

网格中的认证授权技术

郑芸芸¹, 常致全¹, 王冬磊^{1,2}, 蒋 勇¹

(1. 四川大学 计算机学院, 四川 成都 610065;
2. 中国工程物理研究院 化工材料研究所, 四川 绵阳 621900)

摘 要: 由于网格技术广泛的应用前景, 网络安全正受到越来越多的关注。GSI 是目前最为成熟的网格项目 Globus 中的安全设施。文中就 GSI 中涉及到认证与授权机制的方面: 公钥基础设施, SSL 与相互认证进行了研究, 分安全委托与单点登录、在线证书仓库、团体授权服务三个方面重点介绍了认证与授权技术在 GSI 中的应用与扩展及其特点, 并通过其大致应用流程和安全性分析讨论了其优点和尚存在的问题。

关键词: 网格; 网络安全基础设施; 认证; 授权

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2006)10-0139-04

Authentication and Authorization in Grid

ZHENG Yun-yun¹, CHANG Zhi-quan¹, WANG Dong-lei^{1,2}, JIANG Yong¹

(1. Department of Computer Science, Sichuan University, Chengdu 610065, China;
2. Institute of Chemical Materials, Chinese Academy of Eng. Physics, Mianyang 621900, China)

Abstract: Due to a promising prospect of grid technology, grid security draws more and more attention. GSI is the security infrastructure of the Globus project, which is the most famous project in grid area. This paper studies the authentication and authorization aspects in GSI, with emphasis on the expansions and features of the application of authentication and authorization techniques in GSI. At last, it discusses the open questions of authentication and authorization in GSI after giving the illustration of the actual flow.

Key words: grid; GSI; authentication; authorization

0 引 言

网格(Grid)技术是近年来国际上兴起的一种重要信息技术。它的目标是将地理上广泛分布、系统异构的各种计算资源全面整合在一起, 实现网络虚拟环境上的高性能资源共享和协同工作。

1 网格概念及其安全问题和安全需要

(1) 网格是一个异构的环境; (2) 用户数量很大且是动态可变的; (3) 资源数量巨大, 并且是动态变化的; (4) 网格计算环境中的计算过程可在其执行的过程中动态地请求、启动进程和申请、释放资源; (5) 不同的资源可能支持不同的认证和授权机制。

授权是由其中一方决定另一方可以拥有的权限, 而认证指的是一方验证另一方的身份是否合法或是否得到合法的授权, 若认证通过, 则允许其使用授权方指定的权限, 否则拒绝其申请。由于网格环境的许多特殊性, 这就给授权与认证提出了新的挑战。

2 基础安全技术

2.1 公钥基础设施

GSI(Grid Security Infrastructure)中实体的身份认证以 PKI(Public Key Infrastructure)体系为基础, 用户和资源通过数字证书认证对方身份, 与数字证书绑定的私钥可以仅用于某种用途, 如仅用于签名或加密。资源管理者能够认证属于不同 VO^[1]的用户所持有的证书, 用户不必再为得到其他 VO 实体的认证而管理一堆不同的证书。

下面给出一个签署过的安全证书的例子:

Certificate :

Data :

Version : 3 (0x2)

Serial Number : 28 (0x1c)

Signature Algorithm: md5WithRSAEncryption

// 认证机构名字

Issuer : C = CN , O = Globus , CN = Globus Certification

Authority

// 证书有效使用时间

Validity

Not Before : Apr 22 19 : 21 : 50 1998 GMT

Not After : Apr 22 19 : 21 : 50 2003 GMT

// 主体名称

收稿日期: 2006-01-19

作者简介: 郑芸芸(1978-), 女, 四川南充人, 硕士研究生, 主要研究方向为数据挖掘; 常致全, 副教授, 硕士生导师, 主要研究方向为数据库与信息系统。

Subject : C = CN , O = Globus , O = ICT , OU = HP-CLAB , CN = NAME

// 公钥

Subject Public Key Info :

Public Key Algorithm: rsaEncryption

RSA Public Key : (1024 bit)

