基于 BPMN 扩展的安全约束工作流模型

严张凌[1],代 茂[2],彭 强[1]
(1. 四川大学锦城学院,四川 成都 611731;
2. 四川大学网络教育学院,四川 成都 610065)

摘 要:基于角色的访问控制(role based access control,RBAC)是软件系统中常用的授权机制,而工作流引擎中的核心授权单位是任务,使得 RBAC 难以应用在工作流系统中。文中在 RBAC 思想的基础上,通过对工作流资源边界的确立,将角色与工作流中的任务相关联来进行资源的访问控制与授权,很好地将 RBAC 融合进工作流,有效地避免了工作流建立自成体系的权限控制而增加系统复杂性,让同一目标对象的授权在工作流引擎内外得到统一。同时,对业务流程建模与标注(business process model and notation,BPMN)的元模型进行安全约束的扩展,以便于在流程图中准确地表达基于角色和任务的安全约束需求,为业务流程的表示与执行提供了良好的支持;最后,将这种扩展应用在了四川省某电力公司的合同与督查管理系统中,并对其具体业务流程的应用进行分析与验证。

关键词:角色和任务;工作流访问控制;最小特权原则;业务流程建模与标注
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2018)03-0146-04
doi:10.3969/j.issn.1673-629X.2018.03.031

A Business Processes Model of Security Constraint Based on BPMN Extension

YAN Zhang-ling[1],DAI Mao[2],PENG Qiang[1]
(1. Jincheng College of Sichuan University,Chengdu 611731,China;
2. Distance Education College of Sichuan University,Chengdu 610065,China)

Abstract:The role based access control (RBAC) is a common authorization mechanism in software system,while task is the core authorization unit in workflow engine,which makes it hard to apply RBAC into workflow system. On the basis of RBAC,we connect the roles and the tasks in the workflow for access control and authorization of resources by defining a resource boundary,which prevents effectively workflow from building a separate authorization control with increase of system complexity,and enables the authorization of the same object to be unified inside and outside the workflow. At the same time,we also extend the meta-model of business process modeling notation (BPMN) in secure constraint so as to accurately express the security constraint requirements based on roles and tasks in the flowchart,which provides a good support for the presentation and execution of business process. Finally,we apply this approach into a typical business process in a power supply company,which is analyzed and verified in specific business application.

Key words:role and task;workflow access control;minimum permission principle;BPMN

1 概 述

流程感知信息系统用于控制和监视业务活动,典型的系统包括工作流管理系统、企业战略资源调配系统和客户关系管理系统等[1]。在构建一个安全的流程信息系统时要考虑很多的安全问题,包括身份认证、授权、访问控制、数据完整性、审计、不可抵赖和可管理性等[2]。文中重点讨论访问控制问题。

工作流扭转的一个经典模型是 Petri 网,将权限与 Petri 网结合是流程感知信息系统研究的一个方向[3-4]。在传统的信息系统的访问控制领域,RBAC 模型应用最为广泛,它是 20 世纪 90 年代迅速发展起来的用于大规模系统中管理和实施安全的一种技术。其中 Ravi Sandhu 提出的 RBAC96 模型[5]最为经典,后经美国国家标准与技术研究院(the national institute of standards and technology,NIST)进行了标准化[6],分为 4 个部件模型:基本模型 RBAC0、角色分级模型

收稿日期:2017-03-29 **修回日期**:2017-07-26 **网络出版时间**:2017-12-05
基金项目:四川省教育自然科学重点课题(16ZA0422)
作者简介:严张凌(1980-),男,硕士,研究方向为软件工程、云计算与智能大数据等。

RBAC1、角色限制模型 RBAC2 和组合模型 RBAC3。RBAC 的基本概念就是把权限与角色关联,通过为用户分配合适的角色而获得相应的权限,如图 1 所示。

