基于 LDAP 的用户统一身份认证管理系统的设计与实现①

Design and Implementation of Unified Identity Authentication Management System Based on LDAP

尹文平 兰雨晴 高 静 (北京航空航天大学软件工程研究所 100083)

摘要:文章介绍了 LDAP 协议和目录服务,阐述了基于 LDAP 的用户统一身份认证管理系统中的自定义模式和目录树的设计方法,以及统一用户身份认证的原理和安全机制,并将该用户统一身份认证管理系统应用于信息资源管理与信息服务平台中。

关键词:LDAP 统一身份认证 目录服务 模式 LDAP 数据交换格式

1 引言

随着高校、政府、企业信息化建设的不断发展,基础设施的不断投入与升级,基于 Web 的应用系统的开发也得到迅速开展。不同的系统如 OA 系统、邮件系统、计费系统等不同的应用同时存在,如何提供一种方便可行的方法,使用户能够更迅速、安全、有效地访问和使用这些网络资源,已越来越受到人们的关注。

目前最常见的解决方案是对于每个应用系统建立独立的身份认证模块,使用独立的身份认证机制对用户进行认证授权。这种机制最明显的缺点是众多用户必须面对系统重复输入帐号,口令等信息,不仅繁琐并且容易出现口令丢失;此外,网上诸如口令等敏感信息的分布式存储,给黑客造就了许多机会,大大降低了数据安全性。

基于 LDAP 的统一身份认证管理系统采用统一的信息数据库存储用户信息,有效的解决了上述问题,同时也避免了由于各个应用系统独立进行用户认证所造成重复开发。国家 863"基于国产 Linux 农牧林业科技综合信息服务平台关键技术研究"项目中需要实现信息资源管理与服务平台(以下简称平台),平台集成多个子系统和服务,包括信息资源管理系统、FTP 服务器、邮件服务器、BBS 服务器,各应用系统和服务器分别有各自的用户权限系统,采用基于 LDAP 的统一用户身份认证有效解决了信息平台用户的统一管理、统一认证和统一授权。

2 LDAP 和目录服务

目录服务是一个特殊的逻辑信息数据库。它对读、浏览和搜索进行了优化,具备完善的安全控制机制,可以用来保存描述性的、基于属性的信息,并且具有支持复杂的过滤搜索能力。

LDAP(Light Weight Access Protocol)轻量级目录访问协议是运行在 TCP/IP 上的目录访问协议。它基于 X.500 协议标准,但比 X.500 简单并且可根据需要定制。

LDAP 以目录信息树(DIT: Data Information Tree)结构的形式存储信息,目录信息树中的节点即为一个 Entry(条目),每个条目包含属性(Attribute)和属性值

① 本文得到了上海中标软件有限公司承担的国家 863 项目"桌面操作系统及其配套环境,编号 2002AA1Z2101,2004AA1Z2020"的资助

的信息。而属性由对象类(Objectclass)确定,每个对象类包含多个必须或可选的属性。对象类和属性类型确定了 LDAP 模式。条目信息通过 LDIF 文件以文本的形式描述。

2.1 LDAP 模式(schema)

LDAP 中把对象类(Objectclass)、属性类型(Attribute)、语法和匹配规则统称为模式。模式确定了存储的数据类型,数据如何被存储以及存储在不同的 Entry 下的数据之间的关系。

LDAP 服务器提供了常用的对象类和属性类型的模式文件,但在实际的应用中,LDAP 提供的属性无法或很难描述实际类型时,用户可以根据实际需要遵照 LDAP 的规范自定义模式。自定义模式需要获取全球唯一的 OID(Object Identifier,对象标识符),添加自定义属性类型和自定义对象类,将定义的属性类型加入自定义对象类。

