网格安全模型中认证策略的研究

赵会洋[1],王 爽[1],魏士伟[2]
(1.许昌学院 计算机科学与技术学院,河南 许昌 461000;
2.桂林电子科技大学 信息科技学院,广西 桂林 541004)

摘 要:对网格安全模型中常用的认证策略Kerberos认证和X.509认证的原理进行了详细分析。针对网格环境下用户和资源数量巨大所带来的管理困难、系统单点失效以及可扩展性差等问题,提出了一种基于自治系统的多级网格安全管理模型(MGSM-AS),最后给出了该模型中认证策略的实现方案,包括证书的申请及审核和代理证书机制。通过对网格用户进行区域划分,使得这些用户不需要与虚拟组织管理者直接进行交互,而是接收自治系统的组织和管理,这样简化了认证过程。

关键词:网格计算;网格安全;自治系统;认证
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2010)04-0171-04

Research on Authentication Policy of Grid Security Model

ZHAO Hui-yang[1], WANG Shuang[1], WEI Shi-wei[2]
(1.College of Computer Science and Technology, Xuchang University, Xuchang 461000, China;
2.College of Information and Technology, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: Gives us a detailed analysis of the normal authentication policy of grid security model, such as Kerberos and X.509. To solve the problem of difficult managements because of tremendous grid users, system's single-point of failure and poor scalability, this paper proposes a kind of multilevel grid security model based on autonomous system(MGSM-AS) and finally presents a paradigm of this model's authentication policy which includes the request and verification of the certificate and proxy certificate application. By zoning grid users do not need to interact with the virtual organization managers directly, but rather to receive the organization and management from autonomous system. This policy simplifies the certification process.

Key words: grid compution; grid security; autonomous system; authentication

0 引 言

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动态虚拟组织VO(Virtual Organization)[1]。与传统网络环境相比,网格计算环境极其复杂,它具有大规模、高速、分布、异构、动态、可扩展等特性。这就对网格安全控制提出了一个极高的要求。网格必须提供基本的安全服务,包括:认证、授权、访问控制、审核、保密以及抗否认性[2]等。文中在分析现有认证技术的基础上,提出了一种基于自治系统的多级网格安全模型(MGSM-AS),并分析了该模型中的认证机制。

收稿日期:2009-08-13;**修回日期**:2009-11-23
基金项目:河南省科技攻关项目(0524220054);河南省自然科学研究计划项目(2008A520023)
作者简介:赵会洋(1981-),男,河南登封人,硕士研究生,讲师,研究方向为网格计算、IPv6。

1 网格安全模型中常用的认证策略

1.1 Kerberos认证机制

Kerberos[3]协议是由麻省理工学院的Athena项目课题组开发的,是一个三方认证协议,根据称为密钥分配中心(KDC)的第三方服务中心来验证网络中计算机相互的身份,并建立密钥以保证计算机间安全连接。KDC有两个部分组成:认证服务器和票据授权服务器。

Kerberos允许一台计算机通过交换加密消息在整个非安全网络上与另一台计算机互相证明身份。一旦身份得到验证,Kerberos协议将会给这两台计算机提

供密钥,以进行安全通讯对话。Kerberos 协议可以认证试图登录上网用户的身份,并通过使用密钥密码为用户间的通信加密。总的来说,Kerberos 是一种基于私钥加密算法的,需要可信任的第三方作为认证服务器的网络认证系统。它允许在网络上通讯的实体互相证明彼此的身份,并且能够阻止旁听和重放等手段的攻击。不仅如此,它还能够提供对通讯数据保密性和完整性的保护。

图 1 给出了使用 Kerberos 认证协议的客户端、KDC 和应用服务器之间的关系。

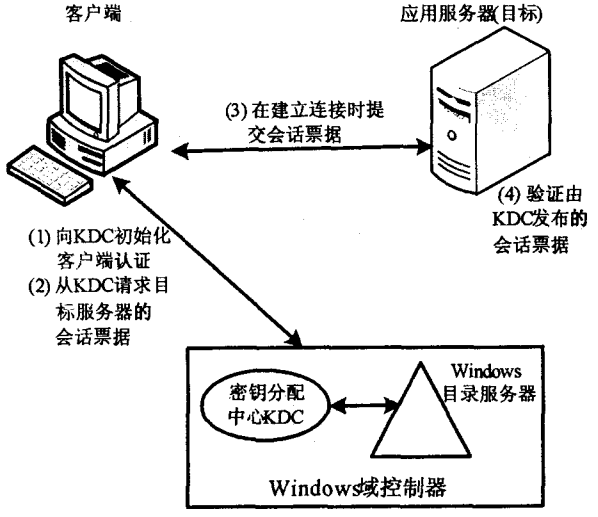

图 1 Kerberos 认证协议流程图

1.2 X.509 证书认证机制

X.509 证书认证机制是由 ITU－T 提出,作为目录服务 X.500 推荐书的一部分[4]。X.509 是一种基于公开密钥加密和数字签名的鉴别机制,这个标准一般推荐使用 RSA 加密算法,而数字签名则使用散列函数的形式。数字证书作为一种经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件,包含了一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间、发证机关(证书授权中心)的名称、该证书的序列号等信息。

