基于 Cookie 的单点登录技术

钟卫东

(山东胜利油田物探研究院,山东 东营 257022)

摘 要：在基于 Web 的多种应用系统中需要统一身份认证和资源访问控制机制，采用基于 Cookie 的单点登录系统是一种很好的解决方案，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。

关键词：Cookie；单点登录；跨域认证

中图分类号：TP393 **文献标识码**：A

Cookie-based single sign technology

ZHONG Wei Dong

(Geophysical Research Institute Shengli Oilfield, Dongying 257022, China)

Abstract: Web-based applications need a variety of uniform identity authentication and resource access control mechanism, based on the Cookie of the single sign on system is a good solution, it is a redirection based on HTTP and ticket, and Cookie to the sharing of cross-domain as the core of the centralized authentication system.

Key words: Cookie; single sign on; cross-domain authentication

随着信息技术和网络技术的发展，企业信息化建设已经进入了快速发展的阶段，随着企业信息化过程的不断深化，Web 应用系统规模也不断扩大，大量 Web 应用系统在办公自动化中得到广泛应用。每个应用系统出于安全因素考虑都建立了登录模块，用户访问不同的应用系统需要多次输入用户名和口令，使用非常不便，工作效率低下；而且众多的用户名和密码增加了系统管理的负担；用户名和密码的冗余存储造成了资源浪费；另外用户为了便于记忆常常会使用简单口令或相同口令，频繁的输入也大大增加了口令被非法截获和破解的几率。这些都会降低 Web 应用系统的安全性。

如何实现方便快捷、管理轻松、成本低、安全性高的认证已经成为当前企业 Web 应用中亟待解决的问题之一。建立一个跨平台、跨应用的基础性服务系统，将企业中各个应用系统的身份认证独立出来，进行集中统一管理，是解决上述问题行之有效的方法。每个用户只需要一套用户名和口令，进行一次身份验证，就可以对所授权的所有信息系统进行无缝访问。从而提高办公效率、方便系统管理、降低使用成本、提升企业 Web 的整体安全。这种解决方案就是单点登录 SSO(Single Sign On)，单点登录在企业 Web 系统中的应用，对于推动网络办公自动化的普及和发展具有十分重要的作用。

1 Cookie 概述

1.1 Cookie 的定义及功能

Cookie 是用户在浏览网页页面时，服务器发送给浏览器的体积很小的纯文本信息，它保存在客户机的内存中，或作为文件保存在客户机的硬盘中，用户以后访问同一个 Web 服务器时浏览器会把它们原样发送给服务器。通过让服务器读取它原先保存到客户端的信息，网站能够为浏览者提供一系列的方便。目前，Cookie 已广泛应用于 Web 应用中，如 Microsoft 的 Passport 单点登录服务就是借助于 Cookie 完成的。

1.2 Cookie 的组成

Cookie 由变量名和值组成。其属性里既有标准的 Cookie 变量，也有用户自己创建的变量，属性中变量是用“变量=值”形式来保存。

Cookie 的基本格式如下：

NAME=VALUE; expires=Date; Path=PATH;

Domain=DOMAIN_NAME; Secure

其中各项以“;”分开，首先是指定 Cookie 的名称，并

为其赋值。接下来分别是 Cookie 的有效期、URL 路径以及域名，在这几项中，除了第一项以外，其它部分均为可选项。

(1)NAME=VALUE 是每一个 Cookie 均必须有的部分。NAME 是该 Cookie 的名称，VALUE 是该 Cookie 的值。在字符串“NAME=VALUE”中，不含分号、逗号和空格等字符。如 NAME 是 role_cookie，其 VALUE 是 manager。

(2)Expires=DATE：Expires 变量是一个只写变量，它确定了 Cookie 有效终止日期。该变量可省，如果缺省时，则 Cookie 的属性值不会保存在用户的硬盘中，而仅仅保存在内存当中，Cookie 文件将随着浏览器的关闭而自动消失。

(3)Domain=DOMAIN_NAME：Domain 是 Cookie 在其内有效的主机或域名。Domain 确定了哪些 lnternet 域中的 Web 服务器可读取浏览器所存取的 Cookie，即只有来自这个域的页面才可以使用 Cookie 中的信息。这项设置是可选的，缺省时，设置 Cookie 的属性值为该 Web 服务器的域名。

(4)Path=PATH：Path 定义了 Web 服务器上哪些路径下的页面可获取服务器设置的 Cookie。该项设置同样是可选的，如果缺省时，则 Path 的属性值为 Web 服务器传给浏览器的资源的路径名。可以看出借助对 Domain 和 Path 两个变最的设置，即可有效地控制 Cookie 文件被访问的范围。

(5)Secure：在 Cookie 中标记该变量，表明只有当浏览器和 Web Server 之间的通信协议为加密认证协议时，浏览器才向服务器提交相应的 Cookie。当前这种协议只有一种，即为 HTTPS。

1.3 Cookie 的使用

有两种方式使用 Cookie，一是当用户用浏览器首次访问某 Web 站点(Web 服务器)时，服务器端先用 Set-Cookie header 来创建一个 Cookie，再用 Response 命令将 Cookie 写入访问者的计算机，此过程称作创建 Cookie；二是当用户用浏览器再次访问此 Web 站点时，用 Request 命令从访问者的计算机中以忽略路径的方式取回 Cookie，此过程称作读取 Cookie。

