面向 ASP 模式的单一登录机制的研究与实现 *

李　博, 葛　声, 沃天宇, 马殿富
(北京航空航天大学 计算机学院, 北京 100083)

摘　要: 提出一种安全域内安全信息的集中存储和统一访问手段,以及账号联合、认证代理和授权代理方法,解决了 ASP 模式下异构安全系统间认证和授权结果的共享及单一登录问题,设计实现了 ASP 模式下安全域内与安全域间统一的单一登录系统。

关键词: 应用服务提供; 单一登录; LDAP; 安全声明标记语言
中图法分类号: TP393.08　　**文献标识码**: A　　**文章编号**: 1001-3695(2005)01-0029-05

Research and Implementation of Single Sign-on Mechanism for ASP Pattern

LI Bo, GE Sheng, WO Tian-yu, MA Dian-fu
(School of Computer, Beijing University of Aeronautics & Astronautics, Beijing 100083, China)

Abstract: Proposes a method which stores information in a uniform format, accesses it in a standard interface and exploits account federation, authentication proxy and authorization proxy to transfer the results of authentication and authorization between different security systems. As a result, a single sign-on system through this method is designed and implemented.

Key words: Application Service Provider; Single Sign-on; LDAP; Security Assertion Marked Language

1　引言

在互联网环境下,ASP 软件平台和 ASP 应用服务是企业信息化与电子商务的一种发展趋势。基于信息门户技术[1]的 ASP 软件平台能够提供或整合企业内部的多种信息系统,如办公自动化、电子邮件、协作平台等,并以统一的用户界面方式提供给用户,为企业相关的管理者、应用提供商和用户提供统一的服务接入点。ASP 软件平台所整合的多种应用系统往往出于安全性考虑,具有相对独立的身份认证和授权机制,使得 ASP 软件平台和用户必须面对安全机制的多样性和异构性,从而导致如下问题[2,3]: ①用户重复登录问题。ASP 软件平台和各系统具有独立的身份认证机制,用户记忆大量账号并多次登录,工作效率低且不安全。②系统授权管理复杂问题。ASP 软件平台用户信息和安全策略独立、分布存储、用户权限管理复杂,存在安全漏洞。③安全信息的共享问题。多个具有异构认证机制的企业 ASP 软件平台协作完成任务时,认证结果无法传递,需要用户跨越企业边界进行多次身份认证和授权。因此,统一用户和安全策略管理、统一认证授权、企业内各应用系统间和企业间统一的单一登录成为 ASP 软件平台建设亟待解决的问题。

针对单一登录问题,国内外开展了大量的研发工作。.NET Passport 技术采用集中式认证、分布式授权实现身份认证和访问控制[4],但没有使用标准协议交换和传递认证信息,实现安全信息共享。Liberty 技术通过多层账号映射建立认证链,合作站点和认证站点间采用 SAML 通信[5],但是存在系统结构复杂和认证链管理复杂等问题。目前已有的 SSO 系统,如 Windows 2000 中集成的 SSO 系统[6]、Netegrity 的 SiteMinder[7]等,它们的共性技术特点是:局限于特定的企业产品环境中实现单一登录功能,难以集成其他公司的应用系统。因此,不适用于解决集成了具有异构身份认证系统的 ASP 软件平台在授权管理和安全信息共享等方面的新需求。

本文通过分析应用需求和已有解决方案,提出了一种基于 LDAP[8]和 SAML[9]的 ASP 软件平台内各系统间以及 ASP 软件平台间的单一登录解决方案,如图 1 所示。通过 LDAP 统一存储和管理 ASP 软件平台的账号信息和安全策略,支持以标准的方式访问目录服务中存储的信息,作为实现统一的身份认证和授权的基础,同时采用 SAML 作为安全域间认证和授权结果的标准化表示和传递方式,从而实现安全信息的共享。