图 1　RBAC 模型结构

RBAC 模型的优点是通过角色能够表达企业内部组织和人员之间的复杂关系,用户能够灵活地在不同角色(职位)之间切换,从而便于授权管理[7]。但 RBAC 中的权限是资源和操作组合,它与工作流中以任务为中心的模型不太吻合,所以 Thomas 等提出了基于任务的访问控制(task - based access control, TBAC)模型[8],其主要思想是通过授权步机制解决工作流运行过程中活动实例与用户权限的同步问题,每个活动对应一个授权步。TBAC 采用面向任务的观点,从任务的角度来建立安全模型和实现安全机制。在这个模型中,权限分配给任务,任务再分配给角色,在任务处理过程中提供动态的、实时的安全管理[9]。

TBAC 模型虽然较好地提供了工作流中的安全模型,却与企业信息系统中普遍采用的 RBAC 模型不兼容,造成取舍困难。对此,邢光林等提出了基于任务和角色工作流改进模型(task role - based controllability, TRBC)[10-11];孙军红等[12]也对该模型进行了扩展与研究,其主要组成部件如图 2 所示。

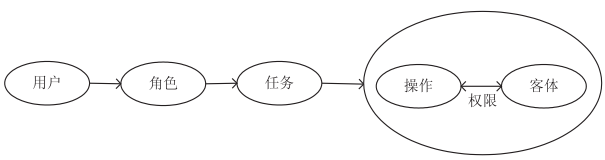

图 2　基于角色和任务的工作流访问控制模型

其基本思想是:角色和权限不直接挂钩而是通过任务把角色和权限联系在一起,然后给用户指派合适的角色,用户通过所指派的角色获得可以执行的任务,然后在执行某个任务的某个具体实例时获得该任务所允许访问的客户的权限,这样更方便权限粒度的控制和管理[12]。

TRBC 模型结合了 RBAC 中的角色与 TBAC 中的任务两个核心概念,将 RBAC 中的权限与角色的绑定移到了与任务绑定,然后将任务分配给角色。对于任务成为了授权中必不可少的一环,这样虽然对于工作流是可行的方法,但却忽略了工作流之外的信息系统的权限控制需求,限制了该模型的使用范围。

文中从信息系统中的资源分配入手,通过定义工作流与信息系统边界,保证信息系统的权限控制模型在工作流引擎中发挥相同的控制作用,而避免了 TBAC 那样在工作流引擎中单独定义权限控制模型,使得 RBAC 模型在工作流引擎内外达到统一。

2　基于角色的安全约束工作流模型

在企业组织机构中的角色概念特别适合于进行细粒度的授权控制,所以基于角色的访问控制受到了特别重视[13]。现在,一般普遍接受的安全工作流系统要满足如下策略[14]:

访问控制:能够控制特定角色访问指定资源或对该资源进行特定操作。

职责分离原则:遵循不相容职责相分离,实现合理的组织分工,工作流程必须由一个以上的角色完成。

最小特权原则:工作流中用户在执行具体的任务实例时,只能访问该任务所允许操作的资源。

下面将讨论这些策略是如何被建模以及如何在工作流驱动的信息系统中被遵循的。

2.1　安全约束的形式化描述

为了给出安全约束的形式化描述,首先定义用户角色关联和任务角色关联的形式化描述。任务角色关联需要解决的是对一个特定角色,如何选择特定的某一个或某些角色来执行,然后通过用户角色分配机制将该任务定位到某个特定的用户。

将任务关联到一个角色集合是该安全约束工作流模型中最基础的一步,其形式化描述如下:

$T = \{t_i \mid i = 1,2,\cdots,l\}$ 是一个任务实例集,一个任务实例是某个任务的动态表示。

$R = \{r_i \mid i = 1,2,\cdots,m\}$ 是一个角色集。

$(R, <)$ 表示对 R 中的元素进行比较,该比较实际上表示的是角色的分级层次。设 $r_1, r_2 \in R$, $r_1 < r_2$ 表示 r_2 对 r_1 有支配权。就企业中的组织关系而言, r_2 即是 r_1 的上级领导。

