基于移动 Agent 的网格跨域安全审计体系结构及实现*)

肖政宏[1,2] 胡忠望[1,3] 尹 浩[1]

(清华大学计算机科学与技术系 北京 100084)[1] (湖南文理学院计算机科学与技术系 常德 415000)[2]

(湖南工程学院计算机科学与技术系 湘潭 411101)[3]

摘 要 网格计算面临的重大挑战之一是开发一系列有效的机制和策略来保证网格任务处理的安全。审计和审核是大规模网格节点的基本需求。本文分析了网格节点的安全审计需求,提出了一种基于移动 Agent 的跨域安全审计体系结构。为了使安全机制的实施对网格性能产生的影响最小,使用了一种新的授权安全机制"审计一次,授权多次",通过构造多值信任关系模型实现动态审计。给出了利用 GT3 用户定义服务和 Aglet 平台所实现的跨域安全审计模型。

关键词 跨域安全审计,移动 Agent,授权安全机制,动态审计,信任关系模型

Cross-Domain Security Auditing Architecture and Implement in Grid Based on Mobile Agent

XIAO Zheng-Hong[1,2] HU Zhong-Wang[1,3] YIN Hao[1]

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084)[1]

(Department of Computer Science and Technology, Hunan University of Arts and Science, Changde 415000)[2]

(Department of Computer Science and Technology, Hunan Institute of Engineering, Xiangtan 411101)[3]

Abstract A significant challenge for Grid computing is to develop an efficient set of mechanisms and polices for securing grid processes. Auditing and accounting are fundamental requirements of large sites. In this paper, we identify security auditing requirements, and propose a Cross-Domain Security Auditing (CDSA) architecture based on Mobile agent. To make the least influence on the performance, a new secure mechanism for authorizing is implemented by way of modifying the traditional manner "route once, switch many" in network to the new manner "audit once, authorize many" in Grid. The dynamic auditing is carried out by constructing a multi-value trust relationship model. The system enforces these mechanisms to enable cross-domain security auditing in the aid of user-defined services of Globus Toolkit Version 3.0 and IBM Aglet.

Keywords CDSA, Mobile agent, Authorize secure mechanism, Dynamic auditing, Trust relationship model

1 引言

网格安全是网格计算中最富挑战性的方面之一。近年来,网格安全作为计算网格、数据网格、语义网格中一个重要的研究领域得到了广泛的关注,但大多数的研究集中在命名和授权、安全通信、信任、策略、授权和存取控制等方面[1]。审计和审核作为大规模网格节点的基本需求,虽然在 GGF (Global Grid Forum)上有一些讨论,但对它们的研究仍然处在早期阶段[2]。网格安全研究中存在的一个重大挑战是跨域的安全审计、私钥管理、否认服务和网格的安全集成[1]。虽然许多学者对网格安全进行了研究,但迄今为止被证明完整地解决网格安全是一件很困难的事情[1]。主要原因如下:第一是网格计算环境的异构性,网格计算环境中的各种软件/硬件资源存在着多方面的差异,这种差别加大了网格安全机制和策略的部署难度;第二是网格计算环境的混沌性,网格中各个虚拟组织之间,其相互关联关系不断发生变化,使得网格安全的实施很难得到有效的控制。

基于移动 Agent 的跨域安全审计体系结构是本文提出的一种新的网格安全系统和技术。为使安全审计对网格用户性能的影响最小,通过修改网络中传统的交换方式"路由一次,交换多次",提出了一种新的授权机制:"审计一次,授权多次"。通过把域之间的信任关系划分为完全信任类型、部分信任类型、最少信任类型来实施动态的审计,研究了使用 GT3 用户定义服务和 IBM Aglet 移动平台对跨域安全审计模型的实现。GT3 的用户定义服务被用来获取网格用户的安全信息,移动 Agent 被用来传送跨域的安全信息。

