基于 Web 服务的单点登录系统的研究与实现

胡毅时 怀进鹏
(北京航空航天大学 计算机学院, 北京 100083)

摘 要: 随着分布式计算技术与应用的不断发展, 基于动态、松耦合环境的业务流程将涉及到多个服务提供商, 以致用户在完成这样的业务时需要面对多次登录的困扰. 针对这个问题, 分析了在分布式环境中基于 Web 服务的用户单点登录机制, 并设计实现了 Web 服务应用支撑环境中的单点登录系统, 使得用户只需登录一次即可完成复杂业务.

关 键 词: 计算机应用; 分布型网络; 认证; 单点登录; Web 服务
中图分类号: TP 393.08
文献标识码: A 文 章 编 号: 1001-5965(2004)03-0236-04

Research and implementation on Web services-based single sign-on system

Hu Yishi Huai Jinpeng
(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

Abstract: Users need to authenticate themselves to each service provider during they finish an operation that involves several services owned by different providers in the dynamic loose-couple environment because of development of distributed technology and application. Analyses the Web services-based single sign-on mechanism in a distributed environment and implements the single sign-on system in the Web services-based supporting application environment.

Key words: computer applications; distributed networks; identification; single sign-on; Web services

随着互联网软件技术和应用模式的不断演变, 基于 Web 服务的分布式计算模式正在成为发展的潮流. 许多企业和政府部门已开始基于 Web 服务在互联网上提供信息共享与应用服务, 并构建跨企业的虚拟组织或虚拟企业, 以实现大规模的资源共享. 出于安全性考虑, 每个企业(或应用系统) 都需要根据用户的身份来进行访问控制及审计等安全操作. 由于用户完成一次活动/交易所要访问的服务可能分布在不同的应用系统中, 用户在进入不同的系统边界时都需要进行登录(如多次输入用户名和口令) , 这将影响执行效率并使用户失去耐心, 影响其对服务提供商的信心. 针对这个问题, 本文在基于 Web 服务的分布式环境中设计实现了一个跨应用系统边界的单点登录机制, 并实际应用于 Web 服务应用支撑环境 WebSASE[1] 中, 其中通过使用安全声明标记语言(SAML, Security Assertion Markup Language)[2] 来描述用户身份以实现身份信息的共享.

1 单点登录机制的设计原理

1.1 设计思想

在基于 Web 服务的企业联盟应用系统中, 可以将单点登录机制的基本需求概括如下:

1) 一致性: 用户在访问联盟中的多个应用系统时, 不需要反复认证自己身份;

2) 分布性: 该机制是基于松散的信任模式, 即不能完全依赖于一个联盟内企业都信任的集中式的身份认证服务器;

3) 可扩展性: 能够适用于多种现有的认证机制, 并能方便地增加新的认证机制;

收稿日期: 2002-11-29
基金项目: 国家 863 高技术研究发展计划资助项目(2001AA113030, 2001AA115110)
作者简介: 胡毅时(1979-) , 男, 江西樟树人, 硕士生, huyishi@travelsky.com.

4) 可管理性: 对于系统管理员来说, 该机制易于配置和管理.

为便于理解和叙述, 首先给出必要的基本概念.

定义 **1**　安全域(security domain). 一个安全域是一个逻辑和管理意义上的范围或区域, 其中由安全服务的管理员定义和实施了一个单独的、一致的本地安全策略[3].

定义 **2**　信任状(credential). 一个信任状是一个实体用来证明自己身份的数据[4].

定义 **3**　本地用户(local user). 本地用户是只能在一个安全域内被管理和被识别的用户身份.

定义 **4**　全局用户(global user). 全局用户是指能被一个企业联盟内所有安全域所识别的用户身份.

基于上述概念, 给出如下基本假设:

假设 **1**　联盟唯一标识假设. 一个企业联盟是由多个安全域组成, 每个安全域在联盟内都有唯一的身份(通过 X. 509 证书[5]来标识), 对该集身份的信任是建立在一个共同信任的 PKI 基础之上的.

假设 **2**　本地用户假设. 每一个安全域都维护一个本地用户身份标识集合.

