文章编号:1008-0570(2007)09-3-0021-02

PDM权限管理模块设计与开发

Design and Realization of Permission Management Model on PDM

(1.广东工业大学;2.艾逖恩控股有限公司)袁高群[1] 陈新度[1] 陈 新[1] 箫良皓[2]
YUAN GAOQUN CHEN XINDU CHEN XIN XIAO LIANGHAO

摘要: 提出了面向服务的架构(Service-Oriented Architecture,SOA)和基于角色的访问控制技术(Role Based Access Control,RBAC)相结合的权限管理模型,为系统提供统一的授权管理和访问控制服务,提高了系统的信息安全。并以该模型在PDM系统的实际应用阐述了权限管理模块的设计方法,实现了开放、动态环境下的权限管理。

关键词: 面向服务的架构;基于角色的访问控制;权限管理
中图分类号: TP391 **文献标识码:** B

Abstract:The permission management model has been developed with service-oriented architecture(SOA) and Role Based Access Control(RBAC) which offers a universal service for permission and access control to enhance information security of system.This paper explains the detailed method to design the permission management model of the PDM system and realizes the permission management in open and dynamic environment.

Key words:soa, rbac, permission management

技术创新

1 引言

产品数据管理(Product Data Management, PDM)是以软件为基础的技术,它以产品为管理的核心,以数据、过程和资源为管理信息的三大要素,从而将所有与产品有关的数据、过程资源集成在一起,管理贯穿于整个产品生命周期的产品数据和开发过程。PDM系统的出现为实现数据的协同和共享提供了有效的解决途径。资源共享和信息安全是一对矛盾体,随着数据和资源共享程度的提高,需要提高PDM系统信息的安全。

权限管理模块为PDM系统的其他功能模块提供认证和授权,控制'谁'能够访问系统的服务,用户访问的是'什么服务",用户被授予什么样的'权限",能进行怎样的操作。权限管理模块一旦确定了权限管理和发布的方式以及安全控制策略机制,就可以保证系统的信息安全。因此,合理设计权限管理模块是确保PDM系统信息安全的基础。本文采用面向服务的架构(SOA)和基于角色访问控制相结合的技术,采用统一授权和访问的控制策略与机制,为系统提供统一的权限管理和控制服务,提高系统的信息安全性。

2 权限的基本概念

权限是对资源的一种保护访问,往往是一个极其复杂的问题,但也可简单表述为这样的逻辑表达式:判断"Who对What进行How的操作"的逻辑表达式是否为真。权限的划分包括粗粒度和细粒度两个概念。粗粒度:属于权限逻辑范畴,表示类别级,即仅考虑对象的类别,不考虑对象的某个特定实例。细粒度:属于业务逻辑范畴,表示实例级,即需要考虑具体对象的实例,当然,细粒度是在考虑粗粒度的对象类别之后才再考虑特定实例。权限逻辑配合业务逻辑,即权限系统的目标是向业务逻辑提供服务。设计原则为:'系统只提供粗粒度的权限,细粒度的权限被认为是业务逻辑的职责"。

袁高群: 硕士

基金项目:广东省自然科学基金团队项目(05200197);
国家自然科学基金(50475047)

3 PDM权限管理模型

3.1 面向服务和基于角色

面向服务的架构(Service-Oriented Architecture, SOA)是一个组件模型,它将应用程序的不同功能单元(称为服务)通过这些服务之间定义良好的接口和契约联系起来,以软件服务的形式公开业务功能,使得其他应用程序可以通过已发布的和可发现的接口来使用这些服务。接口是采用中立的方式进行定义的,它独立于实现服务的硬件平台、操作系统和编程语言。服务使用者不必关心与之通信的特定服务,因为底层基础设施或服务'总线'将代表使用者做出适当的选择。基础设施对请求者隐藏了尽可能多的技术。服务通常实现为粗粒度的可发现软件实体,它作为单个实例存在,并且通过松散耦合的基于消息通信模型来与应用程序和其他服务交互。采用SOA架构的PDM系统,具有松散耦合、位置透明、协议独立的特点。因此,面向服务的权限管理模块可以解决在开放、动态环境下认证和授权的问题。

