网格环境中一种基于SPKI证书的授权模型

王 茜 杨广超
（重庆大学计算机学院 重庆 400030）

摘 要 网格环境中的授权问题是网格安全的一个研究热点。社区授权服务CAS是网格安全基础设施GSI中的授权机制，鉴于社区授权服务CAS授权机制中提供各种服务的Resource只能粗粒度地授权给CAS服务器，很难细粒度地控制客户权限，本文提出了一种新的授权模型，采用了SPKI电子证书进行授权。与CAS相比，该模型授权更加灵活，通过委托授权增强了系统的可扩展性，而且能够细粒度地控制用户权限。

关键词 CAS，授权，SPKI

An Authorization Model Based on SPKI Certificate in Grid

WAGN Qian YANG Guang-Chao
(Computer College, Chongqing University, Chongqing 400030)

Abstract Resource on authorization problem in grid environment is a hot topic in grid security. The Community Authorization Service, CAS, is an authorization mechanism of Grid Security Infrastructure, GSI. For resources in CAS authorization mechanism can only provide a course-grained authorization to CAS server, which is difficult to control authorization of client. A new authorization model which adopts SPKI certificate is proposed. Compared with CAS, this authorization model is more flexible, it improves scalability of the authorization system using delegation and can give fine-grained access control to client.

Keywords CAS, Authorization, SPKI

1 引言

近年来，网格计算作为分布式计算一个新的领域得到了人们广泛的关注。网格就是跨多个管理域、异构的计算机和资源的集合，它是继万维网之后出现的一种新型的网络计算平台[1]。目前，网格技术正处在萌芽后的发展阶段[12]。

由于网格系统要求同时使用大量的资源、动态的资源请求等等，因此，网格安全作为网格中最重要的一部分，就成为了网格计算系统正常运行的保证。为了在网格环境中，网格实体对资源的访问得到很好的控制，实体之间的通信能够安全进行，授权问题显得格外重要。所谓授权就是确定一个具有特定标志或一组属性的实体具有某种权限来对特定的资源执行特定操作的过程[5]。这个步骤发生在认证之后。在网格环境中授权分为服务器端(server-side)授权和客户机端(client-side)授权。服务器端授权就是服务器对客户机进行授权；客户机端授权是客户机在调用之前或在调用过程中对服务器进行授权。本文主要讨论服务器端授权。

社区授权服务(CAS)是Globus Project开发用来在大型的分布式网格环境中，实现用户对资源的访问控制[12]。但是由于CAS授权模型中，资源把社区作为一个整体提供粗粒度的访问控制，而社区自身实现细粒度的授权。这样，资源只能对CAS服务器进行权限控制，很难对社区中客户的权限。本文针对这一缺陷，提出一种新的授权模型——GCSAM，该模型采用了SPKI电子证书，通过权限委托实现授权，增强了系统的可扩展性同时达到对客户权限的控制而实现细粒度的访问控制。

2 SPKI电子证书

SPKI(Simple Public Key Infrastructure)是IETF提出的一个公钥证书标准[6]。它是一种通过使用证书对实体进行授权的安全机制。主要用于分布式的访问控制[4]。允许实体对资源有不同的访问权限。对实体的授权可以在SPKI证书中任意定义，实体通过提交证书表明自身的权限以获得对资源的访问。

SPKI证书采用公开密钥技术，它用实体的公钥而不是实体的名字进行安全控制。采用SPKI证书，解决了网格环境中全球域名的局限性。

2.1 SPKI证书结构

SPKI证书结构如图1所示，包含5个域：颁发者(issuer)、主体，也就是接受者(subject)、委托(delegation)、授权权限(authorization)、有效期(validitydate)。

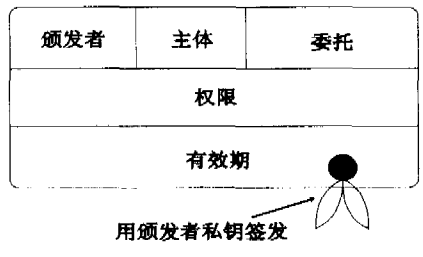

图1 SPKI证书结构

SPKI证书结构这5部分构成的结构体称为5元组，用发

王 茜 副教授，主要研究方向为网格安全，电子商务等。杨广超 硕士研究生，主要研究方向网格安全。

布者的私钥签名成为 SPKI 证书。证书就像是许可证，有了这个许可证，持有者就能得到某种服务；同时，接受者所拥有的权限、有效期、颁发者都很清楚地记录在证书中了。

颁发者：颁发者域可以是公钥、公钥的散列值或者是保留字“self”，表示由谁签发了证书。

接受者：接受者域表明谁会接收到证书所授与的权限。该域可以有 3 种形式：公钥、公钥的散列值、名字（由 SDSI 名字证书确定）。该域意味着这个公钥或名字拥有这份证书，除此之外的任何实体使用这份证书都是非法的。