Modulus : (1024 bit) :

00 : bf : 4c : 9b : ae : 51 : e5 : ad : ac : 54 : 4f : 12 : 52 :

3a : 69 : < snip >

b4 : e1 : 54 : e7 : 87 : 57 : b7 : d0 : 61

Exponent : 65537 (0x10001)

// 数字签名

Signature Algorithm: md5 With RSA Encryption

59 : 86 : 6e : df : dd : 94 : 5d : 26 : f5 : 23 :

c1 : 89 : 83 : 8e : 3c : 97 : fc : d8 :

< snip >

8d : cd : 7c : 7e : 49 : 68 : 15 : 7e : 5f : 24 : 23 : 54 : ca : a2 : 27

: fl : 35 : 17 :

2.2 SSL 与相互认证

SSL 是用于 Web 的一套安全通信标准,主要功能用于验证网络中对话双方的身份,并通过对数据的加解密保证应用层数据的传输不被监听、伪造和篡改。

网络环境中,实体之间通信采取相互认证。GSI 中实现的相互认证协议建立在 SSL 握手协议之上,图 1 是 B 认证 A 的过程,A 通过相反的过程认证 B,即完成一次相互认证。

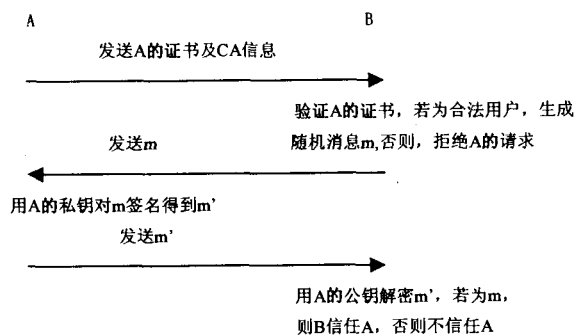


图 1 B 信任 A 的过程

网络中的实体都是动态可变的,用户请求服务,资源调度者根据一定的调度策略为其分配可用资源,用户与资源并不清楚对方所处的具体物理位置,唯一可以标志实体身份的就是实体所持的数字证书。因此,在实体间通信的时候,需要先经过相互认证,使得今后的通信可以建立在相互信任的前提之下。

3 应用与扩展

3.1 安全委托与单点登录

为了减少用户在相互认证中输入密码的次数,GSI 提供了安全委托。安全委托是一个标准的 SSL 协议扩展,一个代理包含一个新的证书,这个证书由 CA 为用户签署

的证书所关联的用户私钥来签署。一旦代理被创建并存储,用户可以使用代理替用户进行相互认证,减少了用户必须输入口令来得到私钥的次数。并且由于用户代理可以继续创建代理证书,即多级代理,这样就在不同的节点之间形成一个安全信任链。如图 2 所示^[2]。

在 Globus 中用户通过代理申请服务,可以不直接与资源服务器交互,而是通过网格门户(Grid Portal)^[3],形成单点登录,即用户只需在开始启动计算时进行一次“登录”(身份认证),然后就可以在无需进一步干预的情况下访问任何被授权可访问的资源。

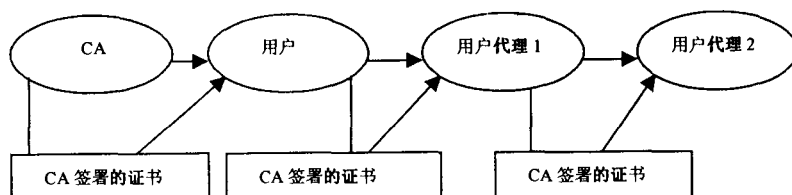


图 2 基于 GSI 的 CA—用户—代理信任链

3.2 在线证书仓库

用户在申请服务或资源时需要使用加密的私钥以及申请代理证书的客户端软件,而在实际情况中用户所处的位置是可变的,基于这种情况,GSI 提出了在线证书仓库(Online Credential Repository, OCR)^[4],并已由 UIUC 的国家超级计算中心实现比较成熟的软件 MyProxy^[4]。

