EH_GRBAC:遍在计算环境中基于知识的访问控制原型

张向刚　张云勇　刘锦德

(电子科技大学计算机科学与工程学院微机所　成都610054)

EH_GRBAC: A Knowledge-Based Access Control Prototype for Pervasive Computing

ZHANG Xiang-Gang　ZHANG Yun-Yong　LIU Jin-De

(College of Computer Science and Engineering, UEST, Chengdu 610054)

Abstract In pervasive computing environment, users can access to various information, resources and services at anytime and anywhere, so access control has become an exigent security problem. In the traditional access control modes, the decisions of access control are entirely dependent on the results of authentication. The access control cannot provide the security-relevant fault-tolerant function. But in pervasive computing environment, because of the various reasons, security system can't assure the results of the authentication are absolutely correct. So we propose to use the knowledge-based access control, which can discovery some rules and knowledge from the previous process of access control and combine these rules with traditional access controls to perfect the security system. The essence of knowledge-based access control is to add some intelligent authentication function into the process of access control. In the paper, we expatiate the idea and principle of knowledge-based access control, as well as the advances of this method. Furthermore, we implement a prototype, called EH_GRBAC, which can discovery historical knowledge from the history of users' using resources to reinforce GRBAC. In the paper, we also explain the architecture and the details of EH_GRBAC.

Keywords Pervasive computing, Access control, Knowledge discovery, Security-relevant fault-tolerance, GRBAC, RBAC

1　基于知识的访问控制

随着计算机和通信技术的发展,各种小型、智能和移动设备(如:移动电话和PDA等)正在成为计算的主流。计算组件通过各种方式嵌入到各种各样的设备中,并且通过各种形式存在于我们生活和工作的方方面面。这就是所谓的遍在计算*。在遍在计算环境中,各种设备通过网络连接到一起,能够让用户更简单、更普遍、更可靠、更直接地访问和使用各种资源和设备,并且不需要更多的专业知识。然而,这种环境的成功运行将极大地依赖于它所能够提供的安全能力。在诸多安全问题中,访问控制已经成为一个非常紧迫的问题。因为遍在计算环境需要向用户提供对资源更广泛的访问,所以,如何提供一种安全的访问控制机制来保证合法用户的授权使用,同时防止非法用户的侵入显得非常必要。

当前存在三种主要的访问控制机制:DAC(discretionary access control)、MAC(mandatory access control)、RBAC和GRBAC(role-based access control and generalized role-based access control)。这些访问控制模式的设计思想都是根据用户、环境、资源等各种情况来共同确定用户的访问权限,这些传统的访问控制模式有一些固有的安全缺陷。首先,访问控制的控制决策都基于认证过程的结果,这种线性的过程有一个缺点是攻击者一旦通过前面的过程将毫无阻难地通过后面的过程,即安全系统不具有容错功能[1],例如:如果一个假冒者窃取了密码同时通过了认证,他能够随意访问合法用户的授权资源,而访问控制系统将不能够意识到所受的攻击。但是在现实生活中,由于系统、人为及环境等各方面因素,我们往往不能够完全保障认证过程的安全性,特别是在遍在计算的环境中,由于设备的异构性,分布的广泛性,连接的多通道性、用户的移动性和复杂性等因素,要求认证过程绝对正确和安全比较困难。其次,在传统的访问控制模式中安全策略需要通过管理人员进行建立和更改,所以这必将增加系统管理人员的负担,特别是在遍在计算这样的环境中,因为用户众多,而且移动性较强,所以管理工作尤为繁重。

针对这样的问题,我们提出了基于知识的访问控制,其思想是:在遍在计算环境下,由于个人的兴趣、爱好、行为习惯、工作内容,以及环境和资源自身的各种特征,不同用户对资源的访问会表现出不同的规律和趋势。比如:用户使用资源的概率和趋势,用户操作事务的概率,以及系统的负载分布等。将这些知识运用到传统的访问控制中,能够增强传统访问控制模式,克服传统模式的缺点,形成一个更加完善的访问控制系统。其实质是发现知识,然后将这些知识运用到访问控制的过程中,在访问控制的过程中自动融入一定的认证功能,以此来提供安全系统的安全容错性。如果用户的请求符合这些规律,安全系统认为该请求是正常的,反之,认为该请求是异常的。

