

计算网格中访问控制策略研究与应用

王 杨^{1,2}, 林 涛³, 王汝传³

(1. 安徽师范大学 计算机系, 安徽 芜湖 241000;

2. 苏州大学 计算机科学与技术学院, 江苏 苏州 215006;

3. 南京邮电大学 计算机学院, 江苏 南京 210003)

摘 要: 网格是未来分布式计算的主要发展方向, 而网络安全不仅是网格推广应用的前提, 也是计算网格中的一个核心问题。通过对网络安全需求进行分析, 从不同角度观察网络安全, 抽象出网络安全模型的物理视图和逻辑视图。重点研究了网格环境中访问控制策略与授权策略。结合网络安全项目的研究, 设计并实现了利用网络安全认证、访问控制策略进行P2P分布式计算的应用实例。

关键词: 网络安全; 访问控制; 认证; P2P

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2006)08-0231-04

Research and Application on Access Control Policy Based on Computing Grid

WANG Yang^{1,2}, LIN Tao³, WANG Ru-chuan³

(1. Department of Computer Science, Anhui Normal University, Wuhu 241000, China;

2. Institute of Computer Science & Technology, Soochow University, Suzhou 215006, China;

3. Institute of Computer Science, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: Grid is the main developing direction of future distributed computing. Grid security is not only the premise of grid wide application, but also one of the main problems of computational grids. Through analysis of the need of grid security, checking grid security by different aspects, the physical and logic views of grid security model were presented. Then the access control policy and authority policy of grid computing was emphatically researched. At last, an application instance of P2P distributed computing with grid security certification and access control policy were designed and implemented by combining with the research project of grid security.

Key words: grid security; access control; certification; P2P

0 引 言

网格计算的根本目的就是使网格中的每台计算机内部的各种资源和部件都能独立上网, 从而利用地理上分散的资源完成各种大规模的、复杂的计算和数据处理任务。可以说, 网格整合了分布 WAN/LAN 中的资源, 使这些资源成为一个巨大的虚拟计算机系统^[1]。大量个体、机构组织等网格客户利用安全、协同方式创建各自的动态虚拟组

织(VO, Virtual Organization)。基于这种虚拟动态组织的网格计算不仅跨地域, 而且可以延伸到不同的组织、异构的软件硬件平台, 为每一个连接到网格的用户提供一个无限的计算能力、沟通协作能力及信息获得能力。在计算网格环境中, 它具有以下与一般网络的不同之处: 大量动态的用户群体; 大量动态的资源; 计算动态增长和收缩; 多种通信机制; 不同的本地安全解决方案; 不同的本地信任机制; 跨国界的用户和资源。网格计算, 在提供了一种崭新的资源协作和共享方式的同时, 因为其自身的一些特点, 也使得安全问题成为网格计算技术得到普遍使用的一大阻碍。网格必须提供的基本的安全服务包括: 认证、授权、访问控制、完整性、审核、保密以及抗否认等^[2]。此外, 良好的体系结构中还应包括安全的单点登录、合并的审核日志和日志分析、安全性管理、会话保护、统一的安全性粒度等特性。网络安全策略需要与具体的应用环境相结合。文中主要讨论了网络安全需求中访问控制与授权机制, 并结合项目研究实践介绍了一个具体应用。

收稿日期: 2005-11-16

基金项目: 国家自然科学基金(60573141, 70271050); 江苏省自然科学基金(BK2005146); 江苏省自然科学基金预研项目(BK2004218); 江苏省高技术研究计划(BG2004004, BG2005038); 江苏省计算机信息处理技术重点实验室基金(kjs050001); 安徽师范大学校青年基金资助项目(2005xqn05)

作者简介: 王 杨(1971-), 男, 安徽芜湖人, 博士研究生, 研究方向为计算机软件理论、计算机网络与对等计算安全等; 王汝传, 教授, 博士生导师, 研究方向为计算机软件理论、计算机网络及信息安全、移动代理技术、网格计算技术等。