自定义模式最大的优点是能够更恰当地描述系统,并且可扩展性好,但是自定义模式中的对象类和属性类型只能被添加该模式的系统应用,不具有一般性。

2.2 LDAP 数据交换格式(LDIF)

LDIF 是 LDAP Data Interchange Format 的缩写形式,它以文本的形式描述目录信息树中条目的信息。LDIF 是 LDAP 目录树信息交换的基础,许多操作如拷贝、添加、修改、数据导入、导出等都是基于 LDIF 文件进行的。条目的 LDIF 文件的基本格式如下所示,dn 是条目在目录信息树中的唯一表识。

dn: <distinguished name>
<attrdesc>: <attrvalue>
<attrdesc>: <attrvalue>

3 统一身份认证管理系统的设计与实现

3.1 用户自定义模式的应用

Openldap 自带的对象类和属性类别无法或者很难描述某些信息,比如用户的状态、级别、上线统计,平台提供的服务之间的关系等,为了更恰当地描述统一用户身份认证系统的需求,对于应用系统的实际需要,系统中常会引入自定义模式。表 1 列出对象 USER 所有的属性。

以 userName 属性为例,在平台的用户统一身份认证系统中,它对应的自定义属性类型(attributetype)和 USER 对象类(Objectclass)的定义设计如下所示:

表 1　USER 对象的属性表

序号	USER	描述
1	uid	
2	userName	
3	userPassword	
4	userEmail	
5	userState	用户状态,表示用户是否激活,注销,封禁
6	userCreatedate	
7	userDescription	
8	userExpertpoints	用户的专家计分
9	userAvailpoints	用户的可用计分
10	userCertificate	用户证书

attributetype (1.3.6.1.4.1.15490.1.1 NAME 'userName'
DESC 'user name'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE)
objectclass (1.3.6.1.4.1.15490.2.1 NAME 'objUser'
SUP top STRUCTURAL
DESC 'object class'
MUST (userName $ userPassword $ userEmail $ userCreatedate $ userState)
MAY (userExpertpoints $ userAvailpoints $ userCertificate $ userDescription))

其中 1.3.6.1.4.1.15490.2.1 为 USER 的对象标识符 OID,MUST 后面的属性在对象'objUser'中是必须的属性,而 MAY 后面的属性则是可选的。

3.2 目录信息树设计

平台中的目录信息包括三方面的信息,一个是用户帐号信息,再一个是应用系统的信息和证书信息,整个平台用户的目录树结构设计如图 1 所示。

在目录树中,用户 person、用户组 group、应用系统对象 service、角色 role 和数字证书 certificate 分别单独放置在各自的组织单元里面。用户信息包括用户的

账号、密码、所属分组或角色、访问控制权限信息等基本信息。service 节点的子女为各个应用系统的信息，其中每个应用系统有自己的应用模块。这样的目录设计便于细粒度的权限控制，认证服务器的查询以及目录服务信息的管理。

