文章编号:1674-2869(2009)09-0053-02

基于逻辑式的NTFS用户角色计算模型

戴祖旭
(武汉工程大学 理学院,湖北 武汉 430074)

摘 要:为充分利用NTFS提供的文件(夹)级别的基于角色的访问控制技术,根据角色表和用户所需权限矩阵分析了角色指派应满足的逻辑条件,建立了用户角色计算的逻辑可满足式数学模型.该模型可为用户角色指派提供快速准确的决策依据.

关键词:NTFS;基于角色的访问控制;用户角色指派;逻辑公式
中图分类号:TP 309.2 文献标识码:A

0 引 言

RBAC (Role-Based Access Control)[1,2]的安全思想是分离用户和资源,采用的方法是在用户和资源之间引入角色层,资源的访问权限被组织成不同的角色,需要特定权限的用户被指配到合适的角色.这种用户权限管理方法特别适合于那些资源的访问权限相对固定,而用户经常发生变化的环境,比如网络文件服务器与各类管理信息系统[3-4].Windows NT及以上版本的操作系统都支持NTFS(New Technology File System)[5],NTFS又是支持RBAC的[6],因此,在运行上述操作系统的服务器上可直接利用这个便利进行文件(夹)资源安全管理而无需额外的投入.RBAC的实现过程包括两部分,即定义角色和用户角色指派.第一部分通常与应用环境密切相关并且角色一旦定义就具有相对稳定性,后一部分则是系统管理员维护的重点,因为用户以及用户的任务变化较多.本文试图建立NTFS环境下用户角色指派的数学模型,结合逻辑公式计算机求解算法[7-8],快速准确地根据用户的任务来计算合适的角色.

1 NTFS文件(夹)权限与角色

对每一个文件对象,NTFS提供了13个特别访问权限:1)执行文件,2)读取数据,3)读取属性,4)读取扩展属性,5)写入数据,6)添加数据,7)写入属性,8)写入扩展属性,9)删除子文件夹和文件,10)删除,11)读取权限,12)更改权限,13)获得所有权.对每一个文件夹对象,NTFS提供了13个特别访问权限:1)遍历文件夹,2)列出文件夹,3)读取属性,4)读取扩展属性,5)创建文件,6)创建文件夹,7)写入属性,8)写入扩展属性,9)删除子文件夹和文件,10)删除,11)读取权限,12)更改权限,13)获得所有权.系统管理员可通过对象的属性→安全页来设置上述权限.对象的这些访问权限被组织成各种角色,每个角色都是一个多元组的集合,多元组描述了对象标识以及相应的权限列表.

一般的,假设系统有 n 个对象,分别记为 $o_1,\cdots,o_n$,定义了 m 个角色,记为 $r_1,\cdots,r_m$,再用 $p_{ijk}\in\{0,1,2\}$ 表示角色 r_i 对对象 o_j 的第 k 种权限的值,$i=1,\cdots,m$,$j=1,\cdots,n$,$k=1,\cdots,s$,取值0表示没有权限,取值1表示有权限,取值2表示拒绝该权限.角色与对象及其权限的关系如表1所示.

表1 角色示意表

Table 1 Definition of Roles

色色	对象	权限		
r_1	o_1	p_{111}	…	p_{11s}
r_2	o_1	p_{211}	…	p_{21s}
…	…	…	…	…
r_m	o_1	p_{m11}	…	p_{m1s}
…	…	…	…	…
r_m	o_n	p_{mn1}	…	p_{mns}

2 用户角色分配

设新用户 u 为完成某项任务所需要的操作权限表示为矩阵 $\boldsymbol{U}$,且

收稿日期:2008-10-15
基金项目:湖北省教育厅科学技术研究项目(D20081506)
作者简介:戴祖旭(1967-),男,湖北远安人,副教授,博士.研究方向:信息安全.

$$\boldsymbol{U}=\begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1s} \\ u_{21} & u_{22} & \cdots & u_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ u_{n1} & u_{n2} & \cdots & u_{ns} \end{bmatrix} \tag{1}$$

其中，$u_{jk}\in\{0,1,2\}$表示新用户 u 对对象 o_j 的第 k 种权限的值，$j=1,\cdots,n,k=1,\cdots,s$，取值含义同 p_{ijk}. 下面介绍指派 u 到角色的计算方法.