1 计算网格的安全需求

1.1 计算网格的物理安全需求

在网格物理安全需求中,以虚拟组织^[3]为出发点来进行分析。在虚拟组织中抽象出如下组件:虚拟组织(VO)管理中心、网格调度中心、认证机构 CA(Certificate Authority)、资源,以及使用虚拟组织资源的用户。所谓虚拟组织就是一些个人、组织或者资源的动态组合。这一概念强调的是网格是为虚拟组织服务的,网格必须具备动态、协同资源共享的特点。网格整合分布在局域网或广域网的资源,使这些资源成为一个巨大的虚拟计算机系统。目的是在大量个体、机构组织等之间利用安全、协同式的资源共享,创建一个动态虚拟组织(VO-Virtual Organization),基于这种虚拟动态组织的网格计算不仅跨地域,而且延伸到不同的组织、异构的软件硬件平台,为每一个连接到网格的用户提供一个无限的计算能力、沟通协作能力及信息获得能力。在网格计算环境下,采用基于虚拟组织(Virtual Organization)的分布式管理模式,它使得作业实体从资源控制、任务调度和管理的复杂的工作中解脱出来。

虚拟组织服务主要包括:用户服务(注册、登录、注销);认证中心服务;入口结点和网关结点选取及服务;虚拟组织之间交互;虚拟组织注册中心管理;网格服务的描述和管理。为了简化网络安全模型,把虚拟组织的入口结点和网关结点,以及虚拟组织管理服务其他功能抽象为一个 VO 管理中心。同样,为了简化网络安全模型,定义网格调度中心是资源管理和任务调度的功能组合。在网格物理安全需求中,把网格的安全功能细化为一个个安全服务组件,主要包括认证服务、授权服务、委托服务、传输安全、日志审核、数字签名、防火墙等。

1.2 计算网格的逻辑安全需求

这里主要从用户的角度强调安全服务的概念,抽象出网络安全的逻辑视图^[4],如图 1 所示。

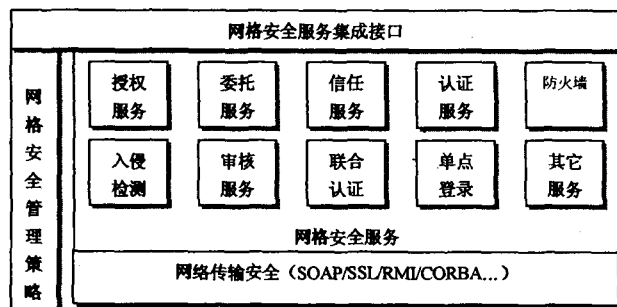


图 1 网络安全需求逻辑视图

图 1 主要分为 3 层:网络安全传输层、网络安全服务层、网络安全服务集成接口层。网络安全服务层中的服务是一个可扩充的结构。在网络安全传输层、网络安全服务层涉及到网络安全管理的策略问题。网络安全管理策略主要是解决网络安全服务之间如何无缝连接、以及对这些服务进行比较灵活的配置的问题。网络安全服务集成接口主要通过其安全服务接口为网格其他非安全服务(例

如,虚拟组织服务、资源管理服务、任务调度服务等)和网络应用提供安全保障机制。网络安全传输为以上的安全服务提供在网络上安全的传输机制。在网络安全需求的逻辑视图中,各个安全功能组件之间存在着交互。安全管理策略将为用户提供灵活的服务界面,让用户自己进行选择。

2 网格中的安全访问控制策略

由于网络安全模型是可扩充的结构,其中最重要的安全策略主要包括:网络安全中 PKI 管理策略;基于虚拟组织的认证策略;访问控制与授权策略;安全审核策略。这里仅讨论访问控制与授权策略^[5]。

2.1 访问控制策略

在网格环境中有很多不同的角色,如网格用户、资源拥有者、虚拟组织管理者等等。不同的角色对在网格环境中操作权限是不同的。基于角色的访问控制(RBAL, Role-Based Access Control)的工作方式如下:用户被指定至不同的角色,对象则被指定至基于所需访问模式的组;角色与权限相关联,用户通过角色来获得对象或对象组的访问权限,通过权限的隐含继承,或者是通过明确拒绝一部分父角色所拥有的权限,可以将角色组织看成一个分级的结构。基于角色的访问控制通过一些规则来实现。

通常,访问控制规则使用以下参数将访问控制规则库定义为一个函数。该函数将一个四元组映射至集合{ALLOW, DENY}。四元组中的字段是:

