文章编号：2095－0411（2012）01－0062－03

基于 Web Services 多技术单点登录的研究与实现*

孙前庆，江　冰，辛元雪
（河海大学 计算机与信息学院（常州），江苏 常州 213022）

摘要：为解决用户在访问多个不同的应用系统而需要进行多次登录认证的困扰，提出了单点登录技术。通过分析现有的单点登录模型的优缺点，结合 Web service、Cookie 及 HTTP 重定向等关键技术，提出了代理和经纪人模型，解决了统一身份认证和异步验证两大比较核心的问题。同时，由于 HTTP 重定向技术以及 RSA 加密技术的采用，使本系统在安全和性能上得到保障。

关键词：单点登录；Web 服务器；内存信息块；HTTP 重定向；公钥加密
中图分类号：TP 393　　**文献标识码**：A

Research and Implementation of Single Sign－on for Multi－Technology Based on Web Services

SUN Qian－qing，JIANG Bing，XIN Yuan－xue
（College of Computer and Information Engineering，Hohai University，Changzhou 213022，China）

Abstract：To solve the problem of user repeated logon from various kinds of applications based on hybrid architecture and in different domains，a single sign－on architecture was proposed. On the basis of analyzing the advantages and disadvantages of existing single sign－on models，combined with the key technology like Web service，Cookie and HTTP redirects，two core problems such as unified identity authentication and asynchronous authentication were resolved. Meanwhile，the security and performance of this architecture were well guaranteed since the HTTP redirects and RSA encryption technology were adopted. The results show that this architecture is of high performance and it is widely applicable.

Key words：single sign－on；Web service；Cookie；HTTP redirects；RSA

伴随着信息化建设的不断深入，信息系统不断增多，用户需要记忆不同的用户名和密码，管理员对用户信息的维护也变得更加困难。同时，随着用户需要登录系统的增多，出错的可能性就会增加，受到非法截获和破坏的可能性也会增大，安全性就会相应降低。单点登录（Single Sign－On，SSO）系统就是为了解决上述问题而提出的一个解决方案。

单点登录是一种认证和授权机制，它允许注册用户只需要在任一应用系统上登录一次，而后授权访问其他应用系统，无需再进行登录[1]。目前实现 SSO 比较典型的模型包括经纪人模型、代理模型、代理和经纪人模型、网关模型以及令牌模型[2]。表 1 中分析了这些模型的可实施性和可管理性。

基于表 1 的比较，代理和经纪人模型因此兼具了集中管理和对原有应用服务程序的修改量少的优点，决定采用这种模型作为本模型的基础。

* **收稿日期**：2011－11－24
基金项目：住房和城乡建设部 2011 年科学技术项目计划（2011－S5）
作者简介：孙前庆（1985－），男，江苏徐州人，硕士生；通讯联系人：江冰。

表 1 各种单点登录实现模型的比较

Table 1 Comparison of a variety of single sign－on implementation model

SSO 实现模式	可实施性	可管理性
经纪人模型	对旧系统的改造量比较大	可实现集中式管理
代理模型	需要为每个旧系统新添加一个代理，移植比较简单	管理比较难以控制
代理和经纪人模型	移植简单，对旧系统的改造量不大	可实现集中式管理
网关模型	需要通过一台专用的网关才能访问各种应用	易于管理，但不同网关之间的数据库需要同步
令牌模型	实施比较简单	需要增加新的组件，增加管理的负担

1 系统整体架构

整个单点登录的架构如图 1 所示。整个系统由多个信任域组成，在每个信任域内有多台 B/S 架构应用的服务器。所有的应用系统都是通过统一门户系统绑定在一起，实现单点登录的功能。可以看出本架构是基于代理和经纪人模型的，其中统一门户系统扮演了经纪人的角色，而各种应用则扮演的是代理人的角色。各 B/S 架构应用都安装了 SSO Client 端，而统一门户系统安装的是 SSO Server 端，它们之间就是通过这两个代理来交互的。另外，图 1 中的认证服务器对外提供的是 LDAP 的认证接口，WebService 服务器提供了将单点登录用户信息和用户权限加载到认证服务器的接口。

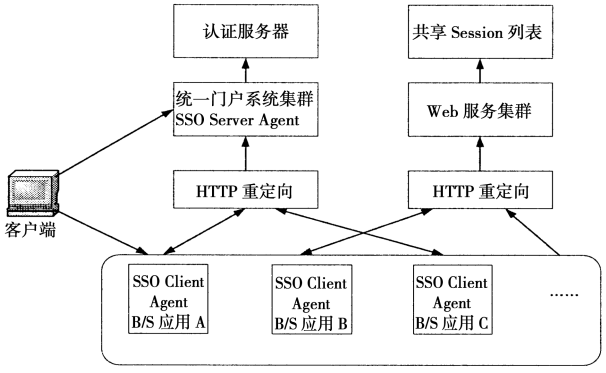

图 1 单点登录系统架构

Fig. 1 Single sign－on system architecture

本系统引入 Cookie 技术，将用户信息储存于客户端内存中，使系统的访问变得更加快捷和方便；同时，本系统采用定点自动发送异步验证请求机制，在用户登入应用系统之后，系统每间隔一定的时间向应用系统发送异步验证请求，定时巡检认证服务器 CaChe，若超时则从 CaChe 中删除用户信息。

