网格安全互操作及其应用研究

邹德清[1)] 邹永强[2)] 羌卫中[1)] 金 海[1)] 覃 安[2)] 王 凯[1)]

[1)](华中科技大学计算机科学与技术学院服务计算技术与系统教育部重点实验室
暨集群与网格计算湖北省重点实验室 武汉 430074)

[2)](中国科学院计算技术研究所 北京 100190)

摘 要 网格计算为地理分布资源的聚合以及大规模计算问题的解决提供了技术途径,国内外大型网格项目都是基于某种网格平台构建,通过这些平台管理着本领域的资源/服务,为了聚合不同网格平台管理的资源/服务,需要实现异构网格平台的互操作.由于不同网格平台的安全机制不同,安全互操作是网格互操作中需要解决的一个关键问题.通过分析,当前网格平台通常具有网格全局用户身份以及虚拟组织层次结构的公共特征,基于网格平台的主体类型研究网格平台互操作映射策略,并提出一种通用的安全互操作流程.CGSP 和 GOS 是国内两大知名的网格中间件,分别管理了大量的教育和科技资源,以 CGSP 和 GOS 的安全互操作为例,阐述了安全互操作策略映射机制及安全互操作流程的具体实现,并分析了网格平台间的授权及其一致性、映射策略的灵活性以及互操作流程的安全性.最后,对 CGSP 和 GOS 的安全互操作的性能进行了测试分析.

关键词 网格;安全互操作;映射策略;网格证书
中图法分类号 TP393 **DOI 号**: 10.3724/SP.J.1016.2009.00514

Grid Security Interoperation and Its Application

ZOU De-Qing[1)] ZOU Yong-Qiang[2)] QIANG Wei-Zhong[1)] JIN Hai[1)] QIN An[2)] WANG Kai[1)]

[1)](*Services Computing Technology and System Laboratory / Cluster and Grid Computing Laboratory*, *School of Computer Science and Technology*, *Huazhong University of Science and Technology*, *Wuhan* 430074)

[2)](*Institute of Computing Technology*, *Chinese Academy of Sciences*, *Beijing* 100190)

Abstract Grid computing emerges as an effective technology to couple geographically distributed resources and solve large-scale computational problems in wide area networks. Each famous international grid project is constructed with a specific grid platform, and different grid projects manage different distributed resources/services. In order to aggregate resources managed by different grid platforms, it's necessary to implement the interoperation among these grid platforms. Security is one of key issues for the interoperation. Current popular grid platforms have such common properties as global user identity and virtual organization. In this paper, interoperation mapping policy and security interoperation process are proposed based on grid common properties. CGSP(ChinaGrid Support Platform) and GOS(Grid Operating System) are two popular grid platforms in China. Taking security interoperation between CGSP and GOS as an example, the implementation of interoperation mapping policy and security interoperation process are introduced. Authorization consistency, flexibility of mapping policies and the security of the interoperation process are analyzed. Finally, grid interoperation process between grid platforms also is analyzed.

Keywords grid; security interoperation; mapping policy; certificate

收稿日期:2007-08-29;最终修改稿收到日期:2009-10-05.本课题得到国家自然科学基金(60973038,60503040)、国家"八六三"高技术研究发展计划项目基金(2006AA01A115)和国家"九七三"重点基础研究发展规划项目基金(2005CB321807)资助.**邹德清**,男,1975 年生,博士,副教授,主要研究方向为网格计算、系统安全. E-mail: deqingzou@hust.edu.cn. **邹永强**,男,1981 年生,博士研究生,主要研究方向为分布式系统、网格系统软件. **羌卫中**(通信作者),男,1977 年生,博士,讲师,主要研究方向为网格计算、系统安全、可信计算. E-mail: wzqiang@hust.edu.cn. **金 海**,男,1966 年生,博士,教授,博士生导师,主要研究领域为网格计算、集群计算、网络安全、分布式存储系统等. **覃 安**,男,1980 年生,博士研究生,主要研究方向为网格系统软件、访问控制. **王 凯**,男,1983 年生,硕士,主要研究方向为网格计算.

1 引　言

网格计算为地理分布资源的聚合以及大规模计算问题的解决提供了技术途径,当前国际上知名的网格中间件有Globus[1-2]、gLite①、ARC[3]、UNICORE②、GPE③等.虽然开放式网格服务架构 OGSA 和 Web 服务资源框架 WSRF 作为网格标准而提出,但由于 OGSA 和 WSRF 本身的不成熟性,众多网格平台并没有严格遵循这两个规范,导致了网格平台之间很难互相访问,而且,网格项目都有一定的应用背景,传统网格平台的技术实现很大程度上都是为了满足某种或某类应用的需求.网格平台之间很难互访的现状是实现更广范围内资源共享需要突破的瓶颈.网格互操作能集成不同异构网格平台下的资源和服务,从而极大扩展了单一网格平台的能力,各种网格中间件通常都包含网格安全、信息服务、资源管理与调度、数据管理等基本模块,网格互操作需要考虑不同平台下同一类型模块的互操作,网格安全互操作是其中一个关键方面,虽然大多数网格系统都采用基于 PKI 的认证方式,但其认证实现的细节以及授权等安全机制各不相同.安全互操作是网格用户跨异构平台访问资源和服务的基础,并且屏蔽异构平台安全机制的差异.

近年来,互操作成为了网格计算领域的研究热点,Web 服务相关的协议和规范逐步在网格互操作中发挥了作用,其中安全相关的协议和规范包括以 WS-Security 为基础的安全协议族、安全性断言标记语言(SAML)、可扩展访问控制标记语言(XACML)等.网格资源互操作项目 GRIP,受欧盟资助,用于实现 UNICORE 和 Globus 之间的互操作.网格编程环境 GPE 和 OMII-Europe 项目是另外两个网格互操作项目,上述项目安全互操作的实现是通过在不同网格平台的 CA 证书之间建立信任关系,这是一种粗粒度的、基于认证级别的互操作.VOMS(Virtual Organization Managemenet Service)[4]是一种网格应用领域普遍使用的基于属性证书(Attribute Certificate)的网格授权系统.VOMS 项目组依托 OMII-Europe 进一步实现了基于 SAML 的属性权威(Attribute Authority)Web 服务,使用 SAML 断言取代传统的 VOMS 系统中的属性证书,以达到属性签发的互操作性.ARC 网格中间件实现了与两个不同版本 VOMS(基于属性证书和基于 SAML 断言)服务的互操作,并可以通过插件的方式解析和使用 VOMS 属性;ARC 还通过在中间件层次整合 SAML2 Web SSO Profile,利用 Shibboleth IDP(身份标示提供者)等实现多种方式的身份认证,避免了网格身份认证中需要申请 X.509 证书的局限;另外,ARC 还通过对 XACML 的支持完成安全策略的互操作性.以上实现均基于全局属性管理的前提,不能很好地解决跨域安全策略管理以及安全互操作问题.GPE4CGSP 项目旨在实现 GPE 和 CGSP 之间的互操作,提出了一系列标准的安全插件接口,如代理插件、令牌插件、证书插件、映射策略插件等,但这些接口的实现需要由网格开发者完成.全球网格论坛 GGF 于 2005 年提出了网格互操作计划 GIN④,GIN 分为不同方向,其中 GIN-aup 是针对异构网格平台的授权与身份管理的互操作.但 GIN-aup 目前还仅停留在技术交流层面.

