# 一种基于 Web Service 的简单 SSO 系统实现

孟有意[1]，何明昕[1,2]
（1. 暨南大学 计算机科学系，广东 广州 510632；
2. 广州市信息技术研究所，广东 广州 510632）

摘 要：分析了现存多种 SSO 技术的优缺点，针对用户跨系统操作较多的分布式系统，提出了一种基于 Web Service 的以权限管理为核心的轻量级的单点登录实现方法。通过在某航空呼叫中心中的运用实践，很好地说明了该方法的实用性。

关键词：单点登录；统一认证；访问控制；Web Service
中图分类号：TP393 文献标识码：A 文章编号：1674-7720(2011)20-0009-04

## Implementation of a simple single sign-on system based on Web Service

Meng Youyi[1], He Mingxin[1,2]
(1. Department of Computer Science, Jinan University, Guangzhou 510632, China)
(2. Research Institute of Information Technology in Guangzhou, Guangzhou 510632, China)

**Abstract**: This paper analyzes the advantages and disadvantages of the many existing SSO technology, based on the kind of distributed system where users will cross the several systems in operation, we developed a simple Single Sign On (SSO) system based on the web service and take rights management as the core of the whole SSO system. By making application for some Call Center of an airline company and the success practice shows the strategy is practical.

**Key words**: SSO; universal authentication; resources access control; Web Service

在分布式构架的软件环境下，各协同站点都拥有各自的用户数据库，为解决同一用户在使用不同站点功能时需多次输入用户密码所带来的安全与管理不便的问题，单点登录机制提供了安全有效的途径。所谓单点登录，即用户在访问多个系统功能时只需进行一次登录操作，就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，即“一次登录，多处漫游”。应用单点登录机制可有效实现统一认证和资源访问控制。

## 1 一般单点登录模型

现有的实现 SSO 的产品和方案众多，典型代表有微软的 Passport 和自由联盟计划[1]。Passport 单点登录技术是 Microsoft 的重要组成部分。它主要采用集中式认证，分布式授权方案实现。从根本上说，Passport 属于一种基于访问票据的集中式单点登录模式，所有的用户信息都存放在 Passort.com 中，由 Passort.com 负责统一的身份验证。自由联盟计划(Liberty Alliance Project)与 Passport 不同，它是基于 SMAL 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，没有设立中心位置的认证系统，它建立了协作站点与认证系统的联盟关系，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。自由联盟计划虽然灵活性很高，但也因其过于自由的联盟组织，当联盟系统过多时将给管理带来不便。

除了以上两个比较有代表性的产品外，目前实现 SSO 的典型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]。其中，经济人模型与 Passport 实现方案类似，采用集中式管理，但是对旧系统改造较大；代理模型要在每个旧系统上添加一个代理，可移植性好，但管理相对困难；代理和经纪人模型结合了以上两者的优点，移植性好、管理相对集中；网关模式需要一台专门的网关，多个网关同步数据库比较困难；代理模式因为需要增加新的组件所以也增加了新的管理负担，但却增加了系统的安全性。

## 2 本文方案

通过分析并权衡上述 SSO 模型的优缺点，针对某些

大型企业内部协同合作站点相对固定且相对独立,需要维护独立的用户数据库,同时又有整个分布式系统环境下某些角色需跨系统操作且跨系统操作较多的特点,本文提出了一种基于 Web Service 和票据的集中授权,分布验证的单点登录实现方法。

### 2.1 Web Service 技术

Web Service 是一种轻量级的独立的通信技术,是符合某些标准的分布式应用构件,这些标准使它们能够在外部被访问,并且能够解决某些类型的行业问题。通过简单对象存取协议 SOAP (Simple Object Access Protoco) 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[3-4]。如图 1 所示,用户通过 UDDI 找到某应用的 WSDL 描述文档后,便可以通过 SOAP 调用该应用提供的 Web 服务中的一个或多个操作。

