网格计算安全构架及其实现*)

应 宏
(重庆三峡学院计算机科学系 重庆404000)

摘 要 网格要实现分布资源的共享,必须构建新的安全体系,制定更高要求的安全机制。通过分析网格计算的安全特性和安全策略,研究了网格计算的安全体系结构,讨论了结构中的主要技术和用户任务的安全认证过程。介绍了Globus Toolkit 3(GT3)中安全机制的实现,探讨了Globus Toolkit 3为体现OGSA思想对安全机制和任务分配流程的改进。

关键词 网格计算,安全构架,认证,授权,安全映射,Globus Toolkit 3

Security Infrastructure of Grid Computing and Security Realization

YING Hong
(Dept. of Computer Science Chongqing, Three Gorges University, Chongqing 404000)

Abstract New security system and higher-standard security mechanism of grid should be constructed in order to realize the share of resources distribution in Internet. By analyzing security characteristics and policies of grid computing, we have researched security infrastructure of grid computing, discussed the key technology in the security infrastructure, and the security certification procedure of the user's task. This paper also introduces the realization of security system in Globus Toolkit 3(GT3), discusses the improvement of the safe system and task allocation procedure of Globus Toolkit 3 based on OGSA.

Keywords Grid computing, Security infrastructure, Certificates, Mandate, Security mapping, Globus toolkit 3

网格计算(Grid Computing)源于元计算(Metacomputing),其初衷是将分布的多台超级计算机连接成为一个可远程控制和访问的元计算系统,并逐步发展为遵循开放标准,聚集网络上广泛分布的计算、存储、数据、软件、仪器设备和传感器等各种资源的分布合作计算平台,以服务的方式支撑大规模计算和数据处理等各种应用,将Internet变为一个功能强大、无处不在的计算设施。

网格计算的应用与传统的客户/服务器应用有很大的不同,它要求同时使用大量的资源,动态的资源请求,对多个管理域中资源的使用,复杂的通信结构以及严格的性能要求等。同时,网格计算环境要求不影响各节点本地的管理和自主性,不改变原有的操作系统、网络协议和服务,允许远程节点选择加入或退出系统,尽量使用已存在的标准和技术以便与已有应用兼容并能提供可靠的容错机制,保证用户和远程节点的安全性。网格计算的这些特点,对安全性提出了新的更高的要求。

1 网格计算安全问题

1.1 网格计算安全特性

网格计算的特点导致分布式系统中已有的安全技术尚不能解决网格计算环境的安全问题,表现出如下特性[1]:

(1)用户数量庞大,参与者变化的频率较高,动态性强。

(2)资源池庞大,且动态可变。一个计算(由计算创建的过程)可能要求在它的执行期间动态地开始使用或释放资源。

(3)组成计算的进程可以用不同的机制进行通信,包括单播和多播。程序执行期间,低级别的通信连接(例如:TCP/IP套接字)可能被动态地创建或撤销。

(4)资源可支持不同的认证和授权机制,包括Kerberos、明文口令、安全套接协议(Secure Sockets Layer,SSL)、Secure Shell(SSH)。

(5)用户在不同的资源上可有不同的标识,资源和用户可属于多个组织。

正是由于网格计算环境的特殊性,要求在设计网格安全机制时,特别要考虑网格计算环境的动态主体特性,并要保证网格计算环境中不同主体间的相互鉴别、信任和各主体间通信的保密性和完整性,以使网格系统中的计算问题能调整不同的访问控制策略并能在不同性质的环境中安全运行。

1.2 安全策略要求

为了解决网格计算的安全问题,网格计算环境应具备相应安全策略[2]:

