网格环境下基于联合代理证书的社区授权服务的UML建模研究

张 梅1，王汝传1，2 ，王海艳1

1.南京邮电大学 计算机科学与技术系，江苏 南京210003；2.南京大学 计算机软件新技术国家重点实验室，江苏 南京210093

2008-06-10

摘 要： 随着网格研究的不断深入，网格安全问题不容忽视。访问控制是安全防范和保护的主要策略，而GSI中的授权机制难以扩展到拥有大量资源和大量用户的大规模网格环境中。社区授权服务(CAS)正是针对这种大规模网格环境中存在的授权机制问题而提出的。通过统一建模语言UML，详细阐述了社区授权服务机制的关键技术，并将联合代理证书机制融合到社区授权服务中，对进一步完善社区授权服务体制具有较大的实用价值。

关键词： 统一建模语言 网格 访问控制 联合代理证书 面向对象

网格社区是参考人类社会中的社区而建立的概念，目的是管理网格中的各种资源，快速实时地把资源请求者和资源提供者联系起来。由于一个社区的管理资源数目有限，只是网格上所有资源的一小部分，因此可以实现粒度更细的资源管理，其上的各种操作也比在网格上进行同样的操作要快。

资源需求相对集中的一个用户群可以构成一个用户集合，这个用户集合需要建立一个资源注册和发现中心，任何一个合法的用户都可以向该中心注册自己拥有的资源或自己发现的、可以被用户集合中的其他用户使用的资源，该集合中的任何一个用户都可以从该中心发现自己需要的资源。通过建立注册和发现中心，可以使这个用户集合中的所有用户与注册在这个注册和发现中心的所有资源构成一个相对独立的实体集合——网格社区。在网格社区中，除了用户和资源外，还包括一些用户和资源都必须服从的策略。

社区授权服务(CAS)就是网格社区中的一种策略，它是一个以社区为单位建立可信任第三方并实现社区内资源访问控制的机制，即在每一个社区内部建立一个CAS服务器来维护社区的策略。在传统的网格授权机制中，网格安全基础设施GSI(Grid Security Infrastructure)要求每一个访问信息资源的全局用户都需要在本地资源服务器上拥有一个自己的账号。这样，在网格这种拥有大量资源和大量用户的环境中，每一个资源服务器都需要维护一个庞大繁琐的全局/本地映射表，这种授权机制越来越显现出难以适应网格环境的一面。CAS正是针对这种大规模网格环境中存在的授权机制问题而提出的。考虑到单点登录问题，可以将联合代理证书加入到社区授权服务机制中，在用户的联合代理证书中加入CAS的授权声明(即策略声明)来实现授权的访问控制。

在研究社区授权服务机制的过程中，对其进行建模是非常重要的一步。统一建模语言UML(Unified Modeling Language)是一种定义良好、易于表达、功能强大且普遍适应的可视化图形建模语言。它融合了Booch、OMT和OOSE三大面向对象方法中的基本概念，而且这些基本概念与其他面向对象方法中的基本概念大致相同，因而，UML成为了这些方法以及其他方法的使用者乐于采用的一种简单、统一的建模语言。UML已被OMG(Object Management Group)接受并推荐使用，成为事实上的业界标准。因此，本文重点讨论使用UML对社区授权服务进行建模的过程。

1 网格环境下的联合代理证书机制

当一个网格计算需要使用几个网格资源(每个都需要双向的认证)或者需要有请求服务Agent来代替一个用户时，创建一个代理可以避免重复敲入用户密码。在网格环境下，GSI以X.509证书实现认证，并通过对X.509证书进行扩展，产生代理证书。用户如果没有创建这个代理证书，则不能提交作业，也不能传输数据。这个代理证书一经创建，就可以用于授权或者拒绝对整个网格内所有资源的访问。

代理证书包含一个不同于用户密钥对的公钥和私钥对，在认证会话中使用的就是这个密钥对。代理证书生命周期很短，一旦过期密钥就失效。这样，即使私钥被暴露，其危害也很有限。这也使得在存储代理证书的私钥时不必用口令进行加密保护。因此，对代理证书来说就没有口令了。这样，用户输入一次口令，用自己的数字证书产生代理证书后，就可在代理证书的有效期内，使用自己的代理证书进行认证，在特定的逻辑安全区域中可多次访问不同的数据资源，而不需要再次输入口令。

