基于角色和任务的CSCW系统访问控制技术研究

朱 君[1,2] 汤 庸[1]

(中山大学信息科学与技术学院 广州 510275)[1] (东莞理工学院计算机学院 东莞 523808)[2]

摘 要 针对现有方法不能很好地满足CSCW系统对访问控制的需求,提出基于角色和任务的CSCW系统访问控制模型RTBAC(Role and Task-Based Access Model)。该模型形式化地描述了用户、角色、任务、权限、工作流等要素及其相互间的关系,通过分配和取消角色来完成对用户权限的授予和取消,并提供了角色间偏序继承和指派关系定义,通过引入任务概念、任务类型划分及角色和任务之间的关系定义,实现了依据任务和任务状态不同对权限进行动态管理。该模型是针对CSCW系统多用户、动态、协作等特性提出的,能较好地满足CSCW系统对访问控制的需求。

关键词 CSCW,访问控制,角色,任务

中图法分类号 TP311 **文献标识码** A

Study of the Role and Task-based Access Control Technology for CSCW System

ZHU Jun[1,2] TANG Yong[1]

(School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, China)[1]

(School of Computer Science, Dongguan University of Technology, Dongguan 523808, China)[2]

Abstract CSCW systems have many new requirements for access control, which cannot be met by existing models. In this paper, a new role and task-based access model (RTBAC) was presented to meet these requirements. This model formally describes the relationship between the key elements of access control such as user, role, task, privilege, and workflow. The model grants and revokes access privileges of users by assigning them roles and canceling their roles, and provides partial inheritance and delegation between roles. In this model the conception to task was introduced, group tasks were divided into workflow task and independence task, and the relationship between roles and tasks was described. From those the model can dynamically manage the permissions through tasks and tasks' status. RTBAC model is brought forward aiming at accommodating with the characteristics of collaborative systems such as multi-user, dynamic, and collaboration. It can meet the requirements for access control in CSCW system adequately.

Keywords CSCW, Access control, Role, Task

1 引言

计算机支持的协同工作(CSCW)自1984年由MIT的Irene Grief和DEC的Paul Cashman正式提出以来,该领域的研究和应用一直受到极大的关注和重视。CSCW为分布式网络环境、开放式协作环境中的用户间提供协同处理和资源共享等任务。安全性问题是CSCW系统能有效提供协同工作的基础,这里的安全问题主要指来自计算环境内部的资源窃取与来自外部的敌意攻击。协作者之间如何安全地共享数据资源、采用何种访问控制策略模型、如何对协同者进行身份鉴别和认证,都是CSCW系统安全面临的关键性问题[1,2]。

从20世纪70年代以来,出现了多种访问控制模型。目前使用频率较高的主要有自主访问控制模型(Discretionary Access Control, DAC)、强制访问控制模型(Mandatory Access Control, MAC)和基于角色的访问控制模型(Role-Based Access Control, RBAC)[3]。自主访问控制DAC中,访问权限的授予是可以传递的,一旦访问权被传递出去将很难得到控制,会带来严重的安全问题。MAC源于对信息机密性的要求以及防止特洛伊木马之类的攻击,虽然增强了信息的机密性,但不能实施完整性控制。在CSCW系统中,对信息的完整性、授权管理和策略配置的便捷性要求较高,而DAC和MAC难以提供这方面的支持。

1992年Ferraiolo和Kuhn提出了基于角色的访问控制模型(RBAC模型)[4]。RBAC模型简化了系统的授权管理过程,通过引入角色实现了用户与权限的逻辑分离。然而,虽然在授权管理上RBAC在使用过程中大大降低了授权管理的复杂性、成本和发生错误的概率,但是由于RBAC模型授权是静态的,没有考虑操作的上下文,授权机制不能适应CSCW环境的动态变化。另外,主体拥有权限的周期长,主体在执行完成任务后继续拥有权限,不符合"最小特权原则",同时其对

