Web 应用系统 PMI 资源管理树的动态生成

A Dynamic Construction of PMI Resource Management Tree for Web Application System

贾忠田 李大兴 （济南山东大学网络信息安全研究所 250100）

摘要：简单介绍了授权管理基础设施 PMI，阐明了在 Web 应用系统的资源管理过程中动态生成 PMI 资源管理树的必要性，分析了两种典型 Web 服务器对其系统资源的管理方式，在此基础上详细论述了 Web 应用系统 PMI 资源管理树的动态生成方法。

关键词：PMI RBAC Role Web PMI 资源管理树

1 引言

随着区域性 CA 和行业性 CA 的建立，PKI 技术在我国得到了广泛的应用，身份认证、数据机密性、数据完整性和抗抵赖性得到了根本的解决，信息安全研究的重点转向了 PMI。在 PMI 系统的应用过程中，为了实现对 Web 应用系统的资源进行有效的管理，提出了 Web 应用系统 PMI 资源管理树的动态生成问题。

2 PMI 简介

授权管理基础设施 PMI(Privilege Management Infrastructure)是一个属性证书、属性权威、属性证书库等部件构成的综合系统，用来实现权限和证书的产生、管理、存储、分发和撤销等功能。其目标是向用户和应用程序提供授权管理服务，提供用户身份到应用授权的映射功能，提供与实际应用处理模式相对应的、与具体应用系统开发和管理无关的授权和访问控制机制，简化具体应用系统的开发与维护。PMI 使用属性证书表示和容纳权限信息，通过管理证书的生命周期实现对权限生命周期的管理。属性证书的申请、签发、注销、验证流程对应着权限的申请、发放、撤消、使用和验证的过程。

PMI 系统主要使用基于角色的访问控制 RBAC(Role - Based Access Control)对应用系统资源进行管理。其中，角色提供了间接分配权限的方法。在实际应用中，用户的属性证书对应一个或多个角色，而每个角色具有的权限通过角色定义来说明，而不是将权限放在属性证书中直接分配给个人。角色定义时需要在角色和具体的应用目标的操作权限之间建立一种映射关系，如图 1 所示。其中，双箭头表示多对多的关系。

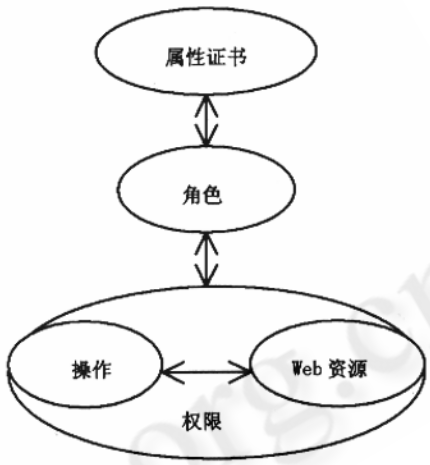

图 1 权限－角色－属性证书关系

3 动态生成资源管理树的必要性

在 PMI 系统中，为了实现对 Web 应用系统的资源进行有效的管理，资源管理服务器的管理方法必须满足：

(1) 管理方便：资源管理服务器应该能够根据 Web 服务器的目录结构实现对 Web 应用系统的主目录和所有虚拟目录下的资源进行层次化管理。

(2) 自发现功能：Web 应用系统的资源是不断变化的，资源管理服务器应该能够及时发现并且体现出这种变化。

(3) 方法的适应性：这种资源管理的方法应该满足 PMI 系统对常见 Web 服务器应用系统的资源进行管理的需要。

因为 Web 应用系统通过主目录和虚拟目录管理系统资源，所以资源管理服务器应该根据管理需求动态地得到 Web 服务器的目录结构。因此，为资源管理服务器动态地构造一棵资源管理树是解决问题的一种有效途径。资源管理树的结构反映了 Web 服务器目录树的结构，资源管理树的动态生成能够及时发现并体现出 Web 应用系统资源的变