假设 **3**　本地授权假设. 安全域内的授权、审计等安全操作只针对本地用户身份标识进行.

根据单点登录的需求, 当用户在一个安全域登录以后, 如果用户需要访问其它安全域的服务, 则需要将这次登录的结果传播到目标安全域. 为了在联盟内实现这样的机制, 本文引进了身份担保机制和身份映射机制, 来实现安全域之间用户身份信息的共享.

定义 **5**　身份担保. 设 I, J 是分布式应用环境中的任意两个安全域, A 为任意一个用户, 身份担保是指 A 在 I 认证自己身份以后, 当 A 想要访问 J 的服务时, 并不是直接向 J 提交用户名/口令来证明自己的身份, 而是由 I 来向 J 证明 A 的身份.

为了实现身份担保机制, 在安全域中引入身份担保服务(如图 1 所示), 用户首先在安全域 I 登录, 并请求它所提供的担保服务, I 的担保服务将生成一个身份担保票据交给用户; 当用户需要访问安全域 J 所提供的服务时, 将该身份担保票据作为信任状提交给 J 来认证自己的身份, J 的认证服务根据该票据得到用户的认证信息; 当需要进一步认证时, J 的认证服务还可以访问 I 的担保服务, 以得到该用户更详细的身份信息.

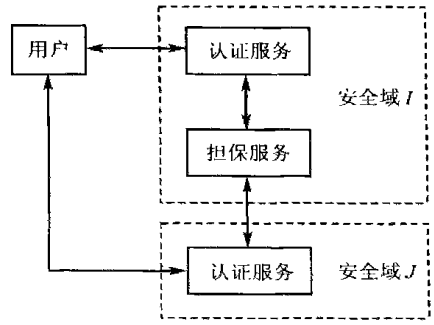

图 1　身份担保

通过身份担保机制, 服务提供者可以确定服务请求者是否拥有来自另一个安全域的身份标识(在这里, 担保者的身份和被担保的用户身份构成一个全局身份), 但是, 根据前面所提出的安全策略, 对于安全域中的授权或审计服务来说, 该身份标识只能识别为属于本地身份集合的一个身份标识, 所以需要把全局身份标识映射为本地的一个身份标识. 因此, 在目标安全域内引入身份映射服务, 完成从全局身份到本地身份的映射工作.

定义 **6**　身份映射. 设 A 为任意一个全局用户身份标识, B 为任意一个安全域 I 的本地用户身份标识, 身份映射是指当拥有身份 A 的某个客户访问 I 时, 所需要进行的从 A 到 B 的转换 $\eta: A \rightarrow B$.

例如: 在 X. 509 V3 数字证书中, 用户的可辨别名(DN, Distinguished Name)、发布者的 DN 和证书序列号三者绑定在一起作为证书拥有者的身份标识. 假设这个证书被用于表达服务请求者的身份, 而目标安全域中使用用户名/口令的方式来标识用户身份, 那么在对请求者授权之前, 身份映射服务通过一定的策略将该基于 X. 509 证书的身份标识映射为一个本地的用户身份标识. 这个映射策略的定义可以很灵活, 如可以将某个安全域的每一个用户都映射成为预定义好的一个本地用户, 也可以映射成为一个动态的本地用户, 甚至可以将其它安全域的所有用户都映射成为一个本地用户.

基于上述讨论, 再进一步对基本假设的限制条件进行分析.

在基本假设中, 假设 1 为联盟建立的基础, 是必须的; 而假设 2 和假设 3 不是必须的, 在不满足假设 2 和假设 3 的情况下, 即如果某安全域不维护本地用户身份集合, 或者允许直接对全局用户身份授权, 在这种情况下, 本系统中的身份映射机

制是冗余的,但系统仍然是实用的.

1.2 系统功能结构

根据身份担保机制和映射机制,本文设计实现了基于Web服务的面向企业联盟应用环境的单点登录系统(WebSSO, Web services-based Single Sign On system).

