校园网统一身份认证系统的开发研究

□ /谢作如

一、问题引出

我校于2000年建立了校园网，现已形成一个初具规模的数字校园系统，该系统由多个子系统构成。然而，系统的开发缺乏标准化、规范化和兼容性，不能实现数据共享、互联互通，出现了一个个“信息孤岛”。尤其是各个系统带有用户身份验证的功能，使得教师必须去记多个用户名和密码，给系统的推广应用带来极大的不便。如何让教师使用一套用户名和密码，就能登录所有应用系统呢？同样，我校后期要开发的应用系统（如选课系统、调查系统）又如何与原有的应用系统接轨？这些问题成为我校教育信息化进一步发展的最大阻碍。

为解决以上问题，一些学校往往在新建校园网系统时，指定某一家软件开发商来做应用系统的整合工作，由该软件开发商修改各个系统的认证方式，让不同系统直接读取一个中心数据库，从而实现用户统一身份认证。但是，这种中心数据库形式的解决方案对我校来说是不现实的。因为它需要耗费一定的财力，而且我校现有系统存在跨网段（中心数据库服务器处于校园网的防火墙后，其他校区无法访问）、跨平台、跨数据库（如我校的网络教学平台系统是PHP开发的，使用Mysql数据库，运行在Linux中）的问题，技术上很难解决，况且直接读取数据库的做法本身是存在安全隐患的。为此，我们尝试自己改造这些系统，设计了以XML技术为核心的统一身份认证方案，并自主开发安全简单的统一身份认证系统（Unified Identity Service），以Web方式对外部系统提供身份验证服务，初步实现了跨系统、跨网段的用户统一认证功能。

二、统一身份认证系统的功能分析

校园网采用统一身份认证，必然要对原有系统改造和整合，这就涉及如何确保原有系统的稳定和安全问题。经多次研究和实践，我们认为把统一身份验证系统作为单独服务系统来开发的做法比较合理，其他应用系统只需按照一定的规范调用这个服务，而不需要对原系统做出较大的改动，减少了系统改造和整合的工作量。

为了方便描述，本文将提供身份验证服务的系统命名为统一身份认证系统，而需要通过该系统来验证身份的各个应用系统，统称为子系统。

1.系统功能要求

统一身份认证系统一般包括三大功能：（1）用户认证。（2）用户的集中管理。（3）应用系统注册。各功能模块相对独立，可以分别实现。其中用户认证模块最重要，其功能是接收子系统提交的用户名、密码信息和其他指令，返回相应的信息。

2.系统性能要求

统一身份认证系统负责多个子系统的用户身份认证。为了确保身份验证的响应速度，系统所在的服务器性能要高，同时带宽也要大，确保大量用户同时提交验证请求时不会响应延迟。

3.系统运行需求和开发工具

运行统一身份认证系统需要数据库服务器（存储用户数据）和Web服务器（响应身份验证）。在子系统数和用户不多的情况下，使用Access数据库即可。开发语言可以使用任何一种动态网页技术语言。

三、统一身份认证系统总体设计

统一身份认证的工作原理如下：当用户访问某成员站点时，子系统将用户名和密码以HTTP的方式提交到统一身份认证系统的认证接口(API)，统一身份认证系统根据接收到的信息和指令，返回用户身份信息，供子系统调用。这一过程对用户来说是透明的，在网络不阻塞的情况下，用户无法察觉验证过程的复杂与否。

1.系统总体设计思想

以Web方式提供身份验证服务，接收子系统（代理）提交的用户名和密码，然后根据密码的错误与否和其他指令返回包含不同数据的XML文件。我们

规定了认证提交的URL参数格式和认证返回的XML文件数据格式。

(1)认证提交的URL参数格式

URL：http://www.wzms.cn/API/checkuser.asp

参数说明：u：用户名，p：密码，ac：请求指令，其中1表示返回基本信息、2表示返回扩展信息、3表示修改密码、p1：要修改的密码。

认证提交的URL范例详见http://www.wzms.cn/api/demo.asp。

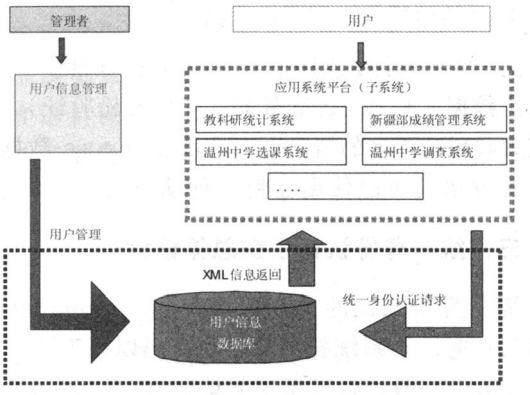
(2)认证返回的XML文件数据格式

XML字段名	XML字段含义（不同状态返回的数据）	是否必需
status	状态（成功返回1，失败返回0）	是（基础属性）
message	错误提示（成功返回“无”）	是（基础属性）
userid	用户id（成功返回用户id，失败返回0）	否（基础属性）
…	…	…

2.统一认证系统的数据库设计

在中心数据库服务器上建立一张完整的用户信息表，作为学校用户信息数据源，我们称之为统一身份表。该表至少包括姓名、工号、登录密码、所属部门、身份证号等信息（符合国家教育部《教育管理信息化标准》）。