2 跨域安全审计体系结构

2.1 安全审计需求

网格资源审计是资源使用和付费的审计。网格审计作为一个安全的组件,与网格的审核、授权和授权组件等进行无缝的联接。对系统管理员和网格管理员而言,网格资源的安全审计是必要的,这些审计信息不仅能够被用来计费或者进行安全审计,也可以用到入侵检测系统。审计的内容和审计的粒度由网格管理员决定,安全审计的需求如下:(1)网格用户对站点资源的存取必须有严格的记录,这些记录包括存取时

*)本课题得到国家自然科学基金(60372019)、湖南省自然科学基金(04JJ3045)、湖南省教育厅科研项目(02C107)资助。肖政宏 副教授,主要研究方向为 Agent、信息安全、网格计算;胡忠望 副教授,主要研究方向为计算机网络与安全、网格计算;尹 浩 博士、讲师,主要研究方向为计算机网络、信息安全。

间、网格用户 ID、工作 ID 等等。例如，在使用 Kerberos 认证系统时，需要记录证书的内容。(2)使用特定策略的登陆系统，只有授权的用户能够浏览相关的记录，没有授权的用户的踪迹应该被登记。(3)由于网格用户的数量巨大，采用合适的策略来增强审计的效率是必要的。(4)在监控网格资源使用的过程中，网格异常的行为应该被标识(像入侵检测)，并采取对应的措施。(5)对所建立的安全审计记录，建立一种能够验证其授权策略是否依据本地资源被正确实施的机制是必要的。

2.2 CDSA 体系结构

跨域安全审计(Cross-Domain Security Auditing，CDSA)结构涉及到网格环境中站点安全信息的收集、跨域信息的传送、授权管理策略、基于信任关系类型的审计策略。CDSA 的结构如图 1 所示。

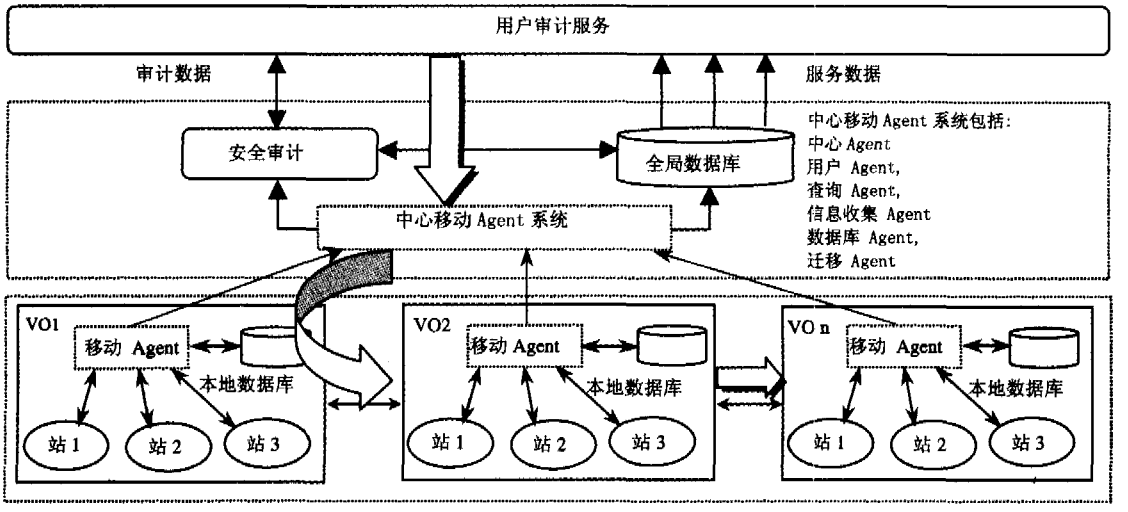

图 1 跨域安全审计体系结构

2.3 “审计一次，授权多次”的授权安全机制

“路由一次，交换多次”意味着包通过路由交换时，如果包的 IP 地址在硬件路由表中存在，包通过交换硬件直接交换；如果在硬件路由表中没有发现包的 IP 地址，包的传送需要路由，包通过过滤模块处理以后，CPU 把路由入口写入硬件路由表。在本文的跨域安全审计系统中，为使安全审计系统对网格用户产生的影响性能最小，使用“审计一次，授权多次”的类似方式来提高授权的效率。授权请求的基本结构如图 2 所示。

