# 一种基于 ASP 的动态用户权限管理解决方案*

吴应良, 汪　闯
(华南理工大学 工商管理学院 电子商务研究中心, 广东 广州 510640)

**摘　要:** 以医院网上医疗管理信息系统的研究和开发为背景,针对专家答疑系统的安全问题,对 B/S 模式下系统用户权限管理的需求进行了分析,采用结构化方法和基于角色的安全管理策略进行了系统功能和业务流程的设计,并采用 ASP 等技术实现了系统用户权限的动态管理。

**关键词:** 网上医疗; Web 计算; 浏览器/服务器模式; ASP; 动态权限管理
**中图法分类号:** TP393.02　　**文献标识码:** A　　**文章编号:** 1001-3695(2005)02-0115-03

# An ASP-based Solution for the Dynamic User Privilege Management

WU Ying-liang, WANG Chuang
*(Research Center of E-business, School of Business Administration, South China University of Technology, Guangzhou Guangdong* 510640, *China)*

**Abstract:** The security problem of specialist reply system is studied under the background of research and development of hospital management information system based on Internet. The requirement of user privilege management based on three ties B/S mode is analyzed, the design of system functions, business process and database structure by means of the structural method and the role-based security management strategies is presented, and it is discussed that how to realize the dynamic management mode of users privilege based on ASP.

**Key words:** On-line Medical Service; Web Computing; B/S Mode; ASP (Axtive Server Pages); Dynamic Privilege Management

## 1　需求分析

随着电子商务的发展和应用,医院为了适应网上医疗发展的需要,往往需要建立基于 Internet/Intranet 技术架构的网上医疗服务信息系统,具体实现如下三个主要在线功能:

(1) 建立医院的企业信息门户(Enterprise Information Portal, EIP)[1] 系统,及时发布医院或行业的动态信息,以使病人、医生和医院之间更有效地进行沟通,提高信息的价值;

(2) 通过从网上系统收集用户的反馈资料,并加以整理、分析,提炼出有价值的信息,搞好客户关系管理(Customer Relation Management, CRM),从而指导和改进医院的工作;

(3) 在网上开通专家答疑系统,即在线为用户(主要为病人)提供相关咨询服务,从而提高客户满意度和忠诚度。

基于 Web 的分布式信息系统[2,3] 由于摆脱了时间与地域上的限制,使得信息系统的服务和管理变得更加方便;同时,它又必然地增加了信息系统设计和实现的复杂性,如其中的权限管理问题。因为在网络计算环境下,不同的用户具有不同的权限,怎样合理地分配权限和有效管理权限变得非常重要。具体表现为:在设计专家答疑系统时,如何区分专家用户和普通用户并进行有效的管理。这是因为:①该系统不同于一般的 BBS 系统,无论是何种身份的用户,都具有相同的权限,都可以在上面自由发表言论,这涉及到权限管理问题;②如果非专家用户在网上随意、不负责任地回答用户的问题,这样不但会损害医院的形象,还可能会危及到病人的生命安全。基于以上两点认识,在系统设计和实现时,如何解决用户身份的鉴别和权限的管理问题[4,5] 显得十分重要。因此,我们以网上医疗实际应用系统研究和开发问题为背景,主要针对上述第三个问题,运用结构化的方法,以及基于角色的安全管理模式,对系统业务流程、数据结构、系统处理流程等进行了系统化的分析和设计,采用微软的 ASP(Active Server Pages)、ADO 等技术实现用户权限的动态管理,提出了一种简便、有效的动态管理策略和解决方案。

收稿日期: 2004-01-21; 修返日期: 2004-05-01
基金项目: 国家自然科学基金资助项目(79931000);国家自然科学基金资助项目(70272047);华南理工大学社会科学基金重点项目(126-N71350)

## 2　系统分析与设计

### 2.1　系统业务流程

通过对上述实际问题的需求识别,发现在线医疗专家答疑系统必须具备下面的功能:

(1) 当用户注册时,专家用户和普通用户能在该系统分别注册,即系统能识别出用户的角色类别。

(2) 当用户成功登录系统后,系统能自动分配给他们不同的权限,即系统能对用户的权限进行管理。用户的权限具体分配为:未注册或未登录的用户进入系统后只能浏览上面的文章,而不能进行发表文章等其他操作;普通用户登录系统后,该用户不但可以浏览上面的文章,还可以发表自己的观点(如提出需要专家用户回答的问题),但不能回复别人的问题;专家

用户登录系统后,除具备普通用户的功能之外,还具有提供咨询的权限。该系统的业务流程如图 1 所示。

### 2.2 用户权限管理方案

根据上面的需求和业务流程分析,我们提出了实现该专家答疑系统用户权限管理的方案。系统关联图如图 2 所示。

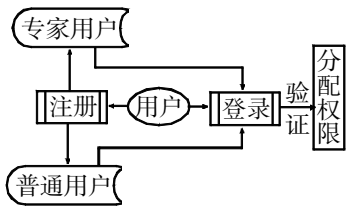


图 1 系统业务流程图

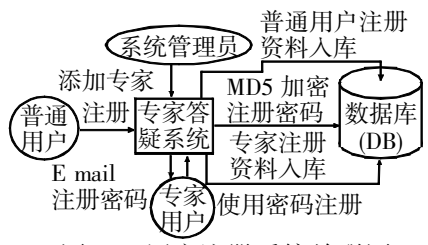


图 2 用户注册系统关联图

注册页面和登录页面同时为专家用户和普通用户提供服务。为了区分专家用户和普通用户,我们采取了以下措施:普通用户随时可以注册,但专家用户就不同了。在专家用户注册前,由系统管理员首先向数据库添加专家用户的姓名和注册密码信息,该注册密码是系统随机产生的一个六位数(由数字、字母或下画线组成),经过 MD5 散列算法[6]加密处理后存入数据库,同时系统将注册密码通过邮件服务器自动发送到预知的专家邮件地址。这样,当专家用户注册时,首先需要从注册页面选择自己的姓名,同时提供系统随机产生的注册密码,当两者与数据库中的信息相吻合时,才被确认为专家用户,并给予成功注册的机会,这样就能很好地满足系统的功能了。当用户登录系统时,系统根据用户所提供的登录信息与数据库中的信息进行比较,区分专家用户和普通用户,并给予相应的权限。其中,专家用户注册使用的注册密码必须与数据库中的注册密码相符,否则专家用户注册将失败。

### 2.3 系统数据库设计

为方便起见,该数据库中只建立一个用户表(User Table)进行注册权限管理。该表包括真实姓名、用户名(用户登录时使用)、密码(若是专家用户,则系统管理员添加的注册密码先保存在该字段,当专家用户注册成功后,专家用户使用的登录密码将其覆盖)、用户邮件地址、是否专家(判别字段)和权限分配等字段。其数据结构如表 1 所示。

表 1 用户表数据结构

| 真实姓名 | 用户名 | 密码 | 邮件地址 | 是否专家 | 权限分配 |
|---|---|---|---|---|---|
| User_name | User_oname | User_psw | User_email | User_specialist | User_power |
| Char[20] | Char[20] | Char[6] | Char[24] | Char[2] | Char[2] |

当用户为专家时,是否专家字段和权限分配字段的值均为 1,否则均为 0。两字段的初始值均为 0,其他字段可以为空值。

### 2.4 系统处理流程

专家答疑系统分为三个部分:系统管理员后台添加专家资料、确定注册密码子系统,用户注册子系统,用户登录子系统。下面以用户注册子系统处理流程为例,讨论系统处理流程的设计和工作原理。