GSI使用grid-proxy-init产生一个本地代理证书，用户输入口令来解密私钥，私钥被用于签发代理证书。代理证书签发之后，在代理证书的有效期内，用户的私钥将不再使用。Proxy被存储在/tmp下，对用户为只读信息。图1是用户代理证书的产生过程。

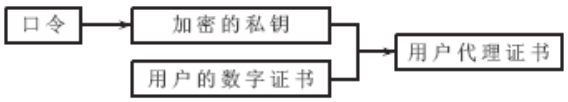

图 1 用户代理证书的产生过程

在认证时，产生用户的代理证书命令，具体如下：

```
%grid-proxy-init
Enter PEM pass phrase: ******
```

该命令将产生一个本地短期有效的临时性用户代理证书，grid-proxy-init的命令选项如下：

-hours<lifetime of credential>

热点专题

- 2008嵌入式技术创新及应用高峰论坛
- 2008飞思卡尔技术论坛
- Altera公司SOPCWorld 2008专题报道
- 第十届高交会电子展
- 科技闪耀北京奥运
- ADLINK DAY—2008年量测与自动化技术国际高峰研讨会
- 中国电子学会Xilinx杯开放源码硬件创新大赛
- 赛灵思公司Virtex-5系列FPGA
- 3G知识
- IPTV
- 触摸屏技术
- RoHS

杂志精华

- 基于CC2430的无线传感器...
- 无线传感器网络应用系统综述
- 无线传感器网络在野外测量中的...
- 基于竞争的无线传感器网络
- 用于矿井环境监测的无线传感器...
- 具有自适应通信能力的无线传感...
- 基于传感器网络技术的深孔测径...
- 基于无线传感器网络的家庭安防...
- 基于ATmega128L与C...
- 无线传感器网络中移动节点设备...

-bits<length of key>

-help

在网格中使用用户代理证书的最大优点是用户仅需要在会话开始时使用grid-proxy-init，之后就不必再输入自己的密码，即支持单点登录，但这个代理证书只局限在特定的逻辑安全区域(即社区)中。而一个网格计算可能涉及到几个社区，为了实现在多个社区中的单点登录，用户可以登录到多个社区中(实施步骤如前)创建一个联合代理证书。这样，用户可以用该联合代理证书访问这些社区中的任何资源。

2 基于联合代理证书的社区授权服务的UML建模

UML适用于系统开发过程中从需求规格描述到系统完成后测试的不同阶段。在需求分析阶段，可以通过用例捕获用户需求。通过用例建模，可以描述系统感兴趣的外部角色及其对系统的功能要求。分析阶段主要关心问题域中的主要概念(如抽象、类和对象等)和机制，需要识别这些类以及它们相互间的关系，并用UML类图描述。为实现用例,类之间需要协作，这可以用UML动态模型描述。

2.1 总体需求建模

通常利用情节或经历描述用户和软件系统的交互方式，从而获取需求。Ivar Jacobson(1992)把这种看法系统地阐述为通过用例的方法进行需求获取和建模。用例图把系统分成角色和用例。用例被定义成系统执行的一系列动作，动作执行的结果能被指定角色察觉到。

角色是指用户在系统中所扮演的角色，单个角色可与多个用例联系；反之，一个用例可与多个角色联系。图2是社区授权服务的UML顶层Use Case图。

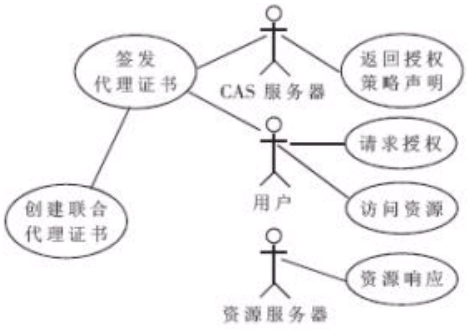

图 2 社区授权服务的 UML 用例图

关于图2的具体描述如下：

在社区授权服务系统中，CAS用户首先得到一个标准的网格联合代理证书；然后向CAS服务器请求信任及授权，CAS服务器根据CAS数据库中所授予这个用户的权限策略，用CAS的私钥签署一个授权策略声明返回给CAS用户；最后用户将这个声明和代理证书提交给要使用的gridftp资源。Gridftp服务器通过验证用户的策略声明决定是否提供服务即响应用户。

