维普资讯 http://www.cqvip.com

一种基于树型结构的 B/S 系统权限控制方法*

李南妮，张 璟，李军怀
（西安理工大学 计算机科学与工程学院，陕西 西安 710048）

摘 要：在应用 RBAC 技术的基础上研究了基于树型结构下的 B/S 系统中权限控制方法，通过系统资源树的生成，提出了用户权限数据报的概念及其设计思想，并在实践中加以应用。实现了系统全局资源的安全访问控制，增加了系统的灵活性。

关键词：树；基于角色的访问控制；B/S；系统资源树；用户权限
中图法分类号：TP311 **文献标识码**：A **文章编号**：1001-3695(2005)10-0128-03

An Authority Access Control Method in B/S System Based on the Tree-structure

LI Nan-ni, ZHANG Jing, LI Jun-huai
(*School of Computer Science & Engineering, Xi' an University of Technology, Xi' an Shanxi* 710048, *China*)

Abstract: Based on the RBAC technology, this paper studies the method of user access control authority which adopted the tree-structure in B/S system. Through generating the system resource tree and then putting it in use, the conception of user authority data package and its design idea is proposed. And the experiments validated that our approach is more effective and flexible.

Key words: Tree; RBAC; B/S; System Resource Tree; User Authority

近年来，在开发基于 Web 的企业内部管理信息系统时，多采用 Browser/Web Server/DB Server 三层体系的 B/S 结构模式，以达到企业级的数据共享和业务处理，在访问控制机制上一般使用基于角色的访问控制技术（RBAC）来实现系统的授权管理。其有效应用的条件是，系统所需要管理的资源可完全预知，以便进行全局的权限规划。但是，当系统所需要管理的资源处于动态变化的时候，使用 RBAC 技术会出现很多问题，如系统资源出现增加，RBAC 不能与之动态适应。Web 信息系统会拥有多层次功能页面，而且在系统动态开发、维护中，页面的增减非常频繁。这就需要我们使用一种有效的权限控制方法，开发出可以封装成组件的用户管理模块。

Web 信息系统的页面资源通常表现为树型结构。本文吸取了 RBAC 技术的优点，针对 B/S 系统的树型页面资源，通过页面资源树的建立，提出一种用户权限的控制访问方法，解决了页面资源动态增删时，用户权限动态生成及对页面操作权限的重新定位的问题，在实际的系统开发中取得了良好的效果。

1 树型结构的系统页面资源

1.1 系统资源树

基于 B/S 结构的 Web 信息管理系统的开发过程，可看作是建立系统页面资源树的过程。Web 信息管理系统一般可以分为若干个功能模块，每个功能模块实质上是一些具有特定功能的页面文件的集合，功能的细分将产生更小的文件集合，页面文件是这种划分的最小单位[2]。因此，可以把整个系统的所有页面文件构成一颗树，该树的节点皆由页面文件组成。在本文中称为系统资源树。在这颗树中，节点的所有子节点都无需按一定的次序排列，构成一颗无序树。树中每一个节点代表一个页面文件，故页面文件是最小的访问控制单元。

这颗系统资源树可用二元组 (V,E) 表示，其中 V 是一非空有限集合，E 是集合 V 上的二元关系，并满足下列条件：

(1) E 是反自反的；

(2) 对于每一个 $v' \in V$，最多存在一个 $v \in V$，使得 $<v, v'> \in E$；

(3) 存在唯一元素 $v \in V$，不存在任何 $v' \in V$，使得 $<v, v'> \in E$，元素 v 称为根。

树根的层数定义为 0。

对系统资源树的每一个节点 v（包括根节点）赋予 Web 系统提供的基本操作权限作为其特性，在此称为节点操作特性。

1.2 基于系统资源树的用户权限生成

本文通过以下步骤生成用户权限：

首先为系统中的每一个页面分配一个独一无二的标志符，该标志符在系统资源树中指向对应的节点。以下为页面标志符与系统资源树之间的对应关系，如图 1 所示。设标志符为 $K-L-M-N$ 的页面在系统资源树中表示的具体含义如下：

K 表明该节点位于系统资源树的第 K 层；
L 表明树根所连的第 L 个节点；
M 表明树根所连的第 L 个节点下连接的第 M 个节点；
N 表明树根所连的第 L 个节点下连接的第 M 个节点下所连的第 N 个节点。

如页面 1-1 表示树根所连的第一个节点；而树根所连节点 2 下所连的节点 1 可表示为页面 3-2-2-3。在图 1 中给

收稿日期：2004-09-23；**修返日期**：2004-10-28
基金项目：国家“863”计划资助项目(2002AA414060)