虚拟组织是网格的基本表现形式,各种网格平台都是基于虚拟组织来组织资源和提供服务的.例如,中国教育科研网格计划 ChinaGrid[5]和中国国家网格 CNGrid[6]是国内著名的两大网格项目,CGSP⑤[7]作为 ChinaGrid 支撑平台,基于域的方式管理资源和服务,遵循 OGSA 和 WSRF 规范.CGSP 的域可以看作一个相对静态的虚拟组织.GOS[8-9]作为 CNGrid 的网格中间件,其所有组件形成 3 个层次:核心层、系统层和应用层.核心层有两个重要概念:社区(agora)和网程(grip).GOS 遵循 Web 服务规范,通过社区组织和管理虚拟化的资源/服务.GOS 中的社区是一个相对动态的虚拟组织.

虚拟组织中有不同类型的主体,如组、角色和用户,本文通过在不同网格平台的虚拟组织主体之间建立映射关系,能够有效地在认证和授权级别提供灵活的安全互操作映射策略.结合 SAML 协议,提出一种通用的安全互操作流程.以 CGSP 和 GOS 的安全互操作为例,阐述了该映射策略和互操作流程的具体实现,本文第 2 节介绍网格安全互操作的映射策略和互操作流程;第 3 节介绍 CGSP 和 GOS 之

① gLite: Lightweight Middleware for Grid Computing. http://glite.web.cern.ch/glite

② Erwin D et al. UNICORE plus final report-uniform interface to computing resources. The UNICORE forum e. V., ISBN 3-00-011592-7, 2003. Online: http://www.unicore.org/documents/UNICOREPlus-Final-Report.pdf

③ The GPE project. http://sourceforge.net/projects/gpe4gtk/

④ Grid Interoperation Now Community Group. http://forge.ogf.org/sf/projects/gin

⑤ ChinaGrid Support Platform. http://www.chinagrid.edu.cn/cgsp/

间的映射策略和安全互操作过程;第 4 节对安全策略的一致性和灵活性、互操作过程的安全性以及安全互操作的性能进行了分析;第 5 节对本文进行了总结,并展望了未来工作.

2 网格安全互操作机制

本节将在分析当前网格平台的安全特征基础上,提出一种通用的安全互操作映射策略和安全互操作流程.

2.1 网格安全互操作映射策略

由于公共密钥框架 PKI 在当前认证领域的权威地位,当前流行的网格平台基本上都采用 PKI 构建其全局的认证体系,X.509 证书通常作为网格用户的全局证书.对于应用于某种应用领域的网格系统而言,由安全中心签署的属性断言也起到了网格用户全局证书的作用,如 ShibGrid[10].虚拟组织在不同的网格系统中表现不一样,有的相对静态,具有较明显的地域或组织特性,如 CGSP;有的相对动态,如群组或社区,如 GOS 和 CROWN.通常虚拟组织采用一种层次结构进行组织,虚拟组织中包含下级虚拟组织,有的网格平台的虚拟组织只具有单层次结构,有的网格平台的虚拟组织则具有多层次结构,层次的多少甚至是可变的,如 VOMS.

本文基于网格用户全局身份以及虚拟组织层次结构的网格平台公共特征,基于网格平台的主体类型来研究网格平台互操作映射策略.在描述映射策略之前,先给出如下符号定义:

(1) U,U'分别表示两个网格系统中具有全局身份的用户集合,其中,$U=\{U_1,U_2,\cdots,U_k\}$, $U'=\{U'_1,U'_2,\cdots,U'_n\}$;

(2) VO 表示网格系统中的虚拟组织,为了区分两个网格系统的虚拟组织,其中一个表示为 VO,另一个表示为 VO'.一个网格系统中的不同虚拟组织可通过下标进行区分,如 VO_1 表示编号为 1 的虚拟组织.一个虚拟组织包含一个或多个主体,主体可表示为 S,主体可以是角色、用户或组,如 $VO_1.r$ 表示虚拟组织 VO_1 中的角色 r,通常主体拥有虚拟组织中部分资源的访问权限.对于层次性的虚拟组织而言,虚拟组织包含下级虚拟组织,如 $VO_1.VO_i$ 表示虚拟组织 VO_1 的下级虚拟组织 VO_i.

对于参与互操作的任一网格平台而言,我们给出如下 4 种类型的映射策略的定义,包括

(1) 全局身份-全局身份映射,可表示为 U-U',即一个网格平台的全局用户身份具有另一个网格平台的全局用户身份在其所在平台上的资源访问权限;

(2) 全局身份-虚拟组织主体映射,可表示为 U-$VO'.S'$,即一个网格平台的全局用户身份具有另一个网格平台的某虚拟组织主体在其所在平台上的资源访问权限.另外,在多层次的虚拟组织中,一个网格平台的全局身份可映射到另一个网格平台的某层虚拟组织的一个主体,为方便起见,下面的映射策略中的虚拟组织主体也可以是某层虚拟组织主体,不再赘述;

(3) 虚拟组织主体-全局身份映射,可表示为 $VO.S$-U,即一个网格平台中获得某虚拟组织主体身份的用户具有另一个网格平台的全局用户身份在其所在平台上的资源访问权限;

(4) 虚拟组织主体-虚拟组织主体映射,可表示为 $VO.S$-$VO'.S'$,即一个网格平台中获得某虚拟组织主体身份的用户具有另一个网格平台的某虚拟组织主体在其所在平台上的资源访问权限.

2.2 网格安全互操作流程

SAML 由标准化组织 OASIS 安全服务技术委员会提出,它是一种基于 XML 的框架,用于用户身份、权限、属性信息的交互,它包括两个关键组件:标识提供者 IDP(IDentity Provider)和服务提供者 SP(Service Provider).IDP 作为认证中心和授权中心,SP 用于校验用户的身份和属性.采用 SAML 实现网格安全互操作具有通用性.为简单起见,假设两个网格平台,Grid1 和 Grid2,各具有一个 IDP 的情形,分别表示为 $IDP1$ 和 $IDP2$.在介绍安全互操作流程之前,给出安全互操作的必要功能要求:

(1) 一个网格中的 IDP 为其平台下的全局用户签发属性断言,该属性断言反映了该用户在本平台下对应的虚拟组织主体集合.一个网格中的 IDP 也签发映射策略的属性断言,反映了另一个网格中的全局用户/虚拟组织主体在本平台中的映射关系;

(2) 两个平台的认证中心 $CA1$ 与 $CA2$ 具有相互信任关系,即一个 CA 签发的用户证书能被另一个 CA 所承认.

在描述安全互操作流程之前,先给出如下的符号定义:

(1) $X->Y$ 表示 X 发送消息给 Y;

(2) $S_X(REQ)$ 表示数据 REQ 由 S_X 签名;

(3) $Cred_{X->Y}$ 表示 Y 的身份证书由 X 签署;

(4) $M1$ 和 $M2$ 分别表示 Grid1 和 Grid2 中的映

射策略集合;

(5) $ATTR(X)$表示一个网格平台的全局用户 X 的属性集.

下面对 Grid1 中的一个全局用户 U_i 访问 Grid2 中的资源/服务的安全互操作流程进行介绍.

1. U_i —>$IDP1$,$REQ(ATTR(U_i))$,

$S_{U_i}(REQ(ATTR(U_i)))$, $Cred_{CA1->U_i}$.