(1)网格计算环境包括多个信任域,它将限制或不影响局部安全策略。

(2)单一信任域内的操作仅受局部安全策略的影响。

(3)对每个信任域,都存在一个从全局到局部主体的映像。

(4)位于不同信任域的实体间的操作要求相互鉴别。

(5)一个被鉴别的全局主体映像为一个局部主体被看作等同于局部主体的本地认证。

(6)所有访问控制决定都由局部主体在本地做出,要求访问控制决定权保留在局部系统管理员手中。

(7)一个程序或过程可以代表用户操作,从属于用户权利的子集。

(8)代表同一信任域内同一主体的过程可以共享一个单一的信用集。

*)重庆市教委科研基金项目(021105)。应 宏 副教授,主要研究方向为网格计算、网络数据库。

2 网格计算安全体系构架

在网格计算环境中，客户和服务器之间的区别消失了，此时单个资源既可以作为服务器（当它接受请求时）同时也可以作为别人的客户（当它向其它资源提交请求时）。因此，在构造网格计算安全体系结构中，主体和对象、认证和授权、代理和局部映射等是最基本的问题。根据上述的安全策略，图1构建了一种网格计算安全体系结构[3]，该结构着重描述了网格计算环境中的安全鉴别问题。

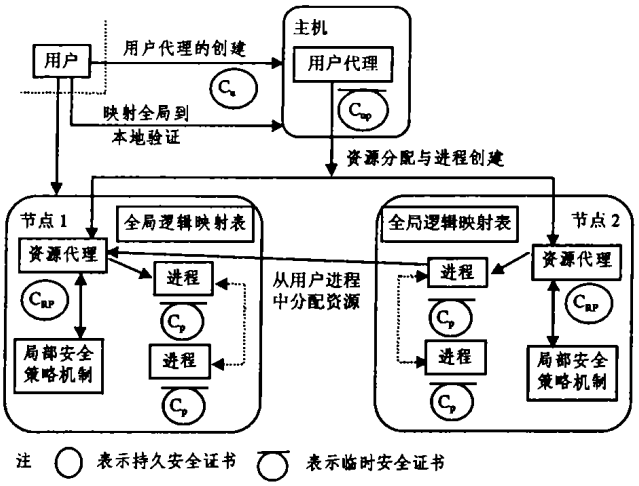

图1 网格计算安全体系结构

2.1 主要技术

主体和对象 安全体系结构中的主体和对象必须包含组成计算的实体，一个计算包括许多进程，每个过程代表一个用户。这样，主体是用户和过程。对象包括可用于网格环境中的大范围的资源：网络、计算机、数据库、显示设备等。

代理 网格计算对资源的使用具有动态性，每次计算得到资源，它就代表一个特定的用户，由于涉及的资源数量可能很多，并且一些应用程序可能运行很长时间（几天或几周）且不需要干预。为此，在安全体系结构中引入用户代理，它在没有用户干预和有时限的情况下代替用户的行为。资源代理实现全局到局部的映射以及资源的分配。

认证 在网格环境中的每一个用户和服务都需要通过认证来验明正身。认证的一个关键点是认证证书，证书中包括用户名称、公钥、认证中心的标识和认证中心的签名。图1中基于用户的私钥创建具有时间戳的用户代理，从而为用户提供一种安全认证的方法。用户如果没有创建这个代理，就不能提交任务，也不能传输数据，这个代理一经创建就可以授权或者拒绝对整个网格内部所有资源的访问，因为这个代理可以在整个系统中使用，这就使得最终用户可以只登录一次，即当需要认证时，由用户代理出示用户签署的认证证书来证明自己的合法性。

授权 即访问控制，其功能用于控制哪些用户可以访问系统中的哪些部分，它是网格系统中一项最基本最重要的操作。处理用户授权的方法是将用户映射为所访问系统的本地用户。当接收请求的系统从代理中读取用户的名字，然后根据一个本地文件将这个名字映射为本地用户名。为了避免在不同的网格系统中创建很多额外的用户ID，管理员可以将用户划分为虚拟的组，某个特定域下面的所有用户在访问某项特定网格资源时，都可以映射到一个公用用户ID上，从而实现集体授权。

安全映射 即全局映射到局部安全机制。不同的网格节点可以使用不同的局部安全解决方案，一个网格安全基础架构需要映射到每个节点的局部解决方案，这样局部操作才能在合适的特权下继续进行。

2.2 认证、授权和安全映射过程

在网格环境中用户任务的提交与安全执行是网格系统的一个基本问题，图1简单描述了用户任务的安全认证过程。

（1）用户获得将要创建用户代理的主机的使用权，接着创建用户代理，并为用户代理创建临时安全证书，该证书包括主机名、用户ID、起始时间、结束时间和安全信息等。用户代理的临时安全证书由用户签署，有给定的有效期，提供其安全身份保证。