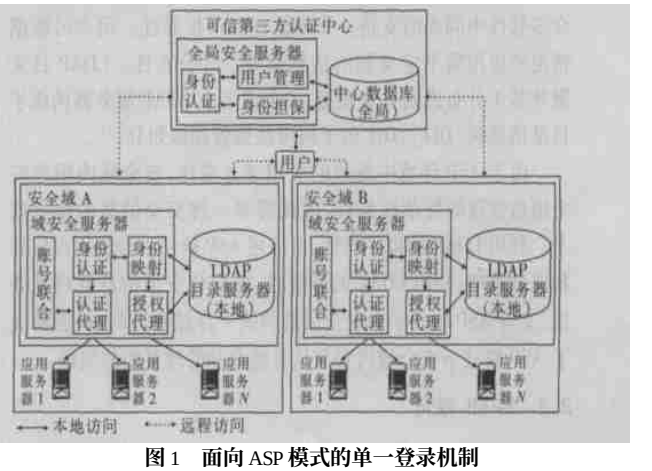

图 1　面向 ASP 模式的单一登录机制

2　单一登录技术背景

面向 ASP 模式的单一登录机制主要以传统的单一登录技

收稿日期: 2004-02-11; **修返日期**: 2004-04-20
基金项目: 国家"863"计划资助项目(2001AA113030,2001AA115110,2001AA414020)

术为基础,同时涉及安全信息的传输、共享技术和安全策略的标准化存储和访问技术。

2.1 传统单一登录技术

单一登录是指当用户需要访问一个分布式环境中各个不同应用系统提供的服务时,只需要在环境中登录一次。这次登录的结果将根据需要传播到各个应用系统中,而不需要用户在每个应用系统处重新登录[10]。长期以来该问题一直受到人们的关注,目前已经有许多协议和技术支持单点登录,其中具有代表性的是.NET Passport 技术和 Liberty 规范。

(1).NET Passport 是 Microsoft 推出的基于 Web 的单点登录技术,采用类似于 Kerberos 协议的身份认证机制,通过 Cookie 和重定向机制,实现单一登录。.NET Passport 的主要技术特点是集中式认证、分布式授权,但没有使用标准协议交换和传递认证信息,实现安全信息共享。

(2)Liberty 1.0 规范于 2002 年 7 月推出,是一个灵活的认证体系,通过多层账号映射的方法建立认证链,在理论上可以实现联盟站点的几乎无限扩展。其中合作站点和认证站点都要求支持 SAML,登录流程采用 SAOP 协议交换 SAML 数据,数据的互操作性较好。但是存在系统结构复杂和认证链管理复杂等问题。

传统的单一登录技术难以解决 ASP 应用模式下单一登录的特殊问题。.NET Passport 不适用于实现安全域内安全信息整合,异构认证机制间认证信息的共享;Liberty 1.0 规范结构和管理均比较复杂,难以应用于较大规模的 ASP 应用模式。

2.2 LDAP 目录服务

LDAP(Lightweight Directory Access Protocol,轻量级目录访问协议)是一种目录访问协议,是跨平台的标准 Internet 协议。目录服务是一种特殊的数据库,它将分布式环境中的用户、应用系统和设备等对象统一组织起来,提供单一的逻辑视图,允许用户透明地访问。

LDAP 的信息模型是以模式(Schema)为基础,以项目(Entry)为核心的,根据项目在树型结构中的位置对项目进行命名,适合于存储不经常变化、读多于写的信息。其优点有:①开放性。LDAP 定义了一套标准的方法访问和更新目录,得到了众多软件中间商的支持。②灵活性和可扩展性。用户可根据特定的应用需求定义新的信息模型。③分布性。LDAP 目录服务基于分布式的 C/S 模型,一个或多个 LDAP 服务器构成了目录信息树(DIT),DIT 的子树可按照管理域划分[11]。