用户 U_i 向本平台的标识提供者 $IDP1$ 发送获取用户 U_i 属性的请求 $REQ(ATTR(U_i))$、该请求的签名以及由 $CA1$ 签发的用户 U_i 信任状.

2. $IDP1$—>U_i,$ATTR(U_i)$,$S_{IDP1}(ATTR(U_i))$,

$Cred_{CA1->IDP1}$.

标识提供者 $IDP1$ 校验用户 U_i 的身份后,响应该用户的请求,返回用户 U_i 属性 $ATTR(U_i)$.

3. U_i —>$IDP2$: $REQ\text{-}MAPPING\text{-}POLICY$,

$S_{U_i}(REQ\text{-}MAPPING\text{-}POLICY)$,$ATTR(U_i)$,

$S_{U_i}(ATTR(U_i))$,$Cred_{CA1->U_i}$.

用户 U_i 向另一个平台的标识提供者 $IDP2$ 发送策略映射请求 $REQ\text{-}MAPPING\text{-}POLICY$,该请求由用户 U_i 签名,同时用户 U_i 把自己的属性集和属性签名以及由 $CA1$ 签发的信任状发给标识提供者 $IDP2$.

4. $IDP2$—>U_i:$M2[U_i]$,$S_{IDP2}(M2[U_i])$,$Cred_{CA2->IDP2}$.

另一网格平台的标识提供者 $IDP2$ 验证用户身份后,根据用户 U_i 的属性集返回给该用户相关的映射策略集 $M2[U_i]$ 和该映射策略集的签名,同时 $IDP2$ 也把自身的信任状发给用户 U_i,若 $M2[U_i]$为空,表示用户 U_i 在另一平台中没有映射关系,互操作流程终止.

5. U_i —>SP_m:$REQ\text{-}S$, $S_{U_i}(REQ\text{-}S)$,$M2[U_i]$,

$S_{IDP2}(M2[U_i])$,$Cred_{CA1->U_i}$.

若 $M2[U_i]$不为空,用户 U_i 向另一网格平台中的服务提供者 SP_m 发送服务请求 $REQ\text{-}S$ 及其签名、$IDP2$ 签署的与用户 U_i 相关的映射策略及其签名以及用户 U_i 信任状.

6. 服务提供者 SP_m 校验用户 U_i 的身份以及映射策略和用户属性的合法性以及完整性之后,确定用户 U_i 是否具有访问相应服务的权限,若有,请求被允许;否则,请求被拒绝.

3　CGSP 和 GOS 的安全互操作

本节将以 CGSP 和 GOS 的互操作为例,阐述网格安全互操作映射策略和互操作流程的具体应用. CGSP 的安全技术是基于 Globus 安全框架 GSI[11] 开发的,而 GOS 的安全技术是基于 Web 服务安全规范以及 X.509 证书开发. 在这一节,将分别介绍 CGSP 和 GOS 的安全机制.

3.1　CGSP 和 GOS 的安全机制

(1) CGSP 安全机制

如图 1 所示,CGSP 安全除了包含 GSI 提供的安全功能,如 GSI 的消息和会话机制(GSI-message and GSI conversion)、身份映射(Gridmap)、代理证书(Proxy certificate)及在线代理证书库(MyProxy),另外还提供了如下新的安全功能:

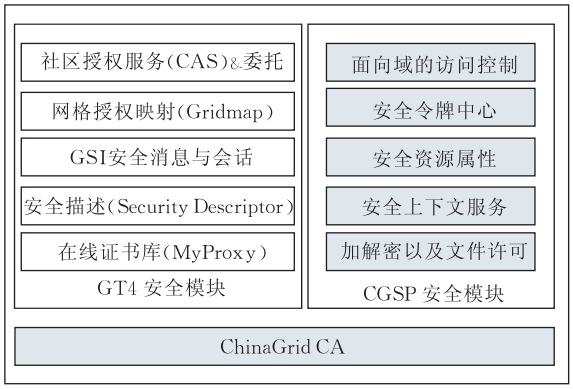


图 1　CGSP 安全框架

① 加解密以及文件许可,用于数据和文件加密、SOAP 消息加密以及文件的访问控制;

② 安全令牌中心(SecurityTokenCenter),用于为进入网格系统的用户产生基于 SAML 格式的令牌;

③ 安全上下文服务,用于解析用户令牌,为部署到 ChinaGrid 平台上的服务生成安全上下文,网格用户能够使用服务包装工具通过 CGSP 的门户定制服务的安全上下文;

④ 安全资源属性,是安全上下文服务的扩展,一个 CGSP 服务能够动态构造它的安全上下文,并通过安全资源属性大纲(Schema)以及它的安全上下文来断言用户令牌;

⑤ 面向域(Domain)的访问控制,用于控制一个域内的资源/服务的访问,网格用户在通过身份认证之后,都映射到域的用户或角色才能使用该域内的服务.

(2) GOS 安全机制

GOS 的安全机制是遵循 WS-Security 标准开发的. GOS 著重提供 CA 中心、认证、授权、访问控制机制,通过消息完整性保护结合传输层安全机制(TLS)保证 SOAP 消息通信的安全性,提供基于日志的审计功能. 它的主要技术特色包括:

①安全机制与用户、服务实现隔离. 在 GOS 平台中,安全机制的实现包括从用户登录到服务资源的执行,安全技术细节对用户/开发者是屏蔽的,如图 2 所示,一个网格用户通过他的终端用户证书(uCert)登录门户,并在 GOS 的网程容器的控制下访问物理资源. GOS 中多种安全机制由 Handler 链实施,可以在部署时进行灵活的配置,与服务开发过程无关.

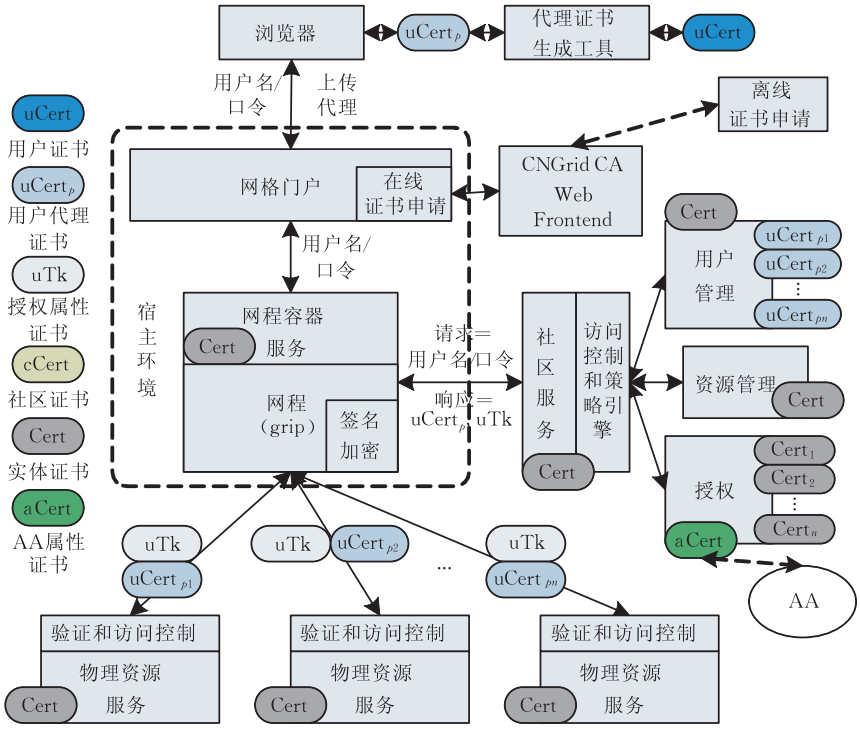


图 2 GOS 安全架构

②基于证书或用户名密码的认证. 在 GOS 系统中,有两种证书,一种是终端用户证书,一种是代理证书(pCert). 代理证书是临时的,被创建来代表终端用户证书. 当用户通过用户证书登录,登录过程网程容器会请求社区认证用户,认证通过后,网程容器使用其代理证书和其它服务进行双向认证. 为了方便用户使用,GOS 也支持通过用户名/密码进行登录.