到稿日期:2009-07-02 返修日期:2009-10-23 本文受国家自然科学基金(60673135),重点项目(60736020),广东省自然科学基金(7003721),广东省科技攻关(07B010200052),广州市科技计划(07Z3-D3191),东莞市科技计划项目(2007108101020)资助。

朱 君(1976—),女,副教授,CCF会员,主要研究方向为角色协同、CSCW等,E-mail:amberzj@dgut.edu.cn;汤 庸(1964—),男,教授,CCF高级会员,博士生导师,主要研究方向为数据库与协同软件、时态信息处理技术。

CSCW 授权过程中的特别约束也支持不够。

为了满足 CSCW 系统中对访问控制方面的需求，本文首先深入分析了影响该类系统访问控制的因素，总结了 CSCW 系统对访问控制的详细需求，然后针对这些需求提出了基于角色和任务的控制模型，并进一步讨论了本模型的安全性和应用实例。

2 CSCW 系统的访问控制需求

2.1 CSCW 系统中与访问控制有关的因素

为了提出适应 CSCW 系统的访问控制模型，我们需要深入了解这类系统的访问控制需求。下面先分析在 CSCW 系统中影响访问控制的因素有哪些。从访问控制的角度出发，CSCW 系统可以用图 1 来描述。

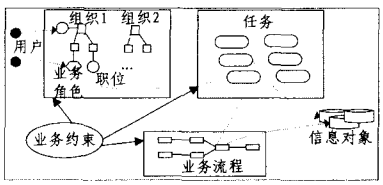

图 1 影响 CSCW 系统中访问控制因素图

从图 1 中可以看出，CSCW 系统中，影响访问控制的主要因素有以下方面：组织结构、业务角色（职位）、任务、业务约束、业务流程、信息对象。担当组织中某个职位（业务角色）的用户在一定业务规则的约束下执行分配给他的任务，从而访问该任务需要的信息对象。其中用户是访问控制的主体，信息对象是访问控制的客体，包括了诸如文件、数据表、可执行程序等资源。任务是业务流程的基础，业务流程可以在计算机系统中用工作流的形式来表示。但是不是所有的任务都必须属于某一业务流程。对于属于某业务流程的任务和独立性任务的访问控制方法应当是不同的。

2.2 访问控制需求

在前人研究的基础上[5-9]，并通过 2.1 节对 CSCW 系统中影响访问控制因素的分析，可以看出 CSCW 系统中对访问控制有独特的需求，归纳为以下几点：

1）用户只能访问执行任务所需的信息对象，即满足“最小特权原则”；

2）组织结构对用户权限是有影响的，业务角色存在层次关系，应当提供角色之间的权限继承能力；

3）角色允许存在私有权限，在该角色被继承时，私有权限不被继承；

4）提供方便的授权/取消机制和操作合法性检查机制；

5）用户之间提供必要的转授权关系；

6）对属于业务流程类型的任务应当根据业务流程的执行动态分配权限；

7）对属于业务流程类型的任务，任务之间存在着多种操作依赖，在访问控制方法中应提供适当的支持。

3 基于角色和任务的访问控制模型（RTBAC）

针对 2.2 节中的访问控制需求，我们提出了基于角色和任务的访问控制模型 RTBAC（Role and Task-Based Access Model）。

3.1 RTBAC 模型概述

RTBAC 模型中，涉及到访问控制的要素包括用户、角色、任务、工作流、权限、约束、对象，这些要素之间的关系从图 2 中可以看出。RTBAC 模型来源于 RBAC 模型，具有 RBAC 模型的很多特性。从图 2 中得知，RTBAC 模型与 RBAC 模型主要差别在于 RTBAC 中权限不是直接授权给角色，而是授权给任务。用户通过角色分配 UR 分配得到合适的角色，再通过角色任务分配 TR 将任务分配给角色。用户在会话过程中，以某种角色执行一项任务，从而获得该任务具有的权限。使得在 RTBAC 中，对象的访问权限控制不是静止不变的，而是能随着执行任务的上下文环境发生变化，从而从任务的角度来建立安全模型。