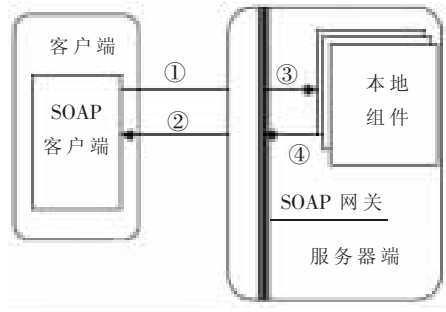

图 1 SOAP 协议模型

Web Service[5]在体系结构、设计、实现与部署等方面都比传统的分布式对象技术更加合理,它对外提供了可调用的接口,允许外来用户访问敏感信息和控制业务逻辑,虽然与传统的 Web 开发方式相比,Web Service 构建的商务逻辑更加开放和标准化,但其在安全性上表现出的弱点也给使用者带来很大难题。本文通过 Web Service 接口暴露的方法来实现系统间部分功能的协同作用,特别是各系统权限的管理也依靠 Web Service 技术实现,因而首先要考虑其访问控制上的安全性问题。

基于 SOAP 的访问控制,多数解决方案利用了 SOAP 基于 XML 的特点[5],在很多方面通过 XML 加密、签名等安全技术对 SOAP 协议 Header 和 Body 进行扩展来实现其安全性的增强。本文采用 Damiani 等人[6]提出的基于 SOAP 消息的过滤机制,通过校验 SOAP 头中的认证信息,过滤、修改,将 SOAP 消息转化为 RMA(远程调用)以实现对本地组件的访问控制。提供服务的服务器端由 SOAP 网关和本地组件组成,请求服务的 SOAP 消息到来时,首先要被 SOAP 网关截获经过解析验证后实现对 Web 服务的访问控制。通过校验的请求远程调用本地接口。其过程如图 2 所示。

### 2.2 权限管理

企业内部各系统间进行协同合作,资源访问控制是一个极其重要的问题。而进行资源访问控制首先要授予用户在各协同站点间的资源访问权限,规定其可访问的页面资源,可进行的操作。由于内部站点间合作密切,一个用户可能拥有多个系统的某些或全部功能权限。本文对权限的授予通过角色分配实现,使某种角色的用户拥有同一类资源访问权限,同一类资源访问权限可能跨越




① SOAP 请求 ② SOAP 响应
③ MRC 调用 ④MRC 响应

(2) SOAP 消息过滤机制

多个系统,集中地对所有权限进行分配,使得分工明确,便于管理。

建立专门的权限管理系统是集中对跨域用户进行权限管理的有效方案,将各系统拥有跨域操作权限的用户导入权限系统,并对这些用户及用户权限通过远程调用接口进行增加、删除、修改和查询。由于各个系统也分别拥有各自的用户数据库并拥有独立的角色分配模块,系统在整合时保留了各自系统管理员对本系统权限的分配管理,同时运用 Web Service 技术,在该系统与权限系统之间分别建立 Web Service 客户端和服务器端,同步权限系统对该系统用户权限角色的修改。同时当用户登录系统对协作系统受保护资源进行访问时,也需要通过 Web Service 调用接口以判断用户是否拥有该权限,这时权限系统就成了服务提供者,其他系统就是服务请求的客户端了。

而对协作系统页面的资源访问控制,则采用单点登录技术。拥有跨域权限的用户存储在中心权限管理系统的数据库中,权限管理系统为其分配访问协作系统的权限时,通过 Web Service 增加特定协作系统帐号到该用户本系统的帐号关联表,该帐号关联表如表 1 所示。用户登录时首先调用权限管理系统的校验程序进行校验,成功后,即主动查询本系统数据库中的帐号关联表,取出所有协作系统的帐号和密码进行加密、封装成票据并保存在 Coockie 中以供下次访问其他系统时直接从 Coockie 中获取使用。

表 1 帐号关联表

| 字段名 | 中文名称 |
|---|---|
| USER_ID | 用户 ID |
| SYSTEM | 协作系统名 |
| USER | 协作系统账号 |
| PASSWORD | 协作系统密码 |

### 2.3 Coockie 和 Ticket

单点登录的思想是使用户只需登录一次就可访问协同系统中的授权资源,这就需要记录用户登录成功的信息,HTTP 协议本身是基于请求/响应模式的,无状态的协议,因而必须采用某种跟踪机制用于记录用户登录成功信息。本文采用 Coockie 存储用户成功登入的信息,当用户验证成功后,后台自动查询账号关联表,并将帐

