基于属性证书的访问控制机制在网格环境中的实现

徐海堂[1]，张浩军[1]，武东英[1]，张 鑫[2]
(1. 中国人民解放军信息工程大学，河南 郑州 450002；2. 解放军 65017 部队，辽宁 沈阳 110121)

摘 要：基于属性证书的网格安全解决方案，能够很好地解决网格环境下的访问控制问题。给出了网格环境下基于属性证书的访问控制框架，讨论了此访问控制机制的工作过程，并描述了符合 Web 服务开放标准的 XML 属性证书。

关键词：网格；属性证书；网格安全基础设施；XML 密钥管理规范
中图法分类号：TP393.08 文献标识码：A 文章编号：1001-3695(2005)06-0116-02

Implementation of Access Control Based on AC over Grid

XU Hai-tang[1], ZHANG Hao-jun[1], WU Dong-ying[1], ZHANG Xin[2]
(1. *Information Engineering University, Zhengzhou Henan* 450002, *China*; 2. *The PLA* 65017 *Unit, Shenyang Liaoning* 110121, *China*)

Abstract: The scheme of security over Grid based Attribute Certificate (AC) stated can settle the problem of access control perfectly. Introduces the feasible access control frameworks based AC that can be used over Grid and its working process. The AC conform to the open Web service standard in XML format is also interpreted.

Key words: Grid; AC; GSI(Grid Security Infrasturcture); XKMS(XML Key Management Specification)

网格作为一种先进的技术和基础设施，目前已经得到广泛的应用。网格的根本特征是资源共享，网格的节点位于不同地域，节点间需要安全地共享数据资源，保证共享数据的完整性，网格提供的计算能力必须保证是持续、稳定和安全的，不应该因为网格内部资源的变化而对网格应用造成影响，网格还应该满足各种形式的安全要求，如数据传输的加密、实体的认证、权限的授权等，避免非法入侵和非法使用资源。在建立完善的安全保障机制的同时，还要避免安全验证耗费过多的处理能力。本文论述了属性证书应用于网格环境，构建安全网格应用框架，从而实现网格环境下的安全。

1 属性证书

属性证书[1]将用户名与一个或多个属性进行绑定，这种数字证书不包含公钥信息，只包含证书所有者 ID、证书颁发者 ID、签名算法、有效期、属性等信息。一般的属性证书有效期比较短，这样可以避免公钥证书在处理 CRL 时的问题。属性(Attributes)由属性类别和属性值组成，属性证书是多个属性的集合。属性证书可以有效地实现用户的身份验证、身份的证实、权限的分配和验证以及访问控制，从而提供了一种解决特权分配和授予的理想途径，实现了基于角色的访问控制，使得权限的管理和分配更加灵活和高效。属性证书的应用可以实现与实际应用处理模式适应、与具体应用系统开发和管理无关的授权和访问控制机制，从而简化应用系统的开发与维护。

2 网格安全基础设施(GSI)

网格安全基础设施[2]是 Globus 项目提出的，它提供在网格计算环境中的安全认证和安全通信等能力。GSI 基于公钥加密体系，采用 X.509 认证和 SSL/TSL 通信协议，并对它们进行了一定的扩展，使得 GSI 可以支持单点登录(Single Sign-on)。GSI 的实现符合 IETF 提出的通用安全性服务应用程序编程接口(Generic Security Service API, GSS-API)[5]。GSI 的主要安全技术手段包括安全认证、安全身份相互鉴别、通信加解密、私钥保护及委托与单点登录。GSI 认证核心是认证证书，在网格环境中的每个用户和服务都需要通过认证证书来进行身份验证，GSI 认证证书采用了 X.509 的证书格式，兼容其他基于公钥的系统。GSI 采用 SSL/TSL 协议作为它的相互认证协议。在缺省情况下，GSI 在通信双方之间不建立加解密通道。一旦相互认证成功，则 GSI 就脱离出来，使得通信双方在进行通信时不会有额外的加解密开销。GSI 对标准的 SSL/TSL 协议进行了扩展，使得 GSI 具有安全委托能力，减少了用户输入口令获得私钥的次数。如果一个网格运算需要请求多个网格资源，GSI 通过创建代理避免口令重复输入，而在不同节点之间形成一个安全信任链，一个代理包含一个新的证书，这个证书由用户来签署(代理证书)，而不是认证中心。