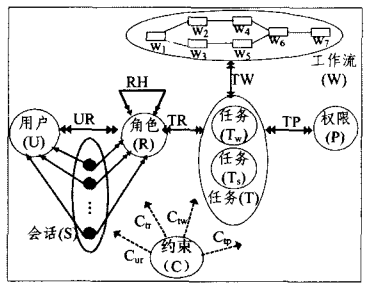

图 2 RTBAC 模型图

3.2 RTBAC 模型定义

定义 1（基本集合定义） 集合 U,R,T,C,P,S,W 分别代表用户 User、角色 Role、任务 Task、约束 Constraints、权限 Permission、会话 Session、工作流 Workflow。

定义 2（任务及分类定义） 任务是用户需要处理的工作集合，简称任务集 T。任务具有多种形态，只有当任务处于运行态时，权限才能被授予。当任务完成后，权限即被收回。在 CSCW 环境中，任务是组成业务流程的工作单元，是一个可独立区分的动作，可能与多个用户相关，也可包括多个子任务。在 CSCW 环境下，任务 T 分为两类：独立性任务 T_S 及流程性任务 T_W。两类任务中均包含私有任务 T_P，即 $T=T_w \cup T_s$，且 $T_w \cap T_p \neq \emptyset, T_s \cap T_p \neq \emptyset$。

定义 3（指派关系定义）

1）$UR \subseteq U \times R$，一个多对多的二元关系，负责将用户指派给角色；

2）$TR \subseteq T \times R$，一个多对多的二元关系，负责将任务指派给角色；

3）$TP \subseteq T \times P$，一个多对多的二元关系，负责将权限指派给任务；

4）$TW \subseteq T \times W$，一个多对多的二元关系，负责将任务指派给工作流，此处的任务只能是 T_W 类型；

5）$user: S \rightarrow U$，从每个会话 s_i 到一个用户 $user(s_i)$ 之间建立的函数映射（此映射在会话的生存期间保持不变）。

定义 4（约束定义）

1）C_{ur} 是角色约束集，限制用户与角色之间的映射关系；

2）C_{tr} 是任务约束集，限制任务与角色之间的映射关系；

3）C_{tp} 是权限约束集，限制任务与权限之间的映射关系；

4）C_{tw} 是工作流约束集，限制工作流与任务之间的影射关系。

定义 5（角色继承关系定义）

$RH \subseteq R \times R$ 是在 R 上的偏序关系，称为角色层次或角色继承关系，记为 $\geqslant$。在 RTBAC 模型的角色继承关系中，如果角色 r_1 是角色 r_2 的上级角色，那么 r_1 只能从 r_2 继承非 T_p

类任务，即 $r_1, r_2 \in RH: r_1 \geqslant r_2 \Rightarrow r_1$ 继承 $\cup(T_i), T_i \in r_2 \wedge T_i \neq T_p$。

定义 6(角色指派关系定义)

$\forall r_1, r_2, r_3 \in R$，如果具有角色 r_1 的用户可以把角色 r_3 赋予具有角色 r_2 的用户，则称 r_1 对 r_2 具有在 r_3 上的指派关系，记为 $r_1 \xrightarrow{r3} r_2$[7]。

定义 7(流程性任务 T_W 性质定义)

如果任务是流程性任务 T_W，那么它应该具有以下属性：

1)激活条件(Activation Condition, AC)：AC 是任务 T_{wl} 能否被执行的条件。如果 $AC=T_{w1} \wedge T_{w2}$，那么当 T_{w1} 和 T_{w2} 都执行完成后，此时 AC 的值为真，否则为假，且 T_{Wl} 可以被激活。

2)激活标记(Activation Flag, AF)：AF 是任务 T_W 处于激活状态的标记。如果 T_W 是激活状态，那么 AF 为真，反之为假。

3)激活可持续时间(Activation Duration Time, ADT)：ADT 表示任务 T_W 可以处于激活状态的时间长度。当任务 T_W 被激活时间达到 ADT 长度后，任务 T_W 马上转入非激活状态。

定义 8(流程性任务 T_W 关系定义)