在联盟中,每个安全域都可以有自己的身份担保服务,负责向用户发放身份担保票据,来向其它安全域担保本安全域已认证的用户身份.在联盟之内,每个成员安全域都可以有选择地信任其它一些安全域,即被这些安全域担保的用户身份可以被映射成为一个本地用户身份进行授权和访问控制.对于某些安全级别不高或者处理能力较弱的成员来说,它可以完全将用户身份认证的工作交给它信任的安全域,而不直接在本地认证用户的身份,从而降低了安全信息管理的难度,提高跨安全域边界认证效率.

由于历史或技术等各种原因,各个安全域内部所采用的认证机制可能不完全一样,因此使得身份描述信息各不相同,为了保证良好的可扩展性和互操作性,需要一个通用的、独立于不同应用系统认证方式的表述格式来描述用户身份.而基于XML的SAML具有很好的可扩展性和强大的描述能力,它可适用于多种认证机制,并且受到标准化组织和大公司的支持,正在被业界广泛采用,因此采用SAML认证声明描述用户身份可以较好地满足上述要求.

在获得用户身份信息后,系统还需根据用户的全局身份信息以及预定义的映射策略,完成从全局身份到本地身份的映射;本地安全域的管理员可以维护一个身份映射表,描述全局用户和本地用户的映射信息.由于全局用户的数量较多且动态变化,为管理员带来较大的负担.因此通过定义一个灵活的策略库来实现这个映射,减轻管理员的负担,并可避免一些人为的错误.

由于现有的Web浏览器不支持对Web服务的调用,因此为了直接访问Web服务,必须使用面向Web服务的通用客户端;同时,为了能够实现单点登录,客户端需要一个票据管理模块来实现必要的票据管理功能,如存储从担保服务返回的身份担保票据;当用户需要访问联盟内的其它成员所提供的服务时,则将身份担保票据附加在SOAP消息头部,作为一种身份信任状传递给服务提供者.

综上所述,提出了单点登录系统WebSSO的主要模块功能如下:

1) 担保服务模块:采用SAML认证声明[2]来描述身份担保机制中的用户身份,实现SAML认证声明的生成、解析、存储和销毁,并对联盟中的合作伙伴提供SAML认证声明的查询服务.同时实现用户身份担保票据(其中包含关于认证声明的引用,代表所在的安全域向其它安全域担保用户身份)的生成、发放、解析和验证;

2) 认证模块:负责对服务请求者的身份进行认证,它除了负责认证本地用户身份以外,还需要支持基于身份担保的认证方式;并能够验证担保者的身份,解析SAML认证声明,识别其中所包含的用户身份信息,得到服务请求者的全局身份,供身份映射模块使用;

3) 身份映射模块:根据预定义的身份映射策略来完成全局用户到本地用户的映射;

4) 通用客户端的票据管理模块:负责用户身份担保票据的获取、存储、使用和销毁.

2 WebSSO系统的实现

2.1 系统运行时结构

基于上述讨论,为了更好的支持面向Web服务的企业联盟中的单点登录,本文把对单点登录的支持作为一个基本特性融入到WebSASE中,使得只需通过一定的配置即可将部署在WebSASE上的Web服务加入现有的企业联盟的单点登录框架中,从而很方便地实现资源和服务的共享.

图2给出了WebSASE的体系结构图[1].其中Web服务容器是Web服务的运行承载体,是Web服务的调用中介,其目的是通过这种"容器"结构使部署在其中的Web服务都能够通过容器获得由运行环境提供的共性基础服务,这些基础服务

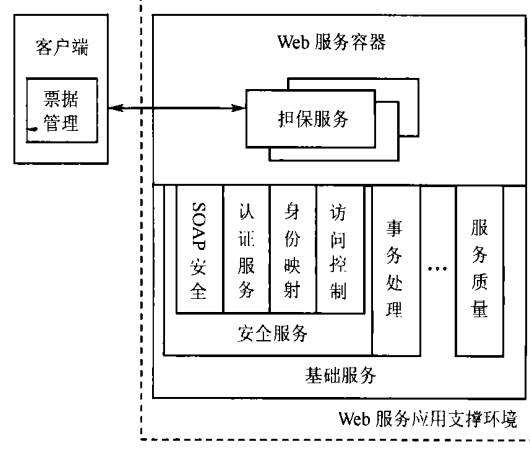

图2 WebSASE体系结构

同 Web 服务的容器一起构成了 Web 服务运行时的支持平台; 用户可以多种通讯协议(如 HTTP, SMTP) 来访问部署在容器中的 Web 服务[1].