由于 ASP 环境中集成的应用动态变化,安全域内用户安全信息管理的复杂性提高,因此需要一种安全信息的整合技术。利用 LDAP 的可扩展性,可描述 ASP 软件平台的用户信息和安全策略;利用 LDAP 的开放性,可简化安全信息管理复杂性,支持 ASP 软件平台安全信息的统一存储和访问,从而解决了 ASP 模式下安全域内安全信息整合和管理复杂的问题。

2.3 SAML 规范

SAML 1.0 规范(Security Assertion Marked Language,安全声明标记语言)由国际标准化组织 OASIS 于 2002 年 2 月发布,主要支持三种类型的安全声明:认证声明、授权声明和属性声明。其主要设计目标是为认证和授权服务提供标准的安全信息描述和共享机制,使得不同企业的安全系统间能够通过共享有关用户、交易等安全信息实现互操作。SAML 并非一种新的认证或授权技术,它关注的重点是使用 XML 实现安全信息的共享,使得在 Internet 环境下,可以用标准的方式描述和使用已广泛采用的安全技术。因此,SAML 适用于描述和共享 ASP 应用环境下异构认证系统间认证和授权结果。

3 单一登录系统设计原理

3.1 概念模型

本文首先给出面向 ASP 模式的单一登录机制的参与主体的定义。

定义 1 单一登录机制的参与主体主要包含三类:U,ASP,AC。其中,U 代表用户,U_C 指普通用户,U_M 指 ASP 软件平台管理员和平台各系统管理员;ASP 代表基于 ASP 应用服务门户的企业 ASP 应用软件平台;AC 代表企业之间的可信第三方认证中心。

定义 2 ASP 应用软件平台由一个五元组表示{DS,LS,P_{AE},P_{AO},P}。其中,DS 代表域安全服务器,进行 ASP 平台内集中的身份认证和授权服务;LS 代表域 LDAP 目录服务器,集中存储 ASP 软件平台内的用户信息和安全策略;P_{AE}代表认证代理,代替用户向应用系统进行身份认证,对用户屏蔽认证过程;P_{AO}代表授权代理,代替用户将授权信息传递给应用系统,对用户进行访问控制;P 代表运行于 ASP 软件平台上的应用系统,PL_i 指遗留系统,PN_i 指新增系统。

3.2 ASP 应用平台内的单一登录机制

安全域内的应用系统分为两种类型:遗留应用(具有身份认证和授权机制)和新增应用(加入单一登录系统的新开发系统,不必构造认证模块,只需具有授权决议执行模块)。单一登录系统的目标是为用户在遗留应用的账号建立联合关系,代替用户将认证信息传递给应用系统的身份认证模块。对用户要访问的新增应用作出授权决定,传递给新增应用的授权执行模块。假设 Web 应用 *A* 代表遗留应用 PL_1,Web 应用 *B* 代表新增应用 PN_1,用户访问应用 *A* 使用图 2 中 1.1～1.6 表示,访问应用 *B* 使用图 2 中 2.1～2.5 表示,则用户 U 在 ASP 应用平台内的应用系统 PL_1 和 PN_1 间单一登录工作机制如图 2 所示。

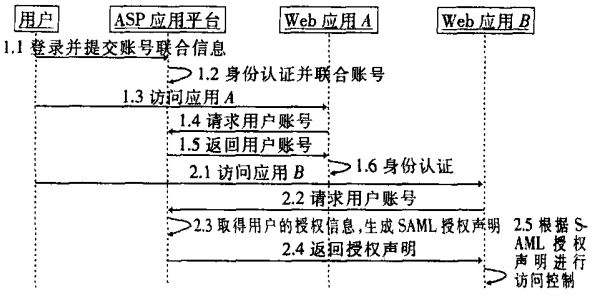

图 2 ASP 应用平台内的单一登录机制

(1)用户 U 在 ASP 应用服务平台登录,同时提供用户在各系统的账号联合信息给 DS_A。

(2) DS_A 进行身份认证,将账号联合信息存储到 LS_A 中,使得域内每个用户拥有唯一的身份标志以及该标志向应用系统用户标志的映射关系。

(3) PN_1 的管理员发布新增系统授权策略,即系统具有的

角色、对应的权限;DS_A 的管理员通过用户管理工具,为用户 U 制定在 PN_i 具有的角色,从而为 U 分配相应的权限。

(4)用户访问 PL_1,PL_1 的认证模块向 DS_A 请求用户 U 在 PL_1 的账号信息,DS_A 根据预先制定的账号联合信息,将相应账号返回给 PN_1 的认证模块。