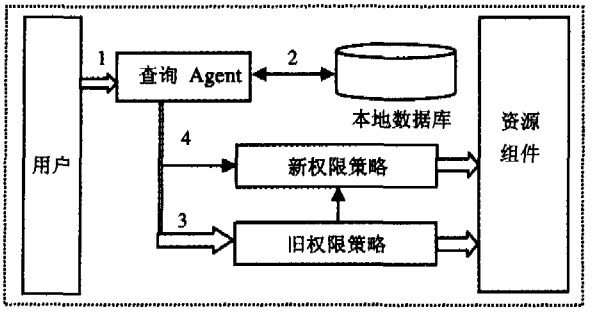

图 2 “审计一次，授权多次”的授权安全机制

(1)通过迁移 Agent，当用户对网格资源的请求到达当前的域，查询 Agent 在本地数据库中查找安全审计记录(如用户 ID、用户授权、任务管理权限等)。

(2)如果用户 ID 没有发现，或者没有对网格资源足够的权限，用户对网格资源的请求需要被审计，根据新的权限策略存取网格资源。这个新的权限策略是由授权反馈的结果结合本地域的权限形成的。最后修改本地数据库。

(3)如果用户的 ID 被发现，也有足够的对网格资源的权限，用户根据旧的权限策略来存取网格资源。

2.4 基于信任关系的动态审计

目前提出了各种各样的网格信任关系模型。文[3]在 GGF 上提出了一个基于 CA 的信任关系模型草案。文[4]提出的 X.509 信任是一个中心化的方法，每一个参加者有一个由中心 CA 授权的证书。SPKI 信任模型[5]通过代理证书提高了灵活性。文[6]提出了一个两层信任模型，上层定义了虚拟组织之间的信任关系，下层定义一个网格域中的信任值。然而，所有的授权仅仅涉及到一个授权机制，而与审计系统没有关系。本文提出一个基于审计策略的信任关系类型，该方法是把域之间的信任关系划分为 3 种信任关系类型：完全信任类型、部分信任类型、最小信任类型。完全信任类型表示两个虚拟组织之间最大的信任类型。当一个虚拟组织中的用户请求另一个虚拟组织的网格资源时，不需要审计和授权。部分信任关系类型表示两个虚拟组织之间具有中等信任关系。当一个虚拟组织中的用户请求另一个虚拟组织中的网格资源时，可以有选择地进行审计。最小信任关系类型表示两个虚拟组织之间具有最小的信任关系。当用户请求网格资源时，必须进行授权和审计。域之间信任关系的变化如图 3 所示。

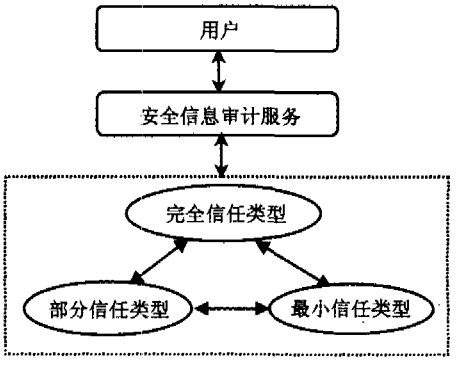

图 3 基于信任关系的动态审计机制

一个实体的信誉是对它行为的一个期望值，该期望值基

于一个给定时间特定的上下文环境中的其它实体的观察或实体过去行为的信息[7]。域之间信任关系的变化，根据 x 和 y 的直接关系以及 y 的信誉。信任值的计算由不同权重的直接信任关系和信誉两部分组成。信任关系指数的计算以及信任关系的转化如下：

