# 一种基于 Globus 的网格安全与管理模型

## A Model of Grid Security and Mangement Based on Globus

詹绍芬 （浙江教育学院 浙江杭州 310006）
杨发荣 （浙江大学计算机科学与技术学院 浙江杭州 310027）

**摘要**：文章首先分析了网格涉及的安全问题，阐述了对其安全机制的考虑和基础技术。经过剖析当今典型系统 Globus 实现的网格安全架构解决方案 GSI（Grid Security Infrastructure），在借鉴其长处的基础上，以资源映射与管理为切入点提出了较为灵活全面的网格安全体系结构模型。然后基于该安全体系结构模型在 Globus 环境下设计和实现了一个安全方案。

**关键词**：网格 网格安全 安全体系结构模型 资源映射与管理

## 1 引言

网格就是将地理分布、系统异构、性能各异的各种资源，通过高速互连网络连接并集成起来，形成的广域范围的无缝集成和协同计算环境[1-3]。这些资源可以是高性能计算机、计算机机群、大型服务器、贵重科研设备、大型通信设备、可视化设备等。网格给最终用户提供的是与具体地理位置、具体计算设施无关的通用的计算能力。它的核心就是突破了过去强加在计算资源上的种种限制，使人们能够以一种全新的、更自由、更方便的方式使用计算资源[4]。但缺乏有效的安全机制将会限制网格技术的进一步发展和网格应用的进一步推广，因此网格的安全问题是网格的基本问题，网格的安全研究成为网格研究中的热点和难点。

## 2 网格安全体系结构模型的提出

### 2.1 网格涉及的安全问题

从本质上说，Internet 的安全保障一般提供下面两方面的安全服务：一方面是访问控制服务，用来保护各种资源不被非法用户使用或者合法用户越权使用；另一方面是通信安全服务，用来提供通信端的双向认证、通信数据的保密性和完整性（防止对通信数据的窃听和篡改）以及通信端的不可否认性服务。但是这两个方面的安全服务只能部分解决网格的安全问题。网格涉及的安全问题可以分为三个管理层次：

（1）远程访问安全管理。主要是保证用户与系统之间的数据安全，包括防止伪装用户、防止伪装服务器、防止对用户数据的窃听和篡改、防止用户否认、防止远程攻击和入侵。

（2）用户权利安全管理。主要是保证合法用户使用授权的资源，包括防止非法用户使用资源、防止合法用户越权使用资源。

（3）作业和任务安全管理。主要是保证作业和任务的安全运行，包括保证进程间的通信安全、防止恶意程序的运行、保证系统的完整性。

对于网格涉及的大部分安全问题，可以采用目前已有的安全技术加以解决。为了防止非法用户使用资源和防止合法用户越权使用资源，需要对用户进行限制性授权，但是在网格这样一个复杂的、动态的、广域的范围内，对用户进行限制性授权无法使用目前已有的安全技术加以解决，这是网格的安全研究领域一个具有挑战性的研究方向。网格的安全集中于解决如何将网格资源安全地分配给网格用户，以及如何保证网格用户安全地使用分配的网格资源。

### 2.2 网格的安全机制的考虑

网格的安全保证是网格正常运行的保证。网格的安全机制必须考虑网格的如下特性：

（1）网格中的用户和资源量非常庞大，可以属于多个不同的组织、用户和资源动态可变。

（2）网格中的同一个用户可以在不同的资源上有不同的用户标识。

（3）网格中的资源可以支持不同的认证和授权机制，可以有不同的访问控制策略。

(4) 网格中的计算可以在执行过程中动态地申请和启动进程,可以动态地申请和释放资源。

(5) 网格中的进程数量非常庞大,而且进程动态可变。一个计算过程可以由大量进程组成,这些进程之间可能存在不同的通信机制,底层的通信连接可在进程的执行过程中动态地创建并执行。

传统的传输层安全机制无法满足网格特有的用户单一登录要求,分布式系统采用的安全机制无法满足与本地的安全方案协同工作要求,特别是在跨多个管理域的资源访问方面。我们无法完全使用现有的安全技术解决网格的安全问题,这就需要研究新的安全技术和新的安全机制。

### 2.3 网格安全的基础技术

网格安全技术是指解决网格安全问题的具体方法,网格安全技术较多,其中 PKI 和 SSL 技术是网格安全关键技术的基础。

PKI(Public Key Infracture,公开密钥基础设施)技术是目前应用最广泛的网格安全认证技术。它是建立在公钥密码学基础上,主要包括加密、数字签名和数字证书等技术。在 PKI 系统中,CA (Certificate Authority)是一个域中的认证中心,是可信认证的第三方机构。用户之间的通信和验证都要依赖 CA 所颁发的证书。其主要组成部分和操作流程如图 1 所示。

