文章编号：1672-2892(2010)03-0349-04

基于脚本和URL传递参数的Web部份访问控制技术

李兰瑛[1]，李晓芸[2]

(1.中国民航飞行学院 新津分院，四川 新津 611431；2.中国人民解放军780456部队，四川 成都 610011)

摘 要：访问控制是信息安全和开放的Web服务器必须满足的安全需要。主流的访问控制技术是从系统整体考虑，提供实施访问控制策略的技术平台。文章从信息安全和经济效益的角度综合考虑，提出了针对不同Web需求的部分访问控制技术，它在整体访问控制技术平台的基础上，根据Web访问浏览实际过程，利用脚本ASP执行访问任务的特点，以及URL传递参数表达资源在数据库中的位置属性，实现对Web信息资源的部分访问控制，在低成本付出的基础上解决了Web访问的安全性问题。

关键词：访问控制；Web服务器；ASP服务器端脚本环境；脚本语言

中图分类号：TN915.08 **文献标识码：**A

Part access technology of Web based on script and pass parameters of URL

LI Lan-ying[1]，LI Xiao-yun[2]

(1.Xinjin Sub-University，Civil Aviation Flight University，Chengdu Sichuan 611431，China；2.780456 Troops of PLA，Chengdu Sichuan 610011，China)

Abstract: Access control technology is necessary for information security and open Web service. Main access control technology considers the system as a whole and provides the technical platform to implement access control policy. In the view of information security and economic benefit, this article presents part access control technologies according to different demands of Web. Based on the platform of whole access control technology, according to the process of Web browsing, part access control of Web information resource can be realized through script Microsoft Active Server Pages(ASP) access and the pass parameters of Uniform Resource Locator(URL) expressing the attributes of location in database. It can resolve security problems of Web access at a low cost.

Key words: access control; Web; Active Server Pages; scripting language

访问控制是根据一套安全策略来限制用户对资源的访问，通过访问控制隔离用户对资源的直接访问，从而保证信息系统资源的合法使用及信息安全。访问控制包括3个要素：主体、客体和访问控制策略。任何一个访问控制系统都可以使用3个要素来表示，它具体的实现过程是根据不同的访问控制策略，限制主体对客体的访问操作或给予主体对客体不同的访问权利的过程。

1 主流的访问控制技术介绍

访问控制机制有2个目的：一是防止非法主体对关键客体的使用；二是防止合法主体对关键客体的非法使用。目前主流的访问控制技术有以下3种[1-2]：

1) 自主访问控制(Discretionary Access Control，DAC)是一种自主策略访问控制技术，可以允许合法主体访问策略规定的客体资源。在实现上，要对主体的身份进行鉴别，然后根据访问控制策略赋予主体对客体资源的访问控制权利，这种模型具有简单、易于实现的特点，是一种单级访问控制模式，显然它所提供的安全防护比较低。

2) 强制访问控制(Mandatory Access Control，MAC)是一种多级访问控制技术，分别对访问控制中的主客体对象分配不同的安全级别属性。在实现上，信息系统对主客体的安全属性级别进行比较，然后确定主体是否能或在多大程度上能访问客体资源。这种模型在安全性上较DAC优越，但是它在策略的操作上缺乏灵活性，因此在使用上具有局限性。

收稿日期：2009-10-19；修回日期：2010-01-06

3) 基于角色的访问控制(Role-based Access Control，RBAC)是指在访问控制系统中，按照用户所承担的角色给予不同的操作集。它的核心思想就是将访问权与角色相联系。角色是根据系统为完成各种不同的任务需要设置的，主体可以在角色间进行切换，系统不仅可以添加和删除角色，还可以添加和删除角色的权限。可以看出 RBAC 具有类似于 MAC 多级控制的安全性，在策略思路上较 MAC 又具灵活性，但是对于 RBAC 的完全实现，却还存在着亟待解决的技术问题。

以上 3 种访问控制技术，DAC 模型提供的安全防护机制是最低的，它不能为系统提供充分的数据保护；MAC 显然具有较高的安全性，但是它不能细化访问控制策略，在操作中缺乏灵活性；RBAC 综合了前两者的优点，它操作灵活，管理简单，并在一定程度上较好地实现了系统的防护策略，但是角色和角色访问权的自由添加和删除，又会反过来破坏安全策略，因此，它在实现上还存在着一定的困难。基于以上 3 种控制技术的优缺点，本文提出了一种在整体访问控制框架下，根据不同 Web 的资源访问安全需求，利用脚本执行任务的特点和 URL 传递参数的属性来实现对信息资源的部分访问控制。

