企业 CMS 中 RBAC 模型的研究与改进实现①

刘一田 孔 震 (国网电力科学研究院 江苏 南京 210003)

摘 要： 传统内容管理系统中,对用户直接授权的方法虽然简单,但不易管理 ;基于角色的访问控制方法(RBAC)增强了权限管理的灵活性和易扩展性，却可能造成权限泄露；给出 ECMSAC 模型，在 RBAC 的基础上，引入可实施的最小特权原则，减少了权限泄露的可能，提高了 CMS 的安全性。

关键词： 基于角色的访问控制；内容管理系统；最小授权原则

Research and Improved Implementation of RBAC Model on Enterprise Content Management System

LIU Yi-Tian, KONG Zhen

(State Grid Electric Power Research Institute, Nanjing 210003, China)

Abstract: The method of granting users directly in traditional content management system is simple to implement, whereas it's difficult to manage. The method of RBAC enhances the flexibility and scalability of privileges management. However, it may lead to the leak of privileges. To slove the problems, this paper proposes a ECMSAC model, based on RBAC. It brings in applicable Least Privilege Theorem, reduces the likelihood of privilege's leak and boosts the security of CMS.

Keywords: role-based access control; content management system; least privilege theorem

当前，企业在建设综合网站与管理信息资源时，主要使用内容管理系统(CMS)以减轻网站管理员的负担。内容管理主要针对的是各种非结构化或结构化的数字资源的发布、管理、查询、浏览等，内容的管理人员使用 CMS 来提交、修改、审批信息内容。

CMS 中所有的信息资源分别隶属在不同的主题栏目中，且同一主题栏目中的信息往往由不同的用户发布、管理。面对多用户的访问，需要有一套权限分配与控制机制来增强 CMS 的安全性。基于角色的访问控制模型(RBAC)是当前开发多用户信息系统常用的安全控制模型，RBAC 的基本思想是将权限与角色相关联，用户根据它的责任和资格被指派到相应的角色而获得权限。在 RBAC 管理模型的各种指派中，可能存在非信任主体执行非法的管理操作，使得非信任主体取得了合法权限，或者非信任主体在执行合法权限时由于权限的隐式操作而取得了合法权限[1]。因此，权限泄露问题依然是 RBAC 管理模型中主要的安全问题。本文给出了 ECMSAC 模型，对 RBAC 模型进行了适当的改进，引入最小授权原则，简化了权限控制操作，基本避免了权限泄露，初步解决了企业内部各组织之间的授权管理和安全控制问题。

1 CMS访问控制框架

通过分析调查电力企业内的信息化系统，企业组织机构内的 CMS 行为角色分为两大类,一类是安全管理员，拥有所有权限，可以增删主题栏目，设置查看主题栏目的角色，以及对主题栏目内的内容进行增删查改等各种设置操作；其次是一般管理员，只能对其角色范围内的主题栏目内的内容进行增删查改，以及在安全管理员的权限设置的基础上增加细粒度的角色访问控制权限。

基于以上访问控制的基本要求，本文设计了以下访问控制模型方案：只有安全管理员允许改变安全属性；角色可以完全或部分地继承权限；模型支持主动或者被动的访问控制，也包括严格的最小特权原则；访问权限可以随着角色的改变而改变。除了这些基本

① 收稿时间:2009-07-12;收到修改稿时间:2009-09-18

要求，根据企业组织的特点，开发一个 ECMSAC 模型也应该考虑以下条件：企业根据职责分为不同的部门，访问的权限和资源对象能够随着部门的改变实时变化，不同的部门所看到的主题栏目是不同的；部门之间公用的主题栏目内只允许内容的创建者进行内容的编辑和删除；模型很容易和其它访问控制模型或策略集成。

图 1 描述了 ECMSAC 模型的基本框架，企业内的 CMS 维护可以归纳为维护公共内容信息和私有内容信息的活动。企业门户网站由不同的主题栏目组成，而各个主题栏目分别由不同的组织进行维护，安全管理员首先为主题栏目设置安全策略，然后将相应安全策略内的角色赋予各组织的一般管理员，一般管理员根据组织内部的私有资源的属性建立子分类，并使用 RBAC 对私有资源的访问进行控制。对于企业内部共享的公共资源，安全管理员授予该主题栏目虚拟的创建者角色，只允许资源的创建者进行权限操作。