在 RTBAC 模型中，流程性任务 T_W 间存在着下列关系：

1)顺序关系：当 $t_{w1}, t_{w2} \in T, r_1, r_2 \in R$ 时，若在同一业务流程中，r_1 必须在 r_2 执行 t_{w2} 之后执行 t_{w1}，则称 t_{w1}, t_{w2} 为顺序任务；

2)相容关系：当 $t_{w1}, t_{w2} \in T, r_1 \in R$ 时，若在业务流程中 r_1 能同时执行 t_{w1} 和 t_{w2}，则称 t_{w1} 和 t_{w2} 为相容任务；

3)相斥关系：当 $t_{w1}, t_{w2} \in T, r_1 \in R$ 时，若在业务流程中 $r1$ 不能同时执行 t_{w1} 和 t_{w2}，则称 t_{w1} 和 t_{w2} 为相斥任务。

任务关系的集合称为任务关系集，记为 $TT, TT \subseteq T \times T$。

定义 9(权限激活)

如果任务是流程性任务 T_W，权限 P_i 被分配给 T_W，授权用户可使用权限 P_i 的条件是 T_W 的激活标记(AF)为真。

3.3 RTBAC 模型访问控制策略

RTBAC 模型是一个随时间、任务执行上下文发生变化的动态访问控制模型。用户获得任务执行权限的过程，是一个动态交互的过程。在业务流程的执行过程中，系统根据任务的类型、任务的状态和约束条件等条件决定任务访问权限的许可。

在 RTBAC 模型中，访问控制的过程分为权限分配、动态权限调整两个阶段。

1)权限分配

权限分配过程中，系统管理员需要进行下列工作：系统角色定义；用户分配角色 UR；任务定义及任务 T_S、T_W 类型划分；将 T_W 任务分配给工作流 TW；为任务分配数据访问权限 TP；为角色分配任务 TR。

RTBAC 模型中用户的权限由用户、权限映射集 $UP = UR \circ TP \circ TR$ 决定，其中 $\circ$ 是复合关系运算符。$\circ$ 的定义为：设有函数 $f: X \to Y$ 和 $g: Y \to Z$，则复合关系 $f \circ g$ 是从 X 到 Z 的函数，并称为 f 和 g 的复合函数。

2)动态权限调整

从上面可知，RTBAC 模型中用户的权限 $UP = UR \circ TP \circ TR$，三元组 (UR, TP, TR) 的值与 UP 相关联。改变三元组中 UR, TP, TR 任一项的值，都将改变 UP 的值。通常情况下，UR, TP 变化的可能性相对不大，权限动态调整主要在 TR 的变化。

在 TR 关系中，当角色对应的任务都是独立性 T_S 类型，那么完成 TR 分配后，角色对应的任务随时间变化不大。当角色对应任务包含流程性任务 T_W 时，用户的权限不仅取决于预定义的授权，而且取决于任务的运行状态。在任务 T_W 归属工作流的执行过程中，角色的权限是动态变化的。将角色 r 动态变化的权限记为 $AR(r)$，它是角色在任务执行过程中的实际权限，是其预定义的角色授权 $TR(r)$ 的子集，即 $AR(r) \subseteq TR(r)$。根据工作流的运行状态和任务关系，可以确定 $AR(r)$：

$$TR(r) \wedge Tw \wedge TT \to AR(r)$$

式中，TT 反映了任务间的逻辑约束关系。比如，假设一个角色 r 的任务集 $TR(r)$ 可以表述为一组授权任务，即 $TR(r) = \{t_{w1}, t_{w2}, \cdots, t_{wn}\}$，其中 t_{w1}, t_{w2}, t_{w3} 为顺序关系，且 t_{w3} 的激活条件 $AC = t_{w1} \wedge t_{w2}$。当 AC 为假时，t_{w3} 无法进入激活状态，也就是说此时角色 r 的实际权限不能包含 t_{w3}，即 $t_{w3} \notin AR(r)$。

3.4 RTBAC 安全性分析

由 3.3 节的分析可知，RTBAC 的访问政策包含在 $UP = UR \circ TP \circ TR$ 中。系统管理员直接进行用户分配角色 UR、任务分配数据访问权限 TP、角色分配任务 TR 进行配置。