当用户进入注册页面后,选择注册方式,即专家用户注册或普通用户注册。当为普通用户时,系统只是核对用户名与数据库中存在的是否冲突,若没有,则注册成功;否则,则重新填写注册资料。当为专家用户时,则系统首先检查注册密码是否匹配,若匹配,则后续流程与普通用户相同;若不匹配,则终止注册过程。图 3 是该子系统的处理流程。

普通用户注册处理流程比较简单,只是上面专家注册处理流程的一部分,故在此省略。当专家用户登记数据,并点击提交按钮后,User_add.asp 页面开始工作,它首先收集来自 Register.asp 页面的信息。然后从数据库的 User 表中查找相应专家名的字段,从中取出注册密码,与收集到的注册密码进行比较,若两者相符(不符,则系统转入 Re_register.asp),则再以收集到的用户名为关键字在 User 表中查询。若存在,则系统转入 re_register.asp,这主要是保证用户名的唯一性;反之,注册成功,所有数据被保存到数据库。同时,User 表中的是否专家和权限分配字段均置“1”。

## 3 系统有关安全问题与策略

Internet 自身的特点决定在网上实现权限管理必须注意安全问题。如网页是标准的 HTML 格式,攻击者可以通过在 Textbox 中添加代码、脚本等手段来对网站进行入侵和破坏。因此,本系统管理所涉及到的安全问题主要有:

(1) Form 表单中 Input 标志用来接收用户输入的信息,如用户名、密码和 E-mail 等。如果没有对用户输入进行很好的检查,恶意的用户会屏蔽一些安全机制,绕过安全认证,从而对系统造成威胁。

(2) Cookie 的问题。很多网站为了方便,将用户名以及口令信息存储在 Cookie 中,有的甚至以明文形式保存口令。如果攻击者可以访问到用户的主机,就可能通过保存的 Cookie 文件得到用户名和口令,因而重要的用户名和口令最好不要保存在 Cookie 文件中。

(3) 信息的完整性问题。信息在网上传输时,容易遭到黑客的攻击,如用户的密码等重要信息很容易被黑客截获。为了防止他们获得明确的信息,数据在传输之前通常要先进行加密。本系统中,我们采用的是 MD5 散列算法,经该算法加密明文信息后再通过 Internet 传输,最后保存到数据库中。

## 4 系统关键实现技术

ASP 技术[7]是 Microsoft 公司于 1996 年底推出的 Web 应用程序开发技术,它属于 ActiveX 技术中的服务器端技术。ASP 的命令和脚本都在服务器中解释执行,送到浏览器的只是处理过的标准 HTML 页面,它具有动态、高交互性、设计迅速、维护方便和源代码隐蔽等多种优点。

### 4.1 动态技术

在此,我们研究和运用的动态方法实现如下主要目标:

(1) 采用 ASP 等动态技术,页面会根据用户的要求和选择而动态地改变和响应;

(2) 无须手动更新 HTML 文档,便会自动生成新的页面,可以大大节省工作量;

(3) 当不同的时间、不同的人访问同一网址时会产生不同的页面,这主要是因为不同用户具有不同的权限。

### 4.2 Web 与后台数据库集成方法

ASP 可通过 ADO[8]提供简便、可靠的访问数据库的方法,有利于开发基于数据库驱动的 Web 应用程序,并支持所有的脚本语言。这样通过 ASP + ADO 技术实现了 Web 与数据库的集成。其工作原理如图 4 所示。

