文章编号：2095-2163(2019)03-0129-04 中图分类号：TP311.52 文献标志码：A

基于 LDAP 协议的统一身份认证系统研究

华建祥[1]，瞿 霞[2]

（1 福建林业职业技术学院 现代教育技术中心，福建 南平 353000；2 福建林业职业技术学院 自动化工程系，福建 南平 353000）

摘 要：针对校园网各应用系统对用户无法统一管理、认证和授权等问题，提出了基于 LDAP 协议的统一身份认证解决方案，该方案实现了对集成系统用户的统一管理、统一认证和统一授权，具有较高的安全性和可靠性。

关键词：LDAP；统一身份认证；目录信息树；SASL

Uniform identity authentication system research based on LDAP protocol

HUA Jianxiang[1], QU Xia[2]

(1 Modern Educational Technology Center, Fujian Forestry Vocational and Technical College, Nanping Fujian 353000, China; 2 Department of Automation Engineering, Fujian Forestry Vocational and Technical College, Nanping Fujian 353000, China)

【Abstract】 Aiming at the problems on the lack of unified management, authentication, authorization on the application systems of campus network, a unified identity authentication solution based on LDAP protocol is proposed. It realizes the unified management, authentication and authorization of users in the integrated system, and has high security and reliability.

【Key words】 LDAP; unified identity authentication; directory information tree; SASL

0 引 言

账号密码是用户进入应用系统的凭证，身份认证的过程就是判断用户凭证是否有效的过程，若有效，即是合法用户，否则为非法用户，一般而言，一套应用系统对一个用户来说只有一套账号密码。统一身份认证，是指一个用户使用一套账号密码，就可访问所有应用系统，从而实现“用户一次登录，一站式访问所有授权应用系统”。

随着校园信息化建设的不断深入，基于校园的应用越来越多，其中有 B/S 架构，也有 C/S 架构[1]，如教务管理系统、学工管理系统、站群管理系统、就业管理系统、自主学习平台、云办公系统、网络云盘等。不管哪一种应用系统，用户要使用都必须进行身份认证，因此，应用系统越多，用户要记住的账号密码就越多，对用户来说，这显然是一种负担。另外，系统管理人员要维护各个应用系统的用户数据，保证同一用户群体在各个系统中都有相应的用户数据，同时针对各个用户在各个系统中分配相应的权限，这是一件比较复杂、耗时的事情，若还要处理用户因忘记用户名或密码要求找回或重置的申请，则更加重了系统管理人员的负担。所以校园信息化建设的首要目的就是要搭建统一身份认证平台，实现对用户身份的统一认证[2]。

用户账户信息的快速检索、统一管理和统一维护是实现统一身份认证的前提条件。本文根据作者学院校园信息化建设经验，提出了一种基于 LDAP 协议的统一身份认证方案，该方案利用 LDAP 协议对各应用系统用户进行统一身份认证，用户通过认证即可访问所有授权的应用系统。基于 LDAP 协议的统一身份认证系统优化了用户登录体验，方便了用户统一管理，提高了系统的安全性。

1 LDAP 目录服务

1.1 LDAP 协议

轻量目录访问协议 LDAP 由美国密歇根大学开发[3]，是一种被广泛接受的目录访问方法，是开放的行业标准。LDAP 是一种特殊的数据库，其中数据以目录方式组织，目录由对象构成，对象具有属性信息，属性在本质上是一种键-值对，是目录中存储数据的一种方式。LDAP 对数据的写入较慢，修改操作只是使用简单的锁定机制实现，不支持复杂的事务，也没有事务的回滚机制[4]，因此，LDAP 主要任务不是数据存储和操作，也并不适合存储大量需要除查询以外操作（如增加、删除、修改等操作）的数据，但 LDAP 的读取性能比其写入性能要强，比一般的关系型数据库的查询速度快很多[5]，同时，LDAP 基于 X.500 标准的安全协议，由简单安全证

作者简介：华建祥（1982-），男，硕士，讲师、高级工程师，主要研究方向：网络信息安全、算法设计、图形图像处理研究。

收稿日期：2019-03-07

明层(SASL)协议提供访问控制,利用 SSL/TLS 认证机制来保护数据完整性和隐私[6]。因此,将 LDAP 用于网络环境下读密集型操作的统一身份认证,是非常高效安全的。

1.2 LDAP 目录信息树

目录信息树(Directory Information Tree,DIT)以树型结构存储对象(条目)[7],其设计的好坏直接关系认证系统的整体查询性能,因此,在设计目录信息树结构时要尽量减少目录信息树的结构层次,因为层次越少,对象(条目)的标识名就越短,受其它因素影响越小。当出现某个部门机构调整时,结构层次越少,对其它部门或分支的影响就越小。