图1说明了服务的调用流程。服务请求者提出服务请求,服务提供者响应服务,将相应的服务发布到服务注册器,服务请求者发现服务和实现相应的功能。可以将权限管理模块的权限管理视为一项服务。

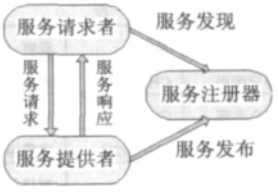

图1 服务的调用流程

基于角色的访问控制(RBAC)引入了角色的概念，角色作为一个用户与权限的接口，所有的授权给予角色而不是直接给用户，实现了用户与访问权限的逻辑分离。权限颗粒表示对资源的访问操作，用户拥有某一种权限是因为用户扮演着某一种角色。基于角色的访问控制方法有两大特征:1.由于角色与权限之间的变化比角色与用户关系之间的变化相对要慢得多，减小了授权管理的复杂性，降低管理开销。2.灵活地支持系统全策略，并对业务变化有很大的伸缩性。因此，基于角色的访问控制可以方便权限管理，很好的描述角色的层次关系，实现最少的权限原则和职责分离的原则。

3.2 PDM系统权限管理模型

图 2 描述了面向服务和基于角色相结合的 PDM系统的权限管理模型。具体的对应过程如下:

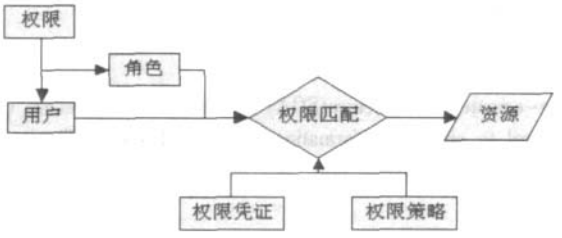

图 2 PDM 系统权限管理模型

1.给用户和角色授权。

2.用户关联角色。

3.用户权限和角色权限与权限凭证相匹配。

4.根据相应的权限策略去操作资源。

用户权限决定用户可以访问的服务(功能模块)。PDM系统采用 SOA 架构，将系统分为用户与权限管理，文档管理、产品结构与配置管理等功能模块，用户权限的权限策略控制和决定用户可以访问哪些已经注册的功能模块，相对于用户权限而言为较粗粗粒度的权限。只具有用户权限的用户并不操作实际的资源。比如用户甲的角色为系统管理员，则用户甲登录系统后，匹配用户权限只能进入用户和权限管理模块，屏蔽了其他的文档管理等功能模块，此时系统管理员对应的角色权限进行匹配后可以进行较细粗粒度层次的操作，实现细粒度的业务逻辑。特定的角色具有统一的权限，方便了权限管理，同时用户权限使得具有相同角色的不同用户具有不同的权限，解决了在开放、动态环境下认证和授权的问题。

3.3 设计实现

3.3.1 数据结构设计

在系统的用户信息表中，为每个用户(userid)设置了用户权限子段 Modulist,角色字段的值 roleid。其中 Modulist 值的匹配结果决定了用户可以使用的系统的功能模块。用户表的主要字段如下表 1 所示。

表 1 用户表

字段	字段说明	类型	说明
userid	用户编码	CHAR(20)	用户代码，主键，唯一
username	用户名称	CHAR(35)	用户真实姓名
modulist	用户权限	CHAR(20)	字段由 0、1 组合而成
roleid	角色编号	INT	用户关联的角色代码
blocked	帐户状态	INT(4)	0 冻结用户，1 用户可用

用户创建界面如图 3 所示。ITM 的 Mini- PDM系统在开源项目 WebERP 的基础上已开发出 main、ppn、ecn、bom 、system四个模块。system模块对应 Mini- PDM系统的用户和权限管理模块。显示 main 选项、显示 ppn 选项、显示 ecn选项、显示 bom 选项四个选项的组合值对应 modulist 字段。默认的角色 E- MANAGER 对应的 roleid 的值为 16。创建用户页面对应的$PageSecurity 变量值为 2，在下一节的权限获取算法中进一步说明。