3 网格环境下基于属性证书的访问控制机制的实现

3.1 实现要求

基于属性证书的访问控制在网格环境中的实现应该满足下面的要求：

(1) 可扩展性。系统的架构应该不必改动或者改动很小就能满足用户和资源数目增多的要求，以确保整个系统具有延续性和良好的业务量适应能力。

(2) 便于管理。增加或删除系统中的用户或资源，修改用户的权限对组织应该尽量简单，避免增加额外的开销。同时，

收稿日期：2004-04-25；修返日期：2004-07-11

用户权限的可管理性保证系统更加健壮。

(3) 资源所有者拥有访问控制权。由资源所有者来决定用户对资源拥有什么样的访问控制权, 并可以及时地更改、发布实时的权限信息。

(4) 尽可能地利用现有访问控制模型。目前许多资源已经利用了现存的访问控制模型, 将授权信息同这些访问控制机制结合起来是非常重要的。

3.2　网格安全架构

3.2.1　安全架构模型

参见 GSI 的定义我们给出了如图 1 所示网格计算环境下的安全模型, 各个部分功能及安全机制实现过程在下面各节中有详细描述。

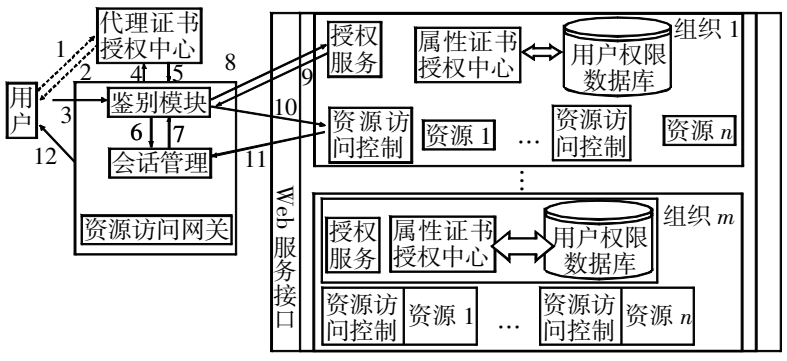


图 1　网格安全架构逻辑图

3.2.2　代理证书授权中心

根据 GSI 定义, 用户不直接与所需资源进行安全交互, 因此引入了用户代理的概念。系统中的每个用户都持有自己的安全证书, 在用户访问资源前通过自己的安全证书来获得代理证书。代理证书是由用户负责签署的有效期较短的临时安全证书, 代理证书有自己的私钥, 由用户设定其合理生存时间, 这样经过用户签署的代理证书表明用户同意用户代理可以代表用户与资源代理进行安全交互, 且限制了用户代理的合法存在时间, 保护了用户的安全信息。

在用户访问资源前, 首先进行初始化, 即用户请求签发生成自己的代理证书。用户向代理证书授权中心提交代理证书颁发请求(如图 1 中过程 1), 为资源的访问生成一个代理证书, 代理证书授权中心处理请求, 并返回一个标识符(如图 1 中过程 2), 并为用户产生代理证书, 将其存储在代理证书授权中心。

3.2.3　资源访问网关

资源访问网关由鉴别模块和会话管理模块组成。

(1) 鉴别模块。当用户要求访问网格资源时, 首先向鉴别模块提出请求(如图 1 中过程 3), 鉴别模块需要鉴别用户是否已有属性证书 AC, 若无 AC, 则与代理证书授权中心进行交互(如图 1 中过程 4, 5), 提取用户的代理证书, 准备为用户向相关组织的授权服务器申请 AC; 若有 AC, 则从会话管理模块中提取该用户的代理证书和 AC, 代理用户进行资源的访问。

