一种基于扩展角色的五层资源访问控制方法

申请号：200510094977.5
申请日：2005-10-24

申请(专利权)人　南京邮电大学
地址　210003江苏省南京市新模范马路66号
发明(设计)人　杨庚　沈剑刚

主分类号　H04L12/24(2006.01)I
分类号　H04L12/24(2006.01)I　H04L9/00(2006.01)I
公开(公告)号　1787456A
公开(公告)日　2006-06-14
专利代理机构　南京经纬专利商标代理有限公司
代理人　叶连生

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 9/00 (2006.01)

[12] 发 明 专 利 说 明 书

专利号 ZL 200510094977.5

[45] 授权公告日 2008 年 1 月 23 日

[11] 授权公告号 CN 100364278C

[22] 申请日 2005.10.24
[21] 申请号 200510094977.5
[73] 专利权人 南京邮电大学
地址 210003 江苏省南京市新模范马路 66 号
[72] 发明人 杨 庚 沈剑刚
[56] 参考文献
CN1537262A 2004.10.13
CN1516401A 2004.7.28
CN1633085A 2005.6.29
访问控制模型分析. 王永，刘秀军，马建峰. 晋中师范高等专科学校学报，第 19 卷第 2 期. 2002
基于访问控制的内网资源管理机制. 李敏，秦志光，蓝天. 福建电脑，第 5 期. 2005
基于任务的动态角色约束关系研究. 皮建勇，刘心松. 四川大学学报（工程科学版），第 37 卷第 1 期. 2005
项目管理系统的动态安全控制模型. 潘善亮，赵杰煜，王小权. 计算机工程，第 30 卷第 7 期. 2004
一种基于用户角色－权限分级的访问控制模型. 袁小芳. 湘潭师范学院学报（自然科学版），第 25 卷第 4 期. 2003
审查员 杨 博
[74] 专利代理机构 南京经纬专利商标代理有限公司
代理人 叶连生

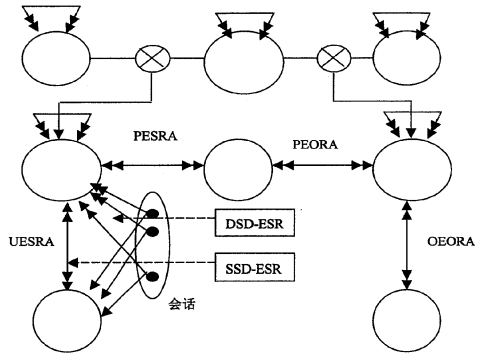
权利要求书 1 页 说明书 5 页 附图 2 页

[54] 发明名称

一种基于扩展角色的五层资源访问控制方法

[57] 摘要

基于扩展角色的五层资源访问控制方法是一种用于信息安全领域中对资源访问进行控制的方法，该方法为：a)应用系统中的用户管理器生成新用户 user1，b)建立一个资源分类文件，对系统中的文件进行资源分类，从而生成客体角色 OR，c)建立一个生成角色控制域文件 K，它包含了目前进行的项目，d)建立一个生成扩展客体角色关系文件 EOR，它将项目中涉及到的资源标注出来，即给出项目与资源的关系，e)建立一个扩展主体角色文件 ESR，它将角色和角色控制域 K 中的项目联系起来，f)将用户 user1 指派为相应的扩展主体角色，g)指派用户 user1 的扩展主体角色的访问权限，从而完成建立访问控制系统的全过程。



1、一种基于扩展角色的五层资源访问控制方法，包括主体、扩展主体角色、角色控制域、扩展客体角色、客体，其特征在于该控制方法为：

a) 应用系统中的用户管理器生成新用户 user1，

b) 建立一个资源分类文件，对系统中的文件进行资源分类，从而生成客体角色 OR，

c) 建立一个角色控制域文件 K，它包含了目前进行的项目，

d) 建立一个扩展客体角色关系文件 EOR，它将项目中涉及到的资源标注出来，给出项目与资源的关系，

e) 建立一个扩展主体角色文件 ESR，它将角色和角色控制域 K 中的项目联系起来，

f) 将用户 user1 指派为相应的扩展主体角色，

g) 指派扩展主体角色的访问权限， 从而完成用户的访问控制系统。

一种基于扩展角色的五层资源访问控制方法

技术领域

本发明是一种用于信息安全技术中对资源访问进行控制的一种新方法，属于计算机与信息安全技术领域。

背景技术

近几年来互联网以及通信网在全球范围内得到了迅猛的的发展，它对人类社会的生活方式产生了极大的影响和改变，而随之而来的网络信息安全问题就显得越来越重要。网络黑客、病毒、信息窃取和干扰等手段的出现，使网络的安全面临严重的挑衅。全球每年都为之付出巨大的代价，高达数亿美元之多，如银行帐户系统被侵入、病毒发作、军事网络干扰等。