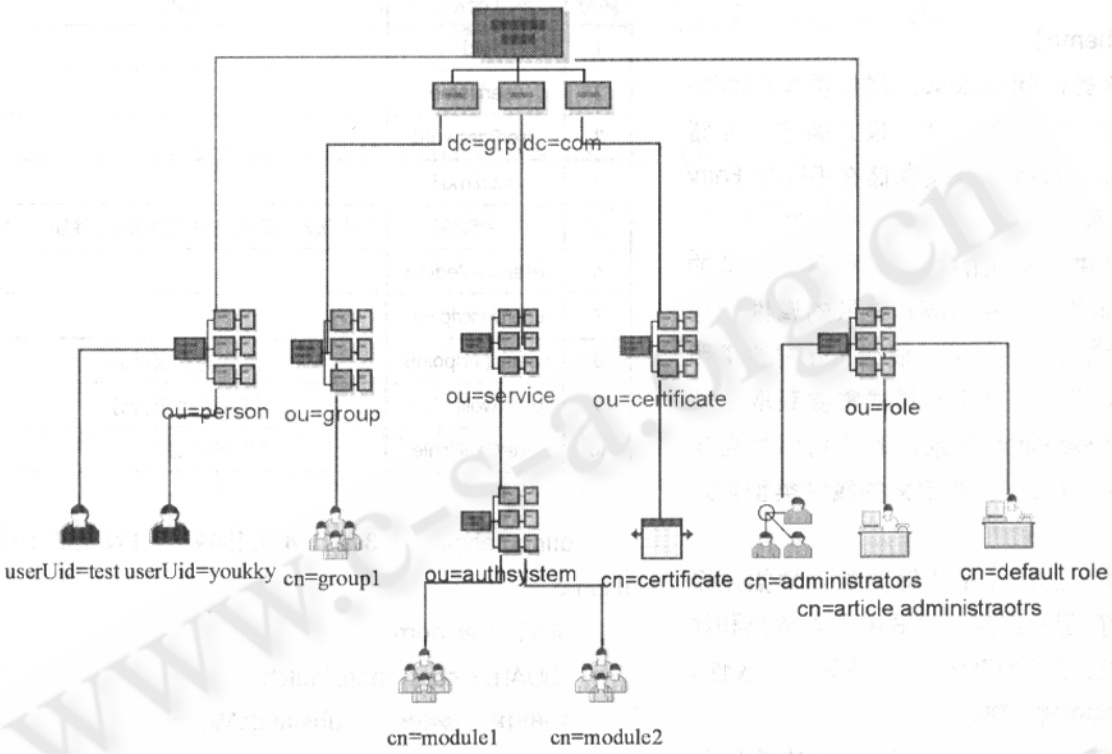

图 1　目录信息树的设计

3.3 安全机制

前面提到，LDAP 和关系数据库很显著的一个差别就是 LDAP 提供了强有力的安全模型。它的安全模型主要通过身份认证、安全通道和访问控制来实现。LDAP 的访问控制机制非常灵活和丰富，它是基于访问控制信息 ACI，通过访问控制列表 ACL 实现的。这点与关系数据库系统不同，关系数据库系统通常采用基于用户组或角色进行权限控制。

LDAP 中提供了三种认证机制，即匿名，基本认证和 SAML（Simple Authentication and Security Layer）认证。

（1）匿名认证。用户不需要提供任何用户信息，这种认证机制只用于完全信息公开的情况下。

（2）简单认证。用户通过提供用户名和密码进行身份识别，分为简单密码和摘要密码认证。

（3）SAML（Simple Authentication and Security Layer）：简单证和安全层，即在 SSL 和 TLS 安全通道基础上进行的身份认证，包括数字证书的认证。

RFC2246 定义了 TLS，它使用 X.509 证书对传输层数据进行加密，向上层提供安全的数据传输。为了使系统具有完备的安全机制，并使系统适用于分布式环境，应该使用在传输层进行数据完整性和私密性保护，因此平台统一身份认证系统采用基于公钥体制的 TLS 认证方式。统一用户身份认证系统的安全认证授权的过程如下图 2 所示。

4 用户统一身份认证管理系统架构

平台中使用统一用户身份认证管理系统将 FTP 服务用户，OA 系统用户，邮件系统用户，论坛用户和信息资源管理系统用户进行统一管理、认证和授权。统一用户身份认证系统分三层架构：用户客户端应用程序，身份认证服务器，用户信息资源库。用户客户端应用指的是平台中的应用系统，如 JIVE 论坛，邮件服务等，身份认证服务器采用 OPENLDAP 服务器，用户信息资源库是 OPENLDAP 内置的 Berkeley DB，存储平台中所有的用户信息。系统架构如图 3 所示。