(1)设 T_a 代表域之间的信任关系指数，其计算类似 I[7]，M 和 N 表示两个域，M 和 N 直接信任关系表示为 $DR(M,N)$，N 的信誉表示为 $RR(N)$，直接关系的权重和信誉关系的权重分别为 α and β，衰减函数为 $\gamma(t-t_{ij})$，这里 t 是当前的时间，t_{ij} 是最后修改时间或 M 和 N 之间最后交易的时间。文[7]引入推荐信任参数 R 来阻止在一个域中同组之间共谋的欺骗。本文中，代替上面提到的参数 R，审计反馈的结果表示为 R，R 的值在 0 和 1 之间。假设一个域与 K 个域之间进行交易，信任关系指数的计算如下：

$$T_a=\alpha * DR(M,N) * \gamma(t-t_{ij})+\beta * T_r \quad (1)$$

$$T_r=\frac{\sum_{k=1}^{n} RR(N) * R(M,N) * \gamma(t-t_{ij})}{K}$$

(2)设 T_η 表示信任关系转换的阈值，如果交易的双方是满意的，域之间的信任关系指数将增加。当 $T_a>T_\eta$ 时，最小信任关系类型将转化为部分信任关系类型，或部分信任关系类型转化为完全信任关系类型。如果交易的双方不满意，域之间的信任指数将减少。当 $T_a<T_\eta$ 时，完全信任关系类型将转化为部分信任关系类型，或部分信任关系类型将转化为最小信任关系类型。

3 基于 GT3 和 Aglet 平台的 CDSA 实现

3.1 基于 GT3 核的安全信息收集服务

本文中定义安全信息收集服务和移动 Agent 服务作为网格节点的用户定义服务[8,13]，这些服务建立在 GT3 核的上一层。移动 Agent 的服务作为 GT3 的一个内部服务，建立在 IBM 的 Aglet 上，通过修改相关组件完成。安全信息收集服务建立在登陆服务、管理服务、数据管理服务等系统层服务的基础上。建立在 GT3 核基础上的安全信息收集服务和移动 Agent 服务的结构如图 4 所示。

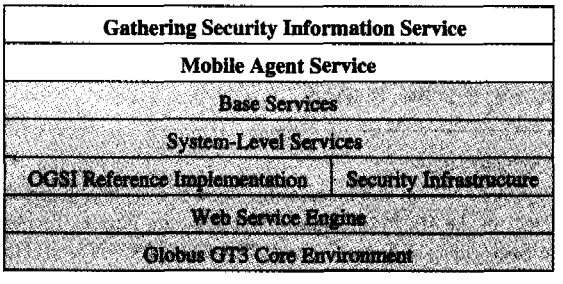

图 4 基于 GT3 核的用户定义服务结构

安全信息收集服务的实施如下：

```
Public class GatheringSecurityInformationImpl extends
  persistentGridServiceImpl {
Public GatheringSecurityInformationImpl() {
  Super(" Gathering Security Information Service ");
                                        }
public void postPersistentCreate (GridContext context)
  throws GridServiceException {
                                        }
                                        }
```

通过增加接口定义、WSDL 描述、stub/impl 文件，把安全信息收集服务部署到 GT3 容器。配置文件安全信息服务的部署如下：

(1)〈service name="ogsa/cmm/GatheringSecurityInformationService" provider = "Handler" style = "Wrapped" use="literal"〉

(2)〈parameter name = "allowedmethods"〉 value = "*"/〉

(3)〈parameter name="className"〉 value="org. ogsa. cor e. cmm. GatheringSecurityInformationPortType/〉"

(4)〈parameter name="baseClassName" value="org. ogsa. core. cmm. GatheringSecurityInformationImpl"/〉

(5)〈parameter name="persistent" value="true"/〉

(6)〈parameter name="schemapath" value="schema/core/ cmm/GatheringSecurityInformation_service. wsdl"/〉

(7)〈parameter name="handlerClass" value="org. globus. o gsa. handlers. RPCURIProvider"/〉

(8)〈parameter name="securityConfig" value="org/globus/ ogsa/impl/core/management/security-config. xml"/〉