③基于社区(Agora)的多粒度授权机制. GOS 中社区是作为虚拟组织的一种形式被提出和开发出来. 社区是用户和资源的管理中心,也是用户和资源提供者共同信任的授权中介(授权权威,AA),资源端可以自主授权,或者将权限代理给社区. 社区中的各实体是动态变化的,可以随时加入,随时退出. 社区有精确定义,它包括主体、客体、上下文、策略. 策略主要指授权策略. 授权信息的主体分为全社区、组、用户 3 种粒度,授权客体分为服务、服务操作两种粒度. 当一个用户想访问资源/服务时,首先由社区签发标准的 SAML 格式的令牌. 最终授权信息在资源端实施.

④提供用户可操作的 SOAP 消息上下文(GOS Context),其中记录社区 id,证书(或代理证书)和授权令牌. 服务开发人员可以操作此上下文,定制安全机制.

3.2 CGSP 和 GOS 的安全映射策略

CGSP 资源/服务以域为单位进行组织,这种组织方式相对静态,但符合现有资源/服务的分布特征. GOS 中的资源/服务以社区方式进行组织. 当一个 CGSP 的全局用户请求 CGSP 平台下的资源/服务时,该用户的证书需要映射到一个域中的局部用户或角色. 在一个域中,局部用户还可以分配一个或多个角色,但域中权限的分配是以角色为单位的. 在 GOS 中,每个全局用户可以加入一个或者多个社区,且至少会加入一个社区,社区可以动态创建和删除. 社区是分组的,每个全局用户可以属于一个或者多个组,且至少会属于一个组.

如 2.1 节所述,CGSP 中的域可看成一个相对静态的虚拟组织,域中的局部用户或角色可看作 CGSP 虚拟组织主体,GOS 中的社区是一个相对动态的虚拟组织,社区组也可看作虚拟组织主体. 由于 CGSP 平台下全局用户和域角色分别提供了跨域和域内资源访问的权限,且域用户也是以角色的身份获得资源/服务的访问权限,故只考虑 CGSP 中全局用户与域角色和 GOS 平台中全局用户与社区组的映射策略. 映射策略采用“X-Y 映射”形式进行描述,其中“X”表示 CGSP 平台下的授权单位,“Y”表示 GOS 平台下的授权单位,包括:(1)用户-用户映射;(2)用户-社区组映射;(3)角色-用户映射;(4)角色-社区组映射,本文所指的角色仅指 CGSP 平台中

某域中的角色.在描述映射策略之前,先给出如下符号定义:

(1)U, U'分别表示由 ChinaGrid CA 签发证书的用户集合,CNGrid CA 签发证书的用户集合,其中,$U=\{U_1,U_2,\cdots,U_k\}$, $U'=\{U'_1,U'_2,\cdots,U'_n\}$;

(2)D, $D.R$, $D.U$, $D.E$ 分别表示 CGSP 平台下所有域的集合,所有域的角色集合,所有域的局部用户集合,所有域的局部身份,其中 $D.E=D.U\cup D.R$;

(3)VO, $VO.G$ 分别表示 GOS 平台下所有社区的集合和所有社区组的集合,其中,$VO=\{Ag_1,Ag_2,\cdots\}$.

根据上述 CGSP 平台和 GOS 平台的安全机制,给出如下定义:

(1)CGSP 平台内全局用户到局部身份的映射关系可表示为 $F:U->2^{D.E}$,例如,$F(U_1)=\{D_1.r,D_2.u\}$表示 CGSP 用户映射到域 D_1 中的角色 r 和 D_2 中的用户 u; F 的逆函数 $F^{-1}:D.E->2^U$ 表示由域角色或域用户获得映射到该域角色或域用户的 CGSP 全局用户集.本文仅考虑域角色到 CGSP 全局用户的映射,即 $F^{-1}:D.R->2^U$;

(2)GOS 平台内全局用户到社区组集合的映射关系可表示为 $F':U'->2^{VO.G}$,例如,$F'(U'_1)=\{Ag_1.g_1, Ag_2.g_2\}$表示 GOS 用户同时加入了社区 Ag_1的分组 g_1 和社区 Ag_2 的分组 g_2;F'的逆函数 $F'^{-1}:VO.G->2^{U'}$ 表示社区组到 GOS 全局用户集的映射关系.

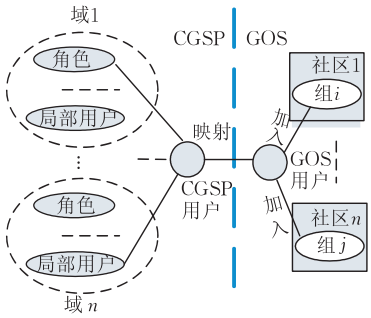
针对每一种映射策略描述如下:

(1)用户-用户映射,用于在 CGSP 用户和 GOS 用户之间建立一种直接映射关系,如图 3(a)所示.CGSP 用户拥有 ChinaGrid CA 签署的终端用户证书,而 GOS 用户拥有 CNGrid CA 签署的终端用户证书.

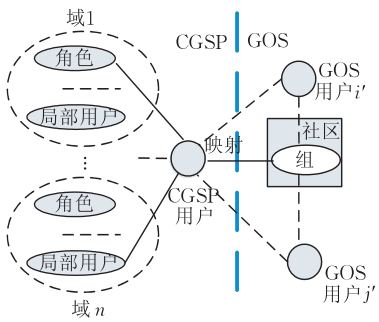
若 CGSP 平台采用了用户-用户映射策略,可表示为 $M1$: $U->U'$,例如,GOS 用户 U'_j被映射到 CGSP 用户 U_i,可表示为 $U'_j=M1(U_i)$.若 $F(U_i)=\{D_1.r_i, D_2.u_j\}$,则 U'_j具有 CGSP 平台下两个局部身份 $D_1.r_i$和 $D_2.u_j$访问资源/服务的权限.即一个 GOS 用户具有其对应的 CGSP 证书身份访问若干个域的资源/服务的权限.

若 GOS 平台采用了用户-用户映射策略,可表示为 $M1^{-1}$: $U'->U$,例如,CGSP 用户 U_i被映射到 GOS 用户 U'_j,可表示为 $U_i=M1^{-1}(U'_j)$.若 $F'(U'_j)=\{Ag_i.g_i, Ag_j.g_j\}$,则 U_i具有 GOS 平台下两个社区 Ag_i的分组 g_i和 Ag_j的分组 g_j访问资源/服务的权限.即一个 CGSP 用户能够以对应的 GOS 用户身份访问若干个社区组的资源/服务.