OCR 的基本思想是:用户在自己的机器上生成有效期比较短(一般是一周或几周)的代理证书,并设定 OCR 服务器鉴别自己身份的用户名和口令,一并提交给 OCR 服务器。此后,用户只需启动客户端的回收程序,输入先前随代理证书一同提交给 OCR 的用户名和口令证明自己的身份,保存在 OCR 服务器中的代理将为用户生成有效期一般为几个小时的新代理,发还给用户,用户即可使用这个新代理请求服务。若用户使用网格门户,通过 Web 浏览器将用户名和密码提交给网格门户并告知 OCR 服务器的位置,则可以令网格门户代替用户向 OCR 服务器发出请求,得到新代理,新代理将在用户从网格门户注销的同时被删除。这样,用户便可不受操作环境的限制请求网格服务。

3.3 团体授权服务

在 GSI 中,授权可以在本地完成。当用户申请服务的时候,用户的身份将被映射到资源本地的某个身份,由本地策略决定该身份可以拥有的权限。而对于用户资源动态可变的网格环境来说,这样的授权机制不便于系统的扩展,为此 GSI 中引入了第三方团体授权服务(Community Authorization Service, CAS)^[5],负责管理用户的访问策略,无须再将用户在网格环境中的身份映射到本地。

CAS 是建立在公钥认证和代理机制之上的基于角色的团体授权技术。一个团体被看成是一个整体,拥有一个 GSI 颁发的团体证书,并可以启动一个 CAS 服务,授权该服务使用团体证书。团体是用户与资源服务器之间的桥梁,在团体的 CAS 服务器中维护了一张团体所有成员的

角色和访问策略表,同时,团体得到各资源服务器的授权,其内容保存在资源服务器本地的数据库中。

GSI 相继推出了 CAS 的两个实现版本 alpha 和 alphaR2^[5]。alpha 包括了一个 CAS Server、用户客户端和一个能够解析 CAS 授权证书的 GridFTP Server。用户的有效访问权限为资源授予团体的权限与团体授予用户权限的交集。CAS Server 颁发给用户的授权证书采用受限代理证书格式,资源服务器无法通过此授权证书获得用户的任何信息。alphaR2 在 alpha 的基础上对此作了改进,废弃了原先的受限代理证书,取而代之的是一个对用户身份、权限及权限有效期的申明,并将这个申明作为用户自签名代理证书的扩展项。资源服务器可以将用户的自签名代理证书看作普通的 GSI 证书进行识别,并可以从中获取申请服务的用户 ID。同时,用户的有效访问权限也改进为资源授予团体的权限、团体授予用户的权限和资源本地授予用户权限三者的交集。

CAS 的引入,减少了用户与资源服务器之间信任关系的数量,设一个团体的用户数量为 U ,资源服务器数量为 S ,则引入 CAS 之前,两者之间的信任关系的数量为 $U * S$,引入 CAS 后减少至 $U + S$ 。资源服务器也无需再将用户身份作本地映射。团体中的用户或资源提供者变动时,只需更新 CAS 数据库中的策略内容即可,大大提高了系统的可扩展性。同时,系统的灵活性也得到了提高,这体现在 CAS 服务器可以将其管辖范围内的资源统一调配给用户,例如某团体 C 的计算资源是由授权给 C 的资源提供者 R1, R2, R3 提供的,提供的数量分别为 2 个、6 个、10 个单位,对于 C 而言,可统一分配授权给它的所有计算资源,如为一次任务请求分配所有计算资源中的 30%,则该请求可得到 $(2 + 6 + 10) * 30\% = 5.4$ 个单位的计算资源。