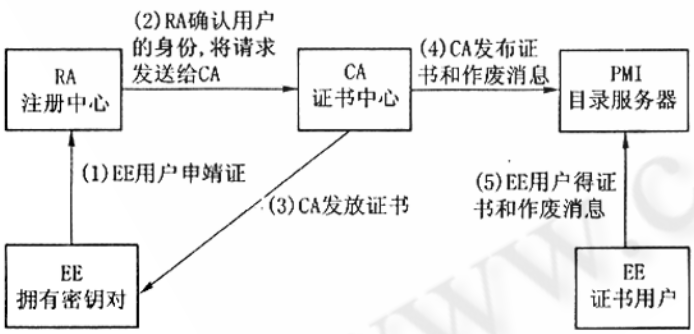


图 1　PKI 的主要组成部分和操作流程

美国密歇根大学开发的 KX.509 试图将 Kerberos 基础设施与 X.509 证书相融合来回避 PKI/ X.509 与 Kerberos 认证机制的不兼容问题,其设计目标就是在 Kerberos 和 PKI 之间建立起一座桥梁。

SSL (Secure Socket Layer) 协议是进行网格安全通信的基本保障。IETF 机构又将 SSL 做了标准化,并将其称为 TLS ( Transport Layer Security)。SSL 建立在 TCP/IP 标准套接字(Socket)之上,采用的是 RSA 算法,是一种安全通信技术。SSL 的主要思想是:发送方先生成一个密钥,然后将该信息传送给接受方,接受方可以用自己的私钥解密来得到密钥。此后双方就可以进行加密的通信。但加密的信息可能被第三方破坏,所以在 SSL 协议中又引入了一种消息认证码(MAC)。MAC 是根据密钥和传输的数据计算出来的。这样通信双方在收到带有 MAC 的加密信息后都可以计算出其摘要并和 MAC 相比较,如果一致则证明消息是没有被篡改的。攻击者很难猜测出正确的 MAC 值。

### 2.4 网格安全架构的 GSI 解决方案及其不足之处

Globus[5-6] 中的网格安全架构 GSI(Grid Security Infrastructure)[7-8] 是一个解决网格的安全问题的一个集成方案,它结合目前成熟的分布式安全技术,并对这些技术进行一定的扩展,以适合网格的特点。GSI 的特点在于保证网格的安全性的同时,尽量方便用户和各种服务的交互,而且 GSI 充分利用现有的网络安全技术,并对某些部分进行扩充,使得在网格下 GSI 具有一个一致的安全性界面,极大地方便了网格的开发和使用。

GSI 中的主要安全技术手段包括:认证证书、双向认证、保密通信、安全私钥、授权委托和用户单一登录。GSI 认证证书采用了 X.509 的证书格式,可被其它基于公钥的软件共享;GSI 采用 SSL 作为它的双向认证协议,实体之间通过认证证书证明彼此的身份;GSI 采用公钥技术与对称加密技术结合的加密方式,在保证通信安全性的同时尽量减少加解密的开销;GSI 将用户的私钥以文件的形式加密存储在用户计算机上,以此来保护用户的认证证书;GSI 对标准的 SSL 协议进行了扩展,使得 GSI 具有授权委托能力,减少用户必须输入口令来得到私钥的次数;GSI 使用用户代理解决用户单一登录问题。

但是 GSI 也存在一些不足之处如实体之间的认证频繁且复杂、执行开销较大,适应性和扩展性比较局限,尤其对系统改变较频繁和规模不断增大的环境。尽管如此,GSI 提出的思想和解决问题的方法,对我们进行网格安全研究具有很好的参考价值。

### 2.5 网格的安全体系结构模型

我们从网格安全设计和实现的角度,对网格提出一个安全体系结构模型。我们考虑以下几点,这几点应该成为安全体系结构模型具有的特点和优点。

(1) 硬件的物理安全和具体的安全技术应该划分

在不同的层次。

(2) 所有的安全技术应该划分在同一个层次。

(3) 不同的安全技术采用不同的协议和实现方法,不同的安全技术彼此不兼容,解决办法是对这些安全技术进行概括和抽象,这种概括和抽象能够"包容"不同的安全技术。

(4) 应该定义一些网格安全协议,这些协议不同于已有的安全协议。

(5) 网格应该架构在网格安全协议的基础上。

我们提出的安全体系结构模型如图 2 所示,安全体系结构模型的层次从下到上依次为:

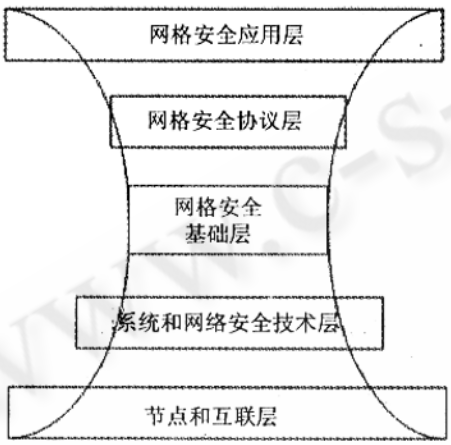


图 2　网格的安全体系结构模型

(1) 节点和互联层(Node and Interconnection Layer)。包括各种各样的硬件,这一层的安全主要是硬件的物理安全。

(2) 系统和网络安全技术层(System and Network Security Technology Layer)。包括各种各样的系统安全技术和网络安全技术,涵盖防火墙、虚拟专用网、SSL、SSH、加密解密、数字签名、入侵检测系统、完整性检查、Kerberos 等。

(3) 网格安全基础层(Grid Security Basic Layer)。提供支撑网格安全协议的基础技术,这些基础技术包括证书的获得和管理以及用户和资源的映射。

(4) 网格安全协议层(Grid Security Protocol Layer)。提供一系列的网格安全协议,这些协议描述网格如何将网格资源安全地分配给网格用户以及如何保证网格用户安全地使用分配的网格资源。

(5) 网格安全应用层(Grid Security Application Layer)。基于网格安全协议的各种各样的网格。

安全体系结构模型具有良好的扩展性、能够适应动态的环境、是研究很多网格问题的良好框架。

## 3　网格安全体系结构模型的描述

网格安全协议层和网格安全基础层是安全体系结构模型中最核心的两个层次,这两个层次是解决网络安全问题的关键。我们考察网格用户使用网格资源进行网格计算时,用户、资源、进程等实体之间如何进行交互,并针对各种交互情况定义相应的安全策略。我们考察的重点放在网格用户申请分配网格资源和使用分配的网格资源时,网格用户和网格进行的复杂交互,这些复杂交互涉及一系列实体间的身份确认。

### 3.1　安全体系结构模型涉及的概念

安全体系结构模型涉及以下几个概念:

证书(Certificate):网格中用来证明实体身份的一段信息或一个文件,证书由可供信任的机构(认证中心)进行签发,有固定的格式,并且有一定的有效时间。双向认证(Mutual Authentication):网格中的两个实体进行交互之前,用来证明彼此身份的真实性的一个过程。

用户代理(User Proxy):用户代理是一个由用户创建的进程,用户将他的部分或全部权限授予该进程,该进程代替用户完成双向认证、申请资源、提交作业、得到结果等工作。

资源代理(Resource Proxy):资源代理是一个由网格创建的进程,网格将一组资源的管理权限授予该进程,该进程负责这组资源的双向认证,以及分配和回收等工作。

中介(Broker):中介是一个由网格创建的进程,中介向用户代理和资源代理提供中介服务,用户代理使用中介提供的中介服务可以协同分配到多个资源代理管理的大量资源。

### 3.2　安全体系结构模型定义的协议

考虑网格计算的执行过程,尤其是资源的分配过程和资源的使用过程,我们就用户如何产生用户代理、系统如何产生资源代理、用户代理如何向资源代理申请分配资源、进程如何(通过用户代理)向资源代理申请分配资源、进程如何向用户代理申请签名进程证书、系统如何产生中介、中介服务如何向用户代理协同分配资源代理管理的大量资源这七个方面定义七个协议:用户代理产生协议、资源代理产生协议、用户代理

申请分配资源协议、进程申请分配资源协议、进程申请签名证书协议、中介产生协议、中介服务协议。

### 3.3 证书的组成、获得和管理

#### 3.3.1 证书的组成

证书是网格中的实体用来证明自己身份的一段信息或一个文件。证书由可供信任的机构(认证中心)进行签发,有固定的格式,并且有一定的有效时间。为了防止伪造证书,证书至少包含以下几部分信息:

(1) 认证中心的名称:签发这个证书的认证中心的名称。

(2) 证书的有效时间:这个证书有效的开始时间和结束时间。

(3) 证书拥有者的名称:拥有这个证书的用户或资源的名称。

(4) 证书拥有者的公钥信息:拥有这个证书的用户或资源的公钥信息,进行双向认证时用来证明证书拥有者的合法性。

(5) 认证中心的数字签名:签发这个证书的认证中心的数字签名,进行双向认证时用来证明证书本身的合法性。

#### 3.3.2 用户或资源获得证书

(1) 用户或资源管理者使用命令行命令或相应的函数创建用于身份鉴别的公钥、私钥和未签名的证书,然后通过电子邮件或其它安全途径把未签名的证书提交给认证中心。

(2) 认证中心收到未签名的证书后,对用户或资源进行考察。

(3) 用户或资源考察合格后,认证中心用自己的证书(认证中心的证书)对未签名的证书进行签名,然后把签名的证书通过电子邮件或其它安全途径返还给用户或资源管理者。

#### 3.3.3 证书的管理

证书的管理最主要的是证书的存储和证书的使用,其它对证书的管理包括:建立可供信任的认证中心、使用函数或软件生成公钥和私钥、使用函数或软件生成未签名的证书、使用函数或软件对证书进行签名、对用户代理和进程创建临时证书、撤销虽然未到期但是不再使用的证书或临时证书、将证书或临时证书的使用绑定在固定的节点上。

