文章编号:1001 - 9081(2007)02 - 0288 - 04

一种简单跨域单点登录系统的实现

刘润达[1,2],诸云强[2],宋 佳[1,2],冯 敏[1,2]
(1. 中国科学院 研究生院,北京 100049; 2. 中国科学院 地理科学与资源研究所,北京 100101)
(liurd.05b@igsnrr.ac.cn)

摘 要:分布式体系架构下多站点协作网络的应用需要统一身份认证和资源访问控制机制,单点登录系统是完成这项功能的必备模块。采用一种应用于 Web 环境下轻量级的单点登录解决方案,它是一种基于 HTTP 重定向和票据,并以跨域 Cookie 的共享为核心的集中式认证系统。本方案在分布式数据资源共享网络建设中实现了多个站点的跨域全局登录、用户认证和用户授权等功能。通过建立规范的登录控制模块,简单地修改配置文件,就可方便地将分散网络节点加入认证体系,完成网络节点单点登录和资源访问控制问题。

关键词:单点登录;用户认证;数据共享
中图分类号: TP393.08 **文献标识码**:A

Implementation of a simple cross domain single sign on system

LIU Run-da[1,2], ZHU Yun-qiang[2], SONG Jia[1,2], FENG Min[1,2]
(1. *School of Graduate, Chinese Academy of Sciences, Beijing* 100049, *China*;
2. *Institute of Geographical Sciences and Natural Resources, Chinese Academy of Sciences, Beijing* 100101, *China*)

Abstract: Distributed structure based multi-sites corporation web applications need a universal authentication and resources access control mechanism, and Single Sign On (SSO) System is an indispensable module for such applications. In practice, we develop a simple single sign on solution that is a central authentication system based on HTTP Redirection and Tickets, with Cross Domain Cookie Sharing as key technology. This solution plays a vital role in distributed data sharing network construction, which realizes cross domain universal user login, user authentication and user authorization. By establishing standard control module, a simple configuration file may conveniently integrate distributed network nodes into one authentication system then accomplish Single Sign On and universal resources access control.

Key words: Single Sign On (SSO); user authentication; data sharing

0 引言

在当今分布式计算环境中,如何安全和方便地鉴别用户并控制其访问权限成为系统设计首要考虑的问题。单点登录(Single Sign On, SSO)提供一种机制,让不同的应用系统迅速获得统一的认证功能,实现全局、安全的软件环境。在实现 SSO 的系统中,用户只需进行一次登录操作,即可获得所需访问应用系统和资源的授权,不必多次输入用户名和密码来确定用户身份[1],即“一次登录,多方认证[2]”。

目前实现 SSO 的产品和解决方案众多[3],如:Microsoft 公司的 Passport[4], IBM WebSphere Portal Server[5]、Netegrity SiteMinder、Oracle 9iAS Portal Server 以及 Liberty 等。上述 SSO 产品的实现机制不尽一样,它们分别有着不同的侧重点并且适合于不同的系统架构。例如 Passport 单点登录身份验证技术采用集中式认证和分布式授权的模式,仅对用户进行单点身份鉴定,但是否允许用户访问某个特定的 Web 服务则由内容授权程序来确定;Liberty 协议是基于 SAML 标准的一个面向 Web 应用单点登录的与平台无关的开放协议,它的核心思想是身份联合(Identity Federation),两个 Web 应用之间可以保留原来的用户认证机制,通过建立它们各自身份的对应关系来达到 SSO 的目的[6]。尽管上述 SSO 产品能够较好地实现单点登录功能,然而,这些方案和产品有着各自的弱点,而且大都比较复杂且缺乏灵活性,在项目实践中很难快速实施。因此,在总结这些方案的基础上,本文在分布式数据资源共享网络系统中,提出一种简单的单点登录解决方案,它采用了基于票据的集中式架构,以跨域 Cookie 共享为核心来完成用户的登录、认证和权限控制。

1 票据和跨域 Cookie 共享

1.1 票据和 Cookie 的使用

在采用票据的 SSO 解决方案中,为维护用户全局登录状态,需要一个用于记录登录用户状态的唯一标识或凭证,这个标识就是票据,称为 Ticket 和 Token,是随机生成的一个全局唯一的字符串。

收稿日期:2006 - 08 - 14 **基金项目**:科技部国家科学数据共享工程:地球系统科学数据共享项目资助(2003DEA2C010)
作者简介:刘润达(1980 -),男,河南许昌人,博士研究生,主要研究方向:地学数据共享、地理信息系统; 诸云强(1977 -),男,江西广丰人,博士,主要研究方向:地球信息科学; 宋佳(1980 -),男,山西太原人,博士研究生,主要研究方向:地学数据共享、地理信息系统; 冯敏(1981 -),男,甘肃庆阳人,博士研究生,主要研究方向:地理信息系统开发与模型共享.