2 脚本程序与 Web 资源访问简介

在 Internet 中，对 Web 资源的访问主要是通过特定协议实现，浏览器利用协议向 Web 服务器发送请求，Web 服务器收到请求后调用脚本程序执行具体的访问任务，最后把执行结果返回给 Web 浏览器[3-4]。

2.1 脚本语言

脚本语言 Script 是使用一种特定的描述性语言，依据一定的格式编写的文本，由脚本解析器(应用程序)解释并执行。脚本语言分为客户机脚本和服务器脚本，它们被广泛地应用于网络设计中，减小网页的规模，提高网页浏览的速度，创建动态的、丰富的网页。目前常用于网页设计的动态脚本语言有 Javascript,Vbscript 等。ASP 网页是一套微软开发的服务器端脚本环境,ASP 内含于微软的 IIS 服务器中,通过 ASP 可以结合脚本语言、HTML 网页、 ASP 指令和 ActiveX 元件建立动态、交互且高效的 Web 服务器应用程序。本文涉及网站的脚本执行环境即是 ASP 脚本。

2.2 HTTP 协议简介

HTTP(Hypertext Transfer Protocol)是应用级协议，它满足了分布式超媒体协作系统对灵活性及速度的要求。HTTP 协议是基于请求/回应机制的。客户端与服务器端建立连接后，以请求方法、URL、协议版本等方式向服务器端发出请求，该请求包含请求修饰符、客户信息及可能的请求体(body)内容的 MIME 类型消息。服务器端通过状态队列(status line)来回应，内容包括消息的协议版本、成功或错误代码，还包含着服务器信息、实体元信息及实体内容的 MIME 类型消息。Web 浏览器之所以能够准确访问 Web 服务器上不同的页面资源，就是利用 HTTP 协议向服务器发送不同的请求，在请求中包含参数信息，使得服务器能够区分用户需要访问的资源。

2.3 URL 与 Web 信息资源的访问过程

URL 统一资源定位符，是 Internet 上用来描述信息资源的字符串，通俗地讲 URL 就是网页资源的地址，简称网址，它用统一的格式来描述各种信息资源，包括文件、服务器地址、目录等，URL 的统一格式如下：

protocol://hostname[：port]/path/[parameters][?query]#fragment

a) protocol(协议)：指的是传输协议，对于 Web 而言，常用的传输协议是 HTTP 协议。

b) hostname(主机名)：指的是存放信息资源的服务器的域名系统或 ip 地址。

c) port 端口号：指的是 Web 服务器的端口号。

d) path(路径)：指的是 Web 服务器存放信息资源的相对路径，path 下的[parameters]指的是信息资源的路径参数。

e) ? query(查询)：以 Get 方式传递参数，用于给服务端动态脚本程序传递参数。可包含多个参数，参数名与参数值之间用“=”隔开。不同的参数之间用“&”隔开。这类传递参数对信息资源做了更为确切的定位和描述。

主体用户对 Web 资源的访问浏览是主体用户在客户端利用浏览器，通过 HTTP 协议与网页服务器交互并获得 URL 指定的 Web 资源的过程。首先浏览器把主体用户的请求 URL 提交给服务器端，服务器端根据 URL 中描述的资源信息，调用服务端脚本程序，然后由脚本程序根据 URL 参数信息执行具体的访问任务，最后脚本执行访问任务后，将资源信息发送给客户端。概括起来 Web 资源的访问浏览就是资源请求发送、脚本调用并执行访问任务、任务结果返回及资源的响应过程，见图 1。