(5) PL_1 的认证模块对用户进行身份认证。

(6)用户访问 PN_1,DS_A 根据预先制定的安全策略和用户的角色指派,生成相应的 SAML 授权声明返回给 PN_1 的授权执行模块。

(7) PN_1 的授权执行模块根据 SAML 授权声明,对用户作出访问控制。

通过该机制,ASP 应用平台能够为遗留应用提供账号联合和存储,为新增应用提供访问控制决策以及平台内安全信息的自动传递,从而实现安全域内集中的身份认证和访问控制,并达到单一登录的目的。

3.3　ASP 应用平台间的单一登录机制

随着企业间联盟的形成,用户的一次业务需要跨越不同的企业边界,从而带来安全域间的单一登录问题,这种情况下关键要解决认证和授权结果在安全域间共享和传递的问题。假设 ASP_A 和 ASP_B 分别代表分布式环境中两个独立的安全域,ASP_A 和 ASP_B 通过发布各自的信任策略,并得到对方的信任策略,达到彼此之间的信任关系的建立。本文假设 ASP_A 和 ASP_B 之间已经建立了信任关系,用户访问 ASP_A 使用图 3 中 1.1～1.8 表示,访问 ASP_B 使用图 3 中 2.1～2.7 表示,则用户 U 在 ASP_A 和 ASP_B 间单一登录工作机制如图 3 所示。

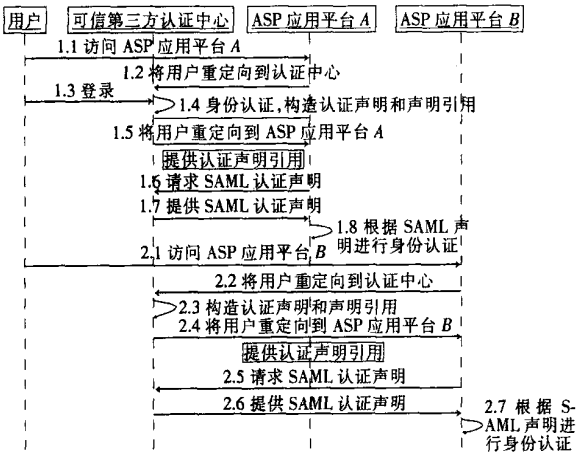

图 3　ASP 应用平台间的单一登录机制

(1)用户访问 ASP_A,ASP_A 将用户重定向到 AC 进行全局登录。

(2)用户在 AC 登录,进行身份认证,AC 根据认证结果为用户生成 SAML 认证声明及票据(对于声明的引用),并建立相应的会话。

(3)AC 将用户重定向到 ASP_A,并携带 AC 颁发的票据,携带票据是为了防止重放攻击。

(4) ASP_A 根据得到的票据向 AC 请求票据对应的完整的 SAML 认证声明,AC 将声明返回给 ASP_A 的认证模块。

(5) ASP_A 的认证模块根据 SAML 认证声明的内容,对用户进行身份认证。

(6)用户访问 ASP_B,ASP_B 将用户重定向到 AC。

(7)AC 根据当前用户的会话信息,为用户生成认证声明及对应的票据,并将用户重定向到 ASP_B,携带 AC 颁发的票据。

(8) ASP_B 根据得到的票据向 AC 请求票据对应的完整的 SAML 认证声明,AC 将声明返回给 ASP_B 的认证模块。

(9) ASP_B 的认证模块根据 SAML 认证声明的内容,对用户进行身份认证,从而达到用户只在 AC 登录一次,就可以在 ASP_A 和 ASP_B 进行访问。