(2)用户-社区组映射,用于建立一个 CGSP 用户与一个 GOS 社区组的映射关系,如图 3(b)所示.



(a) 用户-用户映射



(b) 用户-社区组映射

图　3

若 CGSP 平台采用该映射策略,可表示为 $M2$: $U->VO.G$,例如,GOS 中社区组 $Ag_i.g_i$被映射到 CGSP 用户 U_i,可表示为 $Ag_i.g_i=M2(U_i)$,若 $F'^{-1}(Ag_i.g_i)=\{U'_i, U'_j\}$, $F(U_i)=\{D_i.r, D_j.u\}$,则 GOS 用户 U'_i和 U'_j都具有域角色 $D_i.r$ 和域用户 $D_j.u$ 访问资源/服务的权限.即属于社区的任一 GOS 用户具有对应 CGSP 用户访问若干个域的资源/服务的权限.

若 GOS 平台采用该映射策略,可表示为 $M2^{-1}$: $VO.G->U$,例如,CGSP 平台下用户 U_i被映射到一个社区组 $Ag_i.g_i$,可表示为 $U_i=M2^{-1}(Ag_i.g_i)$,CGSP 用户 U_i具有社区组 $Ag_i.g_i$访问资源/服务的权限.即一个 CGSP 用户具有相应社区组访问资源/服务访问的权限.

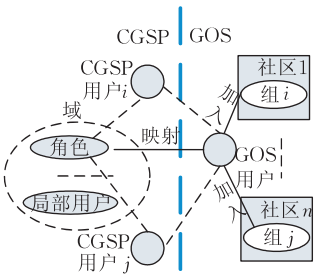
(3)角色-用户映射,用于建立 CGSP 域中的角色与 GOS 用户的映射关系,如图 4(a)所示.

若该映射策略由 CGSP 平台采用,可表示为 $M3$: $D.R->U'$, 例如,GOS 用户 U'_j被映射到 CGSP 中域 D_i中的角色 r_i,可表示为 $U'_j=M3(D_i.r_i)$,GOS

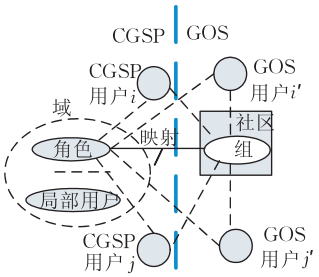
用户 U'_j 具有域角色 $D_i.r_i$ 访问资源/服务的权限. 即一个 GOS 用户具有 CGSP 某域中对应角色访问资源/服务的权限.

若该策略由 GOS 平台采用,可表示为 $M3^{-1}$: $U'->D.R$. 例如,CGSP 中域 D_i 中的角色 r_i 被映射到 GOS 用户 U'_j,可表示为 $D_i.r_i=M3^{-1}(U'_j)$,若 $F^{-1}(D_i.r_i)=\{U_i,U_j\}$, $F'(U'_1)=\{Ag_i.g_i,Ag_j.g_i\}$,则 CGSP 用户 U_i 和 U_j 都具有两个社区分组 $Ag_i.g_i$ 和 $Ag_j.g_i$ 访问资源/服务的权利. 即被分配域角色的任一 CGSP 用户具有若干个社区分组访问资源/服务的权限.

(4) 角色-社区组映射,用于建立 CGSP 域中的角色与 GOS 社区组的映射关系,如图 4(b)所示.



(a) 角色-用户映射



(b) 角色-社区组映射

图 4

若该映射策略为 CGSP 平台所采用,可表示为 $M4:D.R->VO.G$, 例如,GOS 中社区组 $Ag_i.g_i$ 被映射到 CGSP 中域 D_i 中的角色 r_i,可表示为 $Ag_i.g_i=M3(D_i.r_i)$,若 $F'^{-1}(Ag_i.g_i)=\{U'_i,U'_j\}$, 则 GOS 用户 U'_i 和 U'_j 都具有域角色 $D_i.r_i$ 访问资源/服务的权限. 即属于社区的任一 GOS 用户具有 CGSP 某域对应角色访问资源/服务的权限.

若该映射策略被 GOS 平台采用,可表示为 $M4^{-1}$: $VO.G->D.R$, 例如 CGSP 中域 D_i 中的角色 r_i 被映射到一个社区组 $Ag_i.g_i$,可表示为 $D_i.r_i=M4^{-1}(Ag_i.g_i)$,若 $F^{-1}(D_i.r_i)=\{U_i,U_j\}$, 则 CGSP 用户 U_i 和 U_j 都具有社区组 $Ag_i.g_i$ 可访问的资源/服务的权利. 即被分配某域的一个角色身份的任一 CGSP 用户具有相应社区组可访问的资源/服务访问的权利.

3.3 CGSP 和 GOS 的安全互操作流程

目前 CGSP 与 GOS 平台安全互操作只考虑 CGSP 平台与 GOS 平台各具有一个 IDP 的情形. 在介绍安全互操作流程之前,给出两个平台安全互操作的必要功能要求:

(1) CGSP 平台中的 IDP 为 CGSP 中用户签发属性断言,该属性断言反映了 CGSP 用户在 CGSP 平台下的映射关系,如域角色. CGSP 平台中的 IDP 也签发映射策略的属性断言,反映了 GOS 中的用户/社区组在 CGSP 中的对应关系.

(2) GOS 平台中的 IDP 为 GOS 中用户签发属性断言,该属性断言反映了 GOS 中用户加入的社区组. 它也签发映射策略的属性断言,反映了 CGSP 中的用户或域角色在 GOS 中的对应关系.

(3) ChinaGrid CA 和 CNGrid CA 之间具有相互信任关系,即 ChinaGrid CA 签发的用户证书能被 CNGrid CA 所承认,CNGrid CA 签发的用户证书也能被 ChinaGrid CA 所承认.

除 2.2 节的定义外,再给出如下的符号定义:

(1) M, $M[U']$, $M[VO.G]$, $M[U'_i]$, $M[VO.G]_{U'_i}$ 分别表示在 CGSP 的 IDP 中,所有映射策略的集合,属于用户-用户映射和角色-用户映射两种类型的映射策略集合,属于用户-社区组映射和角色-社区组映射两种类型的映射策略集合,与 GOS 用户 U'_i 相关的映射策略以及 $M[VO.G]$ 中与用户 U'_i 相关的映射策略;

(2) M^{-1}, $M^{-1}[U]$, $M^{-1}[D.R]$, $M^{-1}[U_i]$, $M^{-1}[D.R]_{U_i}$ 分别表示在 GOS 的 IDP 中,所有映射策略的集合,属于用户-用户映射和用户-社区组映射两种类型的映射策略集合,属于角色-用户映射和角色-社区组映射两种类型的映射策略集合,与 CGSP 用户 U_i 相关的映射策略以及 $M^{-1}[D.R]$ 中与用户 U_i 相关的映射策略;

下面对 CPSP 用户访问 GOS 资源/服务以及 GOS 访问 CGSP 资源/服务的安全互操作流程分别进行介绍.

CGSP 用户访问 GOS 资源/服务

流程如下:

1. $U_i->IDP_i, REQ(ATTR(U_i))$,
   $S_{U_i}(REQ(ATTR(U_i)))$, $Cred_{C\_CA->U_i}$.

CGSP 用户 U_i 向 CGSP 平台的标识提供者 IDP_i 发送获取用户 U_i 属性的请求 $REQ(ATTR(U_i))$、该请求的签名

以及由 ChinaGrid CA(*C_CA*)签发的用户 U_i 信任状.