定理　仞然用 r_i 表示命题：$u\in r_i,i=1,\cdots,m$，对表 1 中定义的角色和(1)中给定的权限，u 到角色的指派$(r_1,\cdots,r_m)$是逻辑式 $f(r_1,\cdots,r_m)=\bigwedge_{j=1}^{n}\bigwedge_{k=1}^{s}\left[\left(\bigvee_{\substack{u_{jk}=p_{ijk}\neq 0\\ i\in\{1,\cdots,m\}}} r_i\right)\wedge\left(\bigvee_{\substack{u_{jk}+p_{ijk}=3\\ i\in\{1,\cdots,m\}}}\neg\, r_i\right)\right]=1$ 的解. 其中，$\wedge,\vee,\neg$ 分别表示合取、析取和非运算.

证明　任意给定的 $u_{jk}(j=1,\cdots,n,k=1,\cdots,s)$与 $p_{ijk}(i=1,\cdots,m)$的取值有如下情况：

(1)$u_{jk}=0,p_{ijk}\in\{0,1,2\}$，或 $u_{jk}=1\in\{1,2\}$，$p_{ijk}=0$. 表明用户不需要对象 o_j 的第 k 种权限，从而无需指派操作，或角色 r_i 不具备对象 o_j 的第 k 种权限，从而指派与 r_i 无关；

(2) $u_{jk}=p_{ijk}=1$，或 $u_{jk}=p_{ijk}=2$. 表明用户需要对象 o_j 的第 k 种权限，且角色 r_i 具备对象 o_j 的第 k 种权限，因此用户可以指派到 r_i，或用户拒绝对象 o_j 的第 k 种权限，且角色 r_i 也拒绝对象 o_j 的第 k 种权限，因此用户也可以指派到 r_i；

(3) $u_{jk}=1,p_{ijk}=2$，或 $u_{jk}=2,p_{ijk}=1$，即 $u_{jk}+p_{ijk}=3$. 此时用户的需要与角色正好相反，因此用户不能指派到角色 r_i.

综上分析，对权限 u_{jk} 来说，用户与角色的指派关系应满足$\left[\left(\bigvee_{\substack{u_{jk}=p_{ijk}\neq 0\\ i\in\{1,\cdots,m\}}} r_i\right)\wedge\left(\bigvee_{\substack{u_{jk}+p_{ijk}=3\\ i\in\{1,\cdots,m\}}}\neg\, r_i\right)\right]$. 所以，对全部的权限 $\boldsymbol{U}$ 来说，用户与角色的指派关系应满足 $f(r_1,\cdots,r_m)=1$.

当逻辑式 $f(r_1,\cdots,r_m)=1$ 无解时，表示没有合适的角色组合满足用户操作权限，需要添加新的角色，或者是用户权限设置不相容.

2　实验结果

某高校有一个成绩管理系统，共有 5 个文件或文件夹对象，3 种角色. 角色定义如表 2 所示. 新用户所需权限矩阵为：

$$\boldsymbol{U}=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \end{bmatrix}$$

表 2　高校成绩管理系统角色表

Table 2　Roles accessing score database of college

角色	操作对象	权限(13 种具体权限见本文第 2 节)
r_1	o_1	(1,1,1,1,0,0,2,0,0,0,1,0,0)
r_2	o_1	(1,1,1,1,0,0,2,0,0,0,1,0,0)
r_3	o_1	(2,1,1,1,0,0,2,0,0,0,1,0,0)
r_1	o_2	(0,1,0,1,0,0,1,0,0,0,1,0,0)
r_2	o_2	(2,1,2,1,0,0,0,0,0,0,1,0,0)
r_3	o_2	(1,1,1,1,0,0,2,0,0,0,1,0,0)
r_1	o_3	(1,1,1,1,0,0,2,0,1,0,1,0,0)
r_2	o_3	(1,1,0,1,0,0,2,0,0,0,1,0,2)
r_3	o_3	(0,0,0,0,1,1,1,1,0,0,1,0,1)
r_1	o_4	(0,1,2,1,0,0,0,0,0,0,2,0,0)
r_2	o_4	(0,1,0,0,1,1,1,1,0,1,1,0,0)
r_3	o_4	(1,0,1,0,0,0,0,0,2,2,0,0,0)
r_1	o_5	(1,1,1,1,0,0,2,0,0,0,2,0,1)
r_2	o_5	(1,1,1,1,0,1,2,0,0,0,0,0,0)
r_3	o_5	(0,1,1,2,0,0,0,0,1,0,1,0,0)