（2）用户的任务需要创建新的进程来执行和使用远端节点的资源。用户代理与资源代理相互认证，即对二者的安全证书和身份进行鉴别。在这个进程中，资源代理要检查用户代理的证书是否过期，用户代理向资源代理提交签署的请求，资源代理检查用户签署的临时安全证书是否映射到本地安全策略。如果该请求是可信的，资源代理创建一个资源安全证书，证书中包括要分配资源的用户的名字、资源名字等。资源代理安全地将资源安全证书传递给用户代理。

（3）如果任务在执行过程中需要其他的远程资源，则必须在任务进程和资源代理之间进行相互认证，通过安全鉴别后，进行授权、本地ID映射，任务进程才可以使用资源。

（4）为了执行本地访问安全控制，资源代理要把一个主体映射为一个本地资源“知道”的主体，所以要把主体的全局名称转换成本地的局部名称。为了完成名称映射，资源代理必须能够对主体、主体的证书、资源证书和资源主体进行访问。映射的基本思想是通过进程管理者完成对用户安全证书和本地安全证书或本地安全账号的访问。

另外，在这个安全体系结构中，用户所对应的用户代理一旦创建以后，用户可以与用户代理断开连接，由用户代理代表用户与资源进行安全交互。由于该体系结构侧重于用户、资源和过程的鉴别，因此支持用户到资源、资源到用户、过程到资源、过程到过程的鉴别。除此以外，它还提供与本地策略的相互协作及对不同资源的动态请求等。

3 Globus Toolkit 3的安全实现

Globus Toolkit 是Globus网格计算项目在多种平台上运行的网格计算工具包软件。Globus项目提出通过建立网络安全基础设施（Grid Security Infrastructure，GSI）来保障网格计算环境的安全。GSI的主要目标包括：① 支持网格计算环境中的安全通信；② 支持跨虚拟组织的安全；③ 支持网格计算环境中用户的单点登录，包括跨多个资源和地点信任委托和信任转移等。GSI已经在Globus Toolkit 2中得到了实现，Globus Toolkit 3（GT3）继续沿用了GSI的概念，并对其加以了改进[4]。

3.1 GT3安全机制

（1）用户和服务证书。GSI的安全机制基于公钥加密，采用X.509认证和SSL通信协议。GT3使用与GT2相同的用户和服务身份证书，支持代理证书、支持授权和单一登录。参与其中的实体通过其持有的证书，以及事前建立的软件与过程，实现身份的标识和确认[5]。

（2）认证中心。GT3网格认证中心（Certification Authority，CA）可以通过Globus小组发布的Simple CA包生成

CA，从而可以在Globus网格中发出证书。

(3)资源授权。GT3的授权基于简单的访问控制列表，这个列表位于明文文件Gridmap中，Gridmap文件与服务和factory相关联，用于限制谁可以访问所提供的功能。在任务提交的过程中，GT3用这个Gridmap文件将用户映射为远程资源上的用户ID，并实现了对factory和服务的访问控制策略。

(4)应用程序接口。仍然是Generic Security Service API，GSSAPI定义提供了通用的安全服务，支持各种安全机制和技术，还支持应用程序在源码级的可移植性。GSSAPI主要面向主体之间的安全鉴别和安全通信操作，提供的功能主要包括：获得证书、执行安全鉴别、签署消息和加密消息。

3.2 GT3安全机制改进

GT3为了支持OGSA，对网格安全机制作了改进[6]。包括：

(1)改进了用户代理证书格式，按GGF讨论的格式：draft-ietf-pkix-proxy-03.txt，同时向后兼容GT2的代理证书，并且用户使用的创建和交互程序没有改变。

(2)增加了Web Service的安全技术，包括Web Services SecureConversation协议、XML-Encryption、XML-signature。在GT3中，相互认证完全通过标准SOAP头在SOAP层上实现，从而允许使用任何底层传输实现SOAP协议。SOAP层的安全基于Web Service安全机制、XML加密及签名标准。

(3)对资源安全模型进行了改善。采取直接接受来自于网络的服务，进程本身不再拥有特殊的本地权限，使用两个特殊的setuid进程完成需要权限的动作，从而加强服务的安全性。

