第 33 卷 第 5 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.5 Computer Engineering March 2007
·开发研究与设计技术· 文章编号：1000—3428(2007)05—0281—02 文献标识码：A 中图分类号：TP393.08

基于 LDAP 的校园网统一身份认证的实现

常 潘，沈富可
（华东师范大学网络中心，上海 200062）

摘 要：随着高校校园网基础设施的不断建设与升级，基于校园网的应用也得到了迅速发展，为了保证各个应用系统之间用户数据的一致性及易操作性，迫切需要校园网对统一身份认证系统的支持。该文从 LDAP 协议出发，描述了典型的校园网络中如何实现多系统之间的统一身份认证。

关键词：目录服务；统一身份认证；LDAP

Implementation of Single-sign-on Authentication on Campus Network Based on LDAP

CHANG Pan, SHEN Fuke
(Network Center, East China Normal University, Shanghai 200062)

【Abstract】With the upgrade of campus network, the computer applications are widely spread out among the stuff and students, in order to keep the consistence of user data between different applications, it is urgent to develop a single-sign-on system. This article begins with LDAP protocol and explains how to perform a single-sign-on authentication system based on LDAP.

【Key words】 Directory service; Single-sign-on authentication; Lightweight directory access protocol (LDAP)

1 统一身份认证产生的背景

如今的数字化校园通常包括了办公自动化、财务信息查询、教务管理、图书资料借阅管理、电子邮件系统、一卡通系统、科研管理、就业管理系统、网络设备和服务器管理等应用，其中都需要进行身份的认证并且对不同身份所拥有的角色进行授权。一个通用的实现方法是在每一个应用系统中建立独立的身份认证模块，使用独立的认证机制在各自的身份认证文件或数据库系统中进行认证。这种方法虽然简单可行，但却给用户带来了极大的不便性，最大的弊端就是要为每一个用户在每个应用系统中都建立相关的账户，并为每一个账户赋予不同的权限。按照传统的开发模式，每个应用系统都必须开发各自独立的用户认证模块，用户也不得不记忆不同应用系统的账号和口令。这种认证方式存在很多的缺点：消耗开发成本和延缓应用开发进度；用户需记忆多个账户和口令；无法统一认证和授权；无法统一分析用户的应用行为等。另外，传统的开发模式都是基于关系型数据库的用户认证信息管理模型，读取速度慢、可移植性较差。

基于以上一些原因，使得统一身份认证系统的开发和应用显得由为重要。统一身份认证的主要思想就是由一个唯一的认证服务系统接管各认证模块，各应用只需遵循统一认证服务调用接口即可实现用户身份的认证过程，能够解决上面提到的传统的开发模式的诸多弊端。首先，系统实现了统一的用户身份认证信息管理，可以实现用户认证信息的统一管理，避免了在各个应用系统的身份信息数据库的数据同步更新，用户只须在统一身份认证系统中注册或更改自己的认证信息即可，保证了数据的完整性，消除了不一致性，减少了数据冗余，同时避免了各个应用系统的重复开发。其次，系统实现了基于多个应用系统的单点登录，这将极大地方便用户使用，提高系统的易用性。

2 LDAP 协议简介

LDAP(Lightweight Directory Access Protocol)是一种标准的目录服务技术，它基于 X.500 标准。X.500 是一种 OSI 的目录服务模型，这个模型包括了所有的命名空间和查询更新协议，X.500 通常也被称作“DAP”，这个协议运行在 OSI 网络协议层，功能强大，但由于其丰富的数据模型和操作，使得它非常复杂而显得笨重。LDAP 相对来说比较简单，并且它可以根据应用的需要进行定制和扩展。与 X.500 不同的之处在于，LDAP 一开始就设计运行在 TCP/IP 协议上，是目录服务在 TCP/IP 上的实现。LDAP 对 Internet 访问支持非常好，并且对浏览和查找目录及读取内容进行了专门的优化，使得它读取的速度比一般的关系型数据库要快。