通过对权限的动态访问控制，RTBAC 支持两个著名的安全控制原则：

1)最小特权原则。在执行任务时只给用户分配所需要的权限，未执行的任务或任务终止后用户不在拥有所分配的权限。

2)职责分离原则。一些敏感的任务需要不同的用户执行，这可通过私有任务的定义、角色的偏序继承和角色、任务约束来实现。

3.5 RTBAC 对 CSCW 系统访问控制需求满足性分析

RTBAC 模型能较好地满足 2.2 节所述 CSCW 系统对访问控制的需求，分析如下：

1)模型基于角色对用户组进行访问控制。用户的角色代表用户对应的组。改变用户的当前角色集就可改变用户的权限，从而改变某角色包含的权限时即可改变一组用户的权限，满足 2.2 节中第 4)条中的需求，即提供方便的授权/取消机制和操作合法性检查机制；

2)模型中私有任务的定义及角色的偏序继承和角色指派关系定义满足 2.2 节中第 2)条、第 3)条、第 5)条需求，即提供角色之间的权限继承能力、角色允许存在私有权限。在该角色被继承时，私有权限不被继承、用户之间提供必要的转授权关系；

3)模型中基于任务的角色访问控制、任务类型划分及动态权限调整满足 2.2 节中第 1)条、第 6)条、第 7)条需求，即“最小特权原则”、对属于业务流程类型的任务应当根据业务流程的执行动态分配权限、对业务流程类型的任务之间存在着多种操作依赖，可提供适当的支持。

3.6 RTBAC 模型的应用

访问控制是 CSCW 系统的重要组成部分，是有效协同合作的前提条件，访问控制模型可以有效应用于所有的 CSCW 系统。但是，由于构建访问控制模型的侧重点不同，因此针对

不同的运用场景，其应用效果也有差异。RTBAC 模型以角色和任务作为访问控制基础，能较好地应用于下列领域：

1)远程协作办公平台。经济全球化的发展，企业日益分散的物理办公地点导致该方面的应用需求旺盛；

2)远程教育及远程医疗领域。该类系统要求很好的交互和协作性，从而决定系统对访问控制要求很高；

3)电子商务领域。虚拟企业、供应链管理等系统的发展提出了对系统访问控制方面更多的需求。

在分析和建立了 RTBAC 模型后，我们将其应用到了本实验室的学者网(scholat)项目的实践过程中，学者网面向科研工作者和科研团队，提供社交网络服务，管理个人和团队学术信息和资源，分享论文写作、投稿经验，对期刊、会议的评价等，可以帮助研究者发现科研热点或某一领域的研究群体，促进学术交流和创新。

如图 3 所示，学者网的系统架构遵循的是三层模型的体系结构。表示层负责提供用户界面，业务逻辑层负责实现业务逻辑，数据持久层负责业务逻辑层中所有数据的持久化存储。数据存储采用数据库表和 XML 文件两种存储方式。用户的个人信息、角色任务信息、任务权限信息等以数据库表的形式存储在数据库里。而角色的层次结构信息、工作流信息等就以 XML 文件的形式存储。数据持久层主要包含两个部分：1)DBAccess，对数据库表的访问与操作；2)XMLProcess，对以 XML 文件存储的数据进行读取、修改、查询等操作。业务逻辑层的基本模块包括 UserService，RoleService，TaskService，WorkflowService，主要是由 ManagerService 调用来完成业务逻辑的处理过程。