(1)主体:请求访问某个资源的活动实体、过程、用户或系统。主体在请求服务之前假定为已经通过了一些身份标识和认证测试。

(2)对象:访问的被动目标。它可能提供服务、接受消息、返回某个值,或改变状态。对象在能够被访问之前假定已经通过了一些验证性测试。

(3)权限操作:所请求的访问类型。对于数据对象,访问操作可以包括创建、更新、删除、插入、追加、读取或写入模式。

(4)相关环境:关于环境的一个断言,该断言必须有效。相关环境可具有许多环境属性,例如所有权、历史、时间、服务质量、权限、推断等等。

采用如下方式对基于角色的访问控制模型进行描述:

Role Definition:: = role Role Name { Access Control List};

Access Control List:: = Access Control[Access Control List];

Access Control:: = ALLOW | DENY Permission List in Name List;

Permission List:: = Permission[Permission List];

Permission:: = Read | Write | Execute | Create | Delete | Insert | All;

User Definition:: = users Name List act as Role Name.

对 X.509 证书^[6]进行了一定的扩展,主要是把角色信息、授权、委托信息等等封装在证书的扩展信息中。扩展后的证书结构如下:主体标识、主体公钥、发行者标识、签名算法、数字签名信息、有效期(证书创建时间、证书作废时间)、证书的版本号和序列号、证书的扩展信息(角色信息、授权、委托信息等)。网格中的访问控制策略主要有授权策略和委托策略。下面讨论网格环境中的授权策略和委托策略。

2.2 网格环境中的授权策略

在虚拟组织内部定义了授权中心、服务提供者、服务请求者和资源。在网格环境中,授权中心的功能可以由虚拟组织中的调度中心来承担。服务请求者既可以是网格用户,也可以是网格用户委托的代理。在这里,只考虑服务请求者是网格用户的情况;在下面阐述的委托策略中考虑服务请求者是委托代理的情况。服务提供者是资源中的一个专门用于访问控制管理的执行者。网格环境中授权模型如图 2 所示。

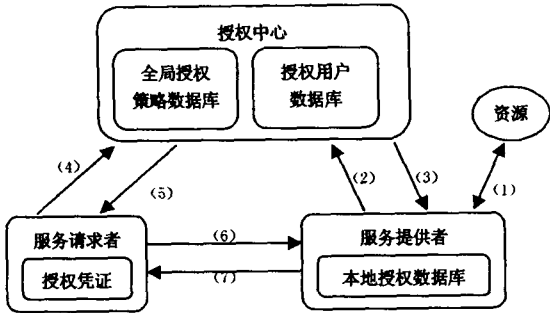


图 2 网格环境中授权模型

图 2 中的相关步骤说明如下:

- (1)资源委托其服务提供者进程负责资源的访问控制策略的管理。
- (2)服务提供者进程向授权中心(虚拟组织中的调度中心)注册资源。
- (3)授权中心依据虚拟组织的安全管理策略得到服务提供者进程管理的资源的访问控制授权,并通知服务提供者。
- (4)服务请求者(用户)向授权中心提出要向服务提供者访问授权的要求。
- (5)授权中心依据服务请求者的要求,授予服务请求者相应的访问服务提供者所管理的资源的访问权限。
- (6)服务请求者利用授权凭证向服务提供者提出访问资源的请求。
- (7)服务提供者验证授权凭证后,依据凭证中的访问权限和本地访问策略做出决策。并答复或同意服务请求者的请求。

2.3 网格环境中的委托策略

委托是把权限的部分或全部给予可信任的代理。为

了避免过度使用系统资源,这些声明被设置了时间限制,在某段特定期限之后就会过期,因此如果声明持有者没有进行操作,系统就可以将资源恢复。在某些情形下,代理可能会给资源超额分配额外的声明,这样即便某些声明不能成功使用资源或是超时,也可以保证资源池被充分利用。这些技术的最终目标是实现按需计算。