为了满足对单点登录的支持, 在 WebSASE 支撑环境中实现了 WebSSO 系统的功能模块, 同时, 为提高系统地可扩充性, 可根据应用需要对原有的模块进行改造, 以适应多种单点登录需求. 图 2 中担保服务、认证服务、身份映射和客户端票据管理模块即为 WebSSO 系统的主体功能模块.

2.2　实例分析

设 *I*, *J* 为任意两个 WebSASE, *A* 为 *I* 中的任意一个用户, *A* 通过 WebSSO 系统实现单点登录的工作机理如下:

1) 用户 *A* 使用信任状(如用户名/口令) 在 *I* 上登录, 并请求部署在 *I* 中的担保服务; 担保服务根据 *A* 的身份生成 SAML 认证声明并存入声明存储库, 将该声明的引用作为用户身份担保票据 *T* 返回给 *A*;

2) *A* 需要访问 *J* 时, 则通过 SOAP 安全扩展[6,7] 将 *T* 作为信任状封装在 SOAP 请求消息头部发给 *J*;

3) *J* 的认证模块访问 *I* 中担保服务所提供的声明查询方法, 得到关于 *A* 的认证声明, 验证该声明的有效性, 然后解析出用户 *A* 的详细身份信息, 并与担保者 *I* 的身份合在一起作为全局身份交给身份映射模块处理;

4) *J* 的身份映射模块根据身份映射表及策略库中的身份映射策略完成从全局身份到本地身份的映射, 然后将本地身份返回给认证模块, 以便交给后续的访问控制及审计等模块使用.

从上述过程中可以看出, 通过 WebSSO 系统, 用户 *A* 只需要使用一次用户名/口令就能访问部署在不同 WebSASE 中的 Web 服务, 既简化了用户的操作, 也减少了口令泄漏的危险; 尤其在动态的分布式环境中, 用户不可能在每个安全域中都拥有身份, 通过使用 WebSSO 系统, 利用身份担保机制, 能够有效地实现用户身份的传递, 完成跨安全域的单点登录.

3　结 束 语

本文实现的 WebSSO 系统能够在分散的信任基础上实现多种认证机制间用户认证信息的交换, 比较好地解决了用户在面向 Web 服务的分布式环境中单点登录的问题.

参考文献 (**References**)

[1] 葛　声, 胡春明, 杜宗霞, 等. 基于 Web Service 的应用支撑环境研究与实现[A]. 见: 梅　宏, 王千祥. 2002' 全国软件与应用学术会议(NASAC) 论文集[C]. 北京: 机械工业出版社, 2002. 97~102
Ge Sheng, Hu Chunming, Du Zongxia, *et al*. A Web service-based application supporting environment [A]. In: Mei Hong, Wang Ganxiang. Proceedings of National Software and Application(2002) [C]. Beijing: China Machine Press, 2002. 97~102(in Chinese)

[2] Hallam-Baker P, Maler E. Assertions and protocol for the OASIS security assertion markup language [EB/OL]. http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf, 2002-05

[3] Shannon B. Java™ 2 platform enterprise edition specification v1.3 [EB/OL]. Sun Microsystems Inc, 2001-07

[4] ITU-T X.800, Security architecture for open systems interconnection for CCITT application[S]

[5] ITU-T X.509, Information technology-open systems interconnection——the directory: public-key and attribute certificate frameworks[S]

[6] Brown A, Fox B, Hada S, *et al*. W3C SOAP security extensions: digital signature[EB/OL]. http://www.w3.org/TR/2001/NOTE-SOAP-dsig, 2001-02-06

[7] Atkinson B, Libera G D. Web services security (WS-security) version 1.0[EB/OL]. http://msdn.microsoft.com/ws/2002/04/Security/, 2002-04-05