PDM/PLM 系统授权模型的研究和应用

北京清软英泰信息技术有限公司　卢亚辉　　耿坤瑛

摘要：本文对几个主流 PDM/PLM 系统授权模型进行分析和比较，并着重介绍了 TiPLM 的授权模型的结构和特点，为企业实施 PDM 系统的权限管理部分提供了借鉴。

1．前言

产品数据管理系统 PDM 和产品全生命周期管理系统 PLM 是以软件为基础，管理与产品相关的信息和所有与产品相关的过程的技术。随着数据库技术与面向对象技术的应用，PDM/PLM 技术得到了迅速的发展，并且逐步实现了与企业其它信息系统如 CAD、CAPP、 ERP、CRM 等系统的集成。PDM/PLM 系统管理的范围不仅限于设计部门和制造部门，也涉足到销售、制造、财务、售后服务等各个部门。

PDM/PLM 系统的安全是靠认证、访问控制、审计、加密等多种技术共同协作来保证的。访问控制技术处于系统安全的中心环节，保证了数据的保密性、完整性和可用性。在企业信息化程度越来越高的今天，PDM/PLM 系统中的访问控制技术发挥了越来越重要的作用。访问控制技术和授权模型在很大程度上影响着 PDM/PLM 系统的可用性、易用性和安全性。

目前已经提出的针对信息系统的访问控制模型有很多种，如：矩阵模型、自主访问控制模型、强制访问控制模型、基于角色的访问控制模型、工作流访问控制模型等，大多数 PDM/PLM 系统的授权模型往往是上述几种授权模型的综合。

2．主流 PDM/PLM 系统授权模型的比较

表 1 给出了几个主流 PDM/PLM 系统授权模型的比较。下面主要介绍一下这些系统在授权模型方面比较有特色的地方。

2.1 WindChill

WindChill 采用了 Domain（域）的概念，一个 Domain 是一些不同类型的对象的集合。在每个不同的 Domain 上可以定义不同的访问控制策略和访问控制权限。

在每个 Domain 上的访问控制策略是由一系列的访问控制规则组成的。访问规则规定了

主体对客体在各种生命周期状态下的访问权限。规则的一般形式为“if <antecedent> then <consequent>”。这些规则是可以沿类树从父类向子类蔓延。WindChill 采用 ACL（访问控制列表）的方式来体现一个对象上的访问控制规则。

2.2 Teamcenter Enterprise

Teamcenter Enterprise 中的权限控制使用 “基于规则” 的方式，可以通过规则来实现对用户操作权限的控制，控制用户、角色、工作组和部门对一个对象、一类对象或数据仓库的操作权限，并可与电子流程相结合。Teamcenter Enterprise 支持三类规则：

访问控制规则（Message Access Rules）

通知规则（Notification Rules）

数据定位规则（Location Selection Rules）

Teamcenter Enterprise 中提出了动态用户的概念，一个用户，只有在满足某种属性条件的前提下，才可以具有某些权限。

2.3 Teamcenter Engineering

Teamcenter Engineering 通过两种方式控制用户对数据文档的访问：

- 面向对象的访问控制方式
- 以规则为基础对数据对象实行分类访问控制

其中规则方式是一种粗线条的管理方式，在规则控制的访问（Rule_Based Access）控制中，可根据数据对象当前的状态、类型、所属用户或组三个属性统一确定可存取该数据的人员范围。

Teamcenter Engineering 中同样采用了基于角色的访问控制，一个用必须以某种角色登陆，才能获取相应的权限。Teamcenter Engineering 通过存取规则定义表，初始化权限模型，比较容易阅读。

表 1 一些 PDM/PLM 产品的授权模型分析

	WindChill	Teamcenter Enterprise	Teamcenter Engineering	TiPLM
授权方式	基于规则	基于规则	基于规则/矩阵	基于矩阵
授权的作用范围	Domain	全局	全局	全局
授权的等级蔓延	通过类树	通过类树		多级蔓延

访问控制的实现	访问控制列表	规则解析，规则缓存	访问控制列表	访问控制矩阵实时计算
主体	用户、角色、组织	用户、角色、组织、动态参与者	用户、角色、组织	用户、角色、组织
主体的激活和冻结	是	是		是
角色	与 Project 相关	与 Project 相关	与 Project 相关	独立的主体
对象控制粒度	类、对象	类、对象	类、对象	类、对象、属性
基于条件的授权	是	是	否	是
基于生命周期	是	是		是
管理权限范围	通过 Domain 控制授权范围	只有全局的系统管理员	只有全局的系统管理员	管理权限可以分级
管理权限	Administrative		更改所有权	创建/删除用户，创建/删除角色等多种管理权限
负授权	是	否	否	是
操作	Read, Modify, Create,Delete, All 等	Message, MessageGroup	读写删改等	读写删改定版升版等