2. $IDP_i \rightarrow U_i, ATTR(U_i), S_{IDP_i}(ATTR(U_i)), Cred_{C\_CA \rightarrow IDP_i}$.

标识提供者 IDP_i 校验用户 U_i 的身份后,响应该用户的请求,返回用户 U_i 属性 $ATTR(U_i)$.

3. $U_i \rightarrow IDP_j$: *REQ-MAPPING-POLICY*, $S_{U_i}(REQ\text{-}MAPPING\text{-}POLICY), ATTR(U_i), S_{U_i}(ATTR(U_i)), Cred_{C\_CA \rightarrow U_i}$.

用户 U_i 向 GOS 的标识提供者 IDP_j 发送策略映射请求 *REQ-MAPPING-POLICY* 及签名、用户 U_i 的属性集及签名、用户 U_i 的信任状.

4. $IDP_j \rightarrow U_i$: $M^{-1}[U_i] \cup M^{-1}[D.R], S_{IDP_j}(M^{-1}[U_i] \cup M^{-1}[D.R]), Cred_{V\_CA \rightarrow IDP_j}$.

GOS 的标识提供者 IDP_j 验证用户身份后,根据用户 U_i 的属性集返回相关的映射策略集、$M^{-1}[U_i] \cup M^{-1}[D.R]$ 以及该映射策略集的签名,同时 GOS 的标识提供者 IDP_j 把由 CNGrid CA(*V_CA*)签发的信任状发给用户 U_i, 其中 $M^{-1}[U_i]$ 是与用户 U_i 相关的映射策略集,$M^{-1}[D.R]$ 表示的映射策略集与用户 U_i 的域角色属性相关.

5. 用户 U_i 首先验证标识提供者 IDP_j 身份并检查映射策略集的完整性,然后检查映射策略集. 若映射策略集为空,则在 GOS 中没有映射关系,用户终止下一步请求操作. 若用户 U_i 是通过用户-用户映射策略或用户-社区组映射策略和 GOS 中用户/社区组对应的,则执行

$U_i \rightarrow SP_m$: *REQ-S*, $S_{U_i}(REQ\text{-}S), M^{-1}[U_i], S_{IDP_i}(M^{-1}[U_i]), Cred_{C\_CA \rightarrow U_i}$.

若用户 U_i 是通过角色-用户映射策略或角色-社区映射策略和 GOS 中用户/社区组对应的,则执行

$U_i \rightarrow SP_m$:
REQ-S, $S_{U_i}(REQ\text{-}S), M^{-1}[D.R]_{U_i} S_{IDP_j}(M^{-1}[D.R]_{U_i})$, $ATTR(U_i), S_{IDP_i}(ATTR(U_i)), Cred_{C\_CA \rightarrow U_i}$.

用户 U_i 向 GOS 中的服务提供者 SP_m 发送对服务请求 *REQ-S*、GOS 标识提供者 IDP_j 签署的与用户 U_i 相关的映射策略、CGSP 标识提供者 IDP_i 签署的用户 U_i 属性 $ATTR(U_i)$(对于第 2 种情况)以及用户 U_i 信任状.

6. 服务提供者 SP_m 校验用户 U_i 的身份以及映射策略和用户属性的合法性以及完整性之后,确定用户 U_i 是否具有访问相应服务的权限,若有,请求被允许;否则,请求被拒绝.

GOS 用户访问 CGSP 资源/服务

GOS 用户访问 CGSP 资源/服务的安全互操作流程和上述流程的步骤近似. 下面描述其不同之处:

(1) 对于第 1 步和第 2 步,是由 GOS 用户向本平台标识提供者发送查询属性的请求,并由标识提供者返回属性集给该 GOS 用户;

(2) 对于第 3 步和第 4 步,是由 GOS 用户向 CGSP 标识提供者发送查询映射策略的请求,并由 CGSP 标识提供者向该 GOS 用户返回映射策略;

(3) 对于第 5 步,若从 CGSP 标识提供者返回的映射策略中包含用户-用户映射或角色-用户映射,检查这些映射策略中是否存在该 GOS 用户对应的 CGSP 用户或角色,若不存在,根据 GOS 用户的社区组属性信息检查映射策略中是否包含对应的用户-社区组映射或角色-社区组映射,若也不存在,则用户终止进一步操作. 若存在对应映射策略,则向 CGSP 的某服务提供者发送相应的映射策略和用户的服务请求.

(4) 对于第 6 步,CGSP 服务提供者根据 GOS 用户发送的信息,确定该用户是否允许访问服务,并把处理结果返回给该 GOS 用户.

4　安全互操作分析

在这一节中,以 CGSP 和 GOS 平台间的互操作为例分析网格安全互操作的授权及一致性,接着分析映射策略的粒度以及互操作流程的安全性.

4.1　网格平台间的授权及一致性分析

本小节先分别分析 CGSP 平台对 GOS 用户的授权和 GOS 平台对 CGSP 用户的授权,并对授权中的一致性进行分析.

CGSP 平台对 GOS 用户的授权分析

对于任一 CGSP 用户 U_i,根据与用户 U_i 相关的映射策略 $M^{-1}[U_i]$ 可得到:用户 U_i 映射到 GOS 平台的用户(根据用户-用户映射)和社区组(根据用户-社区组映射)的集合. 通过结合 GOS 用户与社区组的映射关系 F':$U' \rightarrow 2^{VO.G}$,得到用户 U_i 映射到 GOS 平台的社区组集合,设为 G. 根据 CGSP 用户和局部身份的映射关系 F:$U \rightarrow 2^{D.E}$,得到用户 U_i 映射到 CGSP 平台内的域角色集合,根据与该集合中所有域角色相关的映射策略,得到集合中每个域角色映射到 GOS 平台的用户(根据角色-用户映射)和社区组(根据角色-社区组映射)的集合,再通过 GOS 用户与社区组的映射关系 F' 得到域角色与社区组集合的映射,对每个域角色映射到的社区组集合取并集,记为 G'. 则 CGSP 用户 U_i 可对应 GOS 平台中的社区组集合为 $G \cup G'$,故用户 U_i 可获得的 GOS 平台中资源/服务的访问权限为 $G \cup G'$ 可访问的权限.

为了简化映射的复杂性和维护授权的一致性,针对于同一个 CGSP 用户,不宜同时采用用户-用户映射以及用户-社区组映射两种策略;针对于同一个 CGSP 域角色,不宜同时采用角色-用户映射以及角

色-社区组映射两种策略.另外,在采用用户-社区组映射以及角色-社区组映射时,不宜采用同一种策略映射到同一个社区的两个不同分组.因为很可能导致同一 CGSP 用户/域角色同时映射到 GOS 平台某社区中的不同分组,为了保证授权的一致性,原则上不宜映射到一个社区的多个分组.