SSO 需要在客户机浏览器长久保留登录状态的票据,HTTP 是一种无状态的协议,用户在关掉浏览器时很难保持会话状态和保留票据。目前,常用而有效的方法是将生成的票据存储在客户机浏览器的 Cookie 里,当客户机在一定的间隔内重复访问服务器时就可以从 Cookie 里提取票据进行认证,不必提供用户名和密码。

Cookie 的存取只对同一域下的主机有效,分布式应用系统往往不能保证所有的主机都在同一域下。当用户登录加入 SSO 认证体系里的一台服务器时,例如:服务器 A,客户机浏览器可以将获得的登录用户票据记录到本地 Cookie 中,当此客户机转而访问服务器 B 的时候,为了实现单点登录,服务器 B 必须要获得标识用户登录状态的票据作为凭证来进行验证,而此票据存储于先前访问服务器 A 时留下的 Cookie,此 Cookie 只对来自服务器 A 域里的访问有效,为获取访问其他域主机的 Cookie,如何能够跨域共享 Cookie 成为本方案的关键。

1.2　跨域 Cookie 的共享

大多数 SSO 解决方案都是通过 HTTP 重定向(HTTP Rediction)或 Cookie 在 Web 应用间传递票据来实现单点登录,必要的时候,Web 应用间的后台通过 SOAP 协议来进行通信。本文采用 HTTP 重定向的方法来获取跨域 Cookie,实现 Cookie 的共享。

假设处于不同域下的服务器 A 和服务器 B 联合组成的网络应用需要统一的用户认证,客户机曾在服务器 A 进行了访问,并且在本地保存了服务器 A 的 Cookie,图 1 显示了客户机在访问服务器 B 的时候共享服务器 A 的 Cookie 的过程。

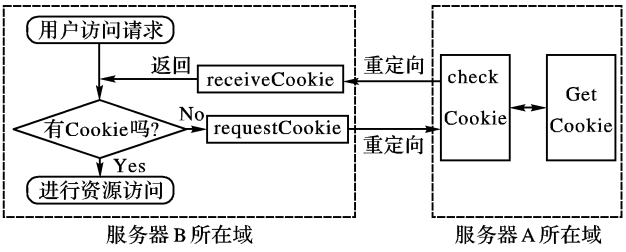

图 1　基于 HTTP Redirect 的跨域 Cookie 共享

1)客户机访问服务器 B 的页面,例如:index. jsp。服务器接到请求,检查客户机是否有对应的 Cookie,如果没有,则获取客户机浏览器访问服务器 A 时留下的 Cookie,通过处理逻辑 requestCookie 通过 HTTP Redirect 将客户机浏览器重定向到服务器 A 的处理逻辑 checkCookie,在发出的重定向请求中通过参数的形式将客户机原先访问服务器 B 的页面(index. jsp)作为返回地址带上。

2)服务器 A 的处理逻辑 checkCookie 收到这个重定向的客户端请求后,检查客户机浏览器是否有访问服务器 A 留下的 Cookie,并将客户端重定向回服务器 A 的接受逻辑 receiveCookie,同时把客户机上的服务器 A 留下的 Cookie 里的相关内容(若没有则为空)以及返回地址存入参数表,并重定向到服务器 B。

3)服务器 B 的处理逻辑 receiveCookie 接到客户端的重定向,从参数表中解析出 Cookie 的内容。利用这些内容在客户机上建立新的 Cookie,这时候客户机上关于服务器 B 的 Cookie 和客户机上关于服务器 A 的 Cookie 是一样的,类似于复制了一个 Cookie,服务器 A 所在域下的 cookie 在服务器 B 所在的域中实现了共享。

2　解决方案

地球系统科学数据共享网(以下简称共享网)是国家科技基础条件平台专项资助的科学数据共享网之一。项目目标是[7]:整合、集成分布在国内外数据中心、高等院校和科研院所以及科学家个人手中的数据,加工生产满足地球系统科学研究的数据产品,构建一个分布式的非盈利数据管理与共享服务系统,最终形成为地球系统科学基础与前沿研究提供数据支撑的国际化信息平台。

