一种社区授权服务的拉式模型

胡群袖,杨长兴
(中南大学 信息科学与工程学院,湖南 长沙 410083)

摘 要:针对目前网格中的社区授权服务(CAS)推式模型所存在的某些安全问题,提出了一种拉式模型。在拉式模型中,引入一个CAS缓存服务器;由资源提供者(而不是用户)向CAS缓冲服务器查询用户的权限声明,并与本地授权策略相结合形成用户在本资源上的最终有效权限。该文详细描述了用户向资源提供者进行服务请求的认证步骤,并从运行效率和安全性、可靠性等方面与推式模型进行了对比分析。

关键词:网格安全基础设施;社区授权服务;拉式模型;推式模型
中图分类号:TP387;TP309 **文献标识码**:A **文章编号**:1673-629X(2006)09-0224-03

A Pulling-Model of Community Authorization Service

HU Qun-xiu, YANG Chang-xing
(School of Information Science and Engineering, Central Sourth University, Changsha 410083, China)

Abstract: In allusion to some questions existed in current community authorization service (CAS) pushing-model, a pulling-model is proposed. In the pulling-model, a CAS caching server is introduced; resource provider, but not users, require user's authorization assertion from the CAS caching server to obtain final effective rights for users on the resource, constrained with local authorization policies. The authentication steps how users require services on providers, are described in detail. It is contrastively analyzed with pushing-model from performance, security and dependability.

Key words: GSI; CAS; pulling-model; pushing-model

0 引 言

虚拟组织(VO)是网格中资源和用户的动态集合[1],为了在虚拟组织的级别上进行访问策略和权限的动态控制,同时不与本地资源的权限和策略管理冲突,社区授权服务[2](Community Authorization Service, CAS)应运而生。CAS允许资源提供者将一部分权限管理委托给虚拟组织,虚拟组织运行一个CAS服务器进行权限和策略的管理,其管理内容包括:对资源的权限控制;服务器本身的管理;虚拟组织的成员列表管理。CAS的引入只是为了能够对大量分布式的资源提供者的动态又复杂的权限策略进行集中的总体的管理,其具体的、细微的权限控制依然在于资源提供者。

Globus工具集[3](GT)是进行网格开发的事实标准。其所采用的网格安全方案是基于网格公共密钥体系(PKI)的网格安全基础设施[4,5](GSI)。目前的Globus工具集(包括2005年4月下旬发布的最新版本4.0[6]),其安全方案GSI采用CAS的推式模型进行虚拟组织的整体授权策略和权限的管理。

文中介绍相关的概念及现有的推式模型,然后在此基础上提出一个拉式模型,并就性能、安全性和可靠性等方面与推式模型进行比较分析。

1 推式模型

所谓推式模型,就是用户将包含了CAS权限声明的代理证书"推"给资源,让资源提供者认证其服务请求。其过程如图1所示。推式模型的操作步骤[6,7]如下:

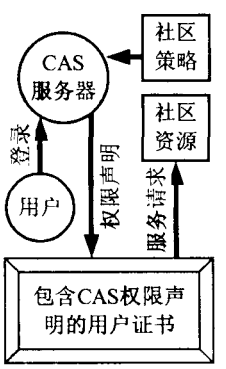

图1 CAS推式模型示意

1)用户用自己的证书创建代理证书,并使用该代理证书登录到CAS服务器。

2)CAS服务器根据社区策略为用户分配权限,签署用户的代理证书,并将关于该用户的权限声明嵌入到代理证书中,然后将该代理证书返回给用户。

收稿日期:2005-11-21
作者简介:胡群袖(1981-),男,湖南湘潭人,硕士研究生,研究方向为网格安全;杨长兴,教授,研究方向为网络技术、医学信息处理。

3)用户使用包含了 CAS 权限声明的代理证书向资源提供者提出服务请求。

4)资源提供者认证用户的代理证书和和代理证书中包含的权限声明的有效性,然后将 CAS 权限声明所包含的权限与通过本地策略分配给该用户的权限结合,所得到的权限交集就是用户在该资源的最终有效权限。

2　拉式模型

2.1　拉式模型详述

推式模型能够满足虚拟组织中进行社区整体权限的动态管理的需求,但是为了降低权限管理的复杂性,在社区中只运行一台集中式管理的 CAS 服务器(基于开放网格服务 OGSA,CAS 服务器实际上也是网格中的一个服务),当 CAS 服务器被攻击或出现故障时,将导致用户无法获得 CAS 服务器所签署的包含权限声明的代理证书,从而社区内的所有资源都无法认证用户的服务请求,社区提供的所有服务瘫痪,大大降低了服务的可靠性;包含了 CAS 权限声明的代理证书是 X.509 证书的非标准扩展格式,不具有通用性;在一个大型网格应用中往往需要多个资源的参与协作,而用户在网格协作应用中是属于资源相对紧张者,由用户登录 CAS 服务器并使用服务器签署返回的证书向资源提出请求,用户需要多次登录到不同的 CAS 服务器以获取签署过的包含权限声明的代理证书,增加了用户的运行负荷和带宽开销;CAS 服务器需要暴露在社区信任域外,其被攻击的可能性大大增加。