张向刚　博士生,主要研究领域为:中间件与遍在计算。张云勇　博士生,主要研究领域为:中间件与agent技术。刘锦德　教授,博士导师,主要研究领域为:开放系统与中间件技术。

* 遍在计算,英文为prvasive computing或ubiquitous computing,意思为无处不在的计算,国内文章一般译为普及计算,但"普及"一词易与推广基础知识的意识相混淆,所以用"遍在计算"一词来表达计算的无处不在更为贴切。

对于异常的请求，安全系统将执行更加严格的安全策略或者直接拒绝该请求。例如：公司的 CEO 能够阅读有关公司技术、财务和销售的所有文档，但是在日常的工作中，他总是阅读相关方面总体性的报告，而很少涉及有关技术细节这样的文档。安全系统通过一定时间的运行能够了解到这样的规律，以后如果系统收到了一个 CEO 的要求阅读技术细节的请求，系统会因为该请求不符合 CEO 的日常规律而怀疑请求的可信度，要求用户提供进一步的认证信息并且对这些请求实施更严格的访问控制过程。这样既能够保证用户的全部权限，同时又增加了一定的安全容错性。其实，这种安全保证模式广泛存在于现实生活中，例如：门卫对来访者的检查不仅要检查来访者提供的证件，同时也会注意到来访者的表情和眼神等情况，对于那些神态慌张者肯定会进行严加盘问。

同时，因为用户只有在访问控制的过程中，才能够表现出其独特的行为特性和其它规律，所以，我们不能在认证过程中完成这个功能。同时，因为用户的行为特性、资源访问趋势等个性化的知识不容易被假冒进攻者所模仿，因此基于知识的访问控制能够有效地防止假冒者的进攻。此外，因为发现知识和基于知识的访问控制过程完全可以自动完成，所以也不会增加管理员人员的负担。

需要指出的是基于知识的访问控制不是一个完整的访问控制模式，它需要和传统的访问控制模式相结合，因为很多这样的知识是一种概率和趋势，而且常常是动态的，所以只能够运用它们来协助判断，而不能用它们进行最终的判断。例如：和 GRBAC 相结合，我们实现了一个原型：EH_GRBAC，它能够根据用户以前对资源的访问历史，发掘一些知识和规律。并将这些知识运用到 GRBAC 模式的访问控制中。在这个原型中，安全系统根据用户以前对资源的访问情况来推断用户将来对资源的访问情况。通过这种方式，系统能够自动提高安全能力。

本文首先回顾了基于角色的访问控制：传统的基于角色的访问控制(RBAC)和基于广泛角色的访问控制(GRBAC)，这是因为 EH_GRBAC 是建立在 GRBAC 的基础之上；然后说明 EH_GRBAC 的体系结构；阐述 EH_GRBAC 的细节。最后，对相关工作进行了一定的比较，总结全文。

2 RBAC 和 GRBAC

在 RBAC[2](role-based access control)中，系统根据用户自身的特性(如在公司的职位、从事的工作等)，将他们分归于不同的主体角色(subject- role)，所谓角色也就是具有相同属性的一类实体。一个用户可以属于多个角色，同时一个角色可以拥有多个用户。每个角色在一定的资源上拥有进行某些事务的权力，具有某个角色的用户能够在角色允许的资源上进行授权操作。RBAC 比较适合大的、结构化的组织，因为通过主体角色来划分权限，与现实中的人员组织和分工比较相似，并且用角色来控制用户的权限有利于人员的工作变动。但是这种模式受限于它只针对主体进行了划分角色，而没有考虑到访问对象和周围环境的特性，所以它不能支持更加灵活的访问控制，例如它不能支持基于时间的访问控制策略，也不能支持基于对象的访问控制策略。而这些访问控制策略在现实中是非常必要的。例如：我们往往需要如像“孩子能够在7:00pm 到9:00pm 之间看电视”这样的访问控制策略。所以，人们扩展了 RBAC，提出了 GRBAC(generalized role-based access control)，通过这种模式达到更加灵活的访问控制。

