基于用户-角色-任务的多约束访问控制模型①

姚 璐, 盛步云

(武汉理工大学 机电工程学院, 武汉 430070)

摘 要: 传统的访问控制模型采用手动的授权方式, 应用在目前混合型组织企业中, 造成权限授权复杂、准确度低. 因此, 提出一种基于用户-角色-任务的多约束访问控制模型(C-URTBAC), 该模型采用用户分级管理、权限在主体和客体间的传播性思想, 实现了半自动化的授权方式, 提高授权效率和准确度; 同时细化了约束分类, 实现了细粒度化的权限管理. 最后将该模型引用到某汽车零部件公司的 PLM 系统中, 验证了该模型的实用性.

关键词: PLM; 访问控制; 分级管理; 传播; 约束

C-URTBAC Model in the Permission Management

YAO Lu, SHENG Bu-Yun

(College of Mechanical & Electrical Engineering , Wuhan University of Technology, Wuhan 430070, China)

Abstract: The manual way of the traditional access control model caused complex access authorization and low accuracy in the hybrid organization enterprise. And the model of C-URTBAC was put forward. The model adopted the idea of the level-to-level management of users and transmission of permissions in the subject and object. It could realize semi-automatic way of authorization, so as to improve the efficiency and accuracy of authorization. And it refined the constraint classification, realizing fine-grained permissions management. Finally the model was introduced in the PLM system of some auto parts company, verifying the practicability of the model.

Key words: PLM; access control; level-to-level management; transmission; constraints

产品全生命周期管理 PLM(Product Lifecycle Management)系统, 是现今普遍应用在企业信息化中的数据管理软件. 该系统可以完整地实施业务中所包含的所有解决方案, 有效地将人、信息和过程整合起来, 进而作用于企业中. 也就是说, 通过该软件平台, 企业用户可以将与产品相关的概念设计、信息创建、研发、资源管理和使用产品的信息等在产品全生命周期中所产生的数据进行统一管理. 为保证 PLM 系统中资源的安全性和易操作性, 使企业中各部门能够高效地协同完成各项业务, 权限控制模型的设计成为研究的关键[1].

PLM 系统是企业级的信息化办理软件, 与其他信息化软件比较, PLM 权限管理的特色[2,3]如下所示:

1) 实体对象的复杂性: PLM 将与项目相关的所有数据集成管理, 实体对象(包括数据、资源等)种类多, 而且它们之间的关系也比较复杂, 这就使得用户对相应的实体操作也各不相同. 因此 PLM 需要细粒度化的访问控制模型.

2) 权限的动态性: PLM 对项目任务的过程进行管理, 任务是动态的, 则与之相应的权限也会改变, 当任务完成后, 相应的权限也会回收; PLM 模块功能入口以及界面的操作权限对于特定角色一般是静态的. 因此 PLM 需要动态的访问控制模型.

3) 用户过多: PLM 系统是企业级的信息化管理平台, 涉及到的用户很多, 不同部门的工作人员权限不一样, 同一部门的不同人员权限也不一样, 这就造成权限配置的复杂性. 因此 PLM 系统需要高效率的、准确的访问控制模型.

① 基金项目:武汉理工大学自主创新研究基金(135204009)
收稿时间:2014-12-22;收到修改稿时间:2015-01-22

针对 PLM/PDM 权限管理特点，目前已有学者做出一些研究. 文献[2]将面向对象的思想运用于访问控制模型中，实现了权限的多层次和多角度管理；文献[3]将 RBAC 模型和工作流概念引入到 PLM 中，实现了权限的动态管理；文献[4]从实体方面提出了细粒度化 RBAC 模型；文献[5-7]在 RBAC 和 TBAC 模型的基础上，提出了一种新的权限管理模型 S-TBAC，该模型加入任务的依赖，细化权限的分类，并加强数据的安全监测性. 文献[8]提出了一种基于域控制的访问控制模型，该模型解决了多法人、多地域公司的权限集中控制. 目前如何高效地、准确地配置权限的模型还未研究. 本文在前人的基础上提出基于用户-角色-任务的多约束访问控制模型(简称 C-URTBAC)，该模型利用用户分级思想、权限的传播性和细化约束类型来实现权限的高效率、准确以及细粒度化管理，最后结合根据某汽车零部件公司需求研发的 PLM 系统给出该模型的应用实例.