共享网架构在分布式体系之上,是由各个分布在不同地理位置的数据分中心组成的逻辑上统一的数据共享网络。共享网的分布式架构呈现出数据资源分散管理的特点,在这个系统中各个不同的数据中心有着不同的域名,并且有独立的门户网站和可供下载使用的数据资源。要实现用户在任意数据中心登录的情况下访问另外一个数据中心并继续保持登录状态而无需再次输入用户名和密码,就必须用到 SSO 机制。共享网跨域 SSO 方案的实施细节如下。

基于 Web 的单点登录的基本模式包含三个参与者:入口检查单元(GateKeeper)、身份认证单元(Authenticator)和用户凭证存储单元(Credential Store)。三者的基本分工是 GateKeeper 对用户的请求进行验证和重定向,Authenticator 对用户进行认证,凭证库存放认证的凭证或票据[8]。本文所提出的解决方案也遵循这三个层次的划分,GateKeeper 相当于单点登录的客户端,共享网的每一个数据中心的受保护资源和应用都受到 GateKeeper 的监控,当客户机访问受保护资源时,GateKeeper 有义务来确定客户机是否有权进行资源的访问;如果需要涉及认证,则它将用户请求重定向到 Authenticator 进行认证。Authenticator 是登录认证中心上单点登录的核心控制模块;Authenticator 通过在 Credential Store 里面进行查询来验证票据。

2.1　登录认证中心的设立

实现 Web 环境下的统一身份认证、集中授权的共享网单点登录系统是实现共享网逻辑上的统一性,简化用户管理的前提,为了简化分布式共享网用户管理,在共享网中我们采用集中式的单点登录系统,集中式的单点登录系统需要用户库和用户权限库的集中管理,因此需要设立登录认证中心(简称认证中心,Certificate & Authentication,CA)负责用户的登录、认证以及授权控制和登出。CA 同时维护用户库,并负责用户的注册等。

登录认证中心需要访问用户表以完成用户的登录验证,

表 1 是登录时所用到的用户表(USER)主要字段及涵义。CA 除了检查用户表来确定用户是否提供了正确的用户名和密码并进行用户全局登录外,还要能够提供用户级别的信息,以实现可访问资源的控制授权。例如,可以将用户级别分为 1、2、3 三级,对应不同的资源浏览、下载权限。在用户表上除了用户名和密码之外,增加控制用户级别的 USER_LEVEL 字段用于标识用户的级别。在用户级别复杂的情况下,也可以单独设立权限控制表(Access Control List,ACL)等,专门用于用户的权限角色管理,本文采用添加 USER_LEVEL 字段的方法。

表 1 登录认证中心 USER 表的主要字段

字段名	字段涵义
USER_ID	用户 ID
PASSWORD	用户的密码(MD5 加密过)
USER_LEVEL	用户级别

经过认证的用户处于全局登录状态,当用户跳转到其他分节点时需要确认用户是否登录,认证中心还要担任票据验证角色。用户全局登录后,登录中心要有记录登录用户的凭证库信息以便客户端查询,并提供票据验证服务,这此信息存储在如表 2 所示的 SSO_USER 表中,它通过外健 USER_ID 和 USER 表关联。TOKEN_ID 是用户登录后所分配到的随机登录票据。TOLERANCE 是本次用户登录所要持续的时间,例如 30 分种或是一天,此信息可在用户输入用户名密码时进行选择并进行记录。用户在提供票据需要认证的情况下,票据是否与某一用户名对应,还要将 CHECK_TIME 与当前时间相比较,如果差值大于 TOLERANCE,则说明当前的登录状态已经超时,则直接删除此条目,并将页面导向登录页面;如果没有超时,则更新 CHECK_TIME,用户认证通过。

表 2 SSO_USER 表

字段	字段含涵义
TOKEN_ID	用户登录标志票据
USER_ID	用户 ID
REG_TIME	首次登入时间
CHECK_TIME	最后认证时间
TOLERANCE	持续时间
LAST_SERVICE	最后一次访问的服务

登录认证中心不仅提供用户身份的统一认证,实现用户的统一管理,方便用户利用资源系统,同时由于采用集中式认证,用户的所有登录以及认证操作都在 CA 进行,这就为整个系统提供了一个日志控制的机会,可以加入适当的日志记录模块来监控整个网络资源的使用情况。例如可以方便地统计分析用户对现有资源系统的利用情况,以及访问资源的用户的所在的行业区域等,更好地为共享网的服务对象提供决策支持[9]。