访问控制主要有70年代形成的自主访问控制(Discretionary Access Control, DAC）和强制访问控制（Mandatory Access Control，MAC），以及1996年提出的基于角色的访问控制模型（Role-based Access Control, RBAC）。

与DAC和MAC相比，RBAC显示了良好的适应性，并在实际中得到广泛应用，许多研究工作者在此领域进行了深入的研究。基于角色访问控制的基本思想是将权限同角色关联起来，而用户则通过赋予角色来获得相应的权限，用户拥有的全部权限由授予该用户所有角色的权限的并集决定。传统的RBAC包含三个最基本的元素：用户(User)，角色(Role)和权限(Permission)。

用户（User)：是一个访问计算机系统中的数据或者其它资源的主体。用U表示全体用户的集合。

角色（Role)：是指一个组织或任务中的职位或工作，代表了一种资格、权利和责任。用R 表示全体角色的集合。

权限（Permission)：是对计算机系统中的数据或者其它资源进行访问的许可。用P 表示全体权限的集合。

近几年来，网格计算研究领域的兴起，为互联网的应用展示了新平台，世界各国投巨资进行这方面的研究，如欧盟的EDG计划等，中国也由国家教育部组织，构件教育计算网格环境，而计算网格中的访问控制是网格安全的重要组成部分。由于网格计算环境资源的动态性，传统的基于用户、角色和权限构成的三层模型已不适应这种资源的动态性，为了有效地对资源的访问进行控制，必须研究新的资源访问控制方法。

发明内容

技术问题：本发明的目的是提供一种基于扩展角色的五层资源访问控制方法 ，该方法提供基于主体、扩展角色、权限、扩展客体和资源的访问控制机制，这种角色与客体关系能更好地描述实际系统中主体、角色、权限与客体之间的联系，为计算网格环境的访问控制提供新的手段。

技术方案：传统的三层访问控制方法为：

在三层模型中有以下元素：

用户（User）：是一个访问计算机系统中的数据或者其它资源的主体，用U表示全体用户的集合。

角色（Role）：是指一个组织或任务中的职位或工作，代表了一种资格、权利和责任。用R 表示全体角色的集合。

权限（Permission）：是对计算机系统中的数据或者其它资源进行访问的许可。用P 表示全体权限的集合。

传统三层访问控制流程：

1. 应用系统中的用户管理器生成新用户user1，
2. 应用系统中的用户管理器生成角色R。如：管理员，程序员，一般用户等，
3. 对用户指定角色。如用户user1为管理员，
4. 对角色指定某种权限。如管理员可以对所有文件进行“读”和“写”操作，
5. 用户user1根据自己的角色和权限实现对文件等资源的访问，从而实现对资源的访问控制。

本发明的五层访问控制模型

五层访问控制模型中包含如下的元素：

- U：用户集，指网格中的各种用户；
- O：客体集，指网格中的各种资源；
- P：权限集合，指对资源的各种操作；
- K：角色控制域集合，指网格中各种角色控制域组成的集合；
- 扩展主体角色 ESR，有结构化信息的主体角色。其语义表示处于角色控制域 k 中的角色 sr；
- 扩展客体角色 EOR，有结构化信息的客体角色,。其语义表示处于角色控制域 k 中的客体角色 or；

访问控制流程：

1. 应用系统中的用户管理器生成新用户 user1，
2. 建立一个资源分类文件，对系统中的文件进行资源分类，从而生成客体角色 OR。如 OR={资源 1，资源 2}，其中，资源 1={文件 1, 文件 2}，资源 2={文件 2，文件 3，文件 4}，
3. 建立一个生成角色控制域文件 K，它包含了目前进行的项目。如 K={项目 1，项目 2}，
4. 建立一个生成扩展客体角色关系文件 EOR，它将项目中涉及到的资源标注出来，给出项目与资源的关系。如 EOR={{资源 1，项目 1}，{资源 2，项目 1}，{资源 2，项目 2}}，
5. 建立一个扩展主体角色文件 ESR，它将角色和角色控制域 K 中的项目联系起来。如 ESR={{项目经理，项目 1}，{项目经理，项目 2}，{程序员，项目 1}}，
6. 将用户 user1 指派为相应的扩展主体角色。如将用户 user1 指派为扩展主体中的“{项目经理，项目 1}”，
7. 指派扩展主体角色的访问权限，从而完成用户的访问控制系统。如“{项目经理，项目 1}”的权限为“读”，就完成了用户 user1 对项目 1 中的资源访问权限设置，他只能读该资源。