2 统一身份认证过程

在多应用系统共存的校园网环境下,采用统一身份认证方案即可实现“用户一次登录,一站式访问所有授权应用系统”,其认证过程如图 1 所示。

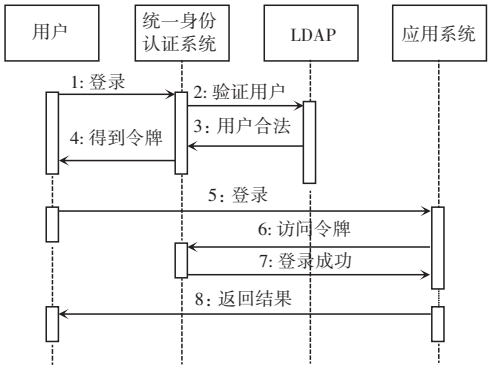

图 1 统一身份认证过程

Fig. 1 Unified identity authentication process

其统一认证过程如下:

(1)用户登录操作,输入账号密码,统一身份认证模块接受用户登录验证请求。

(2)统一身份认证模块根据用户提交的账户密码进入 LDAP 数据库检索,验证用户身份的合法性。

(3)用户身份验证合法,将结果返回给统一身份验证模块。

(4)统一身份验证模块为合法用户发放许可进入已经集成应用系统的身份令牌。

(5)用户登录应用系统并向应用系统提交获得的身份令牌。

(6)应用系统发起查验用户身份令牌操作。

(7)统一身份认证模块证实身份令牌的有效性,则用户登录成功,根据角色授权访问应用系统相关资源。

(8)用户获得服务。

3 系统总体结构

如图 2 所示,统一身份认证系统总体结构主要包括目录服务层、目录服务接口层、应用服务层和对外接口层。其中,目录服务层操作的对象是目录数据库,通过 API 接口与上层通信,目录数据库主要存储用户信息和集成的应用系统信息;目录服务接口层为集成的应用系统服务,负责向目录服务器提交应用系统的操作请求并返回请求结果;应用服务层是一个中间件,负责对外接口层的请求分析和处理;对外接口层面向外部用户,负责处理外部的请求,并将处理结果回送给请求端。

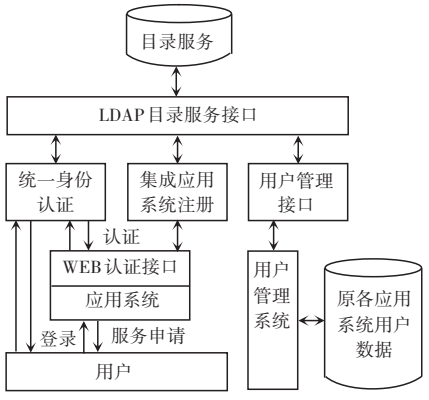

图 2 统一身份认证系统总体结构

Fig. 2 Unified identity authentication system overall structure

应用服务层的功能主要包括用户身份认证、用户集中管理和应用系统注册三个部分。对此可做阐释分述如下。

(1)用户身份认证。用户请求使用网内资源时必须先进行用户的身份认证,合法用户才能取得统一身份认证系统发放的身份令牌,当用户进入应用系统后,应用系统须将用户提供的身份令牌提交给统一身份认证系统进行认证,若为合法用户则根据角色授予相应资源访问权限。

(2)用户集中管理。原有业务系统相互独立,每套应用系统都有一套用户管理系统,如人事管理系统有全校教工的人事基本信息,教务管理系统有全校学生的学生基本信息,用户集中统一管理的目的在于整合上述的教师、学生基本信息,因此,其设计的核心在于实现 LDAP 目录数据库存储的用户信息与应用系统用户管理的信息交互和数据同步。

(3)应用系统注册。应用系统要实现系统集成,就必须在统一身份认证系统中注册,并提交相关注册信息,如应用系统描述、相关用户组及用户条

件、管理员信息、访问 URL 等，统一身份认证系统接收注册信息后需在 DIT 中增加注册系统的节点，并设定相关访问控制信息、系统标识 ID，签发相关数字证书。

4　系统实现

4.1　目录信息树设计

以福建林业职业技术学院统一身份认证系统目录信息树设计为例，目录信息树中主要存储的是用户账户信息和集成的应用系统信息，如图 3 所示，本院的域名为 fjlzy.com，因此，目录树基准标识名（Distinguished Name，DN）为 dc = fjlzy，dc = com。目录树根下主要有 2 类信息，包括：People 用户信息和 Application 集成应用系统信息。为此将给出设计解析描述如下。