在上述机制中,可信第三方认证中心为不同的 ASP 应用平台进行集中的身份认证和身份担保,并将认证结果以认证声明和票据的形式在安全域间进行传递,实现了安全信息的共享,从而使得用户在不同的安全域间实现单一登录。

4　单一登录系统实现

本文设计并实现了一个面向 ASP 模式的单一登录系统(Single Sign-on System for ASP Pattern,ASPSSO),支持不同 ASP 应用平台间的单一登录以及 ASP 应用平台内不同应用系统间的单一登录。

4.1　系统体系结构

按照上述的设计目标和设计原理,本文设计了安全信息存储、域安全服务器、可信第三方认证中心和管理配置工具四个核心部分来构建单一登录系统,体系结构如图 4 所示。

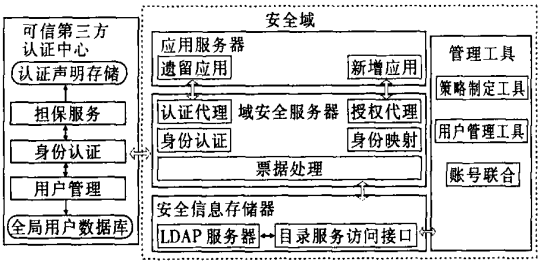

图 4　面向 ASP 模式的单一登录系统体系结构图

(1)安全信息存储。采用 LDAP 目录服务,集中存储一个安全域内用户账号信息和安全策略。用户账号信息主要包括用户在安全域的账号和账号联合信息、身份映射策略和新增系统的授权策略等。目录服务访问接口封装对于目录服务各种条目及其属性进行操作的 API,便于系统其他部分对目录内容进行访问。

(2)域安全服务器。对用户进行平台级身份认证、将全局身份映射成平台用户身份,为用户账号建立联合关系,传递账号给遗留系统的身份认证模块,或传递授权声明给新增系统的授权执行模块。

(3)可信第三方认证中心。对全局用户进行统一身份认证,为用户构造 SAML 认证声明,并颁发声明对应的票据,对认证声明进行存储和管理,响应各安全域对票据对应声明的查询。

(4)管理配置工具。实现对账号联合信息的定制,新增应用访问控制策略的定制以及用户的身份映射策略的定制。

4.2　LDAP 数据模型

作为域内安全信息整合的核心部件,LDAP 数据模型主要用于将 ASP 应用平台内的用户信息和安全策略有机组织起来,包括用户信任状、角色等,ASP 应用平台的身份映射策略、

授权策略、新增应用的角色和权限制定策略。

LDAP 是基于 Entry(条目)的目录服务,Entry 按照层次化方式组织。目录树(图 5)自上而下划分为四个分支:ASP 应用平台的用户、平台的角色、角色对应的权限以及域中的新增应用。其中权限分支的描述采用 RBAC(基于角色的访问控制)授权模型。用户分支存储 ASP 应用平台的所有用户条目;安全域角色分支存储用户对应的角色条目;安全域权限分支存储角色对应的权限条目。这三个分支的信息能够对用户进行集中的身份认证和访问控制。新增应用分支存储新增应用条目,又存在两个分支:①角色分支代表新增应用具有的角色;②权限分支代表角色对应的权限。新增应用分支用于对用户在 ASP 应用平台内的新增应用作出访问控制决策。每个条目具有所代表对象(ObjectClass)的多个属性,如 ActUser 条目包括用户 ID,Password,账号联合信息等属性;新增应用条目包括应用 ID,名称等属性。以上条目构成了 ASP 应用平台完整的账号和安全策略表示,成为统一认证和授权的基础。