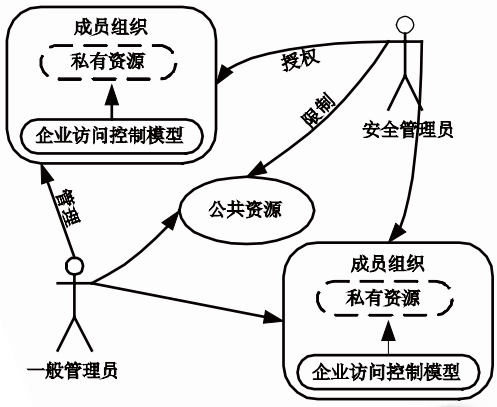

图 1　ECMSAC 模型的基本框架

2　RBAC管理模型及改进

2.1 RBAC 管理模型

定义 1(RBAC 管理模型). 用状态变换系统 M=<K，Σ，δ，Q>来模拟 RBAC 管理模型[2]，其中：

1) K 是状态集；

2) Σ是操作集；

3) δ：K×Σ→K 状态转移函数；

4) Q 是系统策略集。

K 是状态集，假设，k 是一个六元组<U，P，R，UA，PA，RH>。Σ是操作集，假设Σ是 can_assign，can_revoke，can_assignp，can_revokep 和 can_modify 组成的集合。状态变化函数δ定义了状态变换系统的变化规则。如果输入 t，其中 $t \in \Sigma$，系统 M 从状态 k_1 到状态 k_2，这表示当它在状态 k_1 时读入 t，转移到状态 k_2，记为 $k_1 \Rightarrow {}_{\delta}^{t}k_2, k_1 \Rightarrow {}_{\delta}^{*}k_2$ 表示状态系统 M 经过 0 次或者多次状态变化从 k_1 变化到 k_2，并且称在状态变换系统 M 中，状态 k_2 相对于状态 k1 是可到达的。Q 是系统策略集。通常在作访问控制决策时，我们需要考虑诸如此类的安全问题：① 是否有不合法的用户能够取得合法权限从而导致权限泄露? ② 是不是合法的用户取得了合法的权限从而保证操作的可执行性？我们定义的分析模型主要考虑以下两种安全策略：

1) 可能性安全策略。例如，$Own[r] \supseteq \{p\}$ 可能么？这一策略用于查询是否系统 M 存在某个可达状态，在这个状态下，角色 r 拥有权限 p。只有问题“非信任实体是否可能获得了合法权限从而导致权限泄露”的回答是否定的，才意味着系统是安全的。

2) 必然性安全策略。例如，$Own[r] \supseteq \{p\}$ 必然么？这一策略用于查询系统 M 的所有可达状态是否角色 r 拥有权限 p。只有查询“信任实体是否取得了合法的权限从而保证操作的可执行性”的回答是肯定的，才意味着系统是安全的。

2.2 改进的 RBAC 模型

在上面两种安全策略中，让合法的用户拥有最小的合法权限是必要的，最小授权是指系统应该授予用户完成工作必须的最小权限集合，也称为最小特权原则，是授权管理必须遵守的重要原则之一。安全管理员进行授权操作时，授予他人的管理权限可能隐含其它的权限。如果隐含权限能够满足用户请求，将其授予用户能够降低权限滥用和泄漏的风险，实现最小授权。

支持最小特权的授权操作要求相对复杂。通常情况的授权流程如下：用户提出权限请求，管理用户授予其恰当的角色，从而用户间接获得相应权限完成工作。由于存在隐式授权，管理用户首先判断哪些角色是“恰当”的，即能够最小满足权限请求；然后再明确自己是否拥有将这些角色授予用户的“恰当”能力，即最小管理操作集合实施授权。

授权的最终目标是用户获得对资源的访问权限，即客体权限，但实施授权的管理用户需要将“恰当”的角色授予用户。如果角色拥有的隐式授权过多，则

可能造成权限的滥用和扩散；反之，权限过少则无法完成工作。下面给出最小角色的定义。

定义 2. 给定 RBAC 状态错误！未找到引用源。，客体权限 p 的最小角色 r 是所有隐含 p 的角色中基数最小的，表示为

$$p \in OP, r \in R, p \in own(r') \to \left|own(r')\right| \geq \left|own(r)\right|.$$