（注：表 1 中的比较仅限于作者对上述系统用户手册中有关权限介绍内容的理解）

3. PDM/PLM 授权需求的多元化

虽然目前对 PDM/PLM 系统的授权模型的研究和应用有了很大的进展，但是这些模型并不能完全支持客户在实际使用中提出的各种权限需求。这些需求主要表现在下面几个方面：

- 主体的多元化：权限不仅需要定义到用户和角色上，而且必须支持权限定义在其它类型的主体上。比如，用户可以通过分组形成静态组织，也可以通过动态分组形成项目组，有时需要把权限定义到这些静态组织和项目组上。
- 权限的多元化：权限根据不同的客体应用，可以分为对象类权限、对象权限、属性权限、部件权限、管理权限、二次分配权限、代理权限等。普通的基于类的授权，已经不能满足实际的应用需求，必须建立对类的实例化对象以及对象属性的权限控制。另外，相对于用户和类来说，实例化对象的数量非常庞大，如何保证访问验证的效率是授权模型在实现过程中最大的难题。
- 对象在生命周期中的权限变化：同一个用户，对同一个对象，在该对象的不同生命周期，有着不同的权限。如设计员在图纸对象的设计阶段有修改的权限，在该图纸被发布之后，

该设计员就只有浏览和读的权限了。这就要求把权限定义到对象的生命周期上。

- 统一的授权模型框架：随着 PDM/PLM 系统的发展，PDM/PLM 系统中包括的子系统越来越多，比如除了传统的数据管理子系统，很多 PDM/PLM 系统还集成了工作流子系统，ERP 子系统，CAD 子系统等。这就要求必须有一个统一的授权框架来支持在 PDM/PLM 中控制这些子系统中的数据的权限，而不能只由各个子系统的授权模型来控制权限。
- 权限分级管理：目前大部分 PDM/PLM 系统的权限管理都由全局的系统管理员角色来担任，该系统管理员负责分配整个系统的权限。由于该系统管理员可以无所不为，实际上系统管理员成了企业安全最大的漏洞。而在实际应用中，由于部门之间往往存在着各种利益冲突，所以在实施数据的管理中，不仅有全局化的数据，而且各个部门会有各自的数据，这就要求管理员的权限必须受到限制，不能随意访问各个部门的私有数据。此外，从实际的运行管理来讲，该系统管理员也无法详细了解各个部门的人员对权限使用的要求，无法更好地设置企业的权限。所以需要建立分级的权限管理员。
- 规则授权和矩阵授权的结合：基于条件表达式的规则授权有很高的灵活性，但是当规则增多时，系统地效率会大大下降，因为需要逐条对规则判断。另外一个对象可能会出现在多条规则中，所以需要一套复杂的机制来处理规则之间的授权冲突。而基于矩阵的授权因为可以直接利用数据库的查询机制，所以有很高的效率。但是基于矩阵的授权灵活性、扩展性较差。如何把这两种方式结合起来，从而实现灵活高效的授权机制，以适应日益复杂的企业对授权的需求，是对 PDM/PLM 系统权限模型提出的一个更大挑战。

4. TiPLM 的授权模型

清软英泰的产品全生命周期管理系统——TiPLM 是基于.Net 开发的采用多层体系结构的 PLM 系统。在 TiPLM 的底层服务中有专门的安全服务模块，为 TiPLM 的各个模块和应用程序提供统一的安全服务。权限验证就是这些安全服务中的一个重要组成部分。为了满足企业的实际需求，TiPLM 的权限模型在基于角色和基于流程的授权模型的基础上，进行了多方面的扩展。其主要特点体现在下面几个方面。

4.1 统一的授权框架

TiPLM 的授权模型的体系框架如图 1 所示。包括了五个模块和四个接口。授权逻辑模型定义了权限验证的逻辑规则。普通用户使用 TiDesk 模块完成其工作，TiDesk 通过接口 1 进

行用户访问的权限验证。权限管理员使用 TiModeler 模块通过接口 2 进行权限的设置。系统定制员使用 TiPolicy 通过接口 3 定制企业授权的元模型和插件扩展。通过接口 4 可以实现针对不同数据库（如 Oracle，SQL Server 等）的符合逻辑模型的权限验证规则。