(9)〈/service〉

3.2 基于 Aglet 的移动平台的构建

因为网格应用的特性与移动 Agent 的应用的特性非常相似，这两种应用均以构成站点的异质性和变化的信任关系为特征。每个 Agent 具有自治性、合作性、协调性、智能性、推理能力和与其它 Agent 的通信能力。本文利用移动 Agent 解决网格环境中跨域的安全审计问题。CDSA 是一个基于 GT3 的用户定义服务和 IBM Aglet 的分布式移动 Agent 系统，该系统由 6 种类型的 Agent 组成[9~12]：用户 Agent(UA)、中心移动 Agent(CMA)、信息收集 Agent(IGA)、数据库 Agent(DA)、查询 Agent(QA)、迁移 Agent(MA)，它们之间相互合作和协调共同完成跨域的安全信息收集、分析、监控以及控制用户的存取。移动函数如下：

```
int User_Agent(int);                          //用户 Agent
int Central_Mobile_Agent(string,int);
                                    //中心移动 Agent
int Information_Gathering_Agent( string,int );
                                    //信息收集 Agent
int Database_Agent(string,int);          //数据库 Agent
int Query_Agent(string,int);              //查询 Agent
int Migrate_Agent(URL,int).               //移动 Agent
```

(1)UA 提供对用户的服务，接受安全审计请求、返回审计结果。除此以外，用户 Agent 能够把请求转换成 Agent 能够识别的命令。

(2)CMA 是跨域安全审计结构实施的关键，它被用来收集和管理所有的安全审计信息，同时可以作为 CA 中心，确保 Agent 子系统之间的安全通信。通过数据库 Agent，所有 CMA 中的安全信息被存储到全局数据库。

(3)IGA 被分布在每个站点。当认证通过后，它被用来收集用户名、用户 ID、存取时间、用户的数值证书、任务管理权

限等信息。根据用户的请求,这些信息被送往 DA 或 MA。

(4)DA 被用作应用服务或数据库中间件,通过 Servlet 技术,在网格环境中,它被用来作为本地的数据库中安全存取数据接口。经过 DA,IGA 的所有安全信息被存取到本地数据库。

(5)QA 接受 UA 的请求,并根据用户的请求,在全局数据库中查询安全审计信息。如果全局数据库中没有用户的安全审计记录,通过 MA,用户的请求被分派到各个站点,然后在本地数据库中查询安全审计信息。

(6)MA 接收来自 QA 或 UA 的信息,这些信息能够从一个站点传输到另一个站点。

随着 Java 技术的快速发展,越来越多的应用选择纯 Java 语言。在本文中,我们选择基于 Java 的 IBM Aglet 作为移动 Agent 平台。一方面,由于 Java 语言跨平台的特性,有利于用户程序的开发和部署;另一方面、IBM Aglet 提供了移动 Agent 有效的编程模型和 Agent 之间动态的通信机制。此外,通过 Aglet 系统提供的上下文环境,Aglet 能够管理 aglet 的行为。利用 com. ibm. aglets. security 包,能够实现 Agent 的安全性,利用 com. ibm. maf. mAFAgentSystem 包,实现 Agent 的互操作性。利用 Servlet 技术完成与用户的交互,利用 KQML 完成 Agent 之间的通信。最后,通过代理提供安全的接口,当 Aglet 与远程 Aglet 连接时,系统在本地上下文环境中产生一个代理,类似于网格中的授权管理链。

3.3 用户审计服务

用户审计服务由底层的服务构建。审计需求处理使用 Apache AXIS 作为它们 Web 服务的引擎,所有服务在 J2EE/J2SE Web 容器中执行。这些服务也能够直接存取审计结果,监控异质资源和每一个节点的状态。

结论和未来的工作 网格安全的研究与实现是一个难度很大的课题。本文提出的跨域安全审计体系结构,是实现网格安全的一种新的尝试。获取安全的代价常常导致系统开销的增加。为了使安全机制的实施对网格性能产生的影响最小,本文所提出的一种新的授权安全机制"审计一次,授权多次"能有效地降低网格的开销。基于信任关系的动态审计策略非常符合网格自身的动态变化特性。基于 GT3 和 Aglet 平台的跨域安全审计体系结构的实现是本文研究工作的一次新的工程性探索。

未来的工作是计划通过实际复杂的应用来完善 CDSA 体系结构,并研究更优的审计策略。

参 考 文 献

1 Humphrey M, Thompson M R, Jackson K R. Security for Grids. Proceedings of The IEEE, 2005, 93(3): 644~652

2 GGF SAAAR RG. Grid Authentication Authorization and Accounting Requirements Draft 5. May 21, 2004. https://forge.gridforum.org/projects/saaa-rg/document/draft-ggf-saaar-reqs-5.txt/en/1