2.2 用户登录流程和登出

共享网体系中存在很多的数据中心,当客户机访问某一个数据中心的时候,客户机并不知道曾经通过那个数据中心进行了登录验证,也不知道应该跨域获取哪个数据中心的 Cookie。对每一个节点进行遍历是行不通的,因此,把用户登录后的票据(TokenID)存入认证中心的 Cookie 中,客户机需要访问任意其他数据中心的时候,跨域共享认证中心的 Cookie,这样每次客户机都有一种固定的方法去寻找 TokenID,多个数据中心跨域共享 Cookie,简化了流程。

共享网跨域单点登录系统的登录及认证过程涉及客户机、数据中心和登录认证中心三个角色之间的交互,其登录流程如图 2 所示。

1)客户机访问某一数据中心网站的受保护资源,单点登录模块首先接管请求,查询客户机是否持有本数据中心的 Cookie,并试图获取其中的访问票据。如果客户机可以提供,说明用户曾经以合法身份访问过此数据中心,并且尚未在本地注销,转向 4);否则,要通过共享跨域的 Cookie 来确定是否进行全局登录,进行 2)。

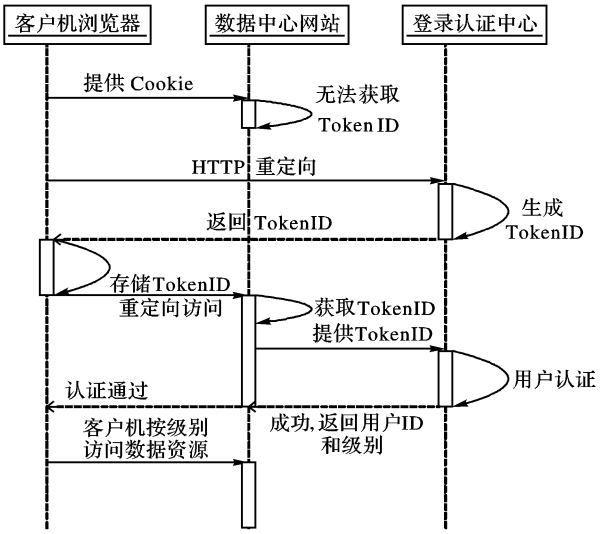

图 2 基于跨域共享 Cookie 的用户认证流程

2)这个步骤的主要工作是跨域获取 Cookie。客户机浏览器被重定向到登录认证中心,CA 试图获取存储于客户机的 Cookie,如果不存在,说明用户尚未全局登录,转向 3);否则,从 Cookie 中获取 TokenID。然后 CA 将客户机浏览器重定向回原先访问的数据中心,数据中心获取 TokenID 和返回地址,把 TokenID 写入客户端 Cookie 并跳转到返回地址,然后进行 1)。

3)重定向客户机浏览器到 CA 上的登录页面,认证中心获取登录用户名和密码并将其与 USER 表的信息核对,进行用户身份确认。如果没有这个用户或密码错误,直接返回登录失败;如果验证成功,随机生成标识此用户登录的唯一 TokenID,并生成一个条目放入凭证库 SSO_USER 表中,并把 TokenID 存入客户机的 Cookie 中。然后,通过跨域 Cookie 共享机制,把此 TokenID 转入客户机所访问的数据中心,将台写到客户机的 Cookie 中,用户完成登录,转向 1)进行资源访问。

4)客户机用 TokenID 来访问认证中心的用户状态查询服务,认证中心访问 SSO_USER 表确定该用户是否依然处于登录状态。如果处于登录状态则将用户名和用户的访问级别返

回数据中心,允许用户访问数据资源。否则,然后转向 3),提示用户输入用户名和密码。

在本方案的整个流程中,除了最初输入的用户名和密码外,其他所传输的都是票据,而最后客户机拿此票据获取登录用户的用户名而结束认证过程。

用户登出相对较简单,客户机只需提供 TokenID 给 CA 服务器,通过调用认证中心的注销服务,认证中心将 SSO_USER 表中标识该用户全局登录状态的记录删除,然后,为了使登出状态立即生效,删除当前数据中心的 Session 和 Cookie。