(4)从信任模型中剔除了面向网络的服务。GSI在GT3中的具体实现通过Java GSSAPI来实现，它仍然继续支持相互认证、安全委托、信息保护以及授权。GT3定义的实现上述安全机制的协议都是基于SSL，为了在SSL上实现GSI，允许信任委托和代理签名在SSL握手后执行，对HTTPS协议加以改进，改进后的HTTPG协议可以实现安全委托，并能在SSL密钥协商后实现代理签名。

3.3 GT3任务分配

在GT3中，对任务提交、安全认证和授权作了一些修改，其任务分配流程见图2。

(1)用户代理签署任务描述，交给资源的MMJFS(Master Managed Job Factory Service，主控受管理作业工厂服务)。

(2)MMJFS属于一个几乎没有任何权限的用户，验证请求和证书，确定用户标识和需要提供服务的本地用户。

(3)如果本地用户没有LMJFS(Local Managed Job Factory Service)，MMJFS将向setuid starter申请启动新的LMJFS，setuid starter具有root权限，调度用户的LMJFS。

(4)LMJFS启动后，访问GRIM(Grid Resource Identity Mapper，另一个setuid进程)，访问本地主机的证书并为LMJFS用户产生代理证书。

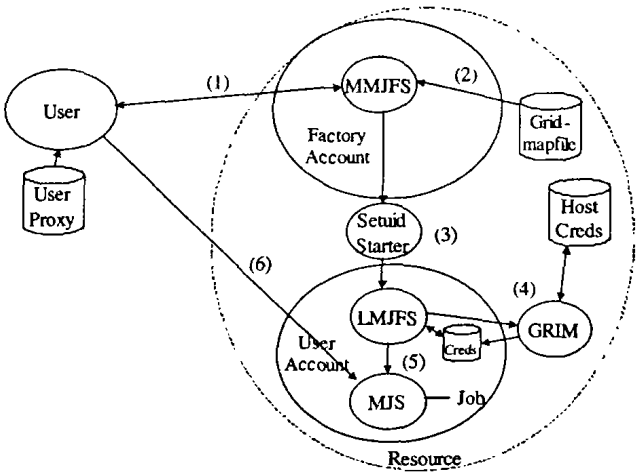

图2 GT3任务分配流程

(5)MMJFS把原始的用户签署的任务描述给LMJFS，LMJFS验证并授权，然后启动一个MJS(Managed Job Sevice)服务，将MJS的应用返回给请求用户。

(6)用户代理和MJS交互鉴别(MJS的证书从GRIM申请获得)。

结语 网格安全问题是网格技术中的一个核心问题，是网格系统成功建造的关键。一个网格计算安全构架必须解决主体相互认证、通信加密、私钥保护以及委托授权与单点登录等关键技术问题。Globus的GSI对网格计算环境中的任务提交与执行的安全性做了大量工作，形成了一些规范。GT3基于OGSA思想，支持网格服务开发，是OGSI(Open Gird Services Infrastructures)标准的第一个参考实现，它包含一组服务和软件库，具有较好的安全机制，成为建造网格环境和网格应用的首选工具。

参考文献

1 都志辉，陈渝，刘鹏. 网格计算[M]. 北京：清华大学出版社，2002，10：67～80

2 应宏，钟静. 网格技术的安全策略[J]. 网络安全技术与应用，2004，7：42～44

3 Foster I，Kesselman C，Tsudik G，Tuecke S. A security architecture for computational grids[EB/OL]. http://www.gridcomputingplanet.com/opinions/article.php/1008821

4 Siebenlish F，et al. OGSA security roadmap global grid forum specification roadmap towards a secure OGSA[EB/OL]. http://www.gridforum.org/meetings/ggf6/ggf6_wg_papers/draft-ggf-ogsa-sec-roadmap-01.doc

5 Thompson M R，et al. CA-based trust model for grid authentication and identity delegation[EB/OL]. http://www.gridforum.org/meetings/ggf6/ggf6_wg_papers/IBM/TrustModel-v6c.pdf

6 Gawor J，Meder S，Siebenlist F，Welch V. GT3 Grid Security Infrastructure Overview[EB/OL]. http://www.globus.org/Security/GSI3/