号关联信息经加密后形成 SSO Ticket 以约定的方式分别存储在相应的 Coockie 中，以备协同系统使用。要取得 Coockie 中的 Ticket 信息，就要知道对应系统 Coockie 存放的位置。这就需要各协同系统对这些协同系统的 Coockie 存放位置进行约定，并将这些信息存储在数据库中。该协同系统 Coockie 信息表结构如表 2 所示。

表 2 协作系统 Coockie 信息表

| 字段名 | 中文名称 |
|---|---|
| SYSTEM | 系统名 |
| COOCKIENAME | Ticke 写入的 Coockie 的名字 |
| DOMAIN | Coockie 的域名 |

Ticket 为密文，存放协同合作系统的帐户信息，包括系统名、用户名、密码。加密 Ticket 前应对 Ticket 的格式进行约定以便于提取使用，如设为：系统名 && 用户名 && 密码。

## 3 实验分析

航空公司业务比较复杂，不同的业务类型分布在不同的系统上，实现一个特定的业务流程往往需要协同合作多个系统，所以资源访问控制是非常重要的问题。运用上节提出的方案，航空公司内部各系统如呼叫中心、投诉系统、B2C 系统等协作站点都将权限管理工作集中到专门的权限管理系统，通过在各个系统之间建入 Web Service 服务器端和客户端，实现远程调用协同合作站点的功能接口，如判断呼叫中心的座席是否有修改客户信息的权利。对协同站点页面资源的访问控制则可由 SSO 机制来实现。

### 3.1 登录流程

现代呼叫中心应用了许多先进的通信和计算机技术，包括硬件和软件方面的技术。本文所论及的呼叫中心只是航空公司整个呼叫中心的软件系统实现部分。其实现需与公司其他相邻系统进行协同合作：如 B2C 系统、B2B 系统、投诉系统、大客户信息管理系统等。以座席为例，说明使用呼叫中心系统时单点登录的过程。流程图如图 3 所示。

(1) 首次登录呼叫中心系统，座席输入用户名和密码信息。

(2) 远程调用权限管理系统的验证程序进行有效性校验。

(3) 若帐号验证有效，系统则自动查询该帐户下所有协作系统的登录帐号信息，以约定的组织格式：系统 && 用户名 && 密码经 DES 加密后保存为 Ticket，并通过查询系统 Coockie 信息表获得对应系统存放 Coockie

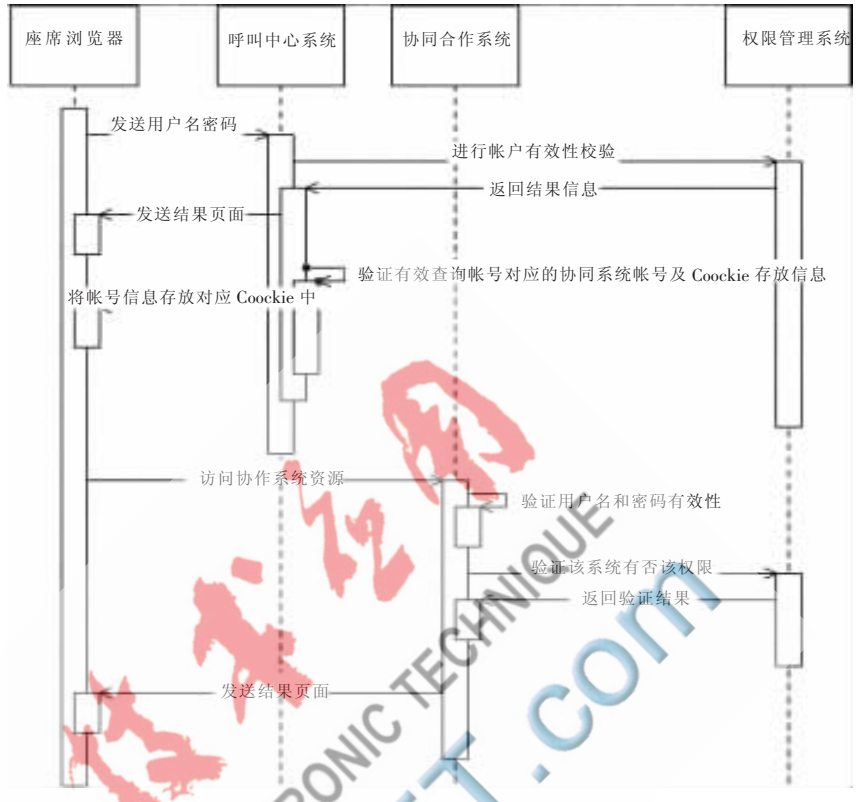



图 3 单点登录流程图

的相关信息，分别查看浏览器中是否存有信息表中对应的 Coockie，有则通过 setCoockies 方法将 Ticket 存入相应 Coockie 并覆盖之，无则创建该 Coockie 并存入指定位置。若帐号信息验证无效，返回(1)。