安全身份的相互认证过程如下[5]:

(1) 为了进行相互认证,甲乙先建立一个连接;

(2) 甲向乙发送自己的证书,证书中的内容包括甲是谁、甲的公钥和签署甲证书的认证中心信息;

(3) 乙收到证书后通过自己的数据库检查证书中认证中心的数字签名来确认证书是否合法;

(4) 证书合法之后,乙要求证明甲是这个证书的主体,于是发条信息要求甲进行信息加密;

(5) 甲用自己的私钥对乙发过来的信息进行加密并发给乙;

(6) 乙用甲证书中的公钥对加密信息进行解密,如果解密结果和初始结果一致,表示通过了对甲的信任,即乙信任甲;

(7) 同样,如果要甲信任乙,则需要将上述过程反过来进行一次即可。

2 MGSM－AS 的认证机制

针对网格环境下用户和资源数量巨大所带来的管理困难、系统单点失效及可扩展性差等问题,提出了一种基于自治系统的多级网格安全模型(MGSM－AS)。该模型旨在通过分级自治的方法,增加网格安全管理的灵活性,降低难度,增加可靠性和可扩展性,形式上类似国家的多级行政管理体制。MGSM－AS 的认证过程如图 2 所示。

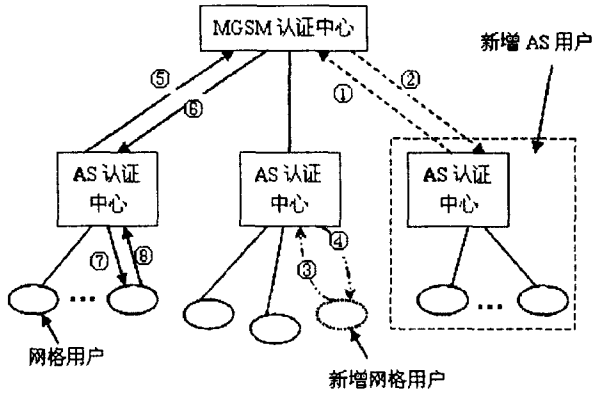

图 2 MGSM－AS 认证机制的结构流程图

2.1 证书的申请及审核服务

自治系统用户证书和网格用户证书的申请及审核过程基本上是一样的,不同之处是自治系统用户证书的申请及审核是在 MGSM 认证中心上运行,而网格用户证书的申请及审核在 AS 认证中心上进行。

下面以自治系统用户为例介绍证书的申请及审核服务[6]。

(1) 新用户的注册与证书申请。

一个自治系统用户要使用认证服务时,首先要在 MGSM 认证中心注册。完成注册后,MGSM 认证中心检查自治系统用户提交的信息是否合法,如果信息属实,则会返回给自治系统用户一些信息,如自治系统的用户名、口令等,自治系统用户以后就可以据此向 MGSM 网格系统证明自己的身份。然后 MGSM 认证中心执行签发证书的一系列检查和操作,直至最后完成证书签发,再将证书、相关私钥以及自治系统用户的其他信息保存在 MGSM 认证中心的数据库里面。自治系统用户通过一定的方式查询到数字证书已经签发后,就可以下载证书。

(2) 证书注销申请。

如果自治系统用户的密钥发生泄漏,或者因自治

系统用户身份变更等原因而需要注销原有证书时,可以向 MGSM 认证中心提出证书注销申请。注销申请包括需要进行注销的证书,证书注销的原因等,如果是在线提交,还需要向 MGSM 认证中心证明提交者身份,MGSM 认证中心确认登记后接受注销申请。MGSM认证中心在接到自治系统用户注销并进行审核通过后,将为自治系统用户注销原有证书使其不再有效,同时将该证书加入到证书注销列表中供其他证书使用者检索。

(3) 密钥及证书更新申请。

依据 X.509 标准,一个数字证书中包含的密钥是有一定的使用期限的,当证书即将到期时,自治系统用户需要向 MGSM 认证中心提出证书/密钥的更新请求。MGSM认证中心会为自治系统用户生产一个新的密钥对,然后为自治系统用户签发新的证书,或者直接延长原证书的使用期限。