(2) 会话管理模块。鉴别模块将授权服务器签发的 AC 和代理证书一起存储在会话管理模块中(如图 1 中过程 6), 当用户请求访问网格中资源时, 由会话管理模块负责提供代理证书和 AC(如图 1 中过程 7), 完成资源的访问。此外, 会话管理模块保持用户的单点登录信息, 用户只需登录一次就可以进行请求、使用和释放资源等操作, 不需要进行多次身份认证。

用户请求访问网格中资源时, 由鉴别模块向会话管理模块提取代理证书和 AC, 鉴别模块通过代理证书鉴别用户要访问的资源, 然后将代理证书、AC 和请求一起交给相应组织(如图 1 中过程 10), 由组织内的资源访问控制模块处理请求验证 AC 的有效性。如果该用户有权访问相应资源, 则授权用户进行资源访问, 此时资源访问控制模块返回访问结果至资源访问网关, 再由资源访问网关将结果返回给用户(如图 1 中过程 11, 12)。

3.2.4　授权服务器

每一个参与资源访问的组织内都有一个授权服务器。实现将资源的访问控制权统一交由授权机构进行管理, 由资源的所有者来进行访问控制管理。用户访问资源前要申请自己的 AC。资源访问网关中的鉴别模块向组织内的授权服务器提交代理证书和访问请求来申请 AC(如图 1 中过程 8)。请求通过标准 Web 服务接口提交给授权服务器处理, 授权服务器验证代理证书的有效性, 通过属性证书授权中心, 按照代理证书的 DN 查询用户权限数据库。属性证书授权中心获知用户的权限后生成一个包含用户 DN、存取权限、有效期, 并用私钥签名的 AC, 然后将 AC 连同用户的代理证书一起返回到资源访问网关的鉴别模块(如图 1 中过程 9), 再由鉴别模块存储在会话管理模块中。

用户的权限以组的形式存放在用户权限数据库中, 一个用户属于一个或多个组, 资源所有者按组分配访问权限, 减少了授权管理工作量。用户访问权限通过属性证书授权中心按组所属策略进行分配, 属性证书授权中心还用来完成添加、删除、修改组中的用户。

3.2.5　资源访问控制

每一个组织内的每一个资源都有一个用于接收请求的资源访问控制模块, 外界用户通过它来访问资源。资源访问控制模块的结构如图 2 所示。资源访问控制模块收到包含代理证书和 AC 的访问请求(如图 1 中过程 10), 它首先通过用户的代理证书鉴别用户的身份, 一旦用户身份被鉴别, 资源访问控制模块内的证书解读模块验证 AC 的 DN 是否与代理证书的 DN 相同, 此 AC 是否为该组织签发, AC 的有效期以及 AC 所在的组, 然后将 AC 连同请求一起交付访问执行模块, 访问执行模块将用户的 DN 和它的请求写入访问日志, 然后访问请求按照资源的本地访问控制机制所赋予的权限来执行, 并将访问结果返回到资源访问网关(如图 1 中过程 11)。