1　C-URTBAC模型的定义

从 20 世纪 60 年代末，一些学者就开始研究访问控制模型以及相关的技术. 建立访问控制模型[9-11]的主要目的是为防止非法用户对企业资源信息的不合理使用. 一般情况下，系统设计的访问控制模型主要包括三部分：主体、客体和控制策略. 其中主体就是操作系统资源、信息等的对象，通常指用户；客体就是被主体访问的对象，通常指企业的资源信息，如文件，会议记录、合同等；控制策略就是一组用来限制主体访问客体的约束集.

本文针对 PLM 权限管理特点，根据控制模型的理论知识设计的基于用户-角色-任务的多约束访问控制模型如图 1 所示.

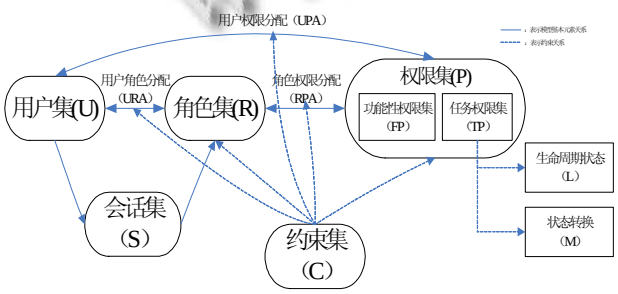

图 1　基于用户-角色-任务的多约束访问控制模型

C-URTBAC 模型将访问控制模型的三大要素更加具体化，其基本元素定义如下：

用户集 U(Users)：在 PLM 系统中，对所有客体进行操作的主体.

角色集 R(Roles)：用户的责任在 PLM 系统中的虚拟呈现.

会话集 S(Sessions)：用户以某个角色登陆 PLM 系统，并与之进行交互. 一个用户集 U 与多会话集 S 相对应.

权限集 P(Permissions)：包含功能性权限集 FP 和任务权限集 TP. TP 是指用户对系统功能模块入口以及界面上的功能操作的权限，如用户管理，订单管理等；TP 是为用户明确地执行企业项目中不同任务而设置的权限，因任务状态是在不断变化的，故任务权限[12]包含生命周期状态 L(如正在设计中，校准中，已完成)和状态转换 M(如任务从设计中到校准中的转换，从校准中到已完成的转换)两个方面的权限.

用户角色分配 URA：根据企业的人员组织形式将用户分配成不同角色. 一个用户可以分配到不一样的角色；一个角色也包括不一样的用户，也就是说用户与角色之间是多对多的对应关系.

角色权限分配 RPA：根据角色的职责将与之相应的权限进行关联. 他们之间的关系是多对多.

用户权限分配 UPA：根据用户一些特权将与之相应的权限进行关联. 他们之间的关系是多对多.

约束集 C(Constraints)：包括 URA 约束集, RPA 约束集、UPA 约束集、角色约束集和权限约束集[13]. 具体介绍见 2.3 所示.

2　C-URTBAC模型的特点

2.1　用户的分级管理

目前企业中主要有三种人员组织形式，分别是静态的组织机构型、动态的项目型以及混合型[14]. 本文只讨论目前大多数企业采用的混合型，对于这种企业，角色划分按照以项目角色为主、以组织机构和行政级别为辅来进行. 按照目前市面上的 PLM/PDM 系统，在分配角色或给角色、用户分配权限时只有一个系统管理员操作，当角色发生改变或是资源发生改变时，系统管理员又要重新配置角色或是权限，这样给系统管理员增加了很大的工作量，而且还经常容易出错. 本系统为用户权限管理提供一种分级管理的方法.

PLM 系统中包含高级管理员、一般管理员和普通

用户. 高级管理员拥有系统所有的权限, 执行对该系统的所有操作, 该类用户通常是企业的信息主管, 主要负责对普通管理员的权限配置; 一般管理员拥有对整个项目操作的所有权限, 该类用户通常是某个项目负责人, 主要负责对项目角色的划分以及角色与用户的权限配置; 普通用户拥有高级管理员或普通管理员赋予一般用户的权限, 该类用户通常是项目的参与人员以及其他普通员工, 主要完成项目任务以及企业日常的行政工作. 其中高级管理员是静态的, 长时间内不会改变, 而普通管理员是动态的, 因为项目是阶段性的, 每个项目负责人是不一样的, 当一个项目完成之后该项目负责人的权限以及负责人分配的所有角色权限都会收回.