(4) 访问其他协作系统时，通过 getCoockie 获取相应 Coockie，若获取成功，则解密 Ticket 分解出帐户信息进行登录验证操作，若获取不成功，说明该用户角色无此资源访问权限。

在本方案的整个流程中，除了最初输入的用户名和密码外，其他每次登录系统时所需帐户信息都是通过获取客户机端对应的 Coockie 中存储的帐户信息进行。关闭浏览器时删除所有 Coockie 信息，即登出系统。

### 3.2 性能分析

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[7]。本文使用专门的权限管理系统对所有协同合作系统中的用户及其权限统一管理，各系统保持其原有用户存储和验证方式，对有需要进行跨域操作的系统中增加 Web Service 客户端远程调用权限系统的校验接口进行有效性校验，主调系统主动保存所有协作系统的登录信息到 Coockie，在需要访问时直接获取 Coockie 中对应系统信息进行对应系统本地验证，这有别于已有的集中式单点登录方案，只需调用系统原有校验程序而不需在跨域时调用权限系统进行校验，可大大减少多用户并行操作时权限管理系统的负担。权限系统对各跨域用户进行权限的分配管理，各系统通过远程调用权限管

理系统接口进行权限的查询。整个 SSO 验证用户过程是受访系统对用户帐号的验证及通过 Web Service 技术远程调用权限系统的验证过程。因而与常见集中式认证 SSO 系统相比,传递的 Ticket 信息包含 SSO 之前所需的用户名密码,验证程序也只需增加存储登录用户协作系统对应帐户信息到相应 Coockie 的功能,改动较少,可实施性较强。对所有协同系统通过采用分步认证与集中管理授权,有较强的可管理性。通过加密票据,并将其存放在对应系统可访问域中,提供了简单的安全措施。另外,新增协同合作系统时,只需对该系统的各角色创建新的用户密码,并在权限系统中将拥有该角色权限的其他系统用户的帐户关联信息进行更新即可,有较强的易用性。

本文基于 Web Service 技术在原有系统的基础上,构建了单点登录机制。通过将 SOAP 消息转换为 RMA(远程调用)对系统间的 Web 服务进行安全的访问控制,实现了用户及权限的管理。同时使用 Coockie,DES 加密技术在系统间传递关联帐号实现了单点登录过程。实验表明,本文采用的方案具有良好的可管理性、可实施性、安全性和易用性。

参考文献

[1] 毛捍东,张维明.一个基于 Web 服务的单点登录系统[J].计算机工程与应用,2004(24):18-20.

[2] DUBOISD, PRADEH. Putting rough sets and fuzzy sets together[M]. Dordrecht,Netherlands: KluwerAcademic Publishers,1992:203-222.

[3] GRECOS, MATARAZZOB, SLOW INSKIR. Fuzzy similarity relation as a basis for rough approximations[C] // Proceedings of RSCTC'98. Heidelberg: Springer Verlag,1998:283-289.

[4] 梁志罡.基于 Webservice 的混合架构单点登录的设计[J].计算机机应用,2010.30(12):3363-3365.

[5] 许峰,林果园,黄皓. Web Service 的访问控制研究综述[J].计算机科学,2005,32(2):1-4.

[6] SIRER E C, WANG K. An access control language for web services.In:Proc.of the ACM Symposium on Access Control Models and Technologies, ACM Press,2002:23-30.

[7] 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.

(收稿日期:2011-07-19)

作者简介:

孟有意,女,1987 年生,硕士研究生,主要研究方向:软件工程。

何明昕,男,1963 年生,硕士,副教授,主要研究方向:软件工程、并行分布式网络计算。