2.2 系统分析建模

在对总体需求分析的基础上，对社区授权服务进行详细设计。类图处于分析建模的核心位置，它模拟的是保证系统正常工作的所有必要资源，其他所有的图如果想获取这些资源的信息，最终都必须访问类图，它是一种静态结构图，描述的是系统的静态结构。它的主要功能有：

(1)定义一个系统的必要资源。(2)定义资源之间的关系。(3)生成代码。(4)用代码生成模型。(5)为其他的图提供基础。

社区授权服务系统中的主要类有：“CAS用户”类、“联合代理证书”类、“CAS服务器”类、“授权请求”类、“授权策略声明”类、“gridftp服务器”类、“资源访问”类，类之间的关系如图3。

系统的动态行为细节使用序列图描述。序列图表示随时间安排的一系列消息，用来描述对象之间动态交互关系，着重体现对象间消息传送的时间顺序。根据系统的总体需求设计并利用UML类图进行本系统行为的全局描述，如图4所示。(1)用户先产生一个密钥对(公钥/私钥对)，通过用户所输入的口令对私钥进行加密，而公钥则被加入到证书请求中。(2)产生证书请求后，用户将这个证书请求发送到CA。(3)CA对证书请求进行签发，并发送给用户。(4)由grid-proxy-init命令产生一个本地代理证书。(5)用户创建联合代理证书。(6)CAS用户使用网格联合代理证书向CAS服务器请求信任及授权。(7)CAS服务器验证代理证书，若证书无效，则授权终止。(8)CAS服务器访问自己维护的策略数据库，根据数据库中所授予这个用户的权限策略，用CAS的私钥签署一个授权策略声明返回给CAS用户。(9)用户将代理证书和从CAS服务器获得的授权策略声明一起发送给要使用的gridftp资源服务器。(10)资源服务器基于本地策略授权用户访问资源。

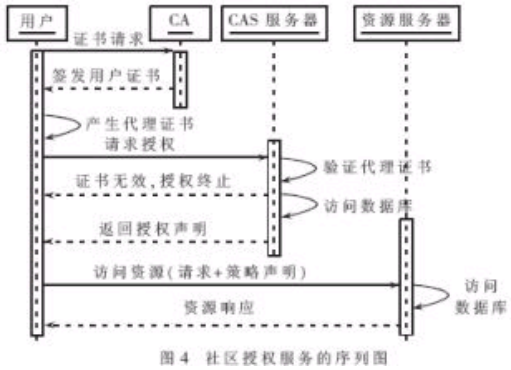

图 4　社区授权服务的序列图

用UML进行社区授权服务设计有许多优点：

(1)UML融合当前一些流行的面向对象开发方法的主要概念和技术，成为一种面向对象的标准建模语言，采用图形描述系统的视图易于理解，起到了桥梁的作用。

(2)UML支持独立于编程语言和开发过程的规范，支持大多数OO语言里定义的面向对象的设计结构，这种一致性保证了能够从模型生成代码或从代码产生模型，即实现建模环境和编码环境的集成。

(3)UML有很好的扩展性，提供了标签、约束、版类等约束机制来进行自我扩展，为以后社区授权服务系统的更深入研究或升级带来了方便。

本文从GSI授权的不足出发，分析了在虚拟组织中建立社区授权服务CAS系统的必要性。考虑到单点登录问题，将联合代理证书加入到社区授权服务机制中，在用户的联合代理证书中加入了CAS的授权声明来实现授权的访问控制，并进一步将基于联合代理证书的社区授权服务机制与统一建模语言UML相结合，给出了CAS系统的总体分析图即用例图、静态类图及描述系统动态行为的序列图。阐述了用UML进行CAS系统设计的优点，为进一步完善社区授权服务体制打下了基础，同时对探讨网格虚拟组织中的访问控制也具有很好的参考价值。

参考文献

1 徐志伟，冯百明，李 伟.网格计算技术.北京：电子工业出版社，2004

2 Pender T.UML Bible.北京：电子工业出版社，2004

3 Pearlman L，Welch V，Foster I et al.A Community autho-rization service for group collaboration.In：Proceedings of the Third International Workshop on Policies for Distributed Sys-tems and Networks 2002 IEEE,2002

4 Selic B.A generic framework for modeling resources with UML[J].Computer:Innovative for Computer Pro-fessionals，Membership Magazine of the IEEE Computer Society，2000；33(6)：64~69

地址：北京海淀区清华东路25号电子六所大厦
联系电话：82306084 / 82306085 传真：62311179 京ICP备05053646号