逻辑式 $f(r_1,\cdots,r_m)=((r_1\vee r_2)\wedge\neg\, r_3)\wedge(r_1\vee r_2\vee r_3)\wedge(r_2\wedge\neg\, r_3)\wedge(r_1\wedge\neg\, r_3)\wedge r_1\wedge(r_1\vee r_2)\wedge r_2$.

求得成真赋值为 $r_1=r_2=1,r_3=0$，即用户应指派到角色 r_1 和 r_2，不能指派到 r_3.

参考文献：

[1] Sandhu R. Conyne E J, Lteinszein H, el al. Pole Based Access Control Models[J]. IEEE Compute, 1996,29(2):38-47.

[2] 汪厚祥，李卉. 基于角色的访问控制研究[J]. 计算机应用研究，2005，(4)：125-127.

[3] 何成万，李健，焦素廷. 基于 MVC 模式的科研成果管理系统开发[J]. 武汉工程大学学报，2009，31(1)：79-82.

[4] 舒攀，陈金刚. 数字校园建设中宿舍管理系统的设计与实现[J]. 武汉工程大学学报，2008，30(4)：108-111.

[5] 王兰英，居锦武. NTFS 文件系统结构分析[J]. 计算机工程与设计，2006，27(3)：418-419，484.

[6] 戴有炜. Windows Server 2003 用户管理指南[M]. 北京：清华大学出版社，2004.

[7] 张会凌. 命题公式真值表的生成与公式类型的判定[J]. 甘肃联合大学学报(自然科学版)，2006，20(1)：252-255.

[8] 徐凤生，李天志. 命题公式真值表的生成算法[J]. 计算机工程与科学，2008，30(1)：86-87.

(下转第 58 页)

[5] 刘妹廷，金太东，胡博，等. BP-PID控制在锅炉蒸汽压力控制中的应用研究[J]. 武汉工程大学学报，2009，31(7)：91-94.

[6] 杨海燕，文一凭. 一种面向特征选择的分类神经网络[J]. 武汉工程大学学报，2008，30(4)：114-117.

[7] (美)Martin T Hagan. 神经网络设计[M]. 北京：机械工业出版社，2003.

[8] 王彩霞. 不确定时滞系统的鲁棒容错控制[J]. 甘肃科学学报，2005，17(1)：70-73.

[9] 薛定宇. 控制系统计算机辅助设计——MATLAB语言及应用[M]. 北京：清华大学出版社，1997.

[10] 楼顺天，施阳. 基于MATLAB的系统分析与设计一神经网络[M]. 陕西：西安电子科技大学出版社，1999.

Analysis and implement of separatte chinese medicine besed on BP network

SHEN Bin, QI Fen-ping, JIANG Wei, HU Zhong-gong

(School of Electrical and Information, Wuhan Institute of Technology, Wuhan 430074, China)

Abstract: Based on the construction principle of work and net model the BP net was introduced the BP net. By applying the network's self-learning and self-adjusting capauty to separate Chinese traditional medicine, for non-linear large-scale industrial control industry to provide reference parameters for wortincar large state industrids was provided and the not model was set up to determine technological parameters and set up net model.

Key words: BP network; self-learning; Chinese medicine's separation

本文编辑：陈晓苹

☆

(上接第54页)

Propositional formula based model for NTFS user-role computing

DAI Zu-xu

(School of Science, Wuhan Institute of Technology, Wuhan 430074, China)

Abstract: To benefit the advantage of RBAC technology that NTFS offered in file and folder security management, the logic condition for user-role assignment was studied with the help of role table and permission matrix firstly, and then a propositional formula which computes user-role was putted forward. The model works for making effective and accurate decision to user role assignment.

Key words: NTFS; RBAC; User-Role assignment; propositional formula

本文编辑：陈晓苹