化，实现资源管理时的自发现功能。

4　Web 服务器及其资源管理方式

Windows2000 平台上运行的 Web 服务器，就其对目录的管理方式来说，可以分为两类，一类是把主目录和虚拟目录的配置信息写入注册表，另一类是通过配置文件来管理主目录和虚拟目录。下面分别给出一种具有代表性的 Web 服务器，具体分析一下它们对系统目录的管理情况。

4.1　IIS5.0

IIS5.0 已经完全成为 Windows2000 操作系统的一个有机组成部分，不仅提供了方便的安装和管理，增强了应用环境，而且基于标准的发布协议，在性能和扩展性方面有了很大的改进，为客户提供更佳的稳定性和可靠性。IIS5.0 通过设置主目录的本地路径实现站点主目录和物理目录的对应，通过建立虚拟目录实现虚拟别名和物理目录的对应。这些对应关系被注册表记录在 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual Roots 下。因此，对于这类 Web 服务器，可以通过注册表获得他们所对应的系统资源。

4.2　Tomcat4.1

Tomcat 是一个开放源代码、运行 Servlet 和 JSP Web 应用软件的基于 Java 的 Web 应用软件容器。通过对 Tomcat4.1 的研究和使用，发现站点主目录和虚拟目录可以在系统配置文件 Server.xml 里进行配置。标记符＜HOST NAME＝"LOCALHOST" DEBUG＝"0" APPBASE＝"WEBAPPS" …＞…＜/HOST＞中的关键字 APPBASE 定义了 Web 服务器的主目录所对应的物理目录，标记符＜CONTEXT PATH＝"/DOCS" DOCBASE＝"D:\TOMCAT-DOCS" …/＞中关键字 PATH 后面的字符串定义了一个虚拟目录，关键字 DOCBASE 后面的字符串标识了与该虚拟目录所对应的物理目录。因此，对于这类 Web 服务器可以通过解析配置文件的办法获得应用系统资源。

5　资源管理树的动态生成方法

5.1　定义

RMS(Resource Management Server)：资源管理服务器，是 PMI 系统的重要组成部分；

RLS(Resource List Server)：与 Web 服务器安装在同一台设备上的服务进程。作用是监听来自 RMS 的请求，获得 Web 应用系统的目录结构并且把目录结构传递给 RMS；

T：资源管理树；

$T_{i,j}$：在 RMS 端表示资源管理树 T 的第 i 层上编号为 j 的子树，在 RLS 端表示 Web 应用系统第 i 层目录下的编号为 j 的子目录树；

$T^{o}_{i,j}$：在 RMS 端表示子树 $T_{i,j}$ 的根结点，在 RLS 端表示 Web 应用系统第 i 层目录下的编号为 j 的子目录树的根结点；

$T^{o}_{0,0}$：资源管理树 T 的根结点；

$T^{k}_{i+1,j}$：在 RMS 端表示 $T^{o}_{i,j}$ 的儿子结点中编号为 k 的非叶子结点，在 RLS 端表示 Web 应用系统子目录 $T^{o}_{i,j}$ 下的编号为 k 的目录名(k=1,2,…)；

$F^{k}_{i+1,j}$：在 RMS 端表示 $T^{o}_{i,j}$ 的儿子结点中编号为 k 的叶子结点，在 RLS 端表示 Web 应用系统子目录 $T^{o}_{i,j}$ 下的编号为 k 的文件名(k=1,2,…)；

0：请求/应答消息中的非叶子结点标志符，即该符号后的字符串是目录名；

1：请求/应答消息中的叶子结点标志符，即该符号后的字符串是文件名；

\r\n：是结点间隔符，即不同的目录或文件名用"\r\n"分开；

N_i：在 RMS 端表示资源管理树 T 的第 i 层上结点个数，在 RLS 端表示 Web 应用系统的目录树第 i 层目录下子目录和文件总数；

$N_{i,j}$：在 RMS 端表示结点 $T^{o}_{i,j}$ 的儿子结点中非叶子结点的个数，在 RLS 端表示 Web 应用系统的目录树子目录 $T^{o}_{i,j}$ 下目录数；