委托：委托域表明发布者是否允许接受者可以将其所接受到的权限再授予其他实体。该域包含了一个布尔值，如果为真则表示发布者允许接受者将证书规定的权限授予其他的接受者。

授权：授权意味着访问的权利，也表明接受者将从颁发者那里得到的权限。权限可以由证书的发布者在证书里自由定义。该域的内容完全依赖于应用程序，不同的应用程序可以定义不同的访问权限。

有效期：有效期通常是由发布者规定的证书的有效时间。SPKI 标准建议使用起止时间的形式作为有效期的表述形式。

2.2 SPKI 证书的优点

SPKI 数字证书的许多优点使得它非常适合在分布式环境中构造授权服务，这些优点包括：

(1)分布式 。证书可以被自由颁发，不再局限于一个中央权威，其他一些标准如 X.509 都假设有一个单独的证书权威 CA 或多级的 CA 体系专门用来颁发证书，这样就大大地限制了分布式环境中的信任范围。

(2)授权委托。访问权限可以被委托。这样必然形成一个证书链，访问权限的委托使系统变的相当灵活。例如具有某个网格磁盘存储服务权限的“父亲”可以将存储权限权限授予他的“子女”，同时还可以在授权域内指定使用磁盘的最大值。

(3)灵活的许可。授权许可可以自由定义并不局限于任何预定域，然而，尽管这种方法提供了最大的灵活性，单为了保证证书的可互操作性，还是应该对一些通用的许可项进行标准化。

(4)有效性。证书的颁发者能够指定一个有效的时间段或其他在线条件确保证书的有效性。这还可以用来对授权委托和访问限制进行细粒度的控制。

(5)隐私性。公钥到授权的直接绑定，而不是名字，因而提供了很好的隐私保护。一位颁发者为主体颁发的证书中使用的公钥是由主体临时产生的，证书的使用完全是匿名的，这种临时身份就使得隐私性得到了保证。

3 授权模型

3.1 系统结构

GCSAM 授权模型如图 2 所示。该授权模型采用“网格社区”的概念，根据网格实体的兴趣、目的等将网格实体划分为不同的网格社区。网格社区是用来辅助它的成员公钥与名字的解析；授权有效性检验，形成授权链等。与 CAS 服务器相比，网格社区服务器（GC server）既不颁发证书，也不授予和委托权限。

授权模型包含如下 4 个组成部分。

网格社区服务器 GC Server：主要用于管理社区内网格实体的信任关系，为资源服务器 Resource Server 提供客户资料，以供角色分配和证书颁发的策略形成；权限委托服务，管理获得证书的 GC user 的权限委托服务。

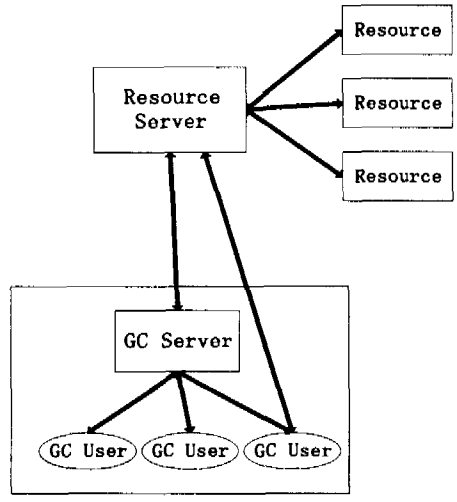

图 2 授权模型结构

资源服务器 Resource Server：提供管理资源策略服务和证书管理服务。主要有如下功能服务：(1)资源策略服务，资源在 Resource Server 建立自己的访问策略，控制对资源的访问权限。GCSAM 授权模型中资源建立的访问策略主要是将客户划分为不同角色，具体的方法这里就不详细叙述了。(2)证书管理服务，负责检验 GC user 用户提供的证书的合法性。(3)证书链服务，形成从资源到 GC user 的 SPKI 证书链。