5 结束语

统一身份认证系统是为了解决多个应用系统之间的用户不统一、权限控制不统一的问题。通用资源管理与信息服务平台利用了 LDAP 的安全认证机制以及

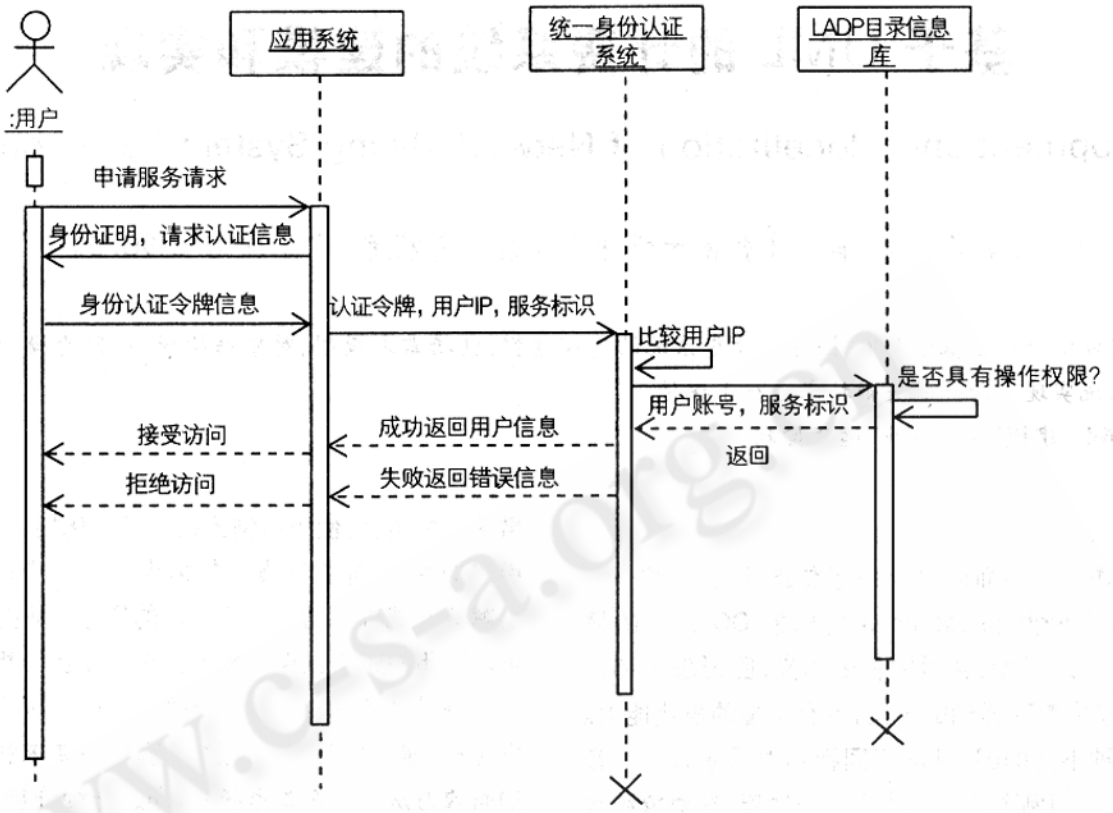

图 2　统一身份认证过程

J2EE 相关技术，实现了对平台中不同系统的用户统一管理。实践表明，统一身份认证管理系统不仅提高了平台的安全性、可靠性，也给用户提供了极大的方便，同时方便了用户的管理。

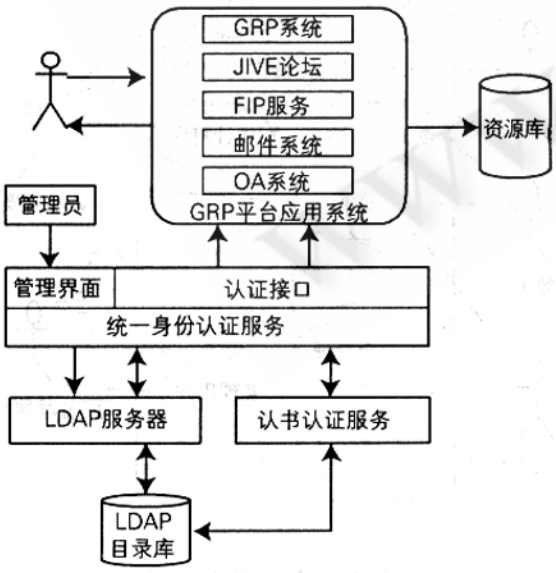

图 3　用户统一身份认证管理系统架构

参考文献

1 OpenLDAP 2. 2 Administrator´s Guide http://www.openldap.org/.

2 RFC2829, RFC2849, RFC2251, RFC2256, RFC2246 http://www.ietf.org/rfc.html.

3 the steps for ACIs http://www.openldap.org/faq/data/cache/634.html.

4 A. V. Maheswara Rao , LDAP Schema Design – case study .

5 Norihiro Sakamoto, Development of a User Authentication System Based Key Certificates for Healthcase Information National University Hospitals.

6 C. S. Yang C. Y. Liu J. H. Chen C. Y. Sung, Design and Implementation of Secure Web – based LDAP Management Systemt.