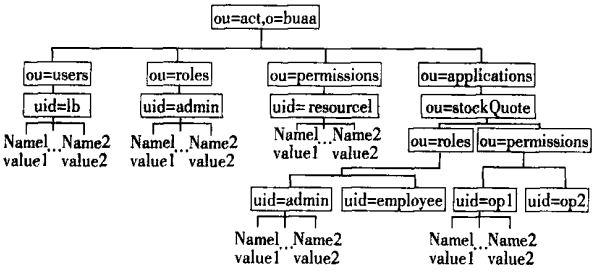

图 5 安全信息目录树结构

根据实际应用需求,在目录信息树的设计中,对 LDAP 类型进行了扩展,增加了自定义的对象类型(ObjectClass)和属性类型(AttributeType),主要包括 actUser,actRole,actPermission, actApplication 等。以 actUser 为例,说明 ObjectClass 的定义:

```
objectclass ( 1.3.6.1.4.1.7915.1.2.4.4 NAME 'actuser'
    DESC 'ACT User'
    MUST (uid $ userPassword)
    MAY (mail $ name $ givenName $ sn $ uidnumber $
    Lastlogindate $lastmodifieddate $ creationdate $
    Disabled $ objectdata $ confirm $ usergrouprole) )
```

根据 LDAP 目录服务标准,每个条目具有唯一标志 DN,能描述条目间的层次关系,便于对特定条目的查询及引用该条目的属性。图 2 中部分节点的 DN 如下所示:

DN:uid = admin,ou = roles,ou = act,o = buaa;
DN:uid = lb, ou = users,ou = act,o = buaa;
DN: uid = employee, ou = roles, ou = stockquote, ou = applications, ou = act,o = buaa;

由此可见,通过这样的目录树组织,域安全服务器通过访问 LDAP 目录服务器,得到用户的身份映射信息、角色信息、权限信息等,从而对用户进行统一的身份认证和访问控制,进而达到用户在安全域内的单一登录。

4.3 认证代理和授权代理实现算法

ASPSSO 系统的认证代理和授权代理主要进行认证和授权结果的传递,是域安全服务器的重要组成部分,认证代理和授权代理的实现算法如下:

(1)认证代理算法(图 6)。①获得用户在 ASP 应用平台的账号;②通过目录服务访问接口从目录服务取得账号联合信息,得到用户在目标遗留应用的账号;③根据目前支持的两种认证方式 BASIC 和 FORM 认证方式,构造 HTTP 认证报文;④将 HTTP 认证报文转发给应用系统的认证模块。

(2)授权代理算法(图 7)。①获得用户在 ASP 应用平台的账号;②通过目录服务访问接口从目录服务取得用户在新增应用的角色;③根据新增系统的授权策略,取得用户的权限;④构造 SAML 授权声明,并传递给新增应用的授权执行模块;⑤新增应用的授权执行模块根据 SAML 授权声明对用户作出访问控制。

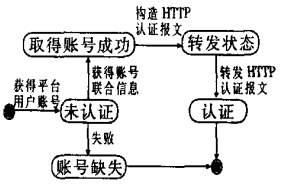

图 6 认证代理状态转换图

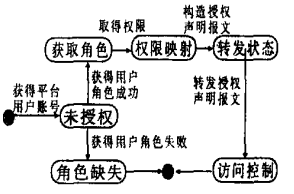

图 7 授权代理状态转换图

为增强安全域间与安全域内新增系统与域安全服务器间的安全信息互操作,本文将 SAML 语言描述的身份认证和授权结果与 HTTP 协议绑定。使用 Michigan 大学发布的运行于 Linux 系统上的开源软件 OpenLDAP 作为目录服务器,在每个安全域配置一台 LDAP 服务器。通过扩充 ObjectClass 和 AttributeType,生成和导入 LDIF(LDAP Data Information Format)文件,构造目录信息树,维护安全域账号信息和安全策略,系统的主要功能模块以类库和 Web 应用形式实现。

5 系统安全性分析

用户使用单一登录系统进行访问时,系统会受到各种安全性攻击,而缺乏安全保证的单一登录系统是没有实用价值的,因此系统的安全性是极其重要的。本文首先从几种主要的攻击方式分析系统消息安全性。