由定义可知，客体权限的最小角色可能为多个。此时，管理用户可以根据具体的安全策略选择授予用户。用户提出的权限请求可能包括多个客体权限，表示为集合 OPS={op$_1$,⋯,op$_n$}。理想的情况是，管理用户找出满足权限请求且包含的客体权限数量最少的最小角色集合 MRS={r$_1$,⋯,r$_m$}，将其授予用户。 事实上，MRS 问题是 NP-hard 的，根据它的可行解[3]计算方法，首先找出与 OPS 相关的角色集合 RQ，根据角色的权重与对客体权限的涵盖性之间的关系递归选择角色集合，直至所选角色集合的权限包含 OPS。

3 ECMSAC模型的权限分配

Web 上的应用权限定义比较简单，很难保障系统运行的安全。CMS 作为 Web 应用的典型代表，简单而大量的角色定义容易导致授权混乱以及权限泄露，需要对其权限集合进行合理划分，从而形成多层粒度的权限体系。

在 ECMSAC 模型中，企业安全管理员拥有 CMS 中的所有权限，各部门都有维护和发布信息的专责，安全管理员根据部门职责为各专责用户创建角色，例如，自动化处专责角色，生技处专责角色等，每个部门都有需要发布的公共信息和仅供内部查看或使用的私有信息。为了便于区分，我们根据信息特征属性将管理信息分为文件、新闻、链接和文本，所有的信息统称为内容，各种类型的内容又可以归类在同一个主题栏目内，根据电力企业的特点，我们约定主题栏目首先按部门属性进行分门别类，并且支持嵌套分级，子栏目自动继承父栏目的权限设置，同时允许子栏目灵活的扩展或覆盖父栏目的权限设置，这样首先从结构上保证了 CMS 的层次清晰，便于管理。

从概念上讲，权限可以直观的定义为是否允许用户的某个操作，定义权限即定义有哪些操作和哪些被操作的对象。对主题栏目以及内容的操作可以简单归纳为创建、编辑、删除、发布和权限设置，因此定义操作集合 O={new, modify, delete, publish, privilegeSet}。假设 C 为所有内容的集合，定义权限 P 如下：

$$P = C \times O \quad ,$$

权限 P 是所有内容和所有操作之间的关系。由于内容数量众多，对内容权限的设置比较繁杂，因此，通过主题栏目进行授权更为方便，设 T(Cat, E)为内容管理系统的层次化分类体系(Taxonomy)，Cat 为主题栏目集合，有以下公式成立[4]：

$E \subseteq Cat \times Cat$. Cat 中的元素由 E 关联，构成一个森林 T(树的集合)。

$CatC \subseteq Cat \times C$. C 中的元素与 Cat 中的元素有从属关系，从而将内容分配到主题栏目中，即

$$\forall (c \in C) \exists cat\left[(cat, c) \in CatC\right].$$

因此，通过对主题栏目集合的授权，间接地对主题栏目内的内容集合实施集体授权，体现了主题栏目和内容之间的一致从属关系，操作直观，提高了授权的效率。

3.1 最小特权下的 CMS 权限设置

以电力系统部门为例，自动化处下有 A、B 两部门，共同使用 CMS 来管理各自的信息资源。定义部门主题栏目为 KIND，主题栏目下的内容为 CONTENT；定义系统角色分别为安全管理员 SSO，部门专责 SR，部门领导 LEADER，一般员工 EMP，其中的角色权限设置关系如表 1 所示：

表 1 角色权限设置关系示例

角色	权限设置
SSO	*P*:{file, {company_KIND, *company*_CONTENT},*admin*}
SR	*P*$_1$:{file,{dep_KIND, dep_CONTENT},*admin*}
LEADER	*P*$_2$:{file, dep_CONTENT,*modify*}
EMP	*P*$_3$:{file, dep_CONTENT,{*read*,*new*}}