2.2 权限的传播

1) 权限在客体间的传播

目前市面上的 PLM 软件中, 用户对文件的权限由该文件所在的文件夹的权限及其所处于状态权限共同决定, 且在删除文件的时候, 必须在文件经过的所有状态中都有删除的权限才能删除掉现有的文件, 这样设计容易导致系统管理员在配置权限时重复操作, 错误率高. 为了实现高效率的授权, 该模型提出了一种客体间传播权限的模式. 本文设计的客体间传播权限的模式如图 2 所示.

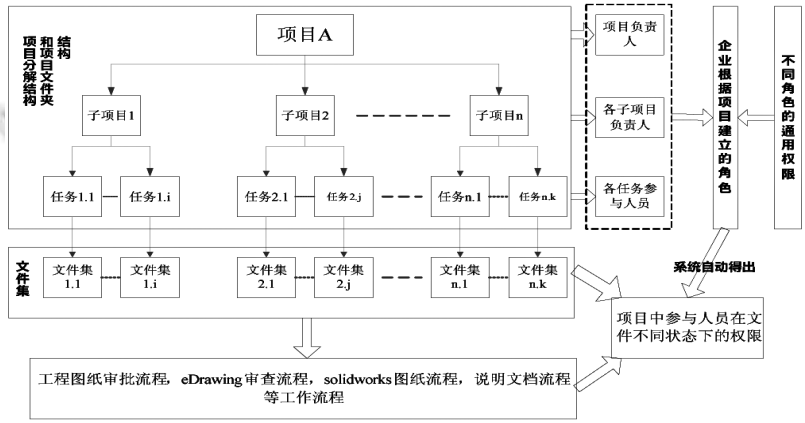

图 2 权限在客体间的传播模式

该模式是通过在分解项目时, 自动在后台的 PLM 资源管理器中生成该项目的文件夹结构, 每个任务对应一个文件夹, 当任务分配好后, 系统会自动地根据任务负责人或是任务参与人员在该项目任务中的角色赋予员工对该任务相关的文件夹的角色通用权限. 该模式可以减少系统管理员配置权限的工作量和数据库中的记录数.

角色通用权限是按照机械行业中常见的角色, 将权限分为设计师通用权限, 校对组通用权限, 工艺组通用权限, 审核组通用权限和批准组通用权限. 设计组通用的权限有创建文件、删除文件、检入/检出文件、添加或重命名文件和读取文件内容; 校对组通用的权限有检入/检出文件、从冷存储恢复文件、准许或拒绝组层对文件的访问、将文件共享到另一个文件夹、添加或重新命名文件、读取文件内容、递增文件修订版本和销毁; 工艺组和审核组通用的权限有检入/检出文件和读取文件内容. 批准组通用的权限有将文件共享到另一文件夹和读取文件内容.

2) 权限在主体间的传播

权限在客体间的传播解决了通用权限授予问题, 但是同一个角色里面的成员在同一个项目中参与的任务是不一样的, 还需要手动对角色中不同成员添加一些私有权限, 目前企业中软件大都针对角色进行授权, 当某个角色中的成员请假或者职位有变化时, 增加角色或是剔除角色中的成员已经无法解决这种问题. 为了让上述权限管理更加细化, 该模型提出了一种权限在主体(角色-用户-管理员)间传播的模式. 该模式如图 3 所示.

该模式提出了用户-角色-管理员对某用户的三种授权方法: 用户手动授权, 角色自动授权, 管理员手动授权. 用户手动授权是当用户 B 的权限大于用户 A 时, 用户 B 因事假或出差将执行某项任务的权限 P_a 授予用户 A, 且该权限具有时效性, 当用户 B 回到正常的工作

岗位时，该授予权限收回；角色自动授权是指用户 A 属于某个角色，系统自动赋予给这个角色的通用权限 P_C 就属于该用户的权限；管理员手动授权是指高级管理员或一般管理员给角色中的特殊用户授予的私有权限 P_P .