4 应用流程及安全性分析

4.1 网格中的应用流程

网格环境中,认证与授权机制的使用极为广泛。下面以用户申请服务的整个过程(见图 3)为例,说明认证与授权机制在网络安全具体应用中的大致流程。

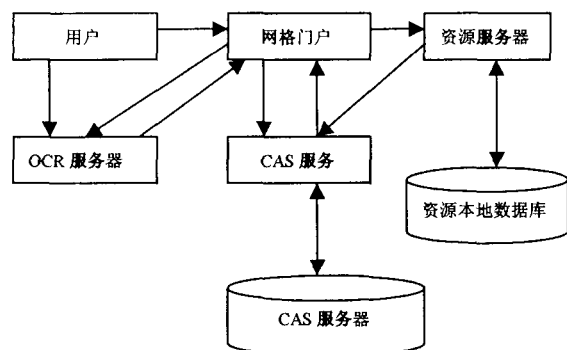


图 3 用户申请服务过程

过程描述如下,其中每两个实体相互通信之前必须进行

行相互认证。

(1) 用户向 OCR 服务器提交代理证书及私钥并确定登录用户名和口令;

(2) 用户向网格门户发送服务请求,并提供存放代理证书的 OCR 服务器所在位置及访问 OCR 所需的用户名和密码;

(3) 网格门户向 OCR 服务器发出请求;

(4) OCR 服务器为用户生成新的代理证书,发送给网格门户;

(5) 网格门户将代理证书发送至 CAS 服务器;

(6) CAS 服务器查看 CAS 数据库,根据用户的请求和在团体中的角色,确定用户的访问权限,并为用户签署权限申明;

(7) CAS 服务器将签了名的权限申明发送给网格门户;

(8) 网格门户代替用户对 CAS 服务器签署的权限申明进行自签名并提交给资源服务器;

(9) 资源服务器查看本地策略中授予用户所在团体的权限,并取其与团体授予用户权限(即用户自签名证书中的申明扩展项)的交集,即为用户访问该资源的权限。如若该用户提交的授权证书的签发团体并未得到所请求资源服务器的授权,则资源服务器需要将用户身份映射到本地,确定其权限并给予授权。

4.2 安全性分析

从图 3 中可以看出,网格门户代替了不同的资源服务器成为用户请求服务的单一交互对象,令用户的操作变得统一和简单化;引入 OCR 之后,减少了用户使用网格服务所受到的硬软件限制,尤其是在互联网极其发达的今天,用户可以随时随地获取他们想要得到的网格环境下的服务;CAS 的使用,增加了整个系统的灵活性和可扩展性,同时也使得资源服务器与用户之间的授权关系变得简单且易于管理。

然而服务器数量的增加,在网格这样的分布式系统中,增加了整个系统的负担和不安全性。从图 3 中可以看出,网格门户是整个申请服务过程中的不安全点,同时,OCR 服务器、CAS 服务器以及用户的代理证书都是容易被攻击的对象。GSI 针对其中部分问题提出了一些解决方案:

(1) 对于服务器可能不能正常工作的情况,采用传统的硬件备份和数据备份可以大大降低造成的损失。

(2) 对于服务器被攻击的情况,在 OCR 服务器上,通过使用用户的口令加密用户自己的代理证书,可以避免一旦服务器被攻击,代理证书泄漏的可能性。而对于 CAS 服务器,可能会因被攻击而为不合法或不具备该权限的用户发放授权申明,因此当 CAS 服务器被攻击时,需要及时通知授权给该 CAS 所管辖团体的所有资源服务器,此后,若再有用户申请资源,将直接由资源服务器进行本地授权,直到 CAS 服务器恢复正常工作。

(3) 在申请资源的过程中,使用代理证书完成大部分操作。如果代理证书及关联的私钥被截获,攻击者便可假冒用户的身份进行破坏行为。目前,大多数服务器尚不为颁发的代理证书提供证书撤销的功能,而是将代理证书的有效期设置得很短,一般是几个小时,这样,即使证书被窃取,也很快就会过期,攻击者很难在剩余的时间里进行破坏,减少了损失。