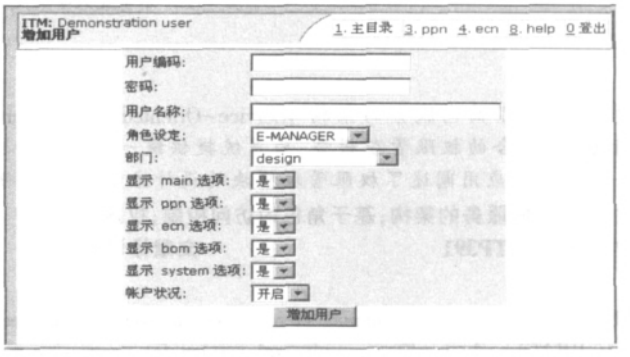

图 3 用户创建界面

本 PDM系统中，一个用户只对应一个角色。用户只有通过角色才能享有角色所具有的权限，经过角色权限匹配后从而访问资源，获得相应的操作权限，角色权限解决了 how的问题。一个角色(roleid)可以对应多种权限(tokenid)，对角色授权后得到角色权限表，可以动态的设定角色的权限，其数据结构如下表 2。

表 2 角色权限表

字段	字段说明	类型	说明
roleid	角色编号	INTEGER	角色代码
tokenid	权限编号	INTEGER	权限代码

3.3.2 权限获取算法

当用户访问 PDM系统的功能模块时，系统首先验证用户提交的身份证书，身份认证通过后进入授权阶段。结合图 1，权限获取的算法如下:

1.使用变量$_SESSION['UserId ']记录用户代号 userid，$_SESSION ['Blocked '] 记录用户状态 blocked，$_SESSION ['modulist '] 记录用户权限，$_SESSION['roleid ']记录角色权限代码。

2.通过判断语句($_SESSION['Blocked ']==1)确定用户状态，为 1 进入用户权限匹配，$_SESSION['modulist ']的值为 0、1 的组合，系统中用的是 xxxxx,每一位对应一个功能模块，最后一位对应的是用户与权限管理模块。若用户甲为系统管理员对应的用户权限是 00001，功能模块用变量$ModuleLink = array (' p_main' ,' p_ppn' ,' p_ecn' ,' p_bom' ,' p_admin')表示，经过用户状态权限匹配后，' p_admin' 功能模块有效，所以用户甲可以进入用户与权限管理模块。

业务操作则需要进行角色权限匹配。

3. 接着从角色权限表中通过 sql 查询找到 roleid 字段等于$_SESSION['roleid ']的记录，返回权限编号 tokenid 的记录集。

(下转第 134 页)

限。这个门限不宜选择太高或者太低,太高会降低匹配的效率,太低则有可能造成匹配的失真。为了进一步解释门限的特点,我们对 63 位 PN 码长度的同步头进行了相关运算,得到的仿真波形如图 6。PN 码越长,获得的峰值的突出程度就越大,这样越有利于选择理想的门限来进行同步捕获。这也验证了为什么较长的 PN 码可以带来扩频系统稳定且性能较高的原因。

3.5 解扩 SOLUTION:

在对接收到的信号进行同步捕获后,继而转入解扩步骤,即用与发射端相同的 PN 码对信号进行再一次的异或运算 (模二加)。这里我们会发现,信号跳变沿处出现了毛刺,因此,在对解扩后的信号需要考虑去毛刺处理。

4 模块封装

在本例中,当各个模块按照预先设计的功能设计完毕后,需要将这些模块进行连接并封装到一个 TOP 模块下,这样在综合时便可以十分清晰的看出电路的结构与模块的各个功能。需要注意的是,在代码设计中,对于既作为一个模块的输出又作为另一个模块的输入的数据流要用 wire 型定义,在测试代码(TestBench)中不必这样定义,只需要在模块列表里对应的写出调用的端口即可。

5 设计的仿真与综合结果

通过观察不同长度的 PN 码产生的仿真结果,对原始信号进行调制之后,信号的频率变化是很明显的。PN 码越长,产生的调制信号的频率就越高,在信道里传输时,频带越宽,抗干扰性能越好;同时信号的多址功能越强大,即信号的复杂度越强。由此可以得出,PN 码是调节扩频系统性能的重要参数之一。在实际应用中,CDMA 的 PN 码实际长度为 $2^{41}-1$,可见这样的长度是相当惊人的。

通过 Symplify 工具,可以查看到综合后的电路与我们当初的设计思路完全一致,可以清楚地看到发送端、接收端各个模块之间的传递关系。因此模块化的思想又为我们提供了高效并且清晰地设计思路。