LDAP 标准定义了目录中访问信息的协议，规定了信息的形式和特性、信息存放的索引和组织方式、分步式的操作模型，并且还指明了 LDAP 协议本身和信息模型都是可以被扩展的。LDAP 目录中可以存放各种不同类型的数据，如简单文本、图片信息、URL、二进制数据、证书等。不同类型的数据存储在不同类型的属性中，每一种属性具有特定的语法。目录中信息存放模型基于项(Entry)，每个项拥有全局唯一的名字(DN)并且包含了基于属性的描述信息。项的存放基于树状模型，层次结构相当清晰，适于对应现实世界的组织模型。LDAP 还为信息的检索提供了复杂的过滤条件，并且提供了相当的访问控制能力。

LDAP 的主要特点包括：层次结构清晰，数据存取速度快；提供了同步复制和分布式服务功能；可以跨越平台和系

作者简介：常 潘(1977－)，男，硕士生，主研方向：计算机网络与通信；沈富可，副教授

收稿日期：2006-04-15 **E-mail：**pchang@ecnu.edu.cn

统；完善的安全控制机制；软件基本免费，且软件不是按并发数收取费用。由于以上的一些特性使 LDAP 服务相对于专门在线事务处理(OLAP)优化关系型数据库的数据处理速度要快上一个数量级。

3 统一身份认证系统的设计

基于以上的一些原因，绝大部分的数字化校园系统都采用了 LDAP 作为中心的认证数据库，其中存放了用户 uid，password 等基本不变的个人信息。其他查询关系复杂的数据仍旧存于关系型的数据库中。

3.1 统一身份认证的实现

华东师范大学从 2003 年开发基于 SUN ONE 的公共数据库系统，其中包含了办公自动化、财务信息查询、教务管理、科研管理等子系统，在各个子系统间，采用 Portal 门户作为数字化校园的入口，利用客户端无处不在的浏览器就可以访问各种所需的服务。Portal 信息平台服务器负责校园网中各种服务信息的展示，集成了校园网内各个服务器向信息平台服务器所提供的入口，并且提供页面与服务定制的功能，通过在 LDAP 中读取用户的各种认证和授权信息，认证通过后，为用户分配基于角色的令牌，用户获得的操作令牌后由 Portal 根据所持有的凭证同需访问的相关模块进行交互，并将用户所需信息展示在页面上。图 1 是这个系统的一个实现框架。

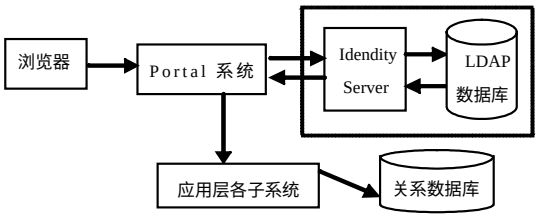

图 1 系统实现框架

由于上面的提及的几个子系统是由软件开发商统一开发的，在开发前期就经过完整的项目规划和调研，因此在 Portal 门户架构下比较容易实现统一身份认证和单点登录。但如何将公共数据库系统同之前单个开发的几个主要的应用系统集成进来成为必须解决的问题，已运行的几个应用系统包括图书管理系统、电子邮件系统、一卡通管理系统、就业管理系统、网络设备和服务器管理、网络认证系统、无线局域网管理系统、各院系 Web 服务系统。