在 GRBAC[3]中，不仅将用户划分为不同的主体角色(subject-role)，而且引进了对象角色(object-role)和环境角色(environment-role)。所谓对象是指一切可利用资源，根据对象的相关特性(特别是安全属性)，将对象划分为不同的类，称为对象角色；所谓环境角色是指一些环境信息的分类。引入这两个角色有利于定义一些以环境为中心的和以对象为中心的安全策略。此外，事务也是 GRBAC 的一个重要的概念，所谓一个事务是指能够在系统中运行的一个特定行为。在 GRBAC 中，一个事务被表达成一个四元组的形式：

$$T=(SRole, ORole, ERole, op)$$

其中 T 代表事务标示符，SRole 代表主体角色，ORole 代表对象角色，ERole 代表环境角色，op 代表在这个事务中需要执行的操作(如：读、写或执行等)。整个四元组的完整语义表示：一个具有 SRole 角色的用户，可以在 ERole 角色指定的环境条件下，对 ORole 角色中的对象进行 op 操作。整个 GRBAC 系统包含一个或多个策略数据库，每个策略数据库包含一系列的策略规则(policy rule)，每个策略规则具有(T，pb)这样的形式，其中 T 代表一个具有以上四元组形式的事务，pb 是一个“允许/拒绝”位，表示该事务是被允许还是被拒绝。整个系统首先是安全管理者制定安全规则，形成安全策略数据库，然后以后的访问需要根据安全策略库中的策略规则进行访问权限的判断。

GRBAC 的优越性主要体现在两个方面，第一是概念简单，因为它只基于角色这样一个中心概念，其次是具有较强的表达能力，将角色这一概念广泛应用到主体、对象和环境，通过三种角色的不同组合能够表达很多不同情况。

3 EH_GRBAC 体系结构

EH_GRBAC (Extend History _Generalized Role-Based Access Control)是一个基于 GRBAC，同时增加了基于知识的访问控制策略的访问控制原型。

在现实世界中，人们对资源的访问会表现出一定的倾向性，即：某用户根据一个具体的访问控制模式能够访问一定的资源和进行相应的操作，但是他对这些资源的访问概率并不是相同的，一些资源的访问频率较高而对另一些资源却很少问津，这种资源访问的倾向性能够体现特定用户所独有的行为习惯和工作特征，因此，我们可以运用这样一些知识来进行用户的识别。例如：在公司，CEO 能够访问所有的文档，但是因为工作性质，他需要经常访问那些总体性的报告，却很少访问有关技术细节和财务细节的文档。在家庭中，某家庭主妇经常使用电冰箱、烤炉这些设备，虽然她也有使用计算机的权限，却很少使用。系统通过一段时间的运行，能够发现这些规律和趋势，在以后的访问控制中，如果用户的请求符合这些趋势，安全系统就认为这个请求是正常的，是符合用户行为习惯的，反之，认为请求是异常的。对于后者，因为它不符合用户日常的行为习惯，所以系统有理由怀疑请求的可信度，因此系统将要求用户提供进一步的口令，来确认用户的身份，以此来提供系统的安全容错性。这种访问控制过程的实质是将用户映射为操作的一个子集，如果用户的请求属于这个子集，安全系统认为请求是正常的，反之系统会认为请求是异常的，需要用户提供进一步的口令来进一步确认其身份。这种映射的思想可以通过图1形象地表现出来。其中，授权集表示用户根据 GRBAC 中的策略被赋予的可操作事务集，而正常集表示系统根据用户使用资源的历史情况而总结出来的用户经常操作