本文作者创新点:本文为设计直序扩频通信系统提供了参考模型。

参考文献

[1]朱近康,扩展频谱通信及其应用。中国科学技术大学出版社,1993 年。

[2]朱近康,CDMA 通讯技术。人民邮电出版社,2001 年

[3] 夏宇闻,Verilog 数字系统设计教程。北京航空航天大学出版社,2003 年。

[4]Scholtz R A,The Spread Spectrum Concept。Special Issue of IEEE Trans,comm 1977。

[5]Pickholtz R L,Schilling D L and Milstein L B,Theory of Spread Spectrum Communications - A Tutorial Special Issue of IEEE Trans,comm1982

[6]周贤伟,刘军. DS-SS 通信扩频序列的估计[J]微计算机信息,2006,1-3: P79-81

作者简介:赵岩,男,北京航空航天大学,软件学院集成电路设计专业在读二年级硕士研究生。作者主要从事 EDA 相关的设计与验证研究。本文是作者独立完成的实验项目。

Biography:Zhao Yan, male, a senior graduate of Software School, Beihang University. The author majors in Integrated Circuit design, especially focuses on EDA and correlated design and verification. This project is a lab experiment fully completed by the author.

(100083 北京 北京航空航天大学)赵岩

通讯地址:(100083 北京海淀区学院路 37 号北京航空航天大学 8-76 信箱)赵岩

(收稿日期:2007.7.03)(修稿日期:2007.8.05)

(上接第 22 页)

4.$_SESSION['AllowedPageSecurityTokens ']对应 tokenid 记录集。根据 tokenid 记录集进行角色权限匹配。系统为 B/S 模式,功能模块及其子功能的页面都有一个$PageSecurity 变量。通过函数 is_array ($PageSecurity, $_SESSION ['AllowedPage SecurityTokens ']进行匹配,如果匹配结果为 0,则给出提示信息"你没有相应的操作权限"。如果为 1,显示相应的功能操作界面。

4 结束语

本文提出面向服务的架构(SOA)和基于角色访问控制技术相结合的 PDM 权限管理模型,可以动态的实现开放环境下的权限管理,并且已经在实际中得到了应用,提高了 PDM 系统各个功能模块的信息安全。

本文作者创新点:采用面向服务的架构(SOA)和基于角色访问控制相结合的技术,采用统一授权和访问的控制策略与机制,开发 PDM 系统的权限管理模块,维护系统的信息安全。

参考文献

[1]Ali.Service-oriented modeling and architecture.http://www-128.ibm.com/developerworks/webservices/library/ws-soa-design1/index.html , 09 Nov 2004.

[2]David F Ferrailo. Proposed NIST standard for role based control [J].ACM Transactions on Information and System Securtiy,2001,4 (3):224-274.

[4]何湘初,陈新度,刘强,李继容. PDM 中工作流管理的研究与应用[J]微计算机信息.2005,21-3:209-210.

[5]庞士宗,肖平阳,唐加福. 产品数据管理(PDM). 北京: 机械工业出版社,2001.

[6]American National Standard for Information Technology—Role Based Access Control.美国国家信息标准.2003.

作者简介:袁高群(1979-),男,湖南双峰人,硕士,主要研究方向:网格技术、企业信息化;陈新度(1967-),男,湖南长沙人,教授,博士,主要研究方向:企业信息化、网络化制造等.陈新(1962-),男,湖南常德人,教授,博士生导师,主要研究方向:敏捷制造等;萧良皓(1970-),香港人,项目经理,MBA,主要研究方向:项目管理。

Biography:Yuan Gao-qun (1979-),male,HuNan,Master,Major in Grid Technology and Business Information;Chen Xin-du(1967-), male,HuNan, Prof, Doctor, Major in Business Information Network Manufacture;Chen Xin(1962-),male,HuNan,Prof,Doctor, Major in Agile Manufacture and etc.

(510090 广州广东 广东工业大学 机电工程学院 CIMS 中心)陈新度 陈新

(518059 深圳广东 艾逖恩控股有限公司)萧良皓

通讯地址:(518000 深圳 深圳市南山区桃源村 92 栋 17 楼 E 房)袁高群

(收稿日期:2007.7.03)(修稿日期:2007.8.05)