$M_{i,j}$：在 RMS 端表示结点 $T^{o}_{i,j}$ 的儿子结点中叶子结点的个数，在 RLS 端表示 Web 应用系统的目录树子目录 $T^{o}_{i,j}$ 下文件的个数；

H：表示资源管理树的高度。

5.2　基本思想

Web 服务器端增加资源列表服务进程(RLS)，负责向资源管理服务器(RMS)提供 Web 应用系统的目录结构。资源管理服务器(RMS)作为客户端，负责资源管理树的构造。RMS 根据资源管理时需要展开的当前结点，实时向 RLS 发出资源管理树的展开请求，RLS 接受来自 RMS 的请求，获得相应的目录结构，按预先定义的响应格式发送给 RMS；RMS 从中解析出目录名和文件名，把它们作为资源管理树 T 当前结点的儿子结点。其中，目录名结点可以继续展开，而文件名结点作为资源管理树 T 的叶子结点，即最小粒度的目标资源，不再进行展开。

5.3　RMS 和 RLS 之间的请求/响应格式

5.3.1　资源管理服务器(RMS)请求格式

(1) 当 RMS 展开目录树 T 根结点时发送的请求格式："$T^{0}_{0,0}$"。

(下转第 5 页)

(上接第 25 页)

(2) 当 RMS 展开目录树 T 的其他结点 $T^0_{i,j}$ 时发送的请求格式为："$T^0_{0,0}$ /T^0_{1,j_1} /T^0_{2,j_2} /… /T^0_{i,j_i}"(T^0_{1,j_1}，T^0_{2,j_2}，…是从树 T 的根结点 $T^0_{0,0}$ 至结点 T^0_{i,j_i} 的路径上的结点，$1\leqslant i\leqslant H$，$1\leqslant j_i\leqslant N_i$)。

5.3.2 资源列表服务器(RLS)应答格式

(1) 当请求为 T^0_{00} 时的应答格式："0 $T^1_{1,1}$\r\n0 $T^2_{1,2}$\r\n…0 $T^k_{1,k}$\r\n"($1\leqslant k\leqslant N_1$)。$T^1_{1,1}$ 表示 Web 服务器的主目录，$T^k_{1,k}$($2\leqslant k\leqslant N_1$)表示 Web 服务器的虚拟目录(此时，结点在本层的编号恰好和结点在 T^0_{00} 的儿子结点中的编号相同，这是上层只有一个根结点的缘故)。

(2) 当请求不是 T^0_{00} 请求时的应答格式："0 $T^1_{i+1,j_{i+1}}$\r\n0 $T^2_{i+1,j_{i+2}}$\r\n…0 $T^n_{i+1,j_{i+n}}$\r\n1 $F^1_{i+1,j_{h+1}}$\r\n1 $F^2_{i+1,j_{h+2}}$…1 $F^m_{i+1,j_{h+m}}$\r\n"($1\leqslant i\leqslant H$，$1\leqslant n\leqslant N_{i,j_i}$，$1\leqslant m\leqslant M_{i,j_i}$，$1\leqslant j_l\leqslant N_{i+1}$，$1\leqslant j_h\leqslant N_{i+1}$)。

6 结束语

Web 应用系统 PMI 资源管理树是 PMI 系统与具体应用系统的接口，怎样构造资源管理树直接影响 PMI 系统对对应用系统的访问控制功能，是 PMI 系统应用能否取得成功的关键。本文论述的 PMI 资源管理树的生成方法已经在 Windows2000 平台上用 VC6.0 实现，效果良好，具有较高的实用价值。

参考资料

1 D Ferraiolo, R Kuhn, "Role－Based Acess Controls" in 15th National Computer Security Conference 1992; proceeding published by NIST, PP554－563.

2 R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, "Role－Based Access Control Models", IEEE Computer 29(2): 38－47, IEEE Press, 1996.

3 ITU－T Recommendation X.509 2000.03

4 [RFC3281] An Internet Attribute Certificate Profile for Authorization. April 2002.

5 安晓江、李大兴，PMI 系统中 RBAC 的实现与管理，计算机工程与应用，2004.7. PP. 115。