(4) 证书审核。

MGSM认证中心在接受到自治系统用户提交的证书审核申请后开始审核,确定能否为该自治系统用户颁发相应的证书。审核范围包括:自治系统用户资料是否真实可信,自治系统用户密钥是否符合系统规定的安全级别,自治系统用户密钥的用途是否正确等。证书的审核结果通过电子邮件或者其他方式通知申请者,如果审核通过,MGSM 认证中心的证书签署模块将为该自治系统用户签署相应的数字证书。

MGSM－AS 两级认证模式将不同的认证对象分类,使认证中心服务器只针对于同一种类型的用户证书进行管理和提供服务,减轻认证中心的负担,更好适应网格环境资源用户数目巨大且动态变化的特点。

2.2　MGSM－AS 的代理证书

代理证书[7]的作用是将一个实体的全部或部分权限授予另一个实体,让另一个实体扮演该实体。代理证书的合法使用范围不超过它的创建者的作用范围。它是一种临时证书,主要用来在网格环境下实现扮演(impersonation)和委托(delegation)[8]等功能,以轻负载方式为动态实体生成身份证明的鉴别解决方案,以此来实现动态授权、单点登录。重复利用已有协议和工具或仅对现有的 X.509 证书进行微小的修改,就得到了 X.509 代理证书。

自治系统用户和网格用户都可以创建自己的代理证书,虽然它们的作用范围不同,但它们的创建流程是一样的。

假如一个网格用户要生成一个代理证书,其基本流程描述如下:

1) 网格用户向代理证书生成程序发出请求;

2) 代理证书生成程序要求该网格用户提交自己的 X.509 证书和所有需要继承的属性信息;

3) 代理证书生成程序随机产生一个公钥/私钥对;

4) 网格用户提交自己的私钥信息,由代理证书生成程序按照证书规范使用该私钥签发代理证书。

在一自治系统内,网格用户 A 的代理证书的授权过程如图 3 所示。

(1) 处在左边的 A 主机上的网格用户与处在右边的 B 主机上的授权服务程序建立安全的连接。网格用户使用自身已经存在的代理证书,授权服务程序使用自身的公钥证书进行相互认证,认证成功后建立起了完整、安全的信道。

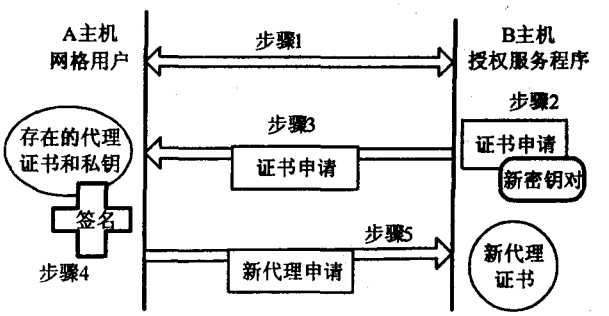

图 3　代理证书的授权过程

(2) 在网格用户 A 向授权服务程序提出授权委托的申请之后,授权服务程序产生一对新密钥对(公钥和私钥)。

(3) 一个代理证书签名的申请通过安全的信道发回给网格用户 A,其中包含新产生的公钥。

(4) 网格用户 A 使用与自己的代理证书相应的私钥对证书申请进行签名,从而生成一个新的代理证书,这个新的代理证书包含来自授权服务程序的新公共密钥。A 填充这个新的代理证书的相应属性字段(PCI 等)实现相应的授权。

(5) 新的代理证书通过安全的信道发还给授权服务程序,授权服务程序将它以及新产生的私钥存放到一个文件中保存起来,应用程序就可以使用此证书用来代理用户完成任务。

2.3　MGSM－AS 的认证过程

MGSM－AS 的认证是基于自治系统的认证,根据认证双方实体对象的不同,可以把 MGSM－AS 基于自治系统的认证分为六种类型:

类型 1:同一自治系统内网格用户之间的认证;

类型 2:网格用户与本地自治系统服务器之间的认证;

类型 3:不同自治系统内网格用户之间的认证;

类型 4:网格用户与远程自治系统服务器之间的

认证；

类型 5：自治系统用户之间的认证；

类型 6：自治系统用户与 MGSM 服务器之间的认证。

实体双方相互协作时，都需要相互认证，以便确认对方的身份和所拥有的权限。当某个实体对另一个实体的代理证书进行验证时，首先向证书签发者请求验证，若验证通过则认为证书可信，否则证书不可信。若签发者出现错误，不能正常工作，则根据证书内的 ICP 找到它的高级签发者并向其请求验证，若验证通过则认为证书可信，否则证书不可信。例如，持证人甲与持证人乙通信时，他首先查找数据库并得到一个从甲到乙的证书路径(Certification Path)和乙的公开密钥，这时甲可使用单向或双向认证验证证书。