GOS 平台对 CGSP 用户的授权分析

对于任一 GOS 用户 U'_i,根据与用户 U'_i 相关的映射策略 $M[U'_i]$ 可得到:用户 U'_i 映射到 CGSP 平台的用户(根据用户-用户映射)和域角色(根据角色-用户映射)的集合.通过结合 CGSP 用户与局部身份(域用户和域角色)的映射关系 $F:U->2^{D,E}$,得到用户 U'_i 映射到 CGSP 平台的局部身份集合,由于域用户也通过映射到域角色获得资源/服务的访问权限,则用户 U'_i 通过映射策略 $M[U'_i]$ 可映射到 CGSP 平台的域角色集合,设为 R.根据 GOS 用户和社区组的映射关系 $F':U'->2^{VO,G}$,得到用户 U'_i 映射到 GOS 平台内的社区组集合,根据与该集合中所有社区组相关的映射策略,得到每个社区组映射到 CGSP 平台的用户(根据用户-社区组映射)和角色(根据角色-社区组映射)的集合,再通过 CGSP 用户与局部身份的映射关系 F 最终得到社区组与域角色集合的映射,并对每个社区组映射到的域角色集合取并集,记为 R',则 GOS 用户 U'_i 可对应 CGSP 平台中的域角色集合为 $R\cup R'$,故用户 U'_i 可获得的 CGSP 平台中资源/服务的访问权限为 $R\cup R'$ 可访问的权限.

为了简化映射的复杂性和维护授权的一致性,针对于同一个 GOS 用户,不宜同时采用用户-用户映射以及角色-用户映射两种策略;针对于同一个 GOS 社区组,不宜同时采用用户-社区组映射以及角色-社区组映射两种策略.因为很可能导致同一 GOS 用户/社区组同时映射到 CGSP 平台某域中的不同角色,为了保证授权的一致性,原则上不宜映射到一个域的多个角色(或局部身份).

4.2 映射策略的粒度分析

理论 1. 网格安全互操作的映射策略是灵活的、精粒度的.

证明. 通过 CGSP 和 GOS 的安全互操作映射策略进行具体分析:(1) 对于 CGSP 平台而言,(i) 如果用户-用户映射策略被采用,一个 GOS 用户能够访问多个 ChinaGrid 中域的资源/服务,只要 GOS 用户对应的 CGSP 证书身份在多个域建立了映射关系;(ii) 如果用户-社区组映射策略被采用,属于某社区组的任一 GOS 用户能够访问多个 ChinaGrid 中域的资源/服务,只要该社区组对应的 CGSP 证书身份在多个域建立了映射关系;(iii) 如果角色-用户映射策略被采用,一个 GOS 用户拥有对应角色访问某域资源/服务的权限;(iv) 如果角色-社区组映射策略被采用,属于某社区组的任一 GOS 用户拥有对应角色访问某域资源/服务的权限.CGSP 通过灵活采用其中一种或几种映射策略,能够使得 GOS 中的某一用户或某类用户拥有 CGSP 平台中单域/多域中资源/服务的权限.(2) 对于 GOS 平台而言,(i) 如果用户-用户映射策略被采用,一个 CGSP 的用户能够访问若干个社区组中的资源/服务;(ii) 如果用户-社区组映射策略被采用,一个 CGSP 用户能够访问对应社区组中的资源/服务;(iii) 如果角色-用户映射策略被采用,则被分配该角色的任一 CGSP 用户能够访问若干个社区组资源/服务的权限;(iv) 如果角色-社区组映射策略被采用,则被分配该角色的 CGSP 用户能够访问对应社区组中的资源/服务.CGSP 通过灵活采用上述一种或几种映射策略,使得 CGSP 平台中一个用户或分配某角色的任一用户能够访问若干个社区组的资源/服务.

证毕.

4.3 互操作流程的安全性分析

理论 2. 网格安全互操作流程是可信的.

证明. 通过 CGSP 和 GOS 的安全互操作流程进行具体分析:(1) PKI 机制和 X.509 证书在互操作流程中被采用,$Cred_{CA->U}$, $Cred_{CA->SP}$ 和 $Cred_{CA->IDP}$ 是 ChinaGrid CA 或 GOS CA 分别为用户、服务提供者和标识提供者签发的信任状,如步 1 和步 2 通过证书在用户和标识提供者之间实现相互认证;(2) 信息完整性通过签名的方式获得,如多个步骤中的 $S_U(INFO)$, $S_{SP}(INFO)$ 和 $S_{IDP}(INFO)$ 分别表示由用户(U)、服务提供者(SP)和标识提供者(IDP)签名的数据,$INFO$;(3) 机密性在本安全互操作流程中是不必要的,因为 CGSP 平台和 GOS 平台仅需要验证从属对方平台的用户证书是否合法以及是否具有完整性,而且,信息的加密和解密机密性将对互操作性能的影响也比较大. 证毕.

5 CGSP 与 GOS 安全互操作性能测试

本文基于 CGSP 2.0 版和 GOS 2.1 版实现了安全互操作.CGSP 和 GOS 都采用 X509 格式的证书,CA 之间通过交叉认证建立信任关系.第 3 节已

经描述了在 CGSP 全局用户与域角色和 GOS 全局用户与社区组之间进行映射的 4 种方式. 为了完成 CGSP 与 GOS 的安全互操作流程,本文采用互操作代理的方法. 在 CGSP 和 GOS 中分别部署一个互操作代理,负责到对方平台的安全互操作,其操作流程详见第 3.3 节. 为了做成通用的代理服务,还需要封装用户参数成统一内部格式,解析服务的 WSDL 并生成一个通用的 Web services 或 WSRF 的请求客户端,将先前的内部格式的参数转换为该平台规定的特有的格式,提交服务请求.

为了测试安全互操作引起的开销,在 CGSP 和 GOS 中分别部署一个 ping 服务. Ping 服务直接返回接收到的参数,其逻辑所占的时间可以忽略不计,可以用来测试系统的开销.

本文主要测试存在安全互操作和不存在安全互操作的情况下的差值来测试安全互操作的开销,采用 1024 位的 RSA 算法来实现认证和签名功能. 主要测试 4 种情况:用 GOS 的客户端调用 GOS 中的 ping 服务,记为 GOS-client;用 CGSP 的客户端调用 CGSP 中的 ping 服务,记为 CGSP-CLIENT;通过 GOS 访问 CGSP 中的服务,记为 GOS-CGSP-CLIENT;通过 CGSP 访问 GOS 中的服务,记为 CGSP-GOS-CLIENT.

由于网络速度受多种不定因素的影响,而本测试主要考虑平台带来的安全互操作开销,故本次测试在局域环境下进行. CGSP 平台和 GOS 平台中的标识提供者 IDP 分别在本平台服务器上安装实现,如 CGSP 平台的 IDP 安装在 CGSP 服务器上. 代理服务器上除了具有用于互操作的代理服务外,还作为平台的客户端使用. 构建的环境由局域网内 4 台主机组成:(1) CGSP 服务器:Pentium III 1000MHz; 512MB; 100 Mbps Full duplex;(2) GOS 服务器: AMD Opteron; 1600MHz; 2GB; 100 Mbps Full duplex;(3) CGSP-GOS 代理服务器: Pentium III; 1000MHz;256MB;100 Mbps Full duplex;(4) GOS-CGSP 代理服务器:Pentium III;1000MHz;512MB; 100 Mbps Full duplex. 另外,局域网机器间传输带宽为 100Mbps. 通过对 ping 服务在上述 4 种调用方式下分别测试了 80 次之后,获得平均值,如表 1 所示.