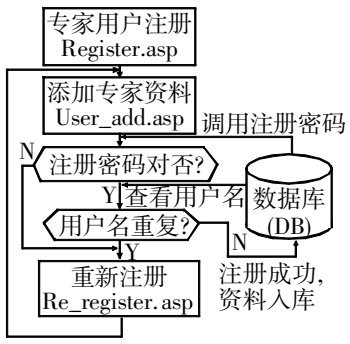


图 3　专家注册处理流程

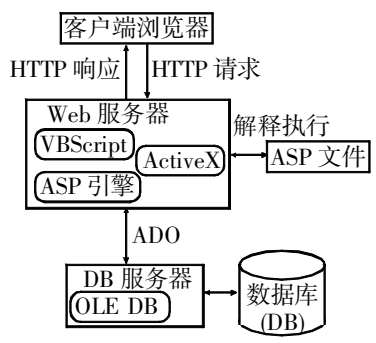


图 4　ASP 工作原理示意图

当客户机向 Web 服务器发出一个 ASP 请求时, Web 服务器响应该 HTTP 请求, 并调用 ASP 脚本引擎( 或解释器) , 解释被请求的 ASP 文件。若脚本中含有访问数据库请求, 就通过数据库访问界面接口( 如 OLE DB) 与后台数据库相连, 并由数据库访问组件 ADO 执行数据库访问操作。ASP 是在服务器端解释执行的, 它依据访问数据库的记录集自动生成符合 HTML 语言语法的网页, 并将 ASP 执行生成的标准 HTML 页面传送到客户端浏览器。

### 4.3　加密算法

我们采用了安全保密中杂凑技术中的散列算法 MD5 实现信息的完整性认证。同时, 这种方法具有很好的开放性和可扩充性。

## 5　结论

本文遵循结构化分析和设计思路, 采用基于 Web 的 B/W/D 三层应用体系结构, 综合运用快速原型法和面向对象方法, 在 Internet/Intranet 技术架构下, 通过 ASP、ADO、散列算法等技术, 为系统管理员提供了简便和可靠的后台管理操作功能, 动态地实现了用户类型的鉴别和权限分配, 大大简化了系统的管理和维护工作。系统实现简单、有效, 并具有开放的系统体系结构。当然也可采用其他的脚本技术, 如 Perl, PHP, JSP, Web Services[9,10] 等来实现相应的系统功能。但我们提出的系统化分析设计、业务流程管理方法和用户权限动态管理解决方案具有普适意义和应用价值。

参考文献:

[1] 吴应良. 一种面向电子商务的知识管理解决方案[J]. 计算机工程与应用, 2002, 38(22): 40-42.
[2] Guenther O, Mueller R, Schmidt P. MMM: A WWW-based Method Management System for Sharing Statistical Computing Modules [J]. IEEE Internet Computing, 1997, 1(3): 59-68.
[3] Upton D M, McAfee A. The Real Virtual Factory[J]. Harvard Business Review, 1996, (7-8): 123-133.
[4] 吴志刚, 方滨兴, 等. 一个安全、原子的电子商务协议及其形式化验证[J]. 计算机研究与发展, 2000, 37(7): 869-873.
[5] 吴应良. 徐学军, 孙东川. 电子商务的安全机制与体系结构模型[J]. 计算机工程与应用, 2001, 28(2): 27-29.
[6] 龚炳铮. EDI 与电子商务[M]. 北京: 清华大学出版社, 1999. 183-188.
[7] Dino Esposito, *et al*. ASP 数据访问高级编程[M]. 程永敬, 等. 北京: 机械工业出版社, 2001.
[8] http://www.swm.com.cn/yingyang/rj-98-yy2/98-y2-yy17.htm, 1998[EB/OL].
[9] Web Services Interoperability Organization(WS-I) [EB/OL]. http://www.ws-i.org/implementation.aspx, 2003.
[10] Apache. http://xml.apache.org/disp/soap/, 2002[EB/OL].