为了解决现有的推式模型中所存在的问题,设计一个"拉"式模型。相对于推式模型中由用户将 CAS 的权限声明"推"给资源提供者,拉式模型中将由资源提供者主动向 CAS 服务器发出权限声明的询问请求,将权限声明从 CAS 服务器"拉"回来。拉式模型示意如图 2 所示。

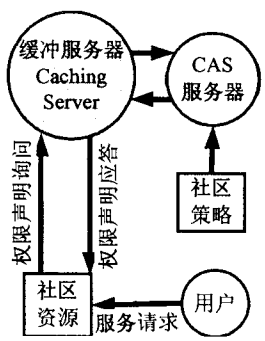

图 2　CAS 拉式模型示意图

在模型中引入了一个 CAS 的缓存服务器(Caching Server)。缓存服务器实际上也是一个网格服务,为了方便集中管理,CAS 服务器运行于主服务器(Master Server)上,而 CAS 缓存服务器则运行于多台分布的从属服务器(Slave Server)上。CAS 缓存服务器只保存 CAS 服务器数据库的部分镜像,并设定每隔一定的时间与服务器进行数据库同步。缓存服务器缓存的内容包括:授权给所有 VO 成员的权限,某一特定成员组所拥有的共同权限,及一部分最近常用的用户所拥有的权限等。资源向缓存服务器(而不是 CAS 服务器)发送关于某用户在社区内的权限询问请求。缓存服务器主要是应答资源的权限声明询问,CAS 服务器则主要是社区资源的权限进行集中管理和控制。为了方便管理与安全性,为每个缓存服务器签发一个单独的、与 CAS 服务器不同的证书,资源可以根据返回的权限声明的签署主体来判断该声明是来自缓存服务器还是来自 CAS 服务器。

拉式模型中资源提供者授权给用户的步骤如下:

(1)用户生成并签署自己的代理证书,将代理证书发送给资源提供者,向资源提供者发送服务请求。就用户程序而言,这一步和推式模型区别不大,只是省略了向 CAS 服务器登录的过程,因此客户端程序并不需要很大的改动。

(2)资源提供者对用户代理证书的有效性进行认证。如果不能通过认证则直接拒绝用户。

(3)通过了资源提供者的认证之后,资源提供者将用户映射为本地用户并为其创建代理证书,然后用该代理证书向 CAS 缓存服务器发送权限声明的询问,向 CAS 缓存服务器询问该用户在 VO 中所拥有的权限。

(4)CAS 缓存服务器在收到权限声明询问请求之后,查询本地的数据库是否有该用户的记录,如果有则直接将该记录中的权限声明进行数字签名(如图 3 所示)后返回给资源提供者,然后转步骤 6。该权限证书是 X.509 证书的标准格式,不需要进行扩展。如果在缓存数据库中没有该条记录则向 CAS 服务器进行同步查询。

```
Authorization Assertion

Subject: /CN=Kingshow
Issuer: /CN=CAS Caching
Valid from: 5/1/05 13:00
Valid to: 5/5/05 21:00
Rights:
These actions are allowed:
   Read gridftp://myhost/mydir/*
   Write gridftp://myhost/myfile

{Signature of assertion by CAS
Caching Server}
```

图 3　缓冲服务器权限声明返回示意

(5)CAS 服务器为该用户创建一个 VO 成员账号,并运用社区权限策略为其分配相应的权限,之后将该条记录反馈给缓存服务器。

(6)资源提供者在接收到缓存服务器返回的权限声明之后,根据本地权限策略为该用户分配权限。本地分配给该用户的权限与 CAS 服务器返回的权限的交集即是用户的最终有效权限,如图 4 所示。

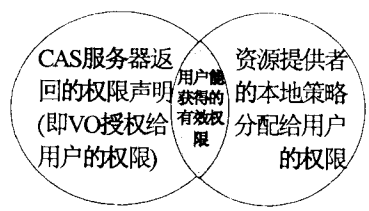

图 4　用户获得的最终有效权限

2.2 拉式模型分析

与推式模型相比,该拉式模型有明显的优点:

(1)在推式模型中,CAS服务器是单一的、集中式的服务器,一旦出现故障将导致整个社区内的所有资源因用户无法获取包含CAS服务器权限签署的代理证书而拒绝提供服务;而在拉式模型中增加多个从属分布式的缓存服务器,大大提高了CAS服务的可靠性,同时也可以将对虚拟组织权限管理与权限查询应答分离开来,大大提高了CAS服务器的运行效率和性能。

(2)在拉式模型中由资源提供者向CAS缓存服务器来获取用户的权限声明,可以节约资源相对紧张的用户的带宽开销和运行负荷,充分利用网格资源。

(3)CAS缓存服务器、CAS服务器没有被暴露在社区信任域以外,而是与资源提供者处于同一信任域中,被攻击的可能性降低,从而大大提高了CAS服务的安全性和可靠性。

(4)在推式模型中需要对X.509证书格式进行非标准的扩展,以在代理证书中嵌入权限声明;而在拉式模型中则可以直接使用X.509的标准证书格式,提高了其适用范围和通用性。

(5)在推式模型中用户需要向资源提供者提出服务请求时,总是要先登录CAS服务器获取权限声明;而拉式模型中,资源提供者先认证用户的服务请求,如果认证失败则不需要向服务器获取权限声明,大大降低了集中式CAS服务器的运行负荷,也间接提高了其运行效率和可靠性。

3 结 论

文中所提出的拉式模型很好地解决了推式模型中所存在的问题,极大地提高了使用CAS服务器进行社区授权管理的网格应用的安全性和可靠性,是一个较为优越的模型。

参考文献:

[1] Foster I, Kesselman C. The Grid 2: Blueprint for a Future Computing Infrastructure[M]. 金 海,袁平鹏,等译. 北京:电子工业出版社,2004.

[2] 徐志伟,冯百鸣,李 伟. 网格计算技术[M]. 北京:电子工业出版社,2004.

[3] The Globus Toolkit[EB/OL]. http://www.globus.org/toolkit,2005.

[4] Foster I, Kesselman C, Tsudik G, et al. A Security Architecure for Computational Grids[A]. The 5th ACM conference on Computer and Communication Security[C]. San Francisco, CA:[s.n.],1998.

[5] 都志辉,陈 渝,刘 鹏. 网格计算[M]. 北京:清华大学出版社,2002.

[6] Sotomayor B. The Globus Toolkit 3 Programmer's Tutorial [EB/OL]. http://www.chinagrid.net/grid/download/prog-tutorial-0.4.3,2003.

[7] GT 4.0: Security: Community Authorization Service[EB/OL]. http://www.globus.org/toolkit/docs/4.0/security/cas/,2005.

(上接第223页)

否合法,从而达到访问控制的目的。在系统的访问控制上实现分级访问控制策略,文献[4]提出了基于多粒度权限的访问控制。

(3) 安全审计模块。

主要用于事后的日志分析。当发生安全问题时,可以根据日志记录,分析问题并可追查事故责任人,同时可以根据访问记录和设置的规则进行安全审计分析,判断系统是否受到安全威胁。

(4) 授权管理服务。

为身份认证模块、访问控制模块和安全设计模块提供支持,包括用户身份管理、资源管理、授权管理、日志管理。用户身份管理包括用户信息管理、角色信息管理及用户角色的分配;资源管理包括系统功能模块、数据库资源、其它数据资源等信息的管理;授权管理实现将不同资源的访问权限授给不同的访问角色,间接实现对用户的授权;日志管理就是对应用系统的日常访问记录进行管理、维护和分析。

(5) 加/减密模块。

加/减密模块为系统中的重要数据提供保密服务,保证数据的传输和存储安全,采用MD5、AES等算法实现数据的加密[5]。

3 总 结

从应用系统角度出发对电子政务安全管理进行了研究和探讨,并给出了相应的基于J2EE的系统平台设计方案。该方案应用到了某工业局电子政务系统当中,取得了一定的效果,达到了用户的安全需求,整个系统实现了较为灵活的安全配置和控制。同时该方案具有一定的普适性,也能应用到其它的电子政务系统当中。

参考文献:

[1] 宋宇波,胡爱群. 电子政务安全体系结构的探析[J]. 计算机工程,2003,29(10):12-13.

[2] 张 宏 陈志刚. 一种新型一次性口令身份认证方案的设计与分析[J]. 计算机工程,2004,30(17):112-113.

[3] 黄 凯,陈 云,阎如忠,等. 基于角色的B/S系统访问控制的研究与应用[J]. 计算机工程与应用,2003(20):228-229.

[4] 叶春晓,符云清,吴中福,等. 基于多粒度权限的访问控制[J]. 计算机应用研究,2004(10):87-88.

[5] 李海燕,徐汀荣. 基于BS的电子政务系统中信息加密技术的设计与实现[J]. 苏州大学学报,2004,24(6):46-47.