此外,尚有以下问题和安全隐患未能得到很好解决。

a. 如上所述,GSI 中未提供代理证书的撤销功能,而只是将代理证书的有效期设置得非常短,一旦代理证书泄漏,只能通过重新签发证书来继续正常操作。

b. CAS 中,如果团体颁发给用户的证书被攻击,攻击者可以假冒用户身份退出团体,这样,用户将不能再从此团体中得到任何授权证书。

c. 引入 OCR 后,用户只需采用在线方式,通过 Web 浏览,输入用户名和口令即可得到代理证书,将原先采用公钥设施数字证书进行认证的安全体系又转变成简单的使用用户名口令这种原始的认证方式,降低了系统的安全性。

由上面的分析可以看出,虽然 GSI 是目前最为完善的网络安全体系,在授权与认证方面仍存在着一些问题,有待进行更深入的研究和改进。

5 结束语

安全问题一直以来都是网络通信中的重要问题,对于网格环境也不例外。授权与认证是网络安全中的核心技术,

而网格环境的特殊性又为其提出了新的挑战,尤其是网格技术尚未成熟,仍在不断的探索之中。文中主要讨论了网络安全设施(GSI)中安全委托、单点登录、在线证书仓库和团体授权服务等技术,并通过图示说明认证授权在网格中的具体流程,讨论了其中仍存在的问题,为以后的研究提供可以参考的内容。

参考文献:

- [1] Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid - Enabling Scalable Virtual Organizations[J]. International J. Supercomputer Applications, 2001, 15(3):1-2.
- [2] Globus. Overview of the Grid Security Infrastructure[DB/OL]. <http://www.globus.org/security/overview.html>, 2002.
- [3] CERN, CNRS, INFN, NIKHEF, PPARC. DataGrid Security Requirement and Testbed Security Implementation[EB/OL]. WP07: Network Service, 2002, DataGrid-07-D7.5-0111-4-0, PUBLIC, <http://grid-auth.infn.it/docs/WP7-security-requirements.pdf>. 2002.
- [4] Novotny J, Tuecke S, Welch V. Online Credential Repository for the Grid: MyProxy[C/OL]. Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10), IEEE Press, 2001, <http://citeseer.ist.psu.edu/novotny01online.html>. 2001.
- [5] Pearlman L, Kesselman C, Welch V, et al. The Community Authorization Service: Status and Future[A]. CHEP03[C]. La Jolla, California:[s.n.], 2003. 24-28.

(上接第 138 页)

```

{
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.ImportParameters(rsaParamsExcludePrivate); //输入 RSA 公钥
    byte[] bytes = Encoding.Unicode.GetBytes(text); //将正文字符串转换成字节数组
    byte[] encryptedData = rsa.Encrypt(bytes, false); //调用 RSA 的 Encrypt() 方法加密数据
    return encryptedData;
}

(3)解密数据。
private byte[] DecryptData(byte[] data) //data 是密文
{
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.ImportParameters(rsaParamsIncludePrivate); //输入包含有私钥的 RSA 参数
    byte[] decryptedData = rsa.Decrypt(data, false); //调用 RSA 的 Decrypt() 方法解密数据
    return decryptedData;
}

```

4 结 语

如果使用非托管的 Win32API 开发数据加解密应用,那么即使是比较简单的操作也需要编写和执行大量的程序代码,不但处理过程复杂而且效率低下。Net Framework 封装了用以实现数据加解密、数字签名等安全操作的一组类,大大简化编码工作,降低程序设计复杂度,进而提高信息安全软件系统的生产率。已经应用上述介绍的 .Net Framework 下数据加解密方法,开发了一个基于 Web 的网络通信系统的安全子系统。

参考文献:

- [1] 钟 诚,赵跃华.信息安全概论[M].武汉:武汉理工大学出版社,2003.
- [2] Thorsteinson P, Gnana Arun Ganesh G. .NET 安全性与密码术[M].梁志敏,蔡建译.北京:清华大学出版社,2004.
- [3] O'Neill M. Web 服务安全技术与原理[M].冉 晓,郭文伟译.北京:清华大学出版社,2003.
- [4] Dournace B. XML 安全基础[M].周永彬,贺也平,刘 娟译.北京:清华大学出版社,2003.
- [5] 吕文达.精通 C# 程序设计[M].北京:清华大学出版社,2004.