网格社区用户 GC user：代表最终的用户，它关心的是资源提供给它的服务，GC user 访问 Resource Server 的资源策略服务，获得资源分配的角色，资源根据角色将 SPKI 证书分配给 GC user，收到授权证书以后，在证书有效期内提交证书请求对资源的访问。

Resource：提供各种不同的资源服务。主要通过颁发证书管理访问权限，提供受限的网格服务。

3.2 系统实现步骤

在 GCSAM 授权模型中，简单实现了网格环境中的授权。具体的步骤如下：

(1)Resource 访问 Resource Server 的资源策略服务，详细描述划分角色的策略。

(2)GC user 访问 Resource Server 资源策略服务，Resource Server 按照资源的角色策略描述决定 GC user 角色之后，将返回给资源 GC user 的角色。

(3)资源根据 GC user 的角色颁发相应的 SPKI 证书。格式如：〈I1，S1，D1，A1，V1〉，其中，I1 代表授权给 GC user 的资源；S1 代表一个 GC user；D1 代表 true，是指 S1 得到的权限可以委托给其他用户；A1 是指资源给 GC user 的权限；V1 是指有效期。

(4)用户与资源服务器交互。将得到的 SPKI 证书提交给资源服务器 Resource Server。资源服务器检验用户的授权的合法性，决定是否允许该客户对资源的访问。

(5)若得到 SPKI 证书的 GC user 将权限委托给其他客户，则该形成授权链。例如形成〈I1，S1，D1，A1，V1〉，〈S1，S2，D2，A2，V2〉证书链，则 Resource Server 根据这两个授权证书形成客户的实际授权〈I1，S2，D2，A1∩A2，V1∩V2〉，最终找出用户的权限和权限的有效期。然后最终用户将提供所有的授权证书给 Resource Server，Resource Server 形成最终的授权之后再

检验合法性决定是否允许该客户对资源的访问。

4 性能分析

GCSAM授权模型，采用SPKI证书实现在网格环境中的授权管理。下面我们将对此授权模型进行评价。

不可伪造性：SPKI证书的签发和传递都是用证书的签发者的私钥进行签名，这样防止了证书的伪造。

不可抵赖性：SPKI证书是采用私钥签名的，公钥发布给接收者，使得资源所有者对所共享的资源负责，用户对资源进行访问受到了保护，不会有恶意病毒入侵的危险。

安全性：由于SPKI是采用密钥签发证书，增强了证书的私密性，也使系统的整体安全性进一步得以保证。

灵活性：采用SPKI证书委托授权，使得授权模型与CAS相比更加灵活。

SPKI电子证书采用"授权-公钥"机制，解决了CAS中的必须全球唯一的名字的限制，增强了系统的可操作性。并且资源通过SPKI证书链可以细粒度的控制客户访问权限。

参 考 文 献

1 Pearlman L, Welch V, Foster I, et al. The Community Authorization Service: Status and Future CHEP, 2003

2 Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of High Performance Computing Applications, 2001, 15(3): 200～222

3 Foster I, Kesselman C. Globus: A Metacomputing Infrastructure Toolkit. International Journal of Supercomputer Applications, 1998, 11 (2): 115～129

4 Boudriga N, Obaidat M S. SPKI-based Trust Manage ment in Communications Networks Computer and Telecommunication Systems[J], SPECTS, 2003. 719～726

5 Authorization processing for Globus Toolkit Java Web services. http://www-128. ibm. com/developerworks/grid/library/gr-gt4auth/ 2005. 12

6 Mjogeman M, Thomasson R. Performance Simulations ,of the UMTS Common Packet Channel. http://citeseer. nj. nec. com/443486. html

7 Koodli R, Puuskari M. Supporting packet-data Qos in next generation cellar networks. IEEE Communications Magazine, 2001, 39 (2)

8 CAS AlpahR2 Web site. http://www. globus. org/Security/cas/alpha-r2/, septmber 2002

9 Simple Object Access Protocal(SOAP)1. 1. W#C, 2000

10 The Globus Toolkit 4. 0 Release Manuals, 2005. http://www.globus. org/toolkit/docs/4. 0/

11 Foster I, Kesseman C. The Grid 2. 电子工业出版社, 2004

12 徐志伟，冯百明，李伟. 网格计算技术. 电子工业出版社, 2004

（上接第69页）

2 Denning D E. An Intrusion Detection Model. IEEE Transactions on Software Engineering, 1987(2): 222

3 Rao A, Georgeff M. Modeling rational agents within a BDI architecture. In: Proceedings of the Second International Conference on Principles of Knowledge Representation and Reasoning, 1991