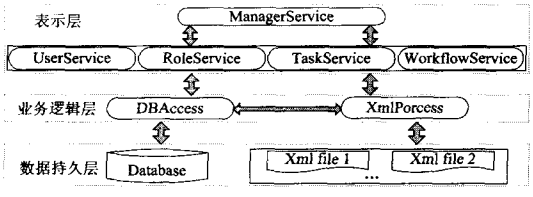

图 3　学者网系统架构设计图

结束语　本文根据 CSCW 系统特点分析了该类系统对访问控制的需求，并进一步针对该需求提出了基于角色和任务的 CSCW 系统访问控制模型(RTBAC 模型)，并将 RTBAC 模型实际用在了学者网(scholat)项目的开发过程中。RTBAC 模型基于角色对用户实现分组权限管理，有方便的授权/取消机制；角色间提供了偏序继承和角色指派关系定义，实现了职责分离原则及用户的转授权关系；通过基于任务的角色访问控制和对任务类型的划分，实现了对独立性任务和流程性任务采用不同的访问控制方法，满足“最小特权原则”及用户权限根据任务的执行过程实现动态分配。

参 考 文 献

[1] 汤庸，冀高峰，朱君. 协同软件技术及应用[M]. 北京：机械工业出版社，2007

[2] 龚能，李玉顺，史美林. 协作环境中的关键技术研究[J]. 计算机科学，2005，32(9)：230-232

[3] Tolone W，Ahn G-J，Pai Tanusree，et al. Access control in collaborative systems[J]. ACM Computing Surveys，2005，37(1)：29-41

[4] David F，Richard K. Role-based access controls [C]// Proceedings of the 15th NIST2NCSC National Computer Security Conference. Baltimore，MD，1992：555-560

[5] Oh S，Park S. Task-role-based access control model [J]. Information Systems，2003，28(6)：535-542

[6] Zhu H B，Zhou M C. Role-based collaboration and its kernel mechanisms[J]. IEEE Trans. on Systems，Man，and Cybernetic-Part C：Applications and Reviews，2006，36(4)：579-580

[7] 李成锴，詹永照，茅兵，等. 基于角色的 CSCW 系统访问控制模型[J]. 软件学报，2001，11(7)：931-934

[8] 邓集波，洪帆. 基于任务的访问控制模型[J]. 软件学报，2003，14(1)：76-80

[9] Sandhu R，Conyne E J，Lfeinstein H L，et al. Role based access control models[J]. IEEE Computer，1996，29(2)：38-43

(上接第 129 页)

[7] Jung I Y，Cho I S，Yeom H Y. A Stateful Web Service with Scalable Security on HVEM DataGrid[C]// Third IEEE International Conference on e-Science and Grid Computing. Washington DC USA：IEEE Computer Society. 2007：360-369

[8] Moses T，Inc E. eXtensible Access Control Markup Language (XACML) Version 2. 0. OASIS Standard[S]. Feb 2005

[9] Winsborough W H，Jacobs J. Automated Trust Negotiation Technology with Attribute-based Access Control[C]// Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03). 2003，2：60-62

[10] Bajaj S，et al. Web Services Policy Framework (WS-Policy) Version 1. 2[S]. March 2006

[11] Ballinger K，Bissett B，et al. Web Services Metadata Exchange (WS-MetadataExchange) Version 1. 1[S]. August 2006

[12] Li Ninghui，Mitchell J C. RT：A Role-based Trust-management Framework[C]// DARPA Information Survivability Conference and Exposition (DISCEX). Washington D. C，2003，1：201-212

[13] Winslett M，Yu Ting，Seamons K E，et al. Negotiating Trust on the Web[J]. IEEE Internet Computing，2002，6：30-37

[14] Coetzee M，Eloff J H P. Towards Web Service access control [J]. Computers & Security，2004，23：559-570

[15] Cantor S，Kemp J，Philpott R，et al. Assertions and Protocols for the OASIS Security Assertion Markup Language(SAML)[S]. OASIS Standard，March 2005

[16] Anderson A. Web Services Profile of XACML (WS-XACML) Version 1. 0. Working Draft 5[S]. October 2006

[17] Turkmen F，Crispo B. Performance Evaluation of XACML PDP Implementations[C]// Proceedings of the 2008 ACM Workshop on Secure WebSservices. New York，USA：ACM，2008：37-44

[18] http://sunxacml. sourceforge. net/

[19] Vedamuthu A S，Orchard D，et al. Web Services Policy 1. 5-Attachment[S]. W3C Recommendation 04，September 2007