以单向验证为例，单向验证是从甲到乙的单向通信。它建立了甲和乙双方身份的证明以及从甲到乙的任何通信信息的完整性，可以防止通信过程中的任何攻击。

具体如下：

(1) 甲产生一个随机数 Ra；

(2) 甲构造一条消息，M = (Ta, Ra, Ib, d)，其中 Ta 是甲的时间标记，Ib 是乙的身份证明，d 为任意的一条数据信息。为安全起见，数据可用乙的公开密钥 Eb 加密；

(3) 甲将(Ca, Da(M))发送给乙(Ca 为甲的证书，Da 为甲的私人密钥)；

(4) 乙确认 Ca 并得到 Ea。他确认这些密钥没有过期(Ea 为甲的公开密钥)。此时若甲代理证书的发放人 Ca 不可达，此时乙需要向甲的祖父级签发人 super issuer 验证来得到 Ea；

(5) 乙用 Ea 去解密 Da(M)，这样既证明了甲的签名又证明了所签发信息的完整性；

(6) 为准确起见，乙检查 M 中的 Ib；

(7) 乙检查 M 中的 Ta 以证实消息是刚发来的；

(8) 作为一个可选项，乙对照旧随机数数据库检查 M 中的 Ra 以确保消息不是旧消息重放。

双向验证包括一个单向验证和一个从乙到甲的类似的单向验证。除了完成单向验证的(1)到(8)步外，双向验证还包括；

(9) 乙产生另一个随机数，Rb；

(10) 乙构造一条消息，Mm = (Tb, Rb, Ia, Ra, d)，其中 Tb 是乙的时间标记，Ia 是甲的身份，d 为任意的数据。为确保安全，可用甲的公开密钥对数据加密。Ra 是甲在第(1)步中产生的随机数；

(11) 乙将 Db(Mm)发送给甲；

(12) 甲用 Ea 解密 Db(Mm)，以确认乙的签名和消息的完整性；

(13) 为准确起见，甲检查 Mm 中 Ia；

(14) 甲检查 Mm 中的 Tb，并证实消息是刚发送来的；

(15) 作为可选项，甲可检查 Mm 中的 Rb 以确保消息不是重放的旧消息。

双向验证与单向验证类似，但它增加了来自乙的应答。它保证是乙而不是冒名者发送来的应答，同时还保证双方通信的机密性并可防止攻击。

3 结束语

在分析现有网格安全模型中常用的认证策略的基础上，提出了在一种基于自治系统的多级网格安全模型 MGSM－AS 中认证策略的实现方案。该认证模型通过对网格用户进行区域划分，使得这些用户不需要与虚拟组织管理者直接进行交互，而是接收自治系统的组织和管理，简化了认证过程，解决了由于网格用户数量巨大而管理困难，服务访问控制复杂以及系统单点失效等问题。

下一步要在此基础上进一步研究网格系统的授权、访问控制等问题的解决策略。

参考文献：

[1] Foster I. The anatomy of the grid: enabling scalable virtual organizations[J]. International Journal of Supercomputer Applications, 2001, 15(3): 6－7.

[2] Foster I, Kesselman C. Globus: A Metacomputing Infrastructure Toolkit[J]. International Journal of Supercomputer Application, 1997, 11(2): 115－128.

[3] 李继勇. 基于 Weil 对改进的 Kerberos 协议设计[J]. 计算机应用, 2008(2): 422－423.

[4] Adams C, Lloyd S. 公开密钥基础设施－概念、标准和实施[M]. 冯登国等译. 北京：人民邮电出版社, 2001.

[5] 李 密. 基于 Globus 下的网格技术和安全分析[D]. 北京：北京邮电大学, 2004.

[6] 戴节勇, 顾 健, 陈克非. PKI 技术在网格安全中的应用[J]. 计算机工程, 2005(5): 159－161.

[7] 戴 怡, 杨 庚. 网格环境下多域间的认证机制研究[J]. 计算机工程与应用, 2007(5): 130－132.

[8] Welch V, Foster I, Kesselman C, et al. X. 509 Proxy Certificates for Dynamic Delegation[EB/OL]. 2009. https://www－unix. globus. org/alliance/publications/papers/pki04－welch－proxy－cert－final. pdf.