由于工作需要，A 部门用户 A_user 需要查看 B 部门文档 B_doc，由于 RBAC 模型中用户无法与权限关联，无法将 B 部门的管理权限直接赋予 A_user，只能转而授予其它角色。在已有的管理权限设置中，为了完成用户所请求的权限，SSO 可以将角色集合 RQ = {B_SR、B_LEADER、EMP}中的任一个或组合授予 A_user，而 A_user 仅需要查看 B_doc，假设 SSO 授予 SR 给 A_user，显然 A_user 拥有的权限过多，造成了权限的潜在泄露，不符合最小特权原则。根据最小角色匹配的计算方法，分别计算 RQ 中每个角色的

t(r)，选择最小的 t(EMP)，即 MRS={EMP}，将其赋予 A_user，完成查看功能所需的最小授权。此时 A_user 仍然获得了创建内容权限，如果有必要，SSO 可以增加新的角色层次 P5：{file，dep_CONTENT,read}，并将其赋予 A_user，实现绝对的最小授权。

3.2 CMS 的权限设置的应用实现

为了实现 CMS 的权限设置，我们设计了如图 2 所示的数据库表结构[5,6]

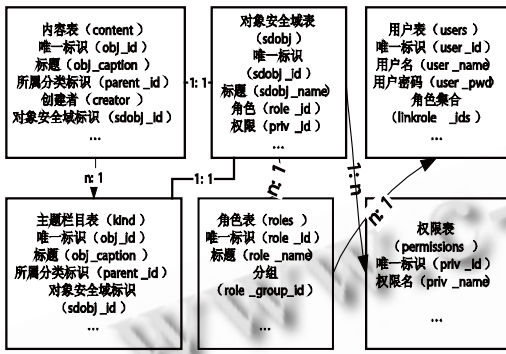

图 2　CMS 权限设置相关数据库构造

图 3 CMS 部分视图

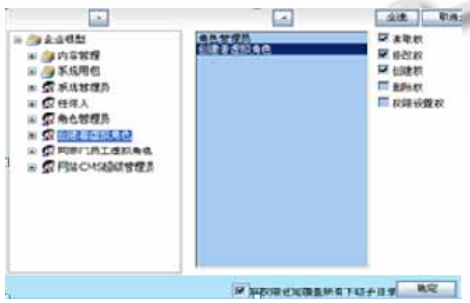

图 4 CMS 权限设置对话框

CMS 视图采用树形结构组件来展现主题栏目，如图 3 所示，树节点代表主题栏目类的实例对象，第一层节点代表了组织结构中各个独立部门需要维护的主题栏目，SSO 负责设置树中第一层节点的对象安全域，设置允许访问主题栏目节点的角色权限关系集合，如图 4 所示。主题栏目的权限设置规则在第 3 节已经定义，针对用户的访问控制规则为：如果用户的角色和所选主题栏目对象的对象安全域中的角色相匹配，则允许在权限范围内操作对象。采用网格列表组件来显示内容集合。对于主题栏目中的内容，根据内容的创建者属性进行权限的限制，只允许内容的创建者对内容进行修改和删除。通过限制对象安全域和用户本身的角色，方便地完成了基于 RBAC 的权限分配，在具体的权限分配中，根据最小匹配算法进行授权，提高了系统的安全性。

4　结语

在研究了 RBAC 的基础上，引入可实施的最小特权原则，有效避免了权限泄露问题；结合应用广泛的内容管理系统，给出了改进的访问控制模型，使权限设置的管理方式简单、高效、安全，能够很好的满足企业应用的需要。

参考文献

1 刘伟,蔡嘉勇,贺也平.基于角色的管理模型隐式授权分析.软件学报, 2009,20(4): 1048－1057.

2 Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. IEEE Computer, 1996,29(2):38－47.

3 Chen L, Carmpton J. Inter-Domain role mapping and least privilege. Lotz V, Thuraisingham BM, eds. Proc. of the 12th ACM Symp. on Access Control Models and Technologies. Sophia Antipolis: ACM Press, 2007. 157－162.

4 曹勇刚,金茂忠,刘超.内容管理系统中基于角色的访问控制模型的改造和应用.北京航空航天大学学报, 2005,31(10):1153－1158.

5 何诚万,何克清.基于角色的设计模式建模和实现方法.软件学报, 2006,17(4):658－669.

6 孟建良,亢建波.角色访问控制模型在两票管理系统中的应用.电力系统自动化, 2004,28(23):81－84.