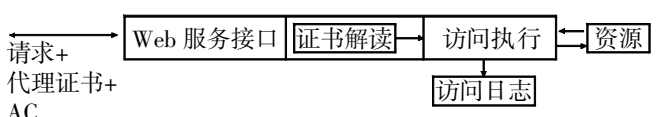


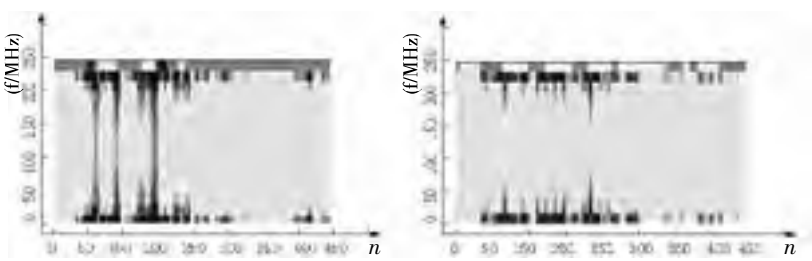
图 2　资源访问控制模块

3.3　属性证书

网格的根本特点是资源共享, 这必然会带来安全问题。将属性证书应用于网格环境中, 通过属性证书绑定用户、设备等实体的属性, 结合到包含安全证书的 GSI 应用当中, 可以有效地拓展基于证书的鉴别与授权功能, 解决网格环境中的安全问题。在此, 授权信息不是加入到代理证书中, 而是由单独的属性证书来表示和容纳。AC 由每个组织的授权服务器产生, 包含用户的唯一标志名 (Distinguished Name, DN), 因此, AC 可以与代理证书相连。

在此, AC 的申请和撤销信息采用扩展标记 (下转第 129 页)

是对数据在测点 340(即第三尖峰处) 和 396(无任何异常处) 进行 STFT(采用 Black-Tukey 窗, 窗长为 32, 步长为 1, 调频系数为 5×10^{-9}) 的时频图显示, 对各处模值进行取对数处理。两图对比不难发现, 在采样点 73, 116, 185 处频率变化显著, 参照图 4(d) , 可以看到大约在采样点 72, 117, 183 处开始确有变化存在。结合对试验所用相控阵探地雷达的速度分析结果, 可以得出第一个异常约在地下 0. 2m 处, 与模型中钢管埋藏情况相符。



(a)测点为 340　　(b)测点为 396

图 5　不同测点的测点切片视图

5　结论

STFT 是一种传统的信号时频分析方法, 在实际工程应用中有着广泛的应用, 但由于采用的是非振荡型低通窗函数, 对时变显著信号分辨率不高。在对一组具体的探地雷达回波信号数据分析中采用了一种改进的 STFT, 并对数据进行多种切片视图显示, 从多个角度、多个侧面对数据进行分析。通过 VC ++程序实现的试验表明, 该方法在相控阵探地雷达的回波信号分析中能取得较好效果, 能较精确地对雷达探测的地质情况进行定位。

参考文献:

[1] 王俊茹. 工程与环境地震勘探技术[M] . 北京: 地质出版社, 2002.

[2] 徐伯勋. 地震勘探信息技术:提取、分析和预测[M] . 北京: 地质出版社, 2001.

[3] Donald R Wehner. High-resolution Radar[C] . London/Boston: Artech House, 1995.

[4] 林茂庸, 柯有安. 雷达信号理论[M] . 北京: 国防工业出版社, 1984.

[5] 戴前伟. 地质雷达的应用条件探讨[J] . 物探与化探, 2000, 24(4) : 157-160.

[6] Milne K. Phased Arrays in Radar[C] . IEE Tutorial Meeting, 1989. 211-230.

[7] 张贤达. 现代信号处理[M] . 北京: 清华大学出版社, 2002.

[8] 徐春光, 谢维信. 一种高分辨自适应信号时频表示[J] . 西安电子科技大学学报, 1999, 26(6) : 720-722.

[9] 胡广生. 现代信号处理教程[M] . 北京: 清华大学出版社, 2001.

[10] 时频分析: 理论与应用[M] . 白居宪. 西安: 西安交通大学出版社, 1998.

[11] 施京, 陈淑珍. 时频分析方法在相控阵探地雷达正演数据中的应用[J] . 武汉大学学报, 2003, 49(5) : 645-648.