表 1　各种 ping 服务的开销平均值　(单位:ms)

GOS-CLIENT	CGSP-CLIENT	GOS-CGSP-MD	CGSP-GOS-MD
132.367	167.114	566.937	533.379

从表中可以看出,通过 CGSP 中的代理服务调用 GOS 中的服务(CGSP-GOS-MD)比直接调用 GOS 中的服务(GOS-CLIENT)多花 533.379−132.367=401.012ms,即可以认为安全互操作引入的开销是 401.012ms;通过 GOS 中的代理服务调用 CGSP 中的服务比直接调用 CGSP 中的服务(CGSP-CLIENT)会多出 566.937−167.114=399.823ms,可以认为是通过 GOS 中的代理进行安全互操作时引入的开销是 399.823. 通过 CGSP 和 GOS 调用对方的服务时,整个安全互操作流程引入的开销主要来自认证和签名的计算开销,本文在测试时把映射策略放在内存中,若映射策略放在磁盘文件中,则安全互操作还需要加上这部分开销. 另外,在映射策略数量为 100 条时,采用常用的排序算法进行策略匹配的时间几乎可以忽略不计.

安全互操作引起的开销相对于服务的业务逻辑往往可以忽略不计. 对于批作业计算任务,作业的运行时间通常是小时、天的数量级,互操作引起的开销可以忽略不计. 对于计算量比较小的作业,本文以 ChinaGrid 中常用的医学图像处理为例. 给出一个由 8 个节点机(16 个处理器)和 1 个前端机通过千兆以太网互连而成的测试系统,其中每个节点上配备 2 块 Intel XEON 3.2G CPU 和 4GB RAM.

表 2　滤波变换算法在平台中的开销

操作名	输入数据和参数	并行度	时间/μs
离散余弦滤波	baghdad-1024-port.bmp 频率阈值 $FD=5$	1	13962250
		2	7209872
		4	3678437
		8	1854901
		16	963578
高通滤波	baghdad-1024-port.bmp 频率阈值 $FD=5$	1	6663251
		2	3726130
		4	1806792
		8	931568
		16	489852
低通滤波	baghdad-1024-port.bmp 频率阈值 $FD=5$	1	6784121
		2	3766735
		4	1901248
		8	963587
		16	490763

由表 2 可知,以上 3 个常用变换操作,对于 1024×1024 的图片而言,16 个 CPU 处理的时间分别为 964、489、491ms,单 CPU 分别为 13962、6663、6784ms,但在实际情况中,较复杂图形图像的处理时间与单图片处理时间相比,存在不止一个数量级的时间差别,远大于互操作引发的开销 401.012ms 和 399.823ms.

通过如上的分析可以得出,在针对计算量比较

大的科学计算时,安全互操作对性能的影响不大,如果只是单个图片的处理,或处理时间比较短的任务,则安全互操作的开销对性能的影响比较大,对于这种小任务,尽量不要采用安全互操作.

6 结论和未来工作

本文对网格安全互操作及其应用进行了研究.基于当前流行的网格公共特性,如全局用户身份、虚拟组织等,提出了通用的网格安全映射策略.基于SAML规范,研究了网格安全互擦作的流程.以CGSP和GOS的互操作为例,阐述了网格安全映射策略以及网格安全互操作流程的实现过程.然后,从3个方面对安全互操作进行分析:(1)平台间的授权及一致性分析;(2)映射策略的灵活性;(3)互操作流程的安全性.最后对安全互操作的性能进行了分析,分析表明,安全互操作对计算量比较大的科学计算的性能影响小.未来的工作将考虑在更多的平台上实现本文提出的安全互操作机制.

参 考 文 献

[1] Foster I, Kesselman C. Globus: A metacomputing infrastructure toolkit. International Journal of Supercomputer Applications, 2003, 11(2): 115-128

[2] Foster I. Globus toolkit version 4: Software for service-oriented systems//Proceedings of the IFIP International Conference on Network and Parallel Computing. Beijing, China, 2005: 2-13

[3] Ellert Mattias et al. Advanced resource connector middleware for lightweight computational grids. Future Generation Computer Systems, 2007, 23(1): 219-240

[4] Alfieria R, Cecchinib R, Ciaschinic V, dell'Agnello L. From gridmap-file to voms: Managing authorization in a grid environment. Future Generation Computer Systems, 2005, 21(4): 549-558

[5] Jin Hai. ChinaGrid: Making grid computing a reality//Proceedings of the 7th International Conference on Asian Digital Libraries (ICADL'04). Shanghai, China, 2004: 13-24

[6] Qian Depei. CNGrid: A test-bed for grid technologies in China//Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems. Suzhou, China, 2004: 135-139

[7] Wu Y, Wu S, Yu H et al. CGSP: An extensible and reconfigurable grid framework//Proceedings of the Advanced Parallel Programming Technologies 2005 (APPT 2005). Hong Kong, China, 2005: 292-300

[8] Xu Zhiwei, Li Wei. Vega grid: A computer systems approach to grid research//Proceedings of the 2nd International Workshop on Grid and Cooperative Computting. Shanghai, China, 2004: 480-486

[9] Li Z, Wei L et al. System software for China national grid//Proceedings of the IFIP International Conference on Network and Parallel Computing (NPC 2005). Beijing, China, 2005: 14-21

[10] Spence D, Geddes N, Jensen J et al. ShibGrid: Shibboleth Access for the UK national grid service//Proceedings of the 2nd IEEE International Conference on e-Scienceand Grid Computing (e-Science). Amsterdam, Netherlands, 2006: 75-75

[11] Foster I, Kesselman C, Tsudik G, Tuecke S. A security architecture for computational grids//Proceedings of the 5th ACM Conference on Computer and Communications Security Conference. San Francisco, CA, USA, 1998: 83-92

ZOU De-Qing, born in 1975, Ph.D., associate professor. His research interests include grid computing, system security.

ZOU Yong-Qiang, born in 1981, Ph. D. candidate. His research interests include distributed system, grid middleware.

QIANG Wei-Zhong, born in 1977, Ph. D.. His research interests include grid computing, system security, trusted computing.

JIN Hai, born in 1966, Ph. D, professor. His research interests include grid computing, cluster computing, network security, distributed storage system.

Qin An, born in 1980, Ph. D. candidate. His research interests include grid middleware, access control.

WANG Kai, born in 1983, M. S.. His research interests focus on grid computing.

Background

The research in this paper covers grid security issues in the context of interoperation bewteen different grid platforms. Current popular grid platforms utilize some common properties such as global user identity and virtual organization's attribute for solving the security interoperation issue, which is actually unable to cover the policy heterogeneous issue. This paper proposes a mechanism which utilizes interoperation mapping policy, and a generic process for security interoperation.

Also, the proposed solution is implemented and tested under two popular grid platforms: CGSP (China Grid Support Platform) and GOS(Grid Operating System). The analysis shows the authorization consistency, flexibility of mapping policies and the security of the interoperation process.

The research is supported by the National Natural Science Foundation of China under grant No. 90412010, and No. 60503040, and the National Basic Research Program of China(973 Program) of China under grant No. 2005CB321807, all of which are related to (or include) the security issue of distributed computing, such as grid computing, virtualization-based computing, etc. Since security issue is a critical issue in distributed computing area, the research here is quiet important.

The main authors of this paper have gained sufficient archivement in terms of reseach and development. In detail, the solution proposed in this paper has been implemented and integrated into CGSP 2.0 platform. Also some related papers have been issued in IEICE Transaction, Journal of Software, and the proceedings of some international conferences, a few national patents and software copyrights have been applied as well.

The achievement of this paper has solved the security interoperation issue beteen different grid platforms.