3 网络安全访问策略的简单应用

由于网络安全策略的复杂性,制定网格访问控制策略可以有多种选择。笔者在相关的网络安全项目研究过程中,引入了基于 JXTA 的 P2P 网络参与任务的计算^[7]。其中 P2P 服务端主要完成 P2P 的计算任务;网格服务器主要完成 CA 认证服务,保证传输安全,对网格内部的资源进行访问控制,并向 P2P 服务端请求资源运行网格客户端提交的任务;网格客户端用于用户证书生成,并设置请求策略和任务,以及提供相关的人机交互界面。客户端生成请求策略后,将策略发往服务器,服务器将其和策略集中的策略进行匹配。客户可以根据需要获得签发后的证书,保存在自己的密钥库中。CA 服务器在运行以后,会一直监听网络上的签发请求,当收到客户发来的证书后,可以自动为客户的证书进行签名,然后将签名后的证书存入新的密钥库中。并可应用用户的请求,自动将签名后的证书返回给用户。CA 服务器为每一个用户开一个线程,可满足实际中多用户的签发需要。工作时序图如图 3 所示。

在系统运行前,需要配置以下 4 个密钥库文件。服务器端:一个是名为 serverKeys 的 KeyStore 文件,该文件中包含了对 server 的授权;另一个名为 serverTrust 的 TrustStore 文件,包含了 server 信任的 CA 的证书;客户端:一个是名为 clientKeys 的 KeyStore 文件,包含了对客户自身的授权;另一个是名为 clientTrust 的 TrustStore 文件,包含了客户端所信任的服务器的证书。通信过程的建立主要有如下步骤:

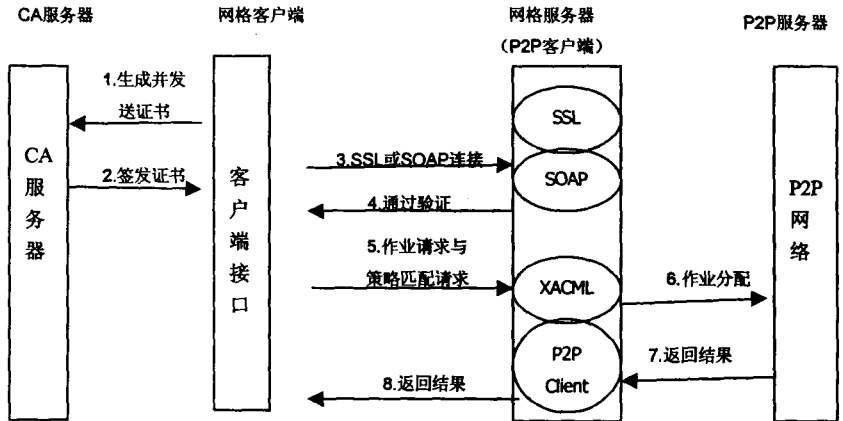


图 3 网络安全访问在 P2P 计算中的工作时序图

- (1) 运行网格服务器,等待客户端发出建立连接的申请。
- (2) 向 CA 发送证书。一般 serverTrust 中没有客户端

自签名的证书,所以客户端要先将自己的证书发给服务器信任的 CA 签发。

(3) 签发证书。CA 服务器收到证书后对证书签名,然后将签字后的证书返还给客户端。

(4) 向网格服务器发出连接请求。由于网格服务器的 IP 和端口号都是公开的,在客户登陆端界面输入需要通信的 IP 和端口号,再将注册时生成证书的用户名和密码填入,提交后,系统从

clientKeys 中提取用户的证书发送到服务器,进行连接请求。

(5) 认证。如果客户端发来的证书存在于 server Trust 中或是经过服务器信任的 CA 签发的,则连接通过,在服务器端显示新连接建立以及从客户证书中提取的信息,此时,客户也顺利进入登陆后的任务处理界面。否则,连接将不成功,转(2)。

(6) 策略请求。用户需要填写请求访问策略信息,生成一个请求策略的 XML 文件。

(7) SSL(安全的 SOAP)传输。通过 SSL 协议(或安全的 SOAP 协议)将生成的 XML 文件以及分布计算任务发送到网格服务器。

(8) 网格服务器首先进行策略匹配,根据策略匹配结果将任务分解并提交给 P2P 网络。

(9) P2P 网络计算完成后,将得到的计算结果返还给网格服务器,而网格服务再将结果进行整合并返回给网格客户端。这里网格服务器也充当了 P2P 网络的客户端角色。