作者简介:

操峰(1979-) , 男, 湖北武汉人, 硕士研究生, 现从事多媒体信号分析与网络技术研究; 陈淑珍 (1946-) , 女, 湖北襄樊人, 教授, 博士生导师, 主要研究方向为多媒体通信技术; 肖柏勋(1956-) , 男, 湖北武汉人, 副院长兼总工程师, 主要从事地球物理勘探方面的研究。

(上接第 117 页) 语言 XML 编码。保证了数据存储、传输的标准性、灵活性、通用性。XML 密钥管理规范(XML Key Management Specification, XKMS) 定义了分发和注册 XML 签名规范所使用的公共密钥的方法。XKMS 以已有的 XML 加密和 XML 数字签名为基础, 其关键的思想是提供 Web 上的可信服务。XKMS 支持客户端把公钥信息的处理委托给信任服务, 为应用提供了可以互操作的安全基础设施。XML 可以广泛地应用于各种平台, 因此基于 XKMS 标准的属性证书用于访问控制, 具有更好的安全性和互操作性。

属性证书的格式用 XML 描述如下, 它包含用户的 DN, 有效期以及用户所在的组, 并被属性证书签发系统用授权服务器的私钥签名。

```
< attributeCertificate >
< acInfo >
< version > 1. 0  < /version >
< holder >  user DN  < / holder >
< issuer >  issuer DN  < /issuer >
< issuerName >  issuerName  < /issuerName >
< issuerSerialNumber >  < /issuerSerialNumber >
< signatureAlgorithm > SHA1withRSA < /signatureAlgorithm >
< validity >
< notBefore >  < /notBefore >
< notAfter >  < /notAfter >
< /validity >
< attributes >
< DPGroup > value < /DPGroup >
< wrapperGroup > value < / wrapperGroup >
< dataAccessGroup > value < /dataAccessGroup >
< /attributes >
< /acInfo >
< signatureAlgorithm > SHA1withRSA < /signatureAlgorithm >
< signature >
< /signature >
< /attributeCertificate >
```

4　结论

在网格环境中, 采用基于属性证书的访问控制机制, 提供了一种解决特权分配和授予的理想途径, 保证了网格的安全性。用户的权限由资源所有者限定, 因为许多应用已经使用了现存的成熟的访问控制机制, 资源所有者拥有访问控制权保持了原来的访问控制模型。将属性证书的应用与网格安全基础设施 GSI 相结合, 提供了网格计算环境中的安全认证和安全通信能力, 使得系统具有易用性、灵活性、可移植性和可靠性。

参考文献:

[1] etwork Working Group. RFC 3281, An Internet Attribute Certificate Profile for Authorization [EB/OL] . http: //www. ietf. org/rfc/rfc3281. txt, 2002.

[2] 都志辉, 陈渝, 刘鹏. 网格计算[M] . 北京: 清华大学出版社, 2002.

[3] Sharon Boeyen. X. 509: Overview of PKI & PMI Frameworks. Entrust Technologies(4th Edition) [EB/OL] . http: //www. entrust. com/resources/technical. cfm, 2000.

[4] Globus Project. Overview of Grid Security Infrastructure[EB/OL] . http: //www. globus. org/security/overview. html, 2001.

[5] Network Working Group. RFC 2744, Generic Security Service API version 2: C-bindings [EB/OL] . http: //www. faqs. org/rfcs/rfc2744. html, 2000-01.

[6] D W Chadwick, O Otenko. The PERMIS X. 509 Role-based Privilege Management Infrastructure[EB/OL] . http: //sec. isi. salford. ac. uk/download/SACMATfinal. pdf, 2001.

作者简介:

徐海堂(1979-) , 女(满族) , 辽宁锦州人, 硕士研究生, 研究方向为信息安全; 张浩军(1969-) , 男, 河南郑州人, 副教授, 博士研究生, 研究方向为信息安全; 武东英(1965-) , 女, 河南郑州人, 副教授, 硕士生导师, 研究方向为网络工程; 张鑫(1979-) , 男, 辽宁沈阳人, 助理工程师, 研究方向为网络工程。