的事务集。

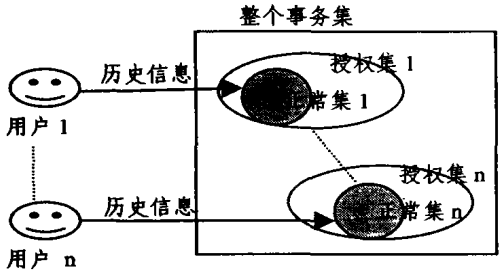

图1 EH_GRBAC 原理图示

我们也能够通过以下的公式来表达这种思想。

$HK_n = FUNC_H(user, HI_n, HI_{n-1}, \cdots, HI_1)$

Normal set = $FUNC_N(user, HK_n)$,

HK_n 表示从某特定用户前 n 次访问过程中发现的知识。HI_n 表示该用户第 n 次访问资源的历史信息。$FUNC_H$ 和 $FUNC_N$ 是两个功能。前者从该用户的 HI_n 到 HI_1 中总结出该用户的 HK_n；后者将 user 和 HK_n 映射成该用户的正常集。User 表示一个确定的用户，两个功能都需要和特定的用户相关联。如果用户的请求属于他的正常集，请求被通过，反之，安全系统将要求用户提供进一步的口令。

这种分阶段递进式地要求口令的方式相对于认证过程中一次性要求用户提供全部口令，然后在访问控制过程中不再提供认证功能，其优势在于：这种策略更具有安全容错性。在认证过程要求用户提供全部的口令，会造成口令的频繁使用，必然会增加口令不安全的因素，例如：如果一旦系统遭受到特洛伊木马病毒的袭击，就会造成口令的全部丢失。而在分阶段递进式要求口令的策略中，因为高级口令的使用频率较低，所以安全性相对较好。此外，虽然在 EH_GRBAC 中，知识仅用作协助识别用户，但是在其它的系统中，我们完全可以运用一些确定性的知识来进行用户的最终认证。

EH_GRBAC 体系结构如图2所示，其中各部件含义如下。

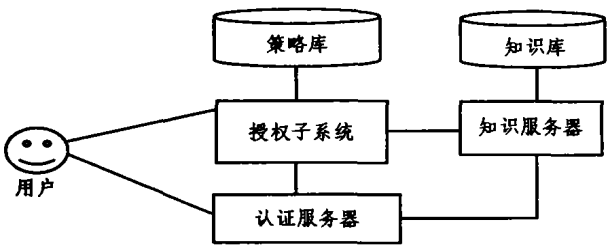

图2 EH_GRBAC 体系结构

认证服务器提供用户在遍在环境中登录时的初始认证；授权子系统的功能是提供用户对资源的访问控制，它是基于 GRBAC 模式，其并不是一个简单的服务器，它包括若干服务器和传感设备，具体细节可参见文[3]，它与 GRBAC 模式中授权子系统的区别在于它在授权时需要与知识子系统进行交互，以确定用户的行为是否满足一定的规律。知识服务器也可能不仅仅是一个简单的服务器，它可能包括若干相互协作的服务器和其他设施，但是在 EH_GRBAC 中知识服务器仅仅是一个服务器，它不断地了解用户对资源的访问历史，并总结出相应的规律和知识。在授权子系统和知识子系统中都包含一个数据库，它们分别是策略库和知识库，分别记录安全策略和历史知识。

4 EH_GRBAC 工作流程

在 EH_GRBAC 中，访问控制过程被分为两个阶段。首先，授权子系统检查请求是否符合策略库中的策略，授权子系统采用 GRBAC 模式；然后，知识子系统检查已经通过授权子系统的请求是否符合知识库中的知识。我们能够用形式化的语言描述这个过程：

```
IF（请求通过了授权子系统）
  THEN
    IF（请求符合知识子系统中的规律）
        THEN 请求通过整个访问控制过程
        ELSE
            IF（用户提供正确的高级口令）
                THEN 请求通过整个访问控制过程
                ELSE 拒绝该请求
  ELSE
      拒绝该请求
```