(1)窃听攻击。对 SAML 声明携带的信息通过编码、解码算法处理,保证认证和授权结果的机密性和完整性,同时使用 HTTPS 技术保证消息传递的机密性。

(2)重放攻击。为声明设置有效期,减少攻击者有效的攻击时间,并且声明访问一次即无效。

(3)消息窜改攻击。使用 SOAP 传递 SAML 认证和授权结果,利用 SOAP 安全扩展中的签字保证消息的完整性。

(4)伪装攻击。利用 SOAP 安全扩展中携带的认证信息验证各方的身份,防止攻击者伪装成合法的站点。

(5)恶意合作站点攻击。通过设置 SAML 声明的作用域防止对担保票据的恶意使用。

同时,LDAP 目录服务器作为安全域内信息存储的核心模块,自身的安全性也是很重要的。LDAP 目录服务的可靠性为系统的安全奠定了基础。系统通过 LDAP 目录服务器的目录复制方法,避免突发的目录服务单点故障,通过在安全域内设置 Slave LDAP 服务器,与 Master LDAP 服务器保持内容的同步。当主服务器出现故障时,从服务器通过配置能够成为主服务器,从而保证了目录信息的安全可靠。

通过目录认证和目录授权两种方式保证目录内容的安全性。目录认证采用基本认证方式与目录服务绑定,使目录信息不被非法用户访问。目录授权使用访问控制列表制定访问控

制策略,保证目录信息不被无权用户访问,从而实现目录内容安全性。

6　结束语

本文针对电子商务中新的安全需求,提出了一种面向 ASP 模式的单一登录机制的完整解决方案,保证了 ASP 应用平台内多个 Web 应用间的单一登录和多个 ASP 应用平台间的单一登录,并在该方案的基础上基于 LDAP 和 SAML 技术实现了 ASPSSO 系统。本文提出的单一登录机制能够解决 ASP 应用模式下安全信息的整合、传递和管理问题,适用于企业内部应用系统集成、政府部门内部的信息系统整合、跨企业的电子商务系统、跨地域或者跨部门的电子政务系统、Internet 环境下的协同计算(如网格计算系统等)应用场景[12]。本文的工作具有如下的特点:①采用 LDAP 目录服务,集中地管理域内用户信息和安全策略,以标准的接口对信息进行统一访问和管理。②采用 SAML 语言,使系统具有标准的认证、授权结果的表示和传递方式,支持异构安全系统间的信息共享。③统一的身份验证和授权操作,简化授权管理复杂性。④使用 Web Service 技术实现可信第三方认证中心核心功能,具有良好的互操作性和可移植性。⑤系统具有良好的安全性和可靠性。

对于大规模并发访问情况下,系统可靠性的研究和性能的仿真评测,目录服务和系统安全性的提高,以及该机制应用于各类场景中将产生的特殊问题是进一步完善该系统的重点。

参考文献:

[1] Christian Wege, *et al*. Portal Server Technology [EB/OL]. http://www.computer.org/internet/ic2002/w3073abs.htm, 2002-05.

[2] Build and Implement a Single Sign-on Solution [EB/OL]. http://www-106.ibm.com/developerworks/java/library/wa-singlesign/?ca=dgr-lnxw914CASsso, 2003-09-30.

[3] Introduction to Single Sign-on [EB/OL]. http://www.opengroup.org/security/sso/sso-intro.htm.

[4] Microsoft Corporation. Microsoft.NET Passport Technical Overview [EB/OL]. 2001.

[5] Jeff Hodges, Sun Microsystems Inc. Liberty ID-FF Architecture Overview [EB/OL]. http://www.projectliberty.org/specs/draft-lib-arch-overview-v1.2-04.pdf, 2003-04-14.

[6] Microsoft Corporation. Windows 2000 网络中的单次登录 [EB/OL]. http://www.microsoft.com/china/technet/windows2000/whitebook/nt2ksso.asp.