作者简介:

吴应良(1963-), 教授, 博士, 主要研究方向为电子商务、信息资源管理与信息系统、知识管理与网络知识工程; 汪闯, 男, 硕士研究生, 主要研究方向为电子商务、信息资源管理与信息系统集成。

(上接第 101 页)

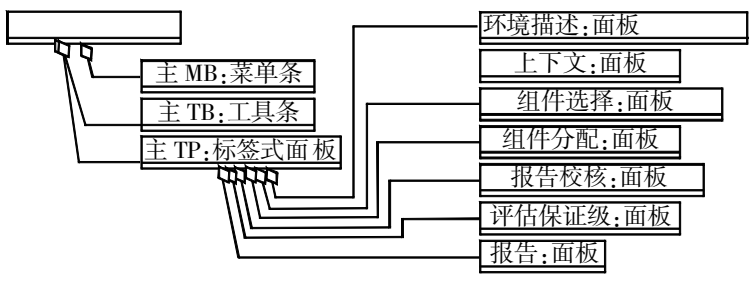


图 4　系统结构图

CC 工具箱系统数据流程图如图 5 所示, 用户可根据 CCEB 专家库生成的 PDE 文件, 对 CC 工具箱中给出的环境描述、上下文、CC 安全组件、评估保证级进行选择, 并对 CC 安全组件进行分配, 最后报告校核, 从报告数据集中生成 PP 和 ST 报告。

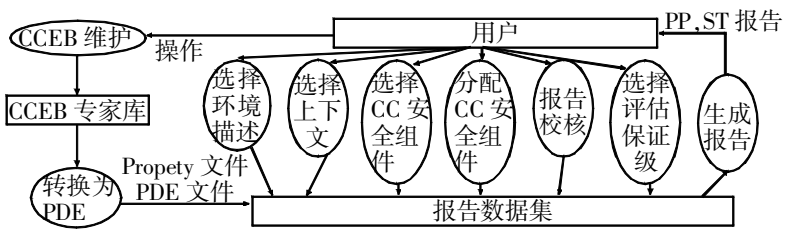


图 5　系统功能流程图

### 3.4　CCEB 专家库与 CC 工具箱的关系

CCEB 是 CC 工具箱的数据库数据维护程序。数据库包括 43 张表, 部分表之间有关联关系。CCEB 的主要功能是维护预定义环境数据以反映环境的变化和安全目的的相应改变。环境包括威胁、假设和策略, 对威胁、假设和策略都有概述表、详细表以及与安全目的的关联表。安全目的也有相应的表。这些表的维护通过程序提供的界面实现。在库表维护工作结束以后, 可以生成 CC 工具箱要使用的预定义环境数据——PDE 文件。CCEB 也提供直接登录 CC 工具箱的界面。

专家库可以编辑修改, 从而可以作为 CC 工具箱新的专家库数据来源。一旦专家库被编辑修改, 它将以一种过渡形式被存储, 从而不能被 CC 工具箱直接访问。所以, 必须将被修改的专家库转换为另外的格式。

## 4　结束语

作为模板化测评信息安全产品的工具, CC 工具箱能帮助认证机构, 客户或授权个人生成与实现无关的一组安全要求的 PP 文档; 也能帮助开发者为存在的或计划的系统及产品生成其 ST 文档。可产生模板, 以增强数据的重复性和使用性。同时还能灵活方便地对系统进行增加、删除、修改等维护性操作。它将在信息安全测评领域中得到广泛的应用。

参考文献:

[1] B/T 18336-2001. 信息技术　安全技术　信息技术安全性评估准则[S]. 中华人民共和国国家标准局, 2001.
[2] 戴宗坤, 等. 信息系统安全[M]. 北京: 电子工业出版社, 2002.
[3] 陈远春. 信息安全检测鉴别监控技术与系统安全性能评估分析标准实用手册[M]. 北京: 人民出版社, 2002.
[4] ISO/IEC 15408-1 INTERNATIONAL STANDARD. The Information Technology-Security Techniques-Evaluation Criteria for Security [S]. 2000.

作者简介:

陈轶佳(1981-), 女, 浙江东阳人, 硕士研究生, 主要研究方向网络技术与信息安全; 周安民(1963-), 男, 四川渠县人, 研究员, 信息安全系系主任, 主要研究方向网络技术与信息安全。