2 系统设计与实现

2.1 异步验证机制实现方案

异步验证机制是为解决用户非正常关闭系统的情况下，单点登录服务器无法判断用户是否已登出系统的问题。在 SSO Client 中内置一个定时器，定时调用 Web Service 的 Get _ SSOCaCheUser（）接口发送异步请求到认证服务器进行身份验证，成功则更新用户缓存，失败则重定向到登录页面。在 SSO Server 引入用户缓存机制，缓存服务器定时进行巡检，将已超时用户信息删除。

Web service 是一种轻量级的独立的通信技术，通过简单对象存取协议（Simple Object Access Protocol，SOAP）在 Web 上提供的软件服务，使用 WSDL 文件进行说明，并通过 UDDI 进行注册[3]。如图 2 所示，用户通过 UDDI 找到某应用的 WSDL 描述文档后，他可以通过 SOAP 调用该应用提供的 Web 服务中的一个或多个操作。Web service 的最大特性还是他的跨平台性，无论是 B/S 架构或者是 C/S 架构的应用，无论是用 J2EE 实现的应用或者是用 .NET 实现的应用等，都可以访问 Web service，只要给出 Web service 服务器的 IP 和接口名称就可以对其进行访问。

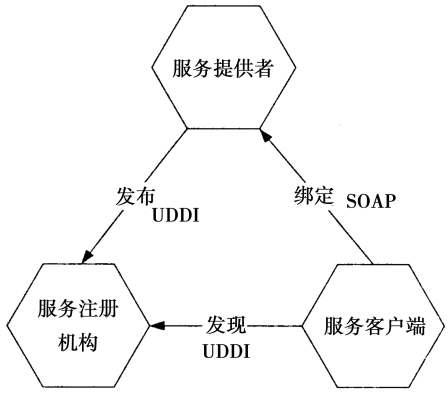

图 2 Web Service 架构

Fig. 2 Web Service architecture

本系统实现异步验证机制的流程如下：①用户成功登录统一门户系统，访问应用系统 A；②启动 SSO Client 中的定时器，每隔 10s 向认证服务器发送异步验证请求；③设置 SSO Server 端 Cache 超时时间为 5min，单点登录服务器用户缓存机制会定点进行巡检，将已超时用户信息删除；④异步验证请求调用 Web Service 中 Get _ SSOCaCheUser（）接口，将用户登录信息通过 XML 文档形式传递到 SSO Server 端；⑤单点登录服务器验证用户身份信息，成功则更新用户缓存，失败则重定向到

登录页面。

2.2 Cookie 技术实现统一身份认证

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他们原样发送给服务器。通过让服务器读取它原先保存在客户端的信息，网站能够为浏览者提供一系列的方便。本系统通过 Cookie 技术实现统一身份认证的流程如下：①检查客户端浏览器（Brower）是否开启 Cookie，如没有开启，则提示开启浏览器 Cookie；②SSO Server 检查 Brower 的 Cookie 中是否存在 SSO Server 发放的数字签名（Sign），若存在，则解密并读取其中的用户信息，若通过认证，跳转至步骤 4，否则将 Brower 重定向到登录认证页面。Sign 内容包括：用户编号 User _ ID、用户令牌 User _ Key、登录用户名称 User _ LoginName、用户名称 User _ Name、当前系统 ID System _ ID；③用户在登录页面中输入用户名和密码，提交给 SSO Server 进行认证；④SSO Server 进行认证，如认证不通过，提示用户名或密码错误。如通过认证，则向 Brower 的 Cookie 中重新写入 Sign，重定向用户 Brower 到原先请求的资源。

3 系统安全性分析

3.1 重放攻击

在数字签名 Sign 中包含用户令牌 User _ Key，它是由全球唯一标识码 Guid. NewGuid（）产生的，也就是在同一台电脑上由它生成的标识码重复的几率为零。这样就可以有效的防止重放攻击。而且在本系统中每个 Cookie 均由产生者加上唯一的 ID 域和时间戳域，都可以有效的防治重放攻击。

3.2 网络窃听

恶意者可以通过截获数据包窃取信息。本系统在用户登录进行身份认证以及发送用户名密码给 HTTP 对象时都采用了 SSL 协议，确保这些信息在传输过程中的保密性和完整性[4]。另一方面，Sign 使用 RSA 加密算法，RSA 加密采用的是公私密钥对，在 Web 应用服务器上保存的只有公钥，即使入侵者获得了公钥，也无法伪造出来相对应的私玥，这样就可以有效的防止入侵者截获 Sign，从而得到用户信息。

3.3 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。

4 结 论

本文构建了一个单点登录，与传统的单点登录模型相比，本文提出了一个基于 Web service 多技术的单点登录解决方案，该方案实现了对用户的统一身份验证和定点异步验证机制，优化了管理员对用户信息的统一管理，方便了用户对各应用资源的访问，提高了用户使用应用资源的效率，增强了用户访问各站点的安全性，也为以后集成更多的子应用系统提供了基础。

参考文献：

[1] PAKER T A. Single sign－on systems－the technologies and the products [EB/OL]. [2010－05－01]. http：//ce. sejong. ac. kr/～shindk/031 _ gia/xml/IEEE/SSO/Single% 20sign－on% 20systems － the% 20technologies% 20and% 20the% 20products. pd. f.

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

[3] IBM，Microsoft. Security in aWeb servicesworld：A proposed ar－chitecture and roadmap [EB/OL]. [2010－03－01]. http：//www. ibm. com/developerworks/library/ws－secmap/.

[4] 梁志罡．基于 Web Service 的混合架构单点登录的设计 [J]．计算机应用，2010，12（30）：3 363－3 365.

[5] 由雪梅，李大兴．基于 PKI 的 Web 单点登录系统设计与实现 [J]．计算机工程与设计，2007，28（9）：2 043－2 046.