[7] Netegrity Corporation. Netegrity SiteMinder 5.5 Technical White Paper [EB/OL]. http://www.netegrity.com/products/products.cfm?page=SMhowitworks, 2002-09-23.

[8] RFC 2251, Network Working Group. Lightweight Directory Access Protocol (v3) [EB/OL]. http://www.ietf.org/rfc/rfc2251.txt?number=2251, 1997.

[9] 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.

[10] Paker T A. Single Sign-on Systems: the Technologies and the Products [J]. IEE. Europe Convention on Security and Detection, 1995.

[11] IBM International Technical Support Organization. Understanding LDAP [EB/OL]. http://www.redbook.ibm.com/redbooks/SG244986.html.

[12] 葛声,怀进鹏,等. 面向 Web Service 中间件的应用支撑环境[C]. 软件技术进展,2002 全国软件与应用学术会议(NASAC)论文集, 2002.97.

作者简介:

李博(1979-),女,硕士研究生,主要研究方向为电子商务与网络安全;葛声(1973-),男,讲师,博士,主要研究方向为分布式计算、电子商务和信息安全;沃天宇(1978-),男,博士研究生,主要研究方向为电子商务与网络安全;马殿富(1960-),男,教授,博士生导师,博士,主要研究方向为网络计算、科学计算可视化。

(上接第 7 页)

[28] Zomet A, Rav-Acha, Peleg S. Robust Super-Resolution [C]. Proceeding of CVPR'2001, 2001.645-650.

[29] Baker S, *et al*. Hallucinating Faces [C], 4th International Conference on Automatic Face and Gesture Recognition, 2000.83-88.

[30] Freeman W, *et al*. Example-based Super-Resolution [J]. IEEE Computer Graphics and Applications, 2002, 22(2):56-65.

[31] Capel D, Andrew Zisserman. Super-Resolution from Multiple Views Using Learnt Image Models [EB/OL]. http://www.robots.ox.ac.uk/~vgg/publications/html/.../papers/capel2001.ps.gz, 2002.

[32] Baker S, Kanade T. Super-Resolution: Reconstruction or Recognition? [C]. IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing, Baltimore, Maryland, 2001.215-219.

[33] Christopher M, *et al*. Super-Resolution Enhancement of Video [C]. Proceedings 9th International Conference on Artificial Intelligence and Statistics, Key West, Florida, 2003.410-414.

[34] Shechtman E, Caspi Y, Zrani M. Increasing Space-time Resolution in Video [C]. Proceedings of ECCV'2002, 2002.753-768.

[35] Tom B, Katsaggelos A K. Resolution Enhancement of Monochrome and Color Video Using Motion Compensation [J]. IEEE Transactions on

[36] Zhongding Jiang, Tien-Tsin Wong, Hujun Bao. Practical Super-Resolution from Dynamic Video Sequenes [C]. Proceedings of IEEE Computer Vision and Pattern Recognition 2003 (CVPR'2003), Madison, Wisconsin, USA, 2003.549-554.

[37] Lertrattanapanich S, Bose N K. Latest Results on High-Resolution Reconstruction from Video Sequences [R]. Technical Report of IEICE, DSP-140, The Institution of Electronic, Information and Communication Engineers, Japan, 1999.59-65.

[38] Bahadir K, Yucel Altunbasak, Russell M. Multi-frame Resolution Enhancement Methods for Compressed Video [J]. IEEE Signal Proces sing Letters, 2002, 9(6):170-174.

作者简介:

王勇(1978-),男,博士研究生,主要研究方向为智能图像识别、基于内容的多媒体检索、多媒体通信;郑辉(1957-),男,教授级高工,博士生导师,主要研究方向为多媒体通信、盲信号处理、移动通信技术;胡德文(1963-),男,教授,博士生导师,主要从事图像处理、神经网络、系统辨识、脑科学等研究。