4 Snapp S R, Smaha S E, Teal D M, et al. The DIDS (distributed intrusion detection system) prototype. In: Proc. of the Summer USENIX Conference. Berkeley, CA, USA, 1992. 227～2335

5 Chen S S, Cheung S, Crawford R, et al. GrIDS -A graph based intrusion detection system for large networks. In: The 19th National Information Systems Security Conference (NISSC), Baltimore, MD, USA, 1996. 361～370

6 Kumar S, Spafford E H. A pattern matching model for misuse intrusion detection. In: Proceeding of the 17th National Computer Security Conference, U. S. A, 1994. 11～21

7 Porras P A, Neumann P G. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In: Proceeding of the 20th National Information Systems Security Conference, Maryland, USA, Oct. 1997. 353～365

8 程显毅. Agent计算. 哈尔滨：黑龙江科学技术出版社, 2003

9 Boudaoud K, Guessoum Z. A Multi-agents System for Network Security Management. In: Proc. of Telecommunication Network Intelligence, IFIP TC6 WG6. 7. Sixth International Conference on Intelligence in Networks (SMARTNET 2000), Austria, September 2000. 172～189

10 Spafford E, Zamboni D. Intrusion detection using autonomous agents. Computer Networks, 2000, 34(4): 547～570

11 Frank J. Artificial Intelligence and Intrusion Detection: Current and Future Directions. In: Proceedings of the 17th National Computer Security Conference, 1994

12 Sebring M, Shellhouse E, Hanna M, et al. Expert Systems in Intrusion Detection: A Case Study. In: Proceedings of the 11th National Computer Security Conference, 1988

13 Siedlecki W, Sklansky J. On Automatic Feature Selection. International Journal of Artificial Intelligence , 1998, 2(2)

14 Sung A H, Mukkamala S. Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks. In: Proceedings of the 2003 International Symposium on Applications and the Internet Technology, 2003. 209～216

15 Zhong S, Khoshgoftaar T M, Seliya N. Clustering-based Network Intrusion Detection. International Journal of Reliability, Quality and Safty Engineering, 2005

16 Shajari M, Ghorbani A A. Application of Belief-Desire-Intention agents in intrusion detection and response. In: Proceedings of Privacy, Security, Trust Conference, Fredericton, New Brunswick, October 2004. 181～191

17 Kahn C. Communication in the Common Intrusion Detection Framework. In: CIDF Working Group document, 1998. 100～105

18 Asaka M, Okazawa S, Taguchi A, et al. A Method of Tracing Intruders by Use of Mobile Agents. In: Proc. 9th Annual Internetworking Conference (INET'99), San Jose, CA, 1999. 1～12

19 Stolfo S, Prodromidisy A L. JAM: Java Agents for Meta Learning over Distributed Databases. In: Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining, CA, August 1997. 74～81

20 Karjoth G, Lange D B, Oshima M. A security model for Aglets. IEEE Internet Computing, 1997, 1(4): 68～77

21 Corradi A, Cremonini M. Mobile Agents integrity for electronic commerce applications. Information Systems, 1999, 24(6): 519～533

22 Karjoth G, Asokan N, Gle C. Protecting the computation results of free-roaming Agents. In: Rothermel K, Hohl F, eds. Mobile Agents: 2nd Int'l Workshop. London: Springer-Verlag, 1998. 195～207

23 Cheng JSL, Victor KW. Defenses against the truncation of computation results of free-roaming Agents. In: Deng RH, Qing SH, Bao F, et al. eds. Information and Communications Security. London: Springer-Verlag, 2002. 1～12

24 Wilhelm G, Staamann M. A pessimistic approach to trust in mobile Agent platforms. IEEE Internet Computing, 2000, 4(5): 40～48

25 Barrière L, Flocchini P, Fraigniaud P, et al. Capture of an Intruder by Mobile Agents. In: 14th ACM Symp. on Parallel Algorithms and Architectures (SPAA '02), Winnipeg, August , 2002

26 Slagell M. The Design and Implementation of MAIDS: [Technical Report TR01-07]. Iowa State University, Department of Computer Science, Ames, IA, USA, 2001