3 Thompson M, Olson D, Cowles R, et al. CA-Based Trust Model for Grid Authentication and Identity Delegation. Grid Certificate Policy Working Group, 2002

4 Mendes S, Huitema C. A New Approach to The X.509 Framework: Allowing A Global Authentication Infrastructure Without A Global Trust Model. In: Proceedings of NDSS'95, 1995

5 Ellison C, Frantz B, Lampson B, et al. SPKI Certificate Theory, Internet Request for Comments: 2693, 1999

6 Li T Y, Zhu H F, Lam K Y. A Novel Two-Level Trust Model for Grid. In: ICICS 2003, LNCS 2836, 2003. 214~225

7 Azzedin F, Maheswaran M. Evolving and Managing Trust in Grid Computing Systems. In: Canadian Conference on Electrical and Computer Engineering, IEEE CCECE 2002, 2002. 1424~1429

8 Foster I, Kesselman C, Nick J, et al. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. http://www.nesc.ac.uk/talks/ggf5_hpdcll/physio_o_grid220702.pdf

9 Gou X T, Jin W D, Zhang G X. Multi-agent Based Security Auditing System of Broadband MAN. In: Proceedings of the 2004 International Conference on Intelligent Mechatronics and Automation, Chengdu, China, 2004. 939~944.

10 Raghnnathan S, Mikler A, Cozzolino C. Secure Agent Computation: X.509 Proxy Certificates in a Multi-lingual Agent Framework. The Journal of Systems and Software, 2005, 75: 125~137

11 Shakshuki E, Ghenniwa H, Kamel M. A Multi-agent System Architecture for Information Gathering, Database and Expert Systems Applications 2000. In: Proceeding 11th International Workshop on, 2000. 732~736

12 Huang Y C, Chen Y, Li, et al. Research On Network Secure Auditing System Using Distributed Agents. In: Proc. of IEEE TECCON'02, 2002. 391~395

13 战晓苏,张少华译. 网格计算. 北京:清华大学出版社,2005

(上接第 6 页)

13 Behrmann G, Bouyer P, Larsen K G, et al. Lower and Upper Bounds in Zone Based Abstractions of Timed Automata. In: Proc. of the 10th International Conf on Tools and Algorithms for Construction and Analysis of Systems (TACAS '2004), Barcelona, Spain, 2004

14 ZHAO Jianhua, LI Xuandong, ZHENG Tao, et al. Removing Irrelevant Atomic Formulas for Checking Timed Automata Efficiently. In: Proc. of First International Workshop on Formal Modeling and Analysis of Timed Systems (FORMATS), Marseille, France, 2003, LNCS 2791: 34~45

15 Godefroid P. Partial-order methods for the verification of concurrent systems: an approach to the state-explosion problem. LNCS1032, Springer-Verlag, January 1996

16 Peled D. All from one, one for all: on model checking using representatives. In: Proc. of the 5th International Conference on Computer Aided Verification (CAV'1993), Elounda, Greece, 1993, LNCS697: 409~423

17 Pagani F. Partial orders and verification of real-time systems. In: Proc. of the 4th International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems (FTRTFT'96), Uppsala, Sweden, 1996, LNCS1135: 327~346

18 Bengtsson J, Jonsson B, Lilius J, et al. Partial order reductions for timed systems. In: Proc. of 9th International Conference on Concurrency Theory (CONCUR'98), Nice, France, 1998

19 Minea M. Partial order reduction for model checking of timed automata. In: Proc. of 10th International Conference on Concurrency Theory (CONCUR'99), Eindhoven, Netherlands1999, LNCS1664: 431~446

20 Zhao Jianhua, Xu He, Li Xuandong, et al. Partial Order Path Technique for Checking Parallel Timed Automata. In: 7th International Symposium on Formal Techniques in Real-Time and Fault Tolerant Systems (FTRTFT 2002), University of Oldenburg, Germany, 2002: LNCS2469. 417~432