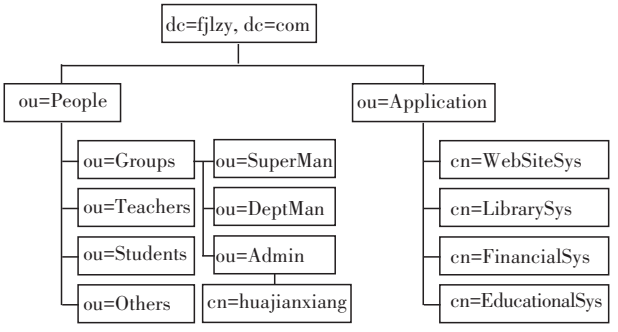

图 3　目录信息树

Fig. 3　Directory information tree

（1）People：主要用于存放用户信息，可细分为 Groups、Teachers、Students、Others 等 4 类组织角色。其中，Groups 用户组可进一步细分为超级管理员角色、职能部门管理员角色和系部管理员角色，院系内部还可继续予以细分；Teachers 指的是教师角色，可进一步细分为院领导、行政上班、行政兼课、专任教师和其它人员五类，根据需要可对细分的角色进行相应的权限控制；Students 指的是学生角色，可根据学制细分为二年制学生、三年制学生、五年制学生、二元制学生和现代学徒制学生等；Others 为临时用户角色。

（2）Application：主要用于存放集成的应用系统的相关信息，如教科研系统、校情展示系统、网站群管理系统、VPN、数字云盘、校友管理系统、招生管理系统、网上办事大厅、移动校园等，包括访问控制信息、系统标识 ID、系统描述、访问 URL 等相关信息。

条目（Entry）是目录管理对象，这是 LDAP 中最基本的颗粒，就像字典中的词条，或者数据库中的记录，每个条目都有一个唯一的标识名 DN，比如 cn = huajianxiang，ou = Admin，ou = Groups，ou = People，dc = fjlzy，dc = com。每个条目都可以有很多属性（Attribute），比如管理人员条目中有姓名、电话、职务、用户 ID、密码、性别、用户状态等属性，每个属性都有名称及对应的值，属性值可以是单个，也可以是多个，比如教师用户或学生用户可以有多个电话，这样电话属性就可以对应多个值。

LDAP 为人员组织机构中常见的对象都设计了属性，详情见表 1，后续可根据实际情况参考表 1 进行设计。

表 1　常见属性

Tab. 1　Common attributes

属性	别名	描述	多值	值（举例）
commonName	Cn	姓名	否	Huajianxiang
Surname	Sn	姓	否	Hua
Organization	O	组织（公司）名称	否	Fjlzy
telephoneNumber		电话号码	是	
Email		电子邮件	是	710979@ qq.com
cardID		证件号	否	050105
UserPassword		密码	否	123456
Owner		条目的拥有者	否	
UserMajor		用户所在专业	否	计算机应用技术
UserStatus		用户状态	否	正常/失效

4.2　角色定义

角色（Role）实际上是一组操作集合，不同的角色被赋予不同的操作集合，每种角色都有某些特定的权限或功能，一般根据用户工作岗位或工作职责分配不同的角色，一旦用户被赋予某种角色，则具有这种角色被赋予的操作权限。在 LDAP 中还可通过设置访问控制表（ACL）来控制角色成员对指定条目的访问权限，比如控制某类用户访问某种资源或资源的某种属性。

校园信息化系统拥有众多的用户，如果对每个用户都进行权限配置，工作量非常大，而且对于用户状态的改变，如学生毕业、教师调岗等都需要对用户权限进行重新分配。一般而言对于拥有众多用户的校园信息化系统不会直接将权限分配给用户，而是通过角色来授予用户权限，角色的引入有 3 个显著优势，具体内容如下。

（1）减少权限分配和调整的工作量，学生毕业或教师调岗只须简单变换角色，即可完成权限的分配和调整。

（2）灵活支持安全策略，过滤某一种角色的权限，即可控制该角色下所有成员的访问权限。

(3)用户管理高效。因此,在本院的信息化系统中,所有用户均归属相应角色,如教师角色细分为院领导、行政上班、行政兼课、专任教师和其它人员五种角色。以共享数据中心应用为例,院领导角色可以查阅、统计分析所有数据,并得到所有数据报表;行政上班角色可以查阅自己所属部门或院系的相关数据及报表;专任教师角色可以查阅本人所在教研室的所有数据及报表;其它人员则只查阅本人相关数据。