维普资讯 http://www.cqvip.com

出了页面 1 - 1 及页面 3 - 2 - 2 - 3 与系统资源树中节点之间的对应关系。

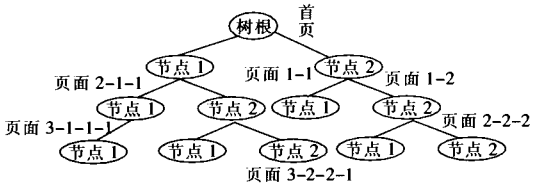

图 1　页面标志符与系统资源树的对应关系

其次定义系统资源树的节点操作特性。设 Web 系统提供如下操作功能:完全控制、浏览、读取、修改、删除、导入/导出和打印这七种功能,其中 0 表示不拥有该权限;1 表示拥有该权限,则系统资源树的每个节点的节点操作特性都用七位由 0,1 组成的字符串表示,本文中称为节点操作特性字符串。

例如用户 A 对于页面 1 - 1 的节点操作特性为:0 1 1 0 0 1 0,就表明用户 A 对页面 1 - 1 拥有浏览、读取和导入/导出的操作权限,而没有完全控制、修改、删除和打印的操作权限。

最后生成系统的用户权限。在应用 RBAC 的访问机制时,根据系统的不同需求,可以确定不同的角色,每个角色对系统拥有不同的权限,不同用户又被赋予不同角色,所以两者在访问系统资源树的节点时,节点访问总数小于等于该树的节点总数。

将某一角色或用户对系统资源树上每一个节点的节点操作特性字符串全部累加起来就可以生成用户权限。(对于某一角色或用户来说,若有节点不包括在访问范围中,则可将其节点操作特性字符串全部置为 0)。

例如用户 A 对系统资源树的权限如下:0110010 0111000 ……0111000,其中 0110010 表明用户 A 对树根的节点操作特性,0111000 表明用户 A 对页面 1 - 1 的节点操作特性,……,0111000 表明用户 A 对页面 $K-L-M-N$ 的节点操作特性。

由于不同用户对于相同节点的操作特性的差异性及节点操作特性本身的差异性,所以用户权限的生成更加复杂多样,获取系统资源树上某节点的节点操作特性就变得相对困难,本文采用了设计用户权限数据报的方法来解决这一问题。

2　用户权限控制实现方法

2.1　用户权限数据报设计思想

用户权限数据报的设计思想是产生一个固定的报头格式,并用用户权限(构成数据域)来形成用户权限数据报。

设计步骤是:

(1)对系统资源树进行顺序编号,如图 2 所示。

(2)对用户权限数据报进行具体设计数据报设计格式,如图 3 所示。

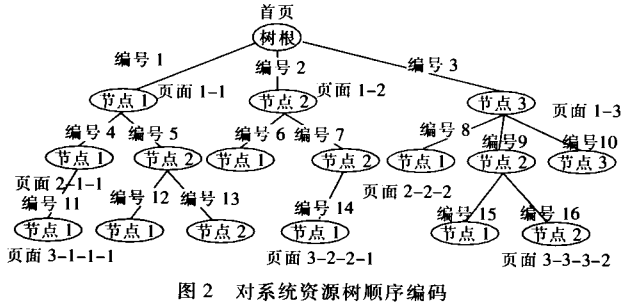

图 2　对系统资源树顺序编码

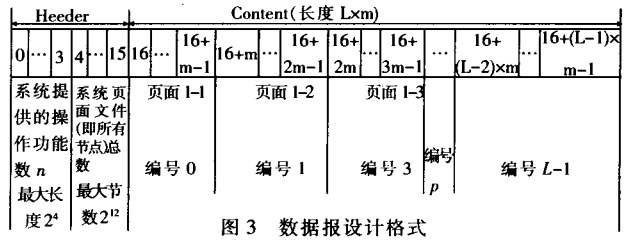

图 3　数据报设计格式

图 2 中以 B/S 结构下的管理信息系统中 17 个页面及其联接关系为例生成系统资源树。图 2 中用编号 1 到编号 16 对系统根页面以下的页面 1 - 1 至页面 3 - 3 - 3 - 2 进行了顺序编号,节点 1 至节点 16 的在系统资源树上表现为页面 1 - 1,页面 1 - 2…页面 3 - 3 - 3 - 2。每一个节点的节点操作特性对应用户所拥有相应页面的操作权限。结合例 1,节点 1 的节点操作特性 0110010 就是用户 A 对页面 1 - 1 的操作权限。由于页面 1 - 1 的序号为 1,所以 0110010 在用户 A 的对 Web 系统的权限字符中处于起始位置。下面设计数据报,用于定位用户 A 对树中某一节点的节点操作特性。