4.1 授权子系统细节

在 EH_GRBAC 中，任何事务被表达成一个4元组 T = ⟨SRole, ORole, ERole, op⟩。当系统接收到一个请求，授权子系统使用 GRBAC 模式来仲裁请求是否满足策略库中的安全策略。其细节可参见文[3]。

4.2 知识子系统细节

知识子系统由知识服务器和历史知识数据库构成。知识服务器从历史信息中发掘相关的规律和知识，历史知识数据库存储相关的历史知识。具体地讲，EH_GRBAC 的历史知识数据库包含一系列的表格，每个表格对应一个用户账号。我们在每个表格中存储相应账号所能执行的全部事务，并且将它们按照一定次序排列成一个队列。在知识库中事务被表达成⟨T, TIME⟩，这里 T 具有⟨SRole, ORole, ERole, op⟩的形式，其含义和 GRBAC 事务的意义相同。TIME 表示该事务最近一次的执行时间。每个表格有一个有效值，如果事务在队列中的位置小于或等于有效值，那么这个事务属于相应账号的正常集。在队列中，有效值以后的事务属于异常集，我们通过如下的算法来排列表格中的事务。

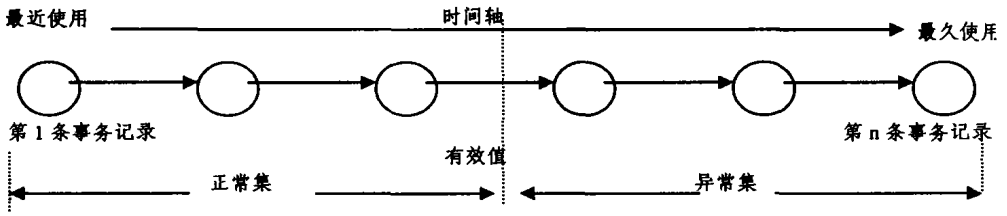

图3 知识库中表格结构示意图

1）在知识数据库初始化时，我们将某个账号能够操作的所有事务拷贝到其对应的表格中，并且使其具有如下的形式：

〈T,TIME〉,这里 TIME 等于初始化该表格时的系统时间。事务的排列次序是任意的。

2) 当事务 T_i 被执行后,运用〈T_i,new_time〉去替换旧的〈T_i,TIME〉,并且将这条记录插到事务队列的最前面,这里 new_ time 代表事务 T_i 的执行时间。

3) 设置该表的有效值 V=0,检查该表格的所有事务,如果(系统的当前时间)-(〈T_i,TIME〉中的 TIME)≤168小时(i=1,2,3,…),则 V=V+1;(这里168小时不是一个固定的值,我们需要根据具体情况调整这个值,在 EH_GRBAC 我们认为168小时内没有操作的事务是很少执行的事务)。

4) 当另一个事务执行后,重复步骤2) 和3)。

我们能够通过图3来表达知识库中表格的结构。

当一个请求通过了授权子系统,知识子系统将判断该请求是否属于相应的正常集,如果它属于正常集,该请求通过访问控制,反之,系统要求进一步的口令,如果用户能够提供正确的进一步口令,请求将通过访问控制,否则被拒绝。

5 相关工作

以下我们将介绍一些相关工作,并且将它们和基于知识的访问控制进行比较。

GRBAC:我们已经在第2节讨论了 GRBAC。GRBAC 通过三种角色的组合能够表达很多情况。但是在这种模式中,访问控制过程完全依赖于认证过程的结果。GRBAC 和基于知识的访问控制相结合能够克服单独运用 GRBAC 的缺点,为系统提供一定的安全容错功能。

上下文感知的访问控制:在文[4]中,Covington 讨论了上下文感知的访问控制,它主要是基于环境角色。而基于知识的访问控制是基于知识和规律。环境角色能够表达各种环境状态,但是知识具有更加广泛的含义,它不仅可以包含各种环境信息,而且包含各种从系统运行中总结出来的带有一定规律性的知识。