一卡通管理系统是学校使用最广泛的一个系统，其中包含了就餐系统、考勤系统、门禁系统、挂失解挂系统。一卡通系统采用基于 Microsoft.net 的系统架构，前端服务程序采用 IIS6.0+ASP.net 方式，后端采用 Oracle 数据库存储卡的各种信息(包括消费记录、密码、权限等)，认证方式采用校园卡的卡序列号加用户 PIN 码的方式进行，通常用户很难记住自己的卡序号，这给用户的查询带来了很大的不方便。为了与现有的系统进行集成，分两步来改变这种状况：(1)将原先以卡序列号作为用户识别符的方式加以改变，采用人性化的教师工号或学生的学号；(2)建立公共数据库到一卡通系统的单点登录，也就是用户通过公共数据库的 Portal 认证后，只需直接点击一卡通系统超链接就可以直接进入一卡通系统。为实现此目的，在一卡通系统 Web 服务器上安装 SUN Portal Identity Server 的 Agent，由 Agent 负责同公共数据库的 Identity Server 进行交互，使一卡通系统信任从公共数据库转过来的查询请求。这主要通过以下方式来实现：将工号或学号的明文同加密的密文及时间戳传输给一卡通系统，一卡通系统通过共享密钥加密明文的工号或学号与密文的工号或学号对比，如果成功匹配，则认为请求合法，由 Web 服务器通过调用相关接口，返回合适的操作界面内嵌在公共数据库的 Portal 页面中，此处时间戳的作用主要是为了防止重放攻击。但如果用户不是从公共数据库的主入口进入而直接访问校一卡通中心的网站，则需要用到如下的方式：在一卡通的主页上输入用户的工号或学号及密码就可以进入一卡通系统，为了使一卡通系统的密码同公共数据库的密码统一，需要到公共认证中心进行认证。为了实现这种想法，开发了组件 LdapAuth，它包含如下的一些功能：

```
LdapAuth.SetLdapIP("192.168.0.1") '初始化 LDAP 服务器的 IP 地址
LdapAuth.LdapInitPort(389) '初始化 LDAP 服务器的端口
LdapAuth.LdapSearch("o=isp",”uid=20000001” ) ‘查找工号 20000001 教师
Dn=LdapAuth.GetEntryDN '得到工号 20000001 教师的 DN
LdapAuth.AuthUser(UserPassword, Dn) '验证此用户的合法性
LdapAuth.LdapFree '释放相关资源
```

一卡通 Web 服务器通过调用此组件，验证用户名与密码的合法性，如验证通过，则进行相关操作，同时将用户的密码用 Md5 进行散列，并在本地系统中保存备份，以便到认证中心出现网络故障时，用户也可以顺利登录。就业管理系统和图书管理系统的实现细节同一卡通系统类似。

学校的电子邮件系统采用 Eyou 公司的邮件系统，为了使电子邮件系统同学校的公共数据库系统进行集成，扩展了 LDAP 目录服务中的用户的属性域，添加了 Usermail 属性，使之对应用户的电子邮件。由于 Eyou 系统内部采用的也是 LDAP 系统，单点登录的实现同上面的实现方式有些类似，在 Portal 系统与 Eyou 之间维护了一个共享密钥，此密钥同前面的密钥可相同也可不相同，当用户通过 Portal 认证后并点击电子邮件的超链接时，则 Portal 系统从本地 LDAP 中查询用户的电子邮件地址，并将用户的电子邮件明文与加密的密文以及时间戳传输给 Eyou 系统，Eyou 系统根据上面的算法检查合法性并为用户提供服务。在实现统一认证时，让 Eyou 公司进行了二次开发，主要思路如下：在 Eyou 系统自带的 LDAP 中扩展用户的属性，增加 uid 属性，并由成功登录的用户输入统一认证的操作字段工号或学号，并将工号/学号同其 Email 地址进行绑定，当用户通过 Webmail 或 Pop3 与 Smtp 登录时，系统则根据其 E-mail 地址从本地的 LDAP 数据库中查找用户 E-mail 地址对应的工号/学号信息，并将用户的工号/学号与密码通过相关接口发送到认证中心进行认证，认证通过后进入用户的电子邮箱。

我校网络认证系统目前采用的是北京城市热点公司的 Bras2133 系统，它是一种基于 Portal 页面的网络管理系统，当用户出校园网访问时，则系统自动弹出网络认证页面让用户进行认证。为了实现统一身份认证，我们委托城市热点公司进行开发，增加了 LDAP 认证模块，在对用户进行认证时，同样也是将用户的用户名与密码发送的认证中心进行认证，认证通过后，用户才能出校园网进行访问。

网络设备的统一身份认证相对较为复杂一些，因为对网络设备或拨号用户来说，目前使用最广泛的是 Radius 协议，其目的为了使网络设备在认证时可以不使用本地的用户信息，否则当有多个管理员时网络设备的配置文件会相当臃肿，

（下转封三）