3　基于 URL 传递参数的部分访问控制技术

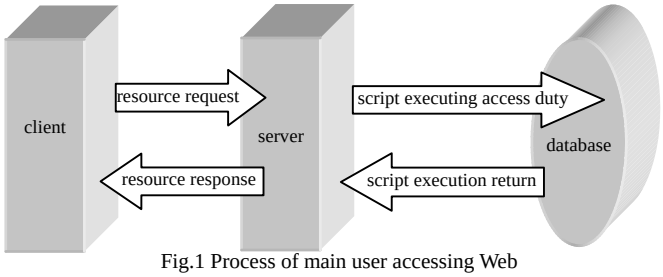

Fig.1 Process of main user accessing Web
图 1 主体用户访问 Web 的基本过程

前面讲到的访问控制技术都是基于整体策略下对 Web 实施的访问控制。但是对于中小型企事业网站，在安全成本核算和经济效益的评估过程中，会遇到这样的问题：如果单独对 Web 中的某种资源信息做访问控制，就需要支付软件系统的开发或者添加硬件设施的费用，很显然这就额外增加了访问控制的成本。但是如果把整体访问控制策略的实施和部分访问控制技术结合在一起，就不需要独立的开发软件或添加加密硬件，既做到 Web 资源信息的开放，又做到 Web 部分资源信息访问控制，既节约了 Web 实施访问控制的成本，又把开放性和安全性在实现效益的同时有机地结合了起来。这就是 Web 部分访问控制技术要到达到的目的。

3.1 基于 URL 参数识别的部分访问控制技术

本文的部分访问控制技术利用 URL 中传递参数的属性和脚本在执行访问任务时对参数的识别判断，实施 Web 部分资源信息的访问控制。URL 中某些传递参数具有标识资源在数据库中位置属性的作用，本文就是利用这类传递参数的属性实施对 Web 的部分访问控制[5]。例如主体用户欲对 URL 信息为：****.open.asp?id=aaaa &path=bbbb 的资源进行访问。假设出于安全策略的需要，网站正是要对参数为 path，值为 bbbb 的信息资源实施访问控制，有访问权限的主体用户，可以访问到该资源信息，无访问权限的主体用户将被拒绝访问。

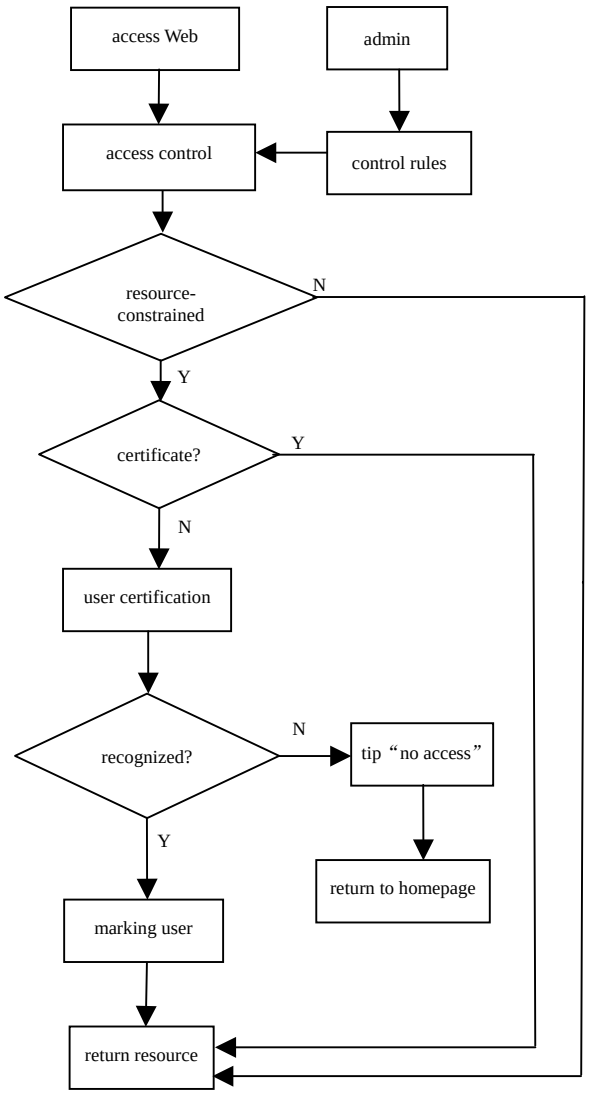

Fig.2 Flow chart of part access control of Web
图 2 网站部分访问控制流程图

服务器端收到请求并调用脚本程序执行数据库访问任务，脚本程序在执行任务的过程中，如果发现传递的查询参数中含有 path 且参数值为 bbbb 时，脚本首先判断该路径参数的资源信息是实施了访问控制的，于是跳转一个需要认证的登陆页面。在认证登陆页面上，如果主体用户通过认证后，脚本将继续执行相应的访问任务，找到资源的确切位置，最后将结果页面返回给主体用户，反之主体用户没有通过认证，将被告知无权访问该信息资源。这样通过识别和判断 URL 中路径参数的值，就可以达到对相关信息资源访问控制的目的，实现起来非常简单。部分访问控制过程可以总结为以下几个步骤：