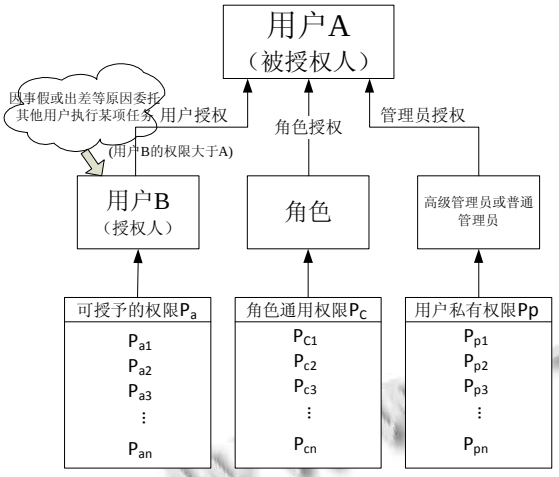

图 3　权限在主体间的传播模式

2.3 约束的分类

该模型中约束集包含五大类，分别为:

1) 角色约束集合(RC)

根据 PLM 系统主体的特点可知，角色之间的关系主要有包容、互斥两种.

很多相关文献已经定义了该关系，这里就省略. 因角色过多导致权限配置过于繁杂，故分配的最大角色数不能超过 N(根据企业而定).

2) 用户角色分配约束集(URAC)

URAC 是指用户分配角色时必须遵循以下原则: a)严格按照企业人员组织形式进行. b)给用户分配角色时需要考虑角色约束集合 RC. 即当一个用户被分配到互相排斥的两个角色时，系统会给出错误警示.

3) 权限约束集(PC)

根据 PLM 系统客体的特点可知，权限之间的关系主要有互斥、依赖和包含.

很多相关文献已经定义了该关系，这里就省略.

4) 角色权限分配约束集(RPAC)

RPAC 是指用户分配角色时必须遵循以下原则: a)严格按照角色在项目中的职责进行. b)考虑角色约束. 如互相排斥的两个角色不能赋予相同的权限；当角色 A 包容角色 B 时，角色 B 的权限会自动授予角色 A，无需管理员重复操作. c)考虑权限约束. 如同一个角色不能授予互斥的两个权限；若权限 P_1 包含权限 P_2、P_3 和 P_4，当授予角色 A 权限 P_1 时，系统会自动给角色 A 赋予权限 P_2、P_3 和 P_4；若权限 P_5 依赖于权限 P_4，P_4 被授予角色 A，P_5 被授予角色 B，只有在角色 A 行使 P_4 完成任务后，角色 B 的权限 P_5 才生效.

5) 用户权限分配约束集(UPAC)

UPAC 是指用户分配权限时必须遵循以下原则: a)考虑用户的职责以及能力. 当用户除了角色赋予的公有权限外，还有其他的私有权限，严格按照该用户的职责进行分配权限；当某个用户请假或是离职，委托不属于该任务但具有完成这项任务能力的相关人员的权限. b)考虑用户角色分配和角色权限分配. 即只有当某个用户承担的角色权限不完整，但角色中其他成员又不具有该权限时，才能进行用户权限分配. c)考虑权限约束关系. 如当用户因承担某个角色已有权限 P_1 时，若 P_1 包含权限 P_2 和 P_3，不能重复给用户分配权限 P_2 和 P_3. d)支持删除角色公有权限中的权限. 如当角色中的成员中某一个没有公有权限中的其中一个时，管理员可以单独通过用户授权将这个权限剔除，这样便于系统授权管理.

3　应用实例

C-URTBAC 模型采用用户分级管理，权限在主体和客体间的传播性以及细化约束分类来实现高效率、准确的和细粒度化的权限管理，下面以某汽车零部件公司 PLM 系统为例，说明该模型的应用.

1) 角色分配

按照该企业的组织形式以及目前进行的某个项目进行的角色分配如表 1 所示.

表 1　角色分配表

项目负责人	项目阶段	部门	角色
项目经理	产品设计	设计部门(部门主管)	Solidworks/CAD 图设计
			Solidworks/CAD 图校对
			solidworks/CAD 图审核
			…….
	工艺设计	工艺部门(部门主管)	工艺设计
			标准化
			工艺校对
			工艺审核
			……
	制造	生产部门	编程
			编程校对

		(部门主管)	资料管理
			……..
	…..	……	…….

角色分配界面如图 4 所示.

图 4 角色分配界面

选中图中所示“角色”右击，选中新角色，可以新建角色；选中某个角色，双击，该界面显示角色成员的基本信息；单击“添加”按钮，打开添加角色成员对话框.

2) 角色配置权限

该系统支持全生命周期状态以及状态转换权限配置. 角色分配状态公有权限的界面如图 5 所示. 该界面主要实现某个任务相关联的文件在“设计中”状态时相应的角色所拥有的公有权限. 当角色中的用户除了公有权限外，还有私有权限，单击“添加用户”，选中用户，界面右边会自动出现该用户所属角色的公有权限，管理员只需在此基础上添加或删除权限即可.