图 4 是一个策略生成界面。

4 结束语

网格的安全性是网格应用的前提。传统的网络安全技术经过一定的调整后可以在网格计算环境中加以应用。认证与信任、授权与访问控制等安全策略在目前国际上没有比较成熟的网络安全体系架构情况下,如何进一步加强分布式计算安全性问题值得关注^[8]。下一步研究工作将基于 OGSA(Open Grid Services Architecture)并结合 Web 服务安全规范(如 WS-Security, WS-Policy, WS-Trust, WS-Authorization 等)进一步研究网格的安全问题。

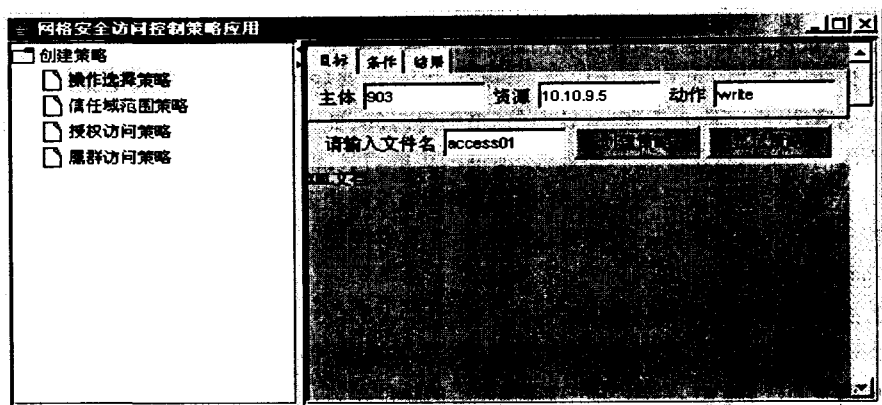


图 4 网络安全策略在 P2P 计算中的应用实例

参考文献:

- [1] Foster I, Kesselman C. 网格计算[M]. 金海等译. 北京: 电子工业出版社, 2004.
- [2] Foster I, Kesselman C, Tsudik G, et al. A security Architecture for Computational Grids[A]. Proc 5th ACM Conference on Computer and Communications Security Conference [C]. USA: ACM Press, 1998. 83-92.
- [3] Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations[J]. International Journal of High Performance Computing Applications, 2001, 15 (3): 200-222.
- [4] Welch V, Siebenlist F, Foster I, et al. Security for Grid services [A]. In: Proc 12th IEEE International Symposium on High Performance Distributed Computing [C]. Seattle, WA, USA: IEEE Computer Society, 2003. 48-57.
- [5] Nagaratnam N, Nadalin A, Janson P, et al. Security Architecture for Open Grid Services[Z]. OGSA Security Workgroup, 2003.
- [6] Housley R, Polk W, Ford W, et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile[S]. RFC 3280, 2002.
- [7] Flenner R, Abbott M. Java P2P 技术内幕[M]. 高岭等译. 北京: 人民邮电出版社, 2003.
- [8] Johnston W E, Jackson K R, Talwar S. Overview of security considerations for computational and data grids[A]. In: Proc 10th IEEE International Symposium on High Performance Distributed Computing [C]. San Francisco, CA, USA: IEEE Computer Society, 2001. 439-440.

致谢: 本文是在我们网络安全项目组的研究基础上整理完成的。对于项目组中的陈宏伟博士、陈建刚博士、张梅硕士等人在工作上的帮助, 作者表示深深的谢意。

(上接第 213 页)

2000, 36(3): 142-144.

- [2] 赵杰. 基于 C/S 和 B/S 混合结构的旅游企业信息系统的设计与实现[J]. 微型电脑应用, 2004, 20(10): 23-25.
- [3] 徐宝民, 姜理. 基于 B/S 模式的新型企业 MIS 的研究与

设计[J]. 计算机工程与应用, 1999, 35(6): 113-115.

- [4] 杨云江, 罗淑英. 基于 Web 环境的科研管理信息系统的设计与实现[J]. 贵州大学学报, 2004(1): 86-88.
- [5] Stephen W. SQL Server 7.0 开发指南[M]. 张蓉, 张燕, 赵红梅, 等译. 北京: 电子工业出版社, 1999.