$U = \{u_i \mid i = 1,2,\cdots,n\}$ 是一个用户集,表示系统中各个特定的用户集合。

$\mathrm{TR} \subseteq (T \times R)$ 表示任务与角色之间多对多的关联关系。

$\mathrm{UR} \subseteq (U \times R)$ 表示用户与角色之间多对多的关联关系。

$R(t) = \{r_m \in R: \exists (t_l, r_m) \in \mathrm{TR}(t)\}$ 表示被授权能够执行任务 t_l 的特定角色集。

$U(t) = \{u_n \in U: \exists (u_n, r_m) \in \mathrm{UR}, r_m \in R(t)\}$ 表示被授权能够执行任务 t_l 用户集。

通过以上定义得出结论,通过任务、角色和用户之间的两个多对多关联,已可以将任务 t_l 具体指定给一个潜在用户集 $U(t)$。当该任务 t_l 被实例化时,潜在用户集 $U(t)$ 的所有用户均可见任务 t_l,直到某一个用户 u_n 对 t_l 声明已占有该任务(即准备执行该任务)。一旦用户声明后,任务实例 t_l 与 u_n 就表现为一对一的关系。

$\mathrm{OP} = \{\mathrm{op}_i \mid i = 1,2,\cdots,o\}$ 表示操作集,表示对信

息系统资源的动作。

$RES = \{res_i \mid i = 1,2,\cdots,p\}$ 表示资源集,表示系统中的资源,也是安全约束模型中需要保护的目标对象。

$P = \{p_i \mid i = 1,2,\cdots,q\}$ 表示权限集,其中 $p_i = (op_i, obj_i)$。

$RP = \{rp_i \mid i = 1,2,\cdots,r\}$ 表示角色的权限集。

$UAP(n) = \{p_n \in P: \exists (u_n, r_m) \in UR, (r_m, p_q) \in RP\}$ 表示用户 u_n 的权限集,首先通过用户与角色的关联获取所有角色,再通过角色与权限的关联获取这些角色的所有权限,然后作并运算得到该用户的所有权限。

需要注意的是,为了满足最小特权原则,UAP(n)不能直接作为工作流运转过程中的权限判断依据,因为它对于完成任务而言太大了,其中可能包含了完成该任务所不需要的权限。例如,某出版社的发文工作流,总经理在审稿人员缺席的情况下可以代为审稿,UAP(总经理)>UAP(审稿员甲),此时就破坏了最小特权原则。因此,还需要定义下面这个与任务关联的权限集:

$UTP(t) = \{p_q \in P: \exists (r_m, p_q) \in RP, (t_l, r_m) \in TR(t)\}$ 表示用户 u_n 在执行任务 t_l 时的角色对应的权限集。由以上定义可以推出:$UTP(t) \subseteq UAP(t)$。

2.2 安全约束的元模型

工作流建模已被许多语言进行了定义,其中 BPMN 是被大家广为接受的一种容易理解且语言丰富的建模符号,由于易于扩展,许多学者从安全角度对其进行扩展,以便表达特定的安全需求。其中较为知名的有文献[14]中安全需求模型的 BPMN 扩展和文献[15]中的安全 BPMN 模型。

根据前文的形式化定义,要想在工作流模型中对安全约束进行建模,就属于在展现人工任务的同时展现附于其上的角色集。另外,为了实际操作方便,在元模型中还对人工任务进行了分组,以便简易快速地表示一群拥有相同权限的任务。在 BPMN 元模型[16]的基础上,为其增加安全约束来表达前文的形式化描述。扩展的 BPMN 元模型如图 3 所示。