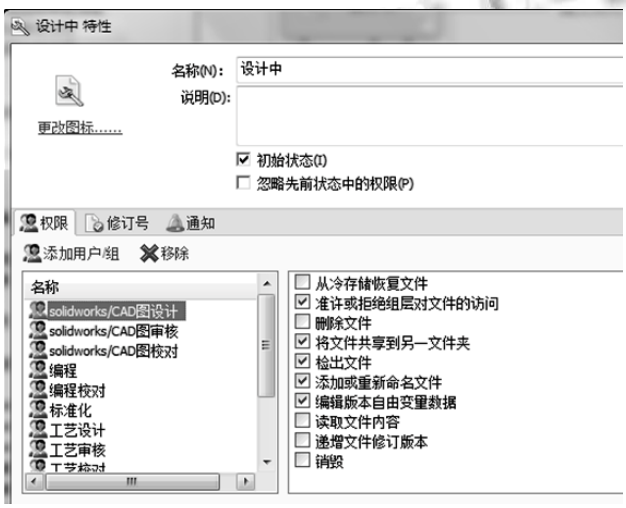

图 5 角色权限配置

3) 任务分配

当项目在任务分配界面(如图 6)分配好任务，单击工具栏中的“保存”按钮，系统在保存任务的同时，也将任务参与人员在角色中的公有权限自动授予给相应的人员了.

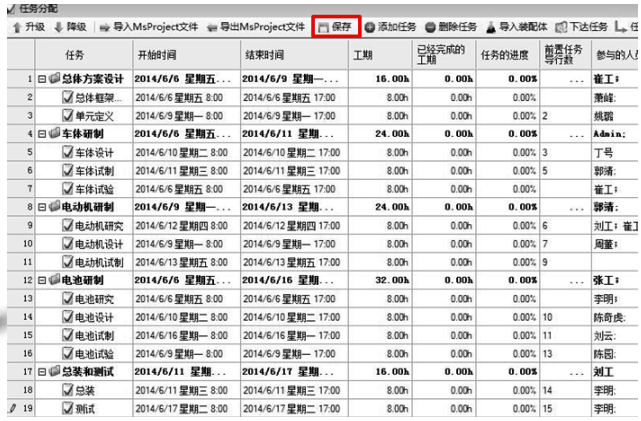

图 6 任务分配

4 总结

根据 C-URTBAC 模型开发出的权限管理模块已经在企业中实施了. 结果表明：该模型能够简化管理员的操作；权限配置更加准确以及高效；当工作流程比较复杂时，能够使权限控制更加细化，满足企业的实际需求.

参考文献

1 曾金.某客车工业集团 PLM 系统解决方案设计[学位论文].武汉:华中师范大学,2012.
2 李良军.PLM 中权限控制的研究与设计[学位论文].西安:西安电子科技大学,2012.
3 万立,关卫林,熊体凡,刘清华.PDM 权限管理模型的研究与实现.机械与电子,2008,7(1):55–57.
4 滕菲.细粒度 RBAC 模型在 PLM 系统权限管理中的研究与应用[学位论文].长春:吉林大学,2011.
5 朱一群,李建华.面向多策略服务的一种基于属性角色访问控制模型.计算机应用与软件,2008,25(11): 143–145.
6 刘先锐.PDM 中权限管理模型的研究与应用[学位论文].长春:吉林大学,2013.
7 赵卫东,毕晓清,卢新明.基于角色的细粒度访问控制模型的设计与实现.计算机工程与设计,2013,26(2):474–479.
8 元祥波,朱云龙,张志冬,王海.基于域控制的权限系统模型设计与实现.机械设计与制造,2014,56(2):178–180.

9 刘强.基于角色的访问控制技术.广州:华南理工大学出版社,2010.
10 李双.访问控制与加密.北京:机械工业出版社, 2012.
11 庞希愚,王成,全春玲.基于角色-功能的 Web 应用系统访问控制方法.计算机工程, 2014,40(5):144–148.
12 刑天扬,曹曼.基于TP-RBAC权限树算法研究及应用.计算机工程与设计,2010,31(5): 950–956.
13 尹建伟,徐争前,冯志林,等.增强权限约束支持的基于任务的访问控制模型.计算机辅助设计与图形学学报,2006,18(1):143–149.
14 李姝柠.基于 PDM 的权限管理研究.机械设计与制造,2005,12(1):122–125.