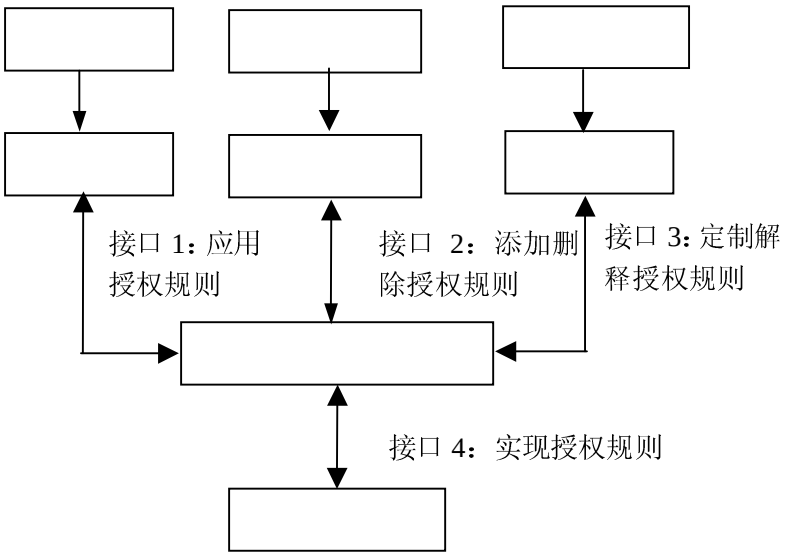

图 1 TiPLM 授权模型

4.2 多级蔓延机制

由于 PDM/PLM 系统中有多种主体和客体类型，比如主体有用户、角色、组织等，客体有类、实例化对象、对象属性等，这些不同的类型有各种依赖和制约关系。所以在实际进行权限验证时，必须综合考虑这些类型之间的关系。TiPLM 系统采用了多级蔓延机制来保证权限验证的正确性和易用性。

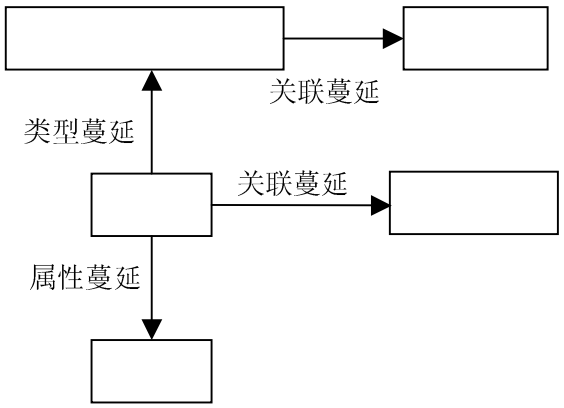

图 2 客体蔓延图

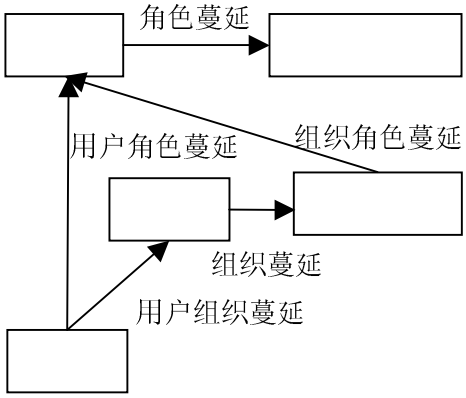

图 3 主体蔓延规则

根据这些不同的蔓延规则，TiPLM 系统授权模型内部定义了不同的权限校验接口，实现

了灵活的可扩展模式。授权模型对外只提供一个统一的验证接口，应用程序通过该接口，就可以获取到各种主客体蔓延后的权限校验结果，而不必关心各种主客体之间的蔓延关系。

4.3 统一的授权机制

随着工作流系统的广泛应用，工作流系统中出现的应用数据越来越多，对于这些数据权限控制的需求也越来越复杂。目前大部分 PDM/PLM 系统都采用了独立于 PDM/PLM 的工作流系统，从而对于 PDM/PLM 中的用户和数据，必须在工作流系统中重新建立一套完整的授权机制，这一方面增加了系统的开发难度，另一方面在实施和运行过程中，增加了管理员的工作量，因为管理员必须同时设置 PDM/PLM 系统和工作流系统的权限。而且目前大部分的工作流系统的权限控制都无法达到 PDM/PLM 系统的权限控制的粒度。