3.统一身份认证系统的运行流程图



四、统一身份认证系统核心代码

我们采用了ASP代码编写该系统。鉴于篇幅，仅提供了部分核心代码，去除了一些关于注入过滤之类的功能函数。用户的管理模块和数据库的说明略。

认证模块的核心代码：

```
Response.Charset="gb2312"
Response.contentType = "text/XML"
    username=(request("u"):userpass=request("p")
    userpass1=request("p1"):ac=request("ac")
    set rs=server.createobject("adodb.recordset")
    sql="select*from user where username='"&username&"'" ‘查询数据库
    rs.open sql,conn,1,3
        if rs.bof or rs.eof then
        call mywriteXML(0,0,0,0,0,0,"用户名错误！",0,0)
        else
        if md5(userpass)<>rs("userpass") then
        call mywriteXML(0,0,0,0,0,0,"密码错误！",0,0)
        else
        select case ac
        case 1’返回基础信息
        call mywriteXML(1,rs("userid"),rs("username"),rs("bqq"),rs("xuekeid"),rs("schoolid"),"验证通过!",0,0)
        case 2’返回扩展信息
        call mywriteXML(1,rs("userid"),rs("username"),rs("bqq"),rs("xuekeid"),rs("schoolid"),"验证通过!",1,rs("sex"))
        case 3’修改密码并返回基础信息
        rs("userpass")=md5(userpass1)
        rs.update
        call mywriteXML(1,rs("userid"),rs("username"),rs("bqq"),rs("xuekeid"),rs("schoolid"),"密码修改成功！",0,0)
        case else
        call mywriteXML(1,rs("userid"),rs("username"),rs("bqq"),rs("xuekeid"),rs("schoolid"),"验证通过!",0,0)
        end select
        end if
    end if
  rs.close
```

注：mywriteXML为生成XML文件的子过程。

五、子系统身份认证的应用

子系统的远程验证代码的核心功能是发送HTTP请求，然后读取远程XML文件，根据XML的字段值判断是否验证成功。在Web开发语言中，一般

使用MSXML2.XMLHTTP对象发送HTTP请求，使用DOM方法（如Microsoft.XMLDOM对象）处理XML文件。因为XML是跨平台的语言，任何系统都可以使用XML的解析器，所以远程验证不受各子系统和统一身份认证系统是否处于同一台服务器或者同一网段的限制，也不受子系统使用的编程语言和数据库的限制，只要子系统所处的服务器能够以HTTP方式访问统一身份认证系统，实现身份统一认证。

1.简单子系统（不带用户管理功能）的身份认证

温州中学“教师读名著”活动调查系统是我校信息中心自主开发的应用系统。为了确保调查数据的准确性，校办要求教师以实名登录。根据统一身份认证系统的认证规范（API），在用户认证方面加上远程验证代码后，虽然该子系统和统一身份认证系统并不在同一台服务器上，但是却与其他应用系统间实现了无缝整合。

远程验证的asp代码：

```
XMLurl = "http://www.wzms.cn/API/checkuser.asp?u="& username &"&p="& userpass
Set http=Server.CreateObject("MSXML2.XMLHTTP")
http.Open "POST",XMLurl,False
http.send
Set Doc=Server.CreateObject("Microsoft.XMLDOM")
Doc.Async=False
Doc.ValidateOnParse=False
Doc.Load(http.ResponseXML)
set nodeLis = Doc.getElementsByTagName("response")
status=nodeLis(0).selectSingleNode("status").text '验证状态
message=nodeLis(0).selectSingleNode("message").text '错误信息
Set Doc = Nothing
'' 判断status是否为1：是，则登录；否，提示错误，要求重新登录
if status<>"1" then
ShowMsg message,"0","login.asp"
else
session("user")=username
response.redirect "main.asp"
end if
```

注：ShowMsg为显示错误信息的子过程。

2.复杂子系统（自带用户管理功能）的身份认证

教科研成果登记系统是我校委托软件公司开发的Web应用系统。该系统虽然具有完整的用户管理功能，但是其用户验证是使用统一身份认证系统验证的。用户第一次登录系统将自动在子系统的数据库用户表中添加新记录，即验证通过后，子系统在自己的用户表中查找用户名是否存在，如果不存在就执行添加用户的操作，用户信息从XML文件中读取。自动添加用户的远程验证asp代码略。

六、统一身份认证系统的应用反思

这种简单的统一身份认证模式，已经能满足大多数应用系统的需求，其优势如下。

1.包容性和扩展性好

该认证系统独立于任何具体的应用系统而自成体系，同时以开放的接入方式，为子系统提供满足其自身权限需求的认证信息，便于子系统的独立开发。而且每一次认证的数据交换量少，响应快速。经测试，使用普通的PC服务器，在ASP+IIS6.0+SQL2000的架构上，同时响应数十次的验证请求，系统没有发现延迟现象。

2.XML的技术门槛低，开发速度快

XML使用一系列简单的标记描述数据，这些标记建立方便，易于掌握和使用开发。如果指定校园网中的某一个应用较广的系统用户数据库为认证系统的用户数据库，还可以省去用户管理模块的开发过程。如果已经建立了用户数据库，仅需改动验证模块的几个关键参数就可以正常运行。

3.符合EMIF规范的开发思路

制定EMIF规范的目的是为了给我国教育城域网和校园网的软件建设提供统一的指导规范，目前已经成立了以北京师范大学为首，以国内各大教育软件开发商为主体的EMIF工作组。而EMIF规范使用的数据对象就是以XML封装，可见我们选择的核心技术是合理的。只要逐步按照EMIF规范来修改，我们的认证系统就能与国内教育开发商的新产品实现无缝整合。@

（作者单位：浙江温州中学）