有益效果：本发明的意义在于克服了传统三层访问控制方法的局限性，为信息安全领域中信息资源的访问控制提供新的方法，以更灵活、更符合实际现

实情况的思路设计和实现对资源的访问控制。

本发明的优点在于符合信息系统访问控制的实际情况，即将角色与参与的项目联系起来。实现的方法简单灵活，仅仅在原来的三层模型基础上，建立角色与项目、项目与资源的关系就可以实现，使实用性大为增强，且便于实施各种安全策略。同时通过五层访问控制模型增强了系统的安全性，可以实现同一种角色，在不同的场合，具有不同的访问权限。

附图说明

图 1 是基于角色的访问控制模型示意图。

图 2 是角色继承示意图。

图 3 是传统的三层访问控制模型示意图，其中单箭头表示一对一关系，双箭头表示多对多关系，虚线表示约束关系。

图 4 是本发明五层访问控制模型示意图。

具体实施方式

在实际应用中，考虑一个软件开发公司，有用户 3 人，分别为 1 位经理和 2 位程序员，有 4 个文件资源可以访问，目前正在进行 2 个项目，则应用 5 层资源访问控制方法如下：

1. 应用系统中的用户管理器生成用户集 U={用户 1，用户 2，用户 3}，
2. 建立一个主体角色文件 SR，它包含了所有的当前角色，即 SR={项目经理，程序员}，
3. 建立一个客体集文件 O，它包含了所有资源，即 O={文件 1, 文件 2，文件 3，文件 4}，
4. 建立一个资源分类文件，对系统中的文件进行资源分类，既生成客体角色 OR={资源 1，资源 2}，其中，资源 1={文件 1, 文件 2}，资源 2={文件 3，文件 4}，
5. 建立操作集 OP={读，写，执行}，
6. 建立一个生成角色控制域文件 K，它包含了所进行的项目，即 K={项目 1，项目 2}，
7. 建立一个扩展主体角色文件 ESR，它将角色和角色控制域 K 中的项目

8. 联系起来，即 ESR={{项目经理，项目 1}，{项目经理，项目 2}，{程序员，项目 1}}，

9. 建立一个生成扩展客体角色关系文件 EOR，它将项目中涉及到的资源标注出来，即 EOR={{资源 1，项目 1}，{资源 2，项目 1}，{资源 2，项目 2}}，

10. 将用户指派为相应的扩展主体角色，如用户 1 指派为扩展主体中的“{项目经理，项目 1}”，

11. 指派扩展主体角色的访问权限，如“{项目经理，项目 1}”的权限为“读”，这样就完成了一个用户 1 对资源{项目经理，项目 1}的访问控制。

上面的流程显示了系统中基于主体、扩展角色、权限、扩展客体和资源之间的访问控制过程。这样的过程使我们能够有效地控制同样一个角色在不同项目中的权利，而同样一个资源在不同项目中被访问的权限。如用户 1 在项目 1 中是经理，他可以读与项目 1 有关的文件，而不能读项目 2 有关的文件。反之，一个文件在项目 1 中就可以给用户 1 读，若在项目 2 中，用户 1 就不可以读。