数据报报头长度为 16 位,用于保存以下数据:

m 表示报头 0 ~ 3 位保存系统提供的功能数,其功能如浏览、添加、删除等。最大功能数为 24 = 16 个。

L 表示报头 4 ~ 15 位保存系统所有页面的数量(页面总数最大为 212 = 4 096个)。

用户 A 的权限字符串长度(即数据报的数据域长度)为 L × m,用户 A 对某节点在数据域中(即在权限中)的操作权限可进行如下获取:

权限(页面 p) = substring[16 + (p - 1) × m ,m]

其中 p 值为该节点的顺序编号;H 为报头长度;m 为系统提供的操作功能数目。

当动态增加、删除系统提供的操作功能或动态增加、删除叶子节点时,通过修改数据报的报头 0 ~ 3 位或 4 ~ 15 位中保存的值可以重新对 m,L 赋值,同时按序号截取数据域中的要删除的页面操作权限或增加数据域中的页面操作权限,对系统资源树重新进行顺序编号,实现了在该树中对某一节点的重新定位的功能。

2.2　数据库设计

由于数据报的设计思想是基于 B/S 结构下中应用 RBAC 的访问控制机制提出的,所以在数据库的设计实现上首先要建立用户表、角色表和用户 - 角色对应表这三个基本的数据表。由于用户与角色、角色是多对多的关系,因此为了编写程序的方便,可建立一张视图,将用户和角色直接关连起来,在进行权限读取时,可以直接查询这一个视图即可。其次建立系统页面定义表用来定义页面名称并进行顺序编号,当页面增减时,进行重新编号。最后建立操作许可表用来存储系统对每一个页面拥有的操作权限,通过修改表中操作权限的有效值来更改页面拥有的操作功能。

综上所述,主要数据表包括:①系统页面定义表(页面编号,页面名称,顺序编号);②操作许可表(页面编号,页面名称,功能名,);③用户表(用户名称,口令,用户权限);④角色表(角色编号,角色名称,角色权限);⑤用户—角色对应表(用户名,角色编号)。图 4 列出了各个表的主要字段名。其中用户表和角色表的权限字段按用户权限数据报的格式保存其权限。

2.3　用户获取页面权限流程

对于一个具体的用户如何获取某页面的操作权限呢?下

维普资讯 http://www.cqvip.com

面介绍这个获取流程。

当一个用户要获取某页面的操作权限时,先判断该用户是否存在,如果不存在则拒绝访问,否则提取用户的权限数据报;若该数据报不存在,对用户进行角色审查,提取角色的权限作为用户默认权限;提取出数据报后,对报头进行分割,再读出页面的顺序编号,最后根据报头信息截取出用户对页面的权限。

图 5 给出了用户获取某页面权限的程序流程图。

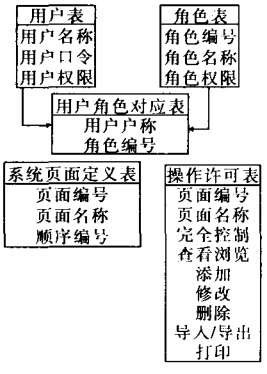

图 4 数据库的设计图

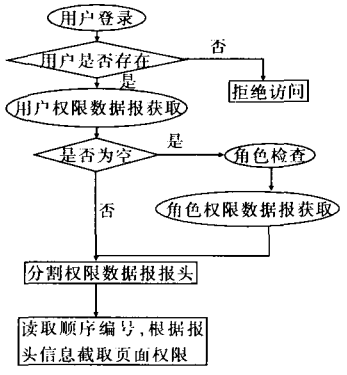

图 5 用户获取某页面权限流程图

2.4 代码实现

按前述方法,在 C#,. NET 平台下实现用户对某页面操作权限的代码片断如下:

```
Int quanxiansum = Convert. ToInt16( "select quanxiansum from Table_yonghu where yonghuming = 'admin' " );
int l = quanxiansum. Substring(0,3);
int m = quanxiansum. Substring(4,15);
string
quanxian = quanxiansum. Substring(16,l * m);//分割数据报报头,提取用户对页面的权限 int bianhao = Convert. ToInt16( "select ShunXuBianHao from Table_yemian where yemianbianhao = '3 -8 -1 -1'");
//提取页面 3 -8 -1 -1 的顺序编号
string
quanxian = quanxiansum. Substring( quanx * l,1);
//提取用户对页面 3 -8 -1 -1 的权限
```

3 结束语

本文在应用 RBAC 策略中的 B/S 信息系统环境下,描述和定义了系统资源树及其节点操作特性;引出了用户权限数据报的概念,提出了数据报的设计思想;解决了系统树型页面资源动态增删时,用户权限动态生成及权限控制问题。最后给出了数据库设计、程序流程图及实现的简单代码。

参考文献:

[1] 叶锡君,许勇,吴国新. 基于角色的访问控制在 Web 中的实现技术[J]. 计算机工程,2002,(1):167-169.