4.3 安全模型设计

分析可知,校园信息化系统中的用户本身就是 LDAP 的访问用户,所以 LDAP 可以针对这些用户提供集中式的身份认证(Authentication)和授权管理(Authorization)功能。根据 LDAP v3 的规范,身份验证的方式有 4 种,分别是:匿名验证、基础验证、SASL 验证和 Kerberos 验证。对此拟展开研究论述如下。

(1)匿名验证:用户登录时不提供账户密码,由系统赋予缺省的身份与访问权限,一旦设置了匿名验证功能,用户不经验证即可访问目录树中的条目,当然因为权限问题会屏蔽掉很多信息,只能看到一些完全公开的信息。

(2)基础验证:最常见的用户密码验证方式,在基础验证中,用户名就是 LDAP 条目的 DN,密码可以用各种算法加密存储。基础验证由于设计简单且与 LDAP 结合紧密,是最常用的一种验证方式,但在使用上也有明显的缺点。首先,验证方需要提供条目的 DN 和口令,DN 其实反映了 LDAP 目录的内部组织结构,用户并不需要了解,要用户记住诸如 cn = huajianxiang, ou = Admin, ou = Groups, ou = People, dc = fjlzy, dc = com 这样的条目 DN 不太现实。其次,基础验证中 DN 和口令在网络中以明码方式传送,这使得远程验证过程容易被监听和盗用。所以,这种方式多用于内网验证,或者通信链路本身已经有加密机制保护。

(3)SASL 验证:LDAP v3 标准引入了 Simple Authentication and Security Layer(SASL)基于连接协议的一种框架,SASL 解决了基础验证存在的问题,用户身份可以是 DN 或者用户名,认证凭据可以是密码或数字证书,SASL 为验证过程设计了不同的安全机制,常用的有 Digest - MD5、Kerberos、TLS/SSL 验证,如此即使得用户名和密码在网络上以密文方式传输,防止监听和篡改,大大提高了安全性。

(4)Kerberos 验证:Kerberos 验证多用于网络认证服务(Network Authentication Service, NAS)。在 NAS 环境中,客户端的密钥由密钥发布中心(Key Distribution Center, KDC)签发,客户端保存私钥部分,KDC 保存公钥部分。在使用时,客户端发送一个凭证请求到 KDC,KDC 创建一个授权凭证(Ticket-Granting Ticket, TGT),以客户端的公钥加密并返回给客户端。客户端收到 TGT 后用自己的私钥解密,如果成功就将该 TGT 当作客户端通信凭证。每隔一段时间 TGT 会超时,这时客户端会发起申请要求派发下一凭证以保持通信连续,这一过程是自动的,无需用户参与。

本院的统一身份认证系统采用了 SASL 身份认证机制,其应用如图 4 所示,LDAP 客户端请求调用服务端的 SASL 协议驱动,再由服务端的 SASL 协议驱动连接认证系统,从而实现对客户端用户的身份验证,由于用户信息均以密文传输,安全性非常高。

图 4 SASL 认证机制

Fig. 4 SASL authentication mechanism

5 结束语

本文重点探讨了基于 LDAP 统一身份认证系统中目录信息树的设计、角色定义和安全模型设计,详细分析了统一身份验证过程。实践证明,基于 LDAP 的统一身份认证系统成功实现了用户的统一管理、认证和授权,系统具有较高的安全性和可靠性。

参考文献

[1] 贺玉明,李晋宏,唐辉. LDAP 在数字校园统一身份认证系统中的应用[J]. 计算机技术与发展, 2011,21(5):139-142.
[2] 黄秀芳,王海. 基于 LDAP 的高校数字化校园统一身份认证集成实施方案[J]. 江苏科技大学学报(自然科学版),2015,29(6):580-584.
[3] 王卫华,王长杰. 基于 LDAP 的统一身份认证在网络中的应用[J]. 清远职业技术学院学报, 2014,7(6):38-40.
[4] 吴晓斌,张月琳. 基于 LDAP 的校园网统一身份认证系统设计[J]. 华中科技大学学报(自然科学版),2003,31(S1):332-334.
[5] 袁轶,宋秋林. 基于 LDAP 的用户认证系统设计与实现[J]. 重庆电子工程职业学院学报, 2012,21(3):161-164.
[6] 谭胜兰. 基于 LDAP 技术的校园网统一身份认证系统的设计与实现[J]. 东莞理工学院学报, 2009,16(3):82-86.
[7] 张希奇. 基于目录服务的统一身份认证和登录系统研究[J]. 安徽电子信息职业技术学院学报,2015,14(2):1-4.