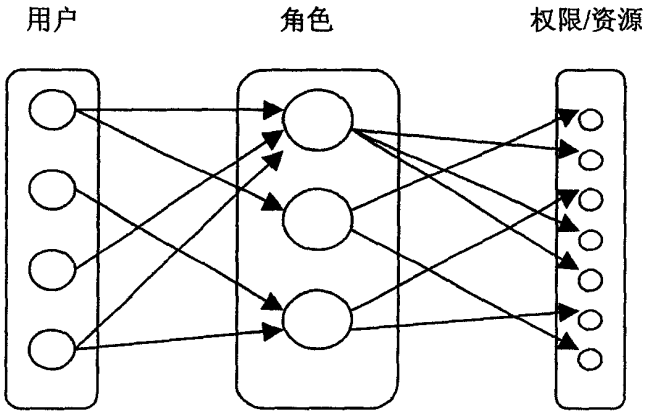


图 1

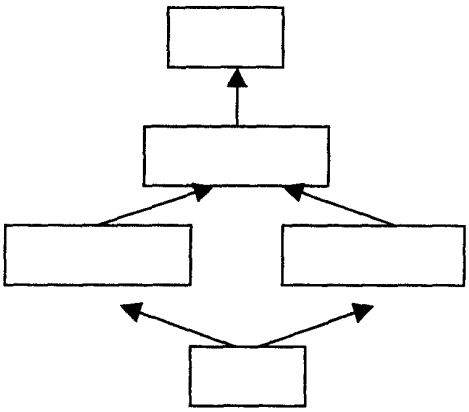


图 2

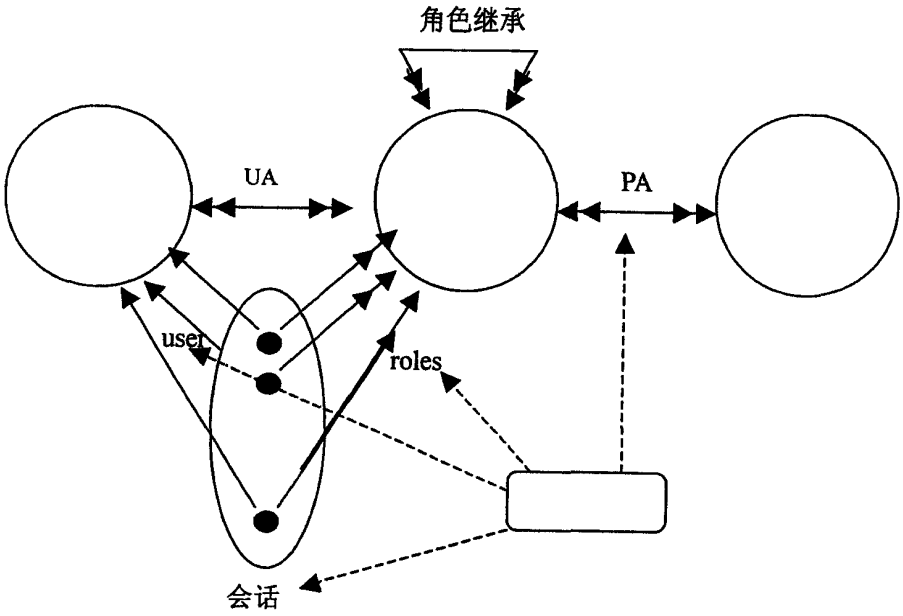

角色继承
UA
PA
user
roles
会话

图 3

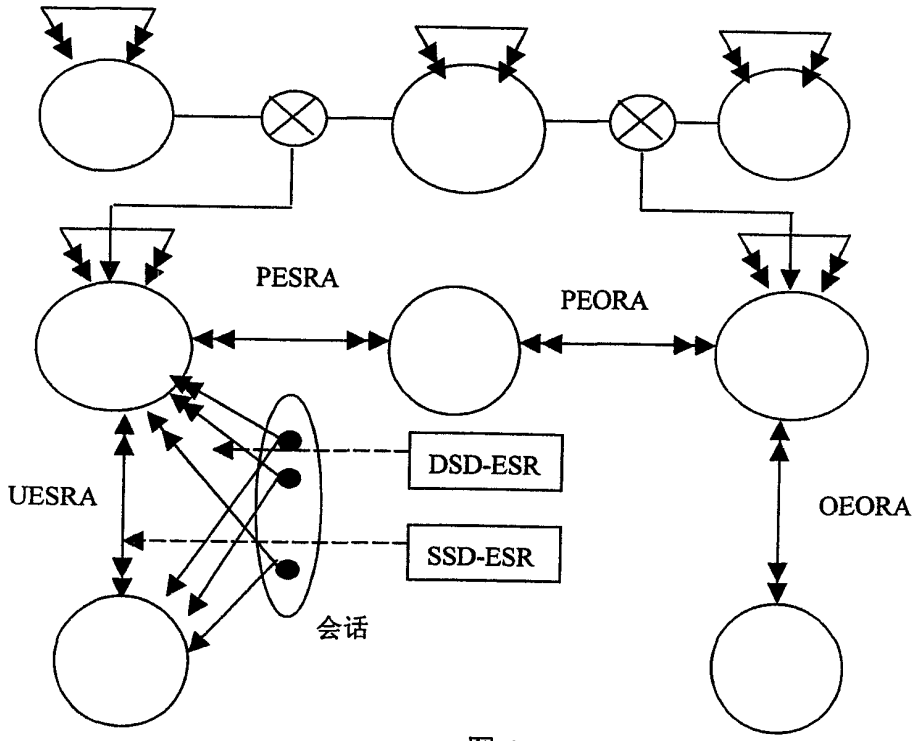

PESRA
PEORA
DSD-ESR
SSD-ESR
UESRA
OEORA
会话

图 4