### 3.4 用户和资源的映射

因为用户和资源在网格的高层(网格用户和网格资源)和网格的低层(本地用户和本地资源)的身份描述是不一样的,所以首先要在这两种身份之间建立某种映射关系,才能进行各种本地安全管理和具体的本地计算。

用户和资源的映射策略和具体的用户管理策略密切相关,不同的用户管理策略将会有不同的用户和资源映射策略。一种简单的用户和资源的映射策略是建立用户和资源映射表,通过查找映射表进行用户和资源的映射。下面先解释客体、主体和信任域的概念,然后列出我们总结的四条映射关系。客体(Object)指网格中受到安全规则保护的资源;主体(Subject)指网格中可能对客体造成破坏的用户或进程;信任域(Trust Domain)指网格中一个逻辑的、可管理的区域,具有明确的边界。存在的映射关系如下:

关系 1:对每一个信任域而言,存在全局客体到局部客体的映射表;

关系 2:对每一个信任域而言,存在全局主体到局部主体的映射表和局部主体到全局主体的映射表;

关系 3:如果将全局安全规则作用于一个全局主体和一个全局客体,这个全局主体通过了全局安全规则,也就是说这个全局主体可以操作这个全局客体,那么将这个全局主体映射到某个局部信任域内的某个局部主体后,这个全局客体也相应地映射到这个局部信任域内的某个局部客体,若这个局部主体通过了这个局部信任域内的局部安全规则,则该局部主体可以操作这个局部客;

关系 4:如果一个操作跨越多个局部信任域,即这个操作涉及多个局部信任域内的局部主体和局部客体,只有当该操作涉及的每个局部主体都通过相应的局部安全规则,也就是该操作涉及的每个局部主体都可以操作相应的局部客体后,该操作才能够执行。

## 4 基于安全体系结构模型的安全方案

我们基于安全体系结构模型设计了一个安全方案,这个安全方案由以下几个模块组成:用户接口模块、用户代理模块、资源代理模块、中介模块、用户和资源映射模块。通过以上五个模块,实现了网格安全协议层的协议和网格安全基础层的技术。Globus 软件为开发人员提供了一系列的 API(Application Programming Interfaces)和 SDK(Software Development Kits),开发人员使用 Globus 提供的 API 和 SDK,可以利用

Globus 提供的底层功能并开发自己的功能。以 Globus 3.0 软件为基础，使用 Globus 软件提供的这些 API 和 SDK，开发相应的功能函数以实现设计的安全方案。

在进一步开展用户和资源的映射策略以及基于计算市场的资源分配策略的研究之前，我们在小规模的网格上部署实现的安全方案，定义用户和资源的相对简单直观的动态映射方法以及证书的管理策略。使用 Globus 软件附带的 CPI 程序（计算圆周率）来测试我们的安全方案的性能。CPI 程序在 GSI 方案和我们方案得出的 Total Time 与 Wall Clock Time 非常接近。

## 5 将来的工作

我们进一步的工作主要包括：完善基于安全体系结构模型设计的安全方案，在我们搭建的跨地域的网格上部署该安全方案，以安全体系结构模型为基础，开展用户和资源的映射策略以及基于网格应用的资源分配策略的研究。

## 参考文献

1 郁志辉、陈渝、刘鹏编，网格计算[M]，北京：清华大学出版社，2002，10.

2 Ian Foster and Carl Kesselman. The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann Pulishers, Inc., San Francisco, California, 1999.

3 William Allock, Ann Chervenak, Lan Foster, Carl Kesselman, and Steven Tuecke. The data grid: Towards an architecture for the distributed agement management and analysis of large scientific datasets[J]. Journal of Network and Computer Applications, 2001, 23: 187 – 200.

4 Li Wei, Xu Zhiwei, Bu Guanying. An effective resource locating algorithm in grid environments. Chinese Journal of Computers (in Chinese), 2003, 26 (11): 1546 – 1549.

5 Ian Foster. Globus Toolkit—Ian Foster' speak in China. http://www.chinagrid.net, 2005, 04.

6 刘文杰、何涛、肖浩，基于 Globus 的网格应用关键技术研究，计算机工程与设计，2006，19(10).