2.3 性能评价和改进

评价 SSO 系统主要考虑其可实施性、可管理性、安全性和易用性[10]。以跨域 Cookie 共享为核心的单点登录方案是一种轻量级的解决方案,认证中心可以作为一个独立的网络应用,单点登录的客户端可以部署在各个需要加入 SSO 认证的网络应用中,通过修改配置文件来指定受保护资源,并可将访问资源设置为完全控制或简单控制。这种机制灵活、简单,可实施性强;集中式的认证方便了对用户以及登录的控制,有较强的可管理性;通过票据,使用 SSO 功能的各个子系统无法直接获取用户的密码,提供了简单的安全措施;另外,模块化的设计方案使应用系统几乎不涉及太多的相关代码就能实现 SSO,简化了系统的复杂性,降低了认证系统与业务逻辑的耦合度,有较强的易用性。

对于集中式的 SSO 解决方案,CA 不仅维护着用户的信息还维护着用户登录状态,所有加入 SSO 体系的网络应用都依赖于 CA 服务器,因此它的健壮性相当重要。为了保证认证中心的畅通,可以在不同的物理位置建立两个登录认证服务器,一个为主认证中心,另外一个是备用认证中心,两个中心进行实时同步,在主认证中心发生故障的时候可以通过域名切换启用备用认证中心,最大限度地保证认证系统的健壮性。

对于认证服务器,简单地可以将用户信息和用户登录状态信息存放到关系数据库中。当用户登录比较频繁的时候,建议将用户信息表放到 LDAP 中,以提高效率。另外,为提高验证速度,把记录用户票据的 SSO_USER 表的部分信息放到内存数据结构中,以提高访问速度。

对于加入 SSO 认证体系的各个子系统,单点登录的控制逻辑中可以利用 Session 来提高访问效率。当用户获取认证后,可以将用户名和用户级别等标识用户已获取了验证状态的信息存入 Session 中,这样当用户访问下一个页面或是资源的时候,就不需要开启下一个认证过程而去访问服务器,降低用户认证系统对系统速度的影响。

3 结语

基于 J2EE 架构,我们实现了单点登录原型系统。系统采用 Tomcat5.x 作为 Servlet 容器,将客户端的功能做成一个独立的模块,并在地球系统科学数据共享网的多个数据中心网站进行部署,实践表明本文提出的以跨域 Cookie 共享为核心,基于票据的简单集中式的认证和授权方法的简单单点登录方案可以灵活地实现了分布式网络资源访问控制和统一的用户身份认证管理。

参考文献:

[1] 孙雷. 基于网格的 Web Services 技术分析及单点登录问题探讨[J]. 中国科技信息, 2005,17:39.

[2] 卢清平,杨柳,许晓东. 一个基于 Yale-CAS 的单点登录解决方案[J]. 合肥学院学报(自然科学版),2005,15(3):37 - 40.

[3] 徐永祥. 统一用户管理系统的设计[J]. 计算机工程,2003,29(5):120 - 123.

[4] Microsoft Passport Review Guide[EB/OL]. http://www.microsoft.com/net/services/ passport/review - guide.asp,2003.

[5] IBM 公司. IBM WebSphere V5.0 Security WebSphere Handbook Series[EB/OL]. http:// www.redbooks.ibm.com/abstracts/sg246573.html,2004.

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

[7] 孙九林. 中国地球系统科学数据共享服务网的构建[A]. 中国基础科学——中国科学数据共享学术讨论会专辑[C]. 2003.

[8] 韩伟,范植华. 基于 SAML 的单点登录技术在 Web 服务是的应用研究[J]. 计算机工程与设计,2005,26(3):634 - 636.

[9] 任河,李杰. 资源访问控制与统一身份认证技术的研究[J]. 机电产品开发与创新,2004,17(11):9 - 11.

[10] 张挺,耿继秀. Web 环境下的 SSO 实现模式的研究[J]. 计算机仿真,2005,22(8):128 - 131.

简　　讯

2006 年 12 月 12 日,《计算机应用》正式被列为英国《科学文摘》(SA,INSPEC)的来源期刊。英国《科学文摘》,简称 SA,是世界上拥有百年创刊史为数不多的检索性刊物之一,也是世界上最具权威性的检索工具之一。被 INSPEC 收录将会扩大我刊在国际上的影响力,并提高所发表论文的引用频次。INSPEC 的收录也有助于吸引高水平的稿件,使《计算机应用》的整体水平再上一个新台阶。

《计算机应用》编辑部

二〇〇七年二月