自适应安全模式:在文[5]中,Covington 通过参数化认证过程设计了一种能够提供自适应安全级别的模型。这个模型根据传感器的信息提供自适应的认证过程。这个模型和 EH_GRBAC 之间主要存在三个区别:首先,在 Convington 模型中,传感器提供的信息主要包括:用户生理信息、口令和识别卡等等,但是基于知识的访问控制策略中,知识不仅可以包括这些信息,而且包括诸如:用户习惯和访问趋势等动态信息。这些知识需要从以前的访问控制过程中进行发掘。特别地,convington 的模型在认证过程中引入了历史信息,但这种信息是指用户操作的上下文以及以前的认证请求。EH_GRBAC 中的历史知识是指从历史信息中总结出来的知识,例如:用户习惯、访问倾向等等。其次,在 Covington 的模型中,认证和访问控制是两个前后过程,但是,在基于知识的访问控制中,我们在访问控制中融入了认证过程。因此,基于知识的访问控制过程能够意识到通过了认证过程的假冒者的进攻,提供一定的安全容错性。第三,在基于知识的访问控制中,基于知识的认证功能不可以在认证阶段完成,因为用户的行为和访问倾向只能在访问控制的过程中才能表现出来。

小结 本文提出了一种新的访问控制策略:基于知识的访问控制策略。在遍在计算的环境中,因为个人的兴趣、行为习惯和工作内容,用户对资源的访问会表现出一定的规律。基于知识的访问控制策略正是利用这些知识和规律,在访问控制的过程中增加额外的认证功能。这种模式相对于传统的访问控制模式具有一些独特的优势:诸如个人兴趣、行为习惯等信息不容易被假冒者模仿,所以系统能够使用这些知识来提供安全容错功能。但是基于知识的访问控制模式不是一个完整的访问控制模式,它需要和传统的访问控制模式相结合来提供一个完善的安全系统。

参 考 文 献

1 张向刚,刘锦德. 多密钥 KDC 的安全容错性及其性能分析. 电子科技大学学报,2001,30(6): 596~599

2 Ferraiolo D,Kuhn R. Role-Based Access Control. In:Proc. of 15th National Computer Security Conf. 1992

3 Moyer M J,Ahamad M. Generalized Role Based Access Control. In:Proc. of the 2001 Intl. Conf. on Distributed Computing Systems (ICDCS), Oct. 2001

4 Covington M J,et al. Securing Context-Aware Application Using Environment Roles. In:Proc. of SACMAT, May 2001

5 Covington M J,Ahamad M,Venkateswaran H. Providing Adaptive Security through Parameterized Authentication. In:2002 IEEE Symposium on security and privacy, May 2002

(上接第147页)

14 Fisher S. Relational Grid Monitoring Architecture. http://hep-unx.rl.ac.uk/grid/wp3/release.html

15 Fisher S. Relational model for information and monitoring. GGF International Draft GWD-GP-7-1. http://www.gridforum.org/1_GIS/RDIS.htm

16 Baker M,Ong H,Smith G. A Prototype Grid-site Monitoring System. http://homer.csm.port.ac.uk/publications/technical/reports/grid/DSGmonitoring.pdf

17 GridRM Project. University of Portsmouths , U.K. http://homer.csm.port.ac.uk/projects/research/grid/grid-monitoring/

18 MDS 2.2 User's Guide. http://www.globus.org/mds/mdsusers-guide.pdf

19 Global Grid Forum Information Systems and Performance Area. http://www.gridforum.org/1_GIS/GIS.htm

20 European DataGrid wp3(Grid Monitoring Services) http://hep-unx.rl.ac.uk/edg/wp3/

21 查礼,徐志伟,林国瑾,刘玉树,刘东华,李伟. 基于 LDAP 的网格监控系统. 计算机研究与发展,2002,39(8)