1) 查询：脚本在执行访问任务时对 URL 路径传递参数值的查询，传递参数值确定的资源信息是否为实施了访问控制的。文章以判断 path 值是否等于 bbbb 为例。

2) 认证请求：如果脚本程序的查询结果为 path=bbbb，那么脚本在执行访问任务的过程中跳转一个需要主体认证的页面。

3) 认证实施：如果主体通过认证，脚本继续执行访问任务，为用户返回结果页面，否则提示主体用户无权访问的信息。

3.2 Web 部分访问控制技术的实现流程

前面已经讲到过部分访问控制技术是基于信息的安全性，综合资源开放性、成本核算和经济效益考虑的一种折中的访问控制策略的技术实现。本小节将给出某网站部分访问控制技术的实施流程(见图 2)，在保证 Web 安全的前提下，网站评估了成本和效益，对网站部分敏感信息实施有限制的访问。如果说 URL 中传递的参数定位了

资源信息在数据库中的位置，那么同样这些参数值也表征了信息资源的内容特征。通过嵌入一段语句，脚本程序就可以识别传递参数和参数值，判断出哪些信息资源是完全开放的，不需要认证即可访问，哪些资源是部分开放的，必须通过认证方可访问[6-8]。

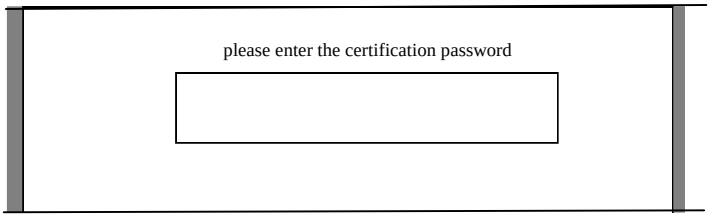

Fig.3 Web certification page of part access control
图 3 部分访问控制认证页面

本网站是基于 VB 语言开发的，采用的是 ASP 脚本执行环境，针对网站部分访问控制流程图，部分访问控制通过嵌入 ASP+VB 语句实现。

该程序的运行结果就是在脚本执行访问任务时候，发现实施部分访问控制信息资源的传递参数和参数值时，就会调转一个需要输入认证密码的页面，见图 3。如果认证通过，脚本继续执行访问任务并返回资源信息，反之则提示无权访问的信息。

4 结论

这种部分访问控制技术是 Web 访问控制技术的一种个性化补充，但是它不具有普适性，对不同语言编写的网站和不同的脚本执行环境需要不同的程序来实现。因为它的具体实施是根据网站自身信息安全的需要和成本效益核算综合考虑的，这就为 Web 访问控制策略的实施提供了灵活性的选择，特别是对中小型企事业单位的网站具有较强的实用价值。一方面可以节约为敏感信息单独开发一套安全系统的费用；另一方面又在原有的网站平台实现了敏感信息对内的开放和对外的安全，并且实施这种部分访问控制技术简单易行。

参考文献：

[1] 宁 葵. 访问控制安全技术及应用[M]. 北京:电子工业出版社, 2005.
[2] 熊 智,刘嘉勇,任伟. 基于角色上下文的强制访问控制的 RBAC 实现[J]. 信息与电子工程, 2009,7(6):589-592.
[3] 朱 俊. 浅谈统一资源定位器[J]. 网络与信息, 2008(6):61.
[4] 罗 玲,白晓颖. Web 服务技术的分析[J]. 计算机科学, 2004,31(4):19-23.
[5] 王建军,宁洪,彭代文. 基于混合访问控制策略的安全机制的研究[J]. 计算机应用研究, 2006,23(3):131-132,135.
[6] Ben Galbraith,Whitney Hankison. Web 服务安全性高级编程[M]. 吴旭超,王黎,译. 北京:清华大学出版社, 2002.
[7] 林 闯,封富君,李俊山. 新型网络环境下的访问控制技术[J]. 软件学报, 2007,18(4):955-966.
[8] Vassilis Kapsalis,Loukas Hadellis,Dimitris Karelis,et al. A dynamic context-aware access control architecture for e-services[J]. Computers&Security, 2006,25(7):501-521.

作者简介：

李兰瑛(1974-)，女，四川省内江市人，硕士，现从事计算机网络通信设备的维护和管理工作. email:lly010214@163.com.

李晓芸(1980-)，女，重庆市人，硕士，现从事计算机网络的维护和管理工作.