[2] 栗松涛,李春文,孙政顺. 一种新的 B/S 系统权限控制方法[J]. 计算机工程与应用,2003,(38):99-101.

[3] 万昌江,张树有. Internet 环境下企业资源的安全访问控制策略[J]. 计算机工程与应用,2002,(5):0161-03.

[4] Ferraiolo D F, Barkley J F, Kuhn D R. A Role Based Access Conrtrol Model and Refernence Implementation Within a Corporate Intranet [J]. ACM Transactions on Information Systems Security, 1999, (2).

[5] http://www-900. ihm. com/developerWorks/cn/security/syscontrol/index. shtml[EB/OL].

[6] 黄凯,陈云,阎如忠,等. 基于角色的 B/S 系统访问控制的研究与应用[J]. 计算机工程与应用,2003,(20):0227-03。

作者简介:

李南妮(1976-),女,湖南长沙人,硕士研究生,主要研究方向为 Web 技术及应用;张璟,教授,博士生导师,主要研究方向为 Internet 技术及其应用;李军怀,副教授,研究方向为分布式计算、CSCW。

(上接第 123 页)

通过这种方式,整个 LD-IDS 系统可以得到优化,留在系统中的将是那些能够检测攻击并且具有学习进化能力的 Agent,从而使整个系统具有很强自适应能力。

4 总结

用代理和移动代理技术实现 LD-IDS,可提高入侵检测系统的效率,减少系统内部通信量,实现实时就地响应。本文提出了一种可应用于 LD-IDS 的任务分派机制,主要通过请求、迁移、使用和回收四个步骤,完成对移动代理的一次使用,实现对任务的处理。不过,这种基于移动 Agent 的 LD-IDS 也存在一定的缺陷,如由于采用移动代理技术,系统效率有待提高;大规模网络环境下,移动代理系统在异构平台上的部署问题以及平台的安全性保障问题[6];同时对于静态 Agent 和移动 Agent 的选取原则也有待进一步研究。要构建一个理想的、完全自学习、自适应的检测系统仍有许多工作要做。我们的基本思路是寻找一种合理、快速、高效的描述方法,对复杂的入侵事件的检测过程进行描述和分解,分解后的每个子任务将由不同类型的移动代理来承担。如何构造合理的移动代理全集是全面提高 LD-IDS 整体性能的关键,这也是我们下一步工作的方向。

参考文献:

[1] A Lingnau, O Drobnik. An Infrastructure for Mobile Agents: Requirements and Architecture [EB/OL]. http://citeseer. ist. psu. edu/lingnau95infrastructure. html, 1995-12.

[2] W A Jansen. Intrusion Detection with Mobile Agents[J]. Computer Communications, 2002, 25(15):1392-1401.

[3] Wayne Jansen, Peter Mell, *et al.* Applying Mobile Agents to Intrusion Detection and Response[EB/OL]. http://csrc. nist. gov/publications/nistir/ir6416. pdf, 1999-10.

[4] M Asaka, *et al.* The Implementation of IDA: An Intrusion Detection Agent System[EB/OL]. http://www. ipa. go. jp/STC/IDA/papers. html, 2001-10-22.

[5] Mark Slagell. The Design and Implementation of MAIDS[EB/OL]. http://latte. cs. iastate. edu/Research/Intrusion/, 2001-11-07.

[6] Danny B Lange. Java Aglet Application Programming Interface (J-AAPI) White Paper-Draft 2[EB/OL]. http://www. trl. ibm. com/aglets/JAAPI-whitepaper. htm, 1997-02-19.

作者简介:

褚永刚(1974-),男,河北正定人,博士生,主要研究方向为网络与信息安全;杨义先(1961-),男,四川绵阳人,长江学者特聘教授,教授,博士生导师,主要研究领域为现代密码学、计算机网络与信息安全、信息伪装与数字水印、移动通信安全等;胡正名(1931-),男,教授,博士生导师,主要研究领域为信号分析、编码密码理论和应用数学方法等。