日期:2007-12-05)