TiPLM 由于采用了统一授权框架，对非流程和流程的数据授权采用了同一套机制，在进行权限验证时，用户可以完全不考虑是否需要通过流程任务来获得权限，底层的逻辑模型可以通过 TiPolicy 定义的元模型自动判断是否需要进行流程授权验证。管理员通过 TiMoldeler 可以直接管理对流程的授权。而且，因为只需要设置流程中特定的权限，而将默认权限交由 TiPLM 系统统一处理，这样大大简化了管理员的工作，又增加了权限验证的粒度。

4.4 多级权限管理

TiPLM 采用了基于管理角色树的多级授权管理模型来进行权限的管理和分配。如下图所示。采用多级管理角色后，分厂 1 的设计部权限管理员只能管理该设计部门的人员、角色、组织、工作流、受控对象等权限，而无法管理分厂 1 的销售部门、制造部门以及分厂 2 和分厂 3 的人员、角色、组织、工作流、受控对象等权限。这样的多级授权管理模型，更好地支持了大型企业或集团型企业的实际权限管理的需求，具有很大的灵活性。

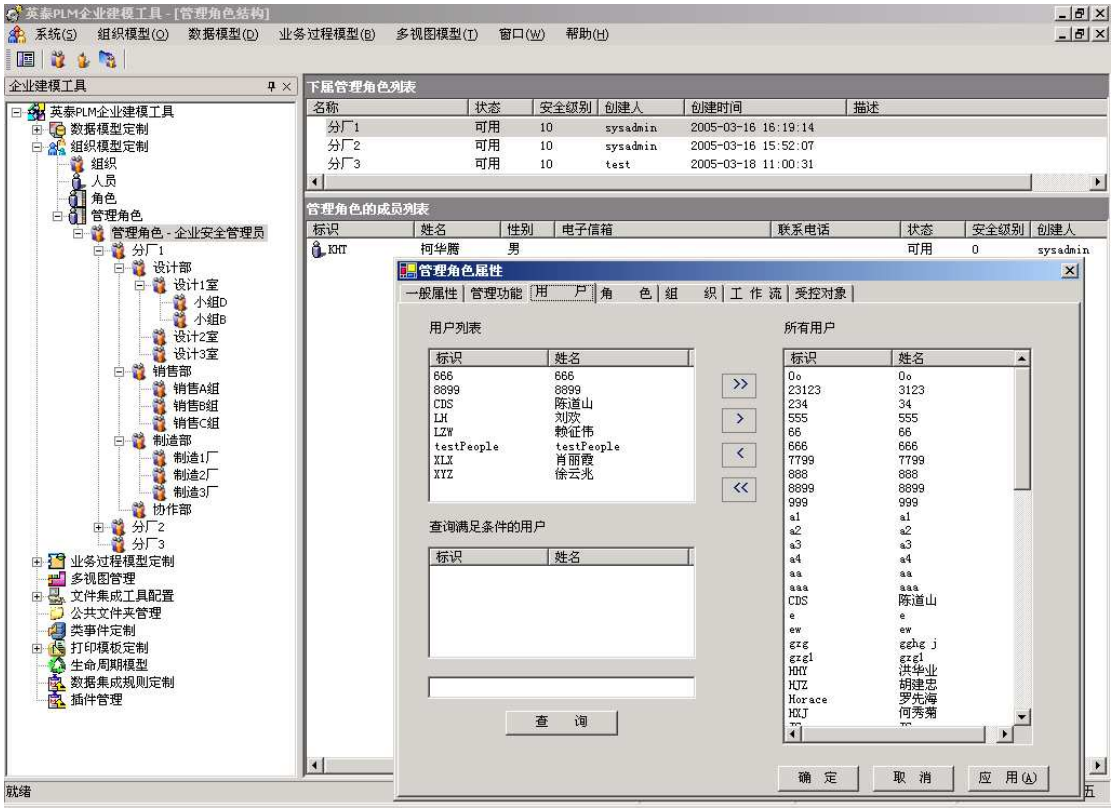

图 4 TiPLM 系统多级权限管理

5. 结束语

企业对 PDM/PLM 系统授权的各种特定需求，是企业 PDM/PLM 系统实施过程中经常遇到的问题。如何准确、快捷、有效、及时地满足这些授权需求，是各个 PDM/PLM 软件厂商都需要考虑的问题。虽然这个问题的影响因素包括很多方面，但是，一个具有支持可定制的、开放的、易扩展的授权模型的系统是至关重要的，也是必须的，否则将无法满足企业日益增长和变化的需求。综上所述，可以看到 TiPLM 系统可以从多个层面满足企业在 PDM/PLM 系统实施和应用过程中对授权的不断变化的需求。