2 单点登录的关键技术

2.1 单域单点登录

单域单点登录指只有一个服务实体域，所有属于该域的服务实体都信任这个机构所认证过的用户，某一用户在成功登录单域中的任意一台 Web 服务实体以后，继续访问同一服务实体不需要再次经过认证，并且访问同一域的其他 Web 服务实体，也不需要经过认证。

采用 Cookie 技术解决 SSO 主要过程描述如下：

首先用户通过客户端浏览器，向应用服务器请求访问和使用受保护的资源，应用服务器分析请求，检查这个用户是否有已经创建好的有效的 Cookie，其中包含有效的用户 SSO 票据。如果没有有效的 Cookie，则应用服务器将用户的 Web 浏览器重定向到登录服务器。若验证成功，登录服务器产生一个有效的 Cookie，其中包含有效的用户 SSO 票据。为安全起见，一般要对此 Cookie 中的信息进行加密处理。登录服务器将含有 SSO 票据的 Cookie 发送给用户的 Web 浏览器，并将用户的 Web 浏览器重定向到原先请求的资源，向应用服务器再次请求访问和使用已申请的资源。验证成功，则向用户提供所请求的资源；若验证不成功，则拒绝用户访问所请求的资源或提示用户重新登录。图 1 显示了单点登录访问流程。

图 1 基于 Cookie 的单域登录流程

2.2 跨域单点登录

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，必需实现跨域共享 Cookie。

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 2 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。

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(CA)三个角色之间的交互。采用 Cookie 技术解决跨域 SSO 主要过程描述如下：

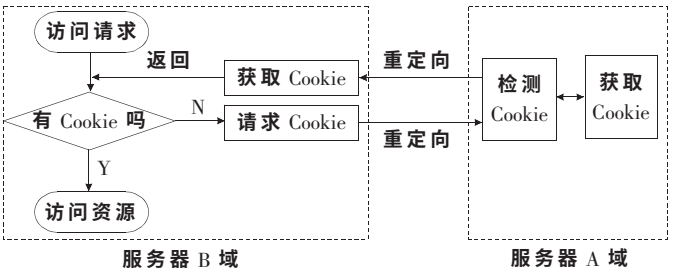

图 2 跨域共享 Cookie

(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)。

(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 中获取票据。然后 CA 将客户机浏览器重定向回原先访问的数据中心,数据中心获取票据和返回地址,把票据写入客户端 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用户信息库信息核对,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票据,并生成一个条目放入用户信息库中,并把票据存入客户机的 Cookie 中。然后,通过跨域 Cookie 共享机制,把此票据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)客户机用票据来访问认证中心的用户状态查询服务,认证中心访问用户信息库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,最后客户机拿此票据获取登录用户的用户名,从而结束认证过程。

3 安全性分析

保存有用户 SSO 票据的 Cookie 需要在客户端和服务器端来回传递,而一般情况下,在传输信道中 Cookie 是以明文形式传输的,本身也不能提供完整性等安全验证机制,而且它在客户端也是明文存储的,因此存在较大的安全隐患。因此,在认证系统中,需要有相应的安全措施,来保护 Cookie 的安全性。

(1)重放攻击。在本方案中每个 Cookie 均由产生者加上唯一的 ID 域和时间戳域,可以抵御重放攻击。

(2)消息篡改。因为 Cookie 存放在客户端浏览器中,虽然 Cookie 技术本身具备防止非授权服务器端篡改的手段,但是目前也发现可以通过伪造 DNS 域名来进行篡改。在本方案中,每个发布的 Cookie 均由发布者进行数字签名,各模块在使用这些 Cookie 时,首先签证数字签名的值是否正确,如果数字签名值为非法,那么拒绝该 Cookie。这样就可以完全杜绝 Cookie 被篡改的情况发生。

(3)窃听及中间人攻击。这种攻击是指认证过程的信息被他人查看,进而进行分析,最后将自己的数据替代原始数据。只要防止 Cookie 被其他人随意查看和分析,即可抵御该种攻击。可以在本方案中引入密钥的分配和管理系统,对系统中的各模块分配密钥和定时更新密钥。在认证过程中,对各种 Cookie 中的关键域值进行对称加密,防止中间人读取有效的数据。

企业单点登录方案将企业内部相对独立分散的网络应用系统进一步得到了统一,消除了企业信息化孤岛和数据冗余等问题,有效地实现了数据共享,使一个用户只要验证一次即可访问多个应用系统,解决了困扰单位内部不同部门应用系统重复登录和反复认证的难题,整个过程对于用户来说是透明的,不需要改变原有的业务流程。这样既方便了用户使用,又提高了网络办公的工作效率。当然,Cookie 的使用需要注意安全问题,要采用相应的安全技术。

参考文献

[1] 陈旭晖,林世平,庄世芳,等.基于 Web 服务的单点登录系统.福建电脑,2006,3.

[2] 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.

[3] 邱航,权勇.基于 Kerberos 的单点登录系统研究与设计[J].计算机应用.

(收稿日期:2009-02-11)