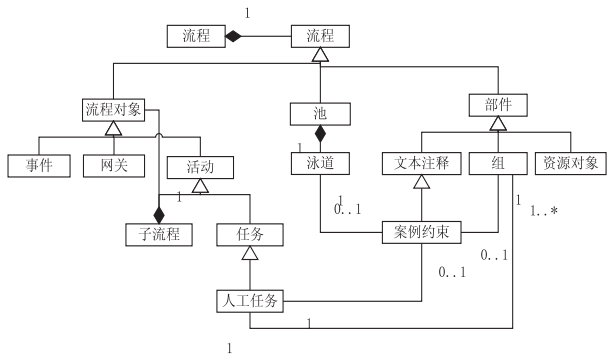

图 3 扩展的 BPMN 元模型

一个活动从通常意义上来说就是一次特定的任务,只是在这些任务中有一个特殊的属于用于标识该任务是否为人工任务,通常人工任务都是阻塞型的,即流程一旦执行到该步骤将会被挂起直到明确地被推进。

任务的分组在本质上并不影响流程的正常运行,组仅仅是用来简化为一系列任务定义和描述安全约束的目的。组可被用于部件、泳道和各种任务。把多个任务实例或循环的任务作为一个组后,即可把它当作一个任务来对待,以此来简化设计和展现形式。

3 实例及安全性分析

在企业信息系统中,合同的签订是一个重要且典型的工作流应用场景,该实例来自某电力企业内部信息系统中的合同签订流程(见图 4),涉及 3 个角色:合同谈判人、项目管理办公室和分管领导。

系统的安全策略为:

(1)合同谈判人只能对合同进行拟稿和提交工作,且只能看到自己提交的合同;

(2)项目管理办公室可对提交的合同初稿进行审

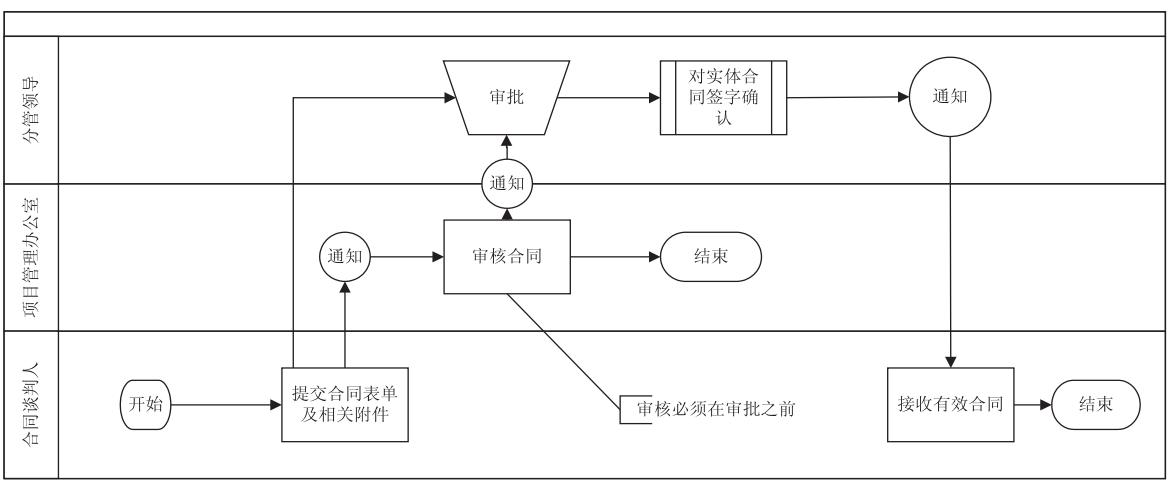

图 4 合同签订流程

核,主要是对单价、数量和总金额的审核;

(3)分管领导只能看到自己分管的部门下属员工提交的合同,并且这些合同必须经过项目管理办公室的审核,分管领导可以进行审批以使合同生效。

上述流程用文中的安全约束模型描述如下:

R = {合同谈判人,项目管理办公室,分管领导,出纳}

RES = {合同,合同附件,票据}

OP = {新增,读取,删除,修改,审核,签订}

P = {(新增,合同),(读取,合同),(删除,合同),(修改,合同),(审核,合同)(签订,合同),(新增,附件),(读取,附件),(修改,附件),(签订,附件),(新增,票据),(读取,票据),(删除,票据),(修改,票据),(审核,票据)}

假设 u1 = 张三,UR(u1) = {项目管理办公室,出纳},则:

UAP(审核) = {(读取,合同),(审核,合同),(读取,票据),(删除,票据),(修改,票据),(审核,票据)}

UTP(审核) = {(读取,合同),(审核,合同)}

通过 UAP 可以发现,RBAC 模型能很好地为用户关联到具体权限,但由于 RBAC 模型未对用户同时扮演的角色数量作限制,所以若直接在工作流中使用 RBAC 则会造成权限超过流程所要求的权限,违反了最小特权原则。但是,通过前文所述的任务与角色的关联,并加上 UTP 限制,可以减小用户在流程运行中所需要的权限,从而有效地进行安全约束。

4　结束语

工作流的安全约束模型是当前 WFMS 研究的一个重要课题,如何在安全性和可操作性间取得平衡是一个难点。在分析了面向信息系统的传统 RBAC 模型,面向工作流的 TBAC 模型和二者的改进 TRAC 模型的基础上,提出了一种更为简便的 RBAC 应用模型,使得信息系统中的 RBAC 与工作流的安全约束达到了统一。然而,在元模型的扩展上,目前使用的是注释的子类形式,缺乏有效的验证机制,期望在 BPMN 2.0 中加以改进。

参考文献:

[1] RUSSELL N, VAN DER AALST W M P, TER HOFSTEDE A H M, et al. Workflow resource patterns: identification, representation and tool support[C]//Proceedings of the 17th international conference on advanced information systems engineering. Berlin: Springer-Verlag, 2005: 216-232.

[2] LI S, KITTEL A, JIA D, et al. Security considerations for workflow systems [C]//Network operations and management symposium. [s. l.]: IEEE, 2000: 655-668.

[3] 张　亮,姚淑珍. 一种新的基于 Petri 网的分层工作流过程模型[J]. 计算机集成制造系统,2006,12(9):1367-1373.

[4] 沈　满,赵嵩正,刘　婧. 依据角色权限的审批工作流模型构建[J]. 计算机工程与应用,2015,51(4):235-239.

[5] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1998, 29(2): 38-47.

[6] FERRAIOLO D F, SANDHU R, GAVRILA S, et al. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.

[7] 徐　宏,邰伟鹏. 面向工作流的 RBAC 模型研究[J]. 计算机工程与设计,2012,33(4):1295-1299.

[8] THOMAS R K, SANDHU R S. Proceedings of the IFIP TC11 WG11. 3[C]//Eleventh international conference on database security XI: status and prospects. [s. l.]: [s. n.], 1998: 166-181.

[9] 杨勇虎,刘振宇. 工作流中 TBAC 权限控制模型的扩展与 UML 描述[J]. 计算机系统应用,2008,17(8):34-37.

[10] 邢光林,洪　帆. 基于角色和任务的工作流访问控制模型[J]. 计算机工程与应用,2005,41(2):210-213.

[11] 周　炜. 具有时空约束的 TRBAC 模型在 OA 中的应用[J]. 网络安全技术与应用,2014(8):116-117.

[12] 孙军红,李　娟. 一种基于任务和角色的工作流访问控制模型[J]. 计算机工程与应用,2008,44(30):21-23.

[13] AHN G, SANDHU R. Role-based authorization constraints specification[J]. ACM Transactions on Information and System Security, 2000, 3(4): 207-226.

[14] RODRÍGUEZ A, FERNÁNDEZ-MEDINA E, PIATTINI M. A BPMN extension for the modeling of security requirements in business processes[J]. IEICE Transactions on Information & System, 2007, 90-D(4): 745-752.

[15] ACHIM D B, GERO L, ISABELLE H, et al. SecureBPMN: modeling and enforcing access control requirements in business processes[C]//Proceedings of the 17th ACM on access control models and technologies. New York, NY, USA: ACM, 2012: 123-126.

[16] KALNINS A, VITOLINS V. Use of UML and model transformations for workflow process definitions[C]//Baltic DB & IS. [s. l.]: [s. n.], 2006: 3-15.