基于目录服务的用户统一电子身份的实现

袁先珍　田斌　钟华　(武汉理工大学　430070)

摘要：在校园网中提供的应用服务越来越多,给用户管理和操作带来许多不便，本文针对这一现状，结合LDAP目录服务与安全访问控制服务器,提出了在校园网上实现统一电子身份的方法。通过系统的配置、编制LDAP客户端程序详细论述与现有系统集成，以至整个系统具体实现过程。

关键词：LDAP　ACS　目录服务　安全认证

1 概述

随着校园信息化建设的不断深入，网络应用日益丰富。应用服务的增加使得网络管理特别是用户管理变得越来越复杂。用户在校园网的不同应用中有着不同的权限，每个应用都需要设置帐号。这就带来了很多问题，管理起来很不方便,用户面对多个应用系统要输入不同的帐号和口令，不仅烦琐，而且容易出现口令丢失等安全隐患。通过具有较高安全控制的身份验证系统和集中用户管理将用户信息与具体应用相对独立，校园网用户只需一个单一的帐号，而对于某个具体的应用则按照一定的规则赋于用户某种角色实现对重要资源的授权访问控制。这样既能保证数据安全，又使用户操作方便，同时加强了网络管理的能力。

2 统一用户认证系统设计

统一电子身份的实现包括两个主要功能模块：用户认证系统模块和用户管理系统模块。用户认证系统采用Cisco公司的安全访问控制服务器ACS（Access Cotrol Server2.6）来完成。Cisco Secure ACS是目前广泛使用的AAA服务器，支持多种认证协议，如RADIUS或TACACS+等。用户管理系统选用iPlanet的Directory Server5.1（下面简称iDS）。iDS是基于开放的LDAP设计的，具有可伸缩性的特点，并对查询进行了优化，每一个服务器可以管理数百万个登录资料，每秒钟可以处理数千个查询作业。而且支持客户端授权的SSL、Verity的集成式检索器、SNMP、出色的数据库联接功能及Web网站内容管理等，从而保证了高效和安全以及利于扩展的性能，近几年在网络用户管理中的应用非常广泛。

图1简要表示了用户身份认证的过程：End_user1,End_user2分别代表局域网用户和远程拨号用户。两大校园网主要用户类型，分别通过PPP、PPPoE协议与AAA Client（AAA Client可以是交换机或防火墙）建立连接。PPP协议具有用户认证及通知IP地址的功能。而PPP over Ethernet（PPPoE）协议，是在以太网络中转播PPP帧信息的技术，尤其适用于DSL等方式。目录服务器将校园网信息服务的所有帐号、密码邮箱地址等基本用户信息存储在目录数据库中，对于所有需要进行帐号与密码验证的信息服务，用户只要输入一次帐号与密码即可，从而对用户实现统一身份认证。用户发出一个服务请求后，由ACS客户端（可以是防火墙或交换机等）发出认证请求，要求用户输入身份信息，输入后AAA Client将其发送到ACS服务器端进行有效性检验，ACS服务器支持外挂数据库，通过TACACS+或RADIUS协议与目录服务器进行通信，校验用户的合法性并返回结果到AAA Client，AAA Client根据认证服务器返回的结

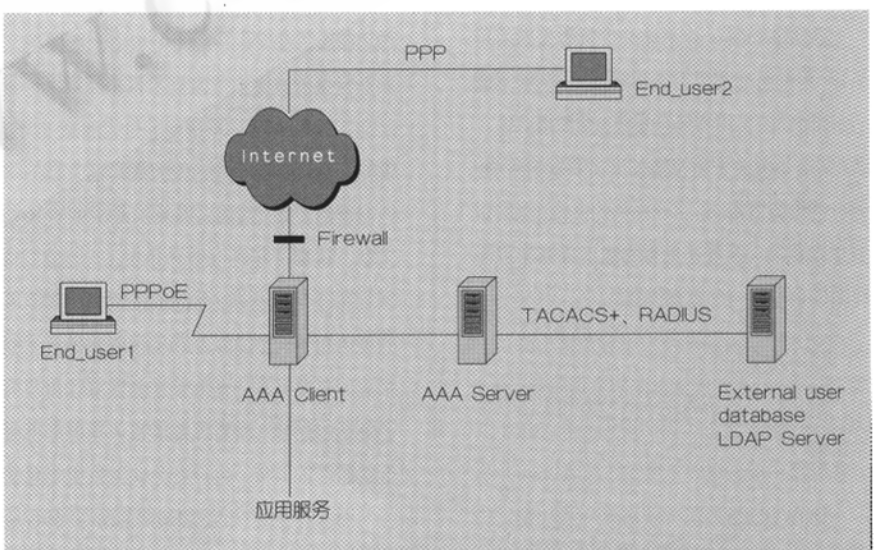


图1　用户认证系统

果及权限信息给予用户放行或拦截，并在AAA Client保存其权限信息和访问记录,同时在SQL Server里储存访问日志。这为基于用户访问信息的计费提供了可能性和现实性。

3 基于LDAP的用户管理与现有系统的集成

在用户认证系统中ACS服务器认证的依据是认证数据库，也就是LDAP服务器中的用户信息。实现统一电子身份首先就是要把校园网中的各种应用服务的用户集中到目录服务器并统一管理，最终每个用户在多个应用服务中都只有一套帐号和密码。网上需要帐号应用服务的主要有以下几种：

(1) 网上图书馆；

(2) 办公系统；

(3) 邮件服务。

采用LDAP服务器和防火墙结合，将用户帐号与IP绑定，从而有效防止了用户帐号盗用和一个用户多个帐号的情况。公文服务器是采用Lotus Domino来实现的。Domino支持第三方基于LDAP标准的目录服务，在服务器上启动LDAP任务，然后运行LDAP协议并设置为连接到服务器的客户机。在Domino Administrator中，将LDAP目录中的群组名称包括在Domino服务器上的数据库存取控制列表(ACL)中。当用户请求邮件服务时先到LDAP服务器上进行用户验证时，如果合法则返回相应的属性，再到公文服务器中进一步判断是否有该操作的权限。因为ACS的授权认证只是对用户可以使用的应用服务进行限制，而具体的权限还是在应用服务中设定。

图书馆的用户管理的后台数据库是关系数据库，那么要解决的问题就是把关系数据库中的用户导入iDS中，通过编写程序进行数据转换，先选择用户在数据库中需要的字段信息，通过Java中提供的JDBC接口来访问关系数据库，得到需要的字段信息，然后在iDS中添加一个Entry，这个Entry包含了上面的用户信息。

4 LDAP客户端管理程序的开发

iDS提供了两种图形界面的管理途径，iPlanet Console和基于WEB的Gateway，都是客户端软件，前者可以对目录服务器进行包括系统参数在内的全面管理，但比较专业化，而且用户管理功能不完备，操作也比较烦琐；后者主要是提供用户和管理员查询、修改属性用的，十分简单，不是很实用。因此开发一个基于WEB的目录服务管理系统是很有必要的，该系统即为LDAP客户端，浏览器通过它访问LDAP服务器，管理员和普通用户都可以通过浏览器来完成各自有权限的操作。

开发工具选用Netscape的Directory Java SDK4.1，先到iPlanet的主页上下载该开发包，解压并重新设置类变量，安装就完成了，然后直接引用开发包带有的封装了LDAP API类和方法来编写程序。认证界面为表单形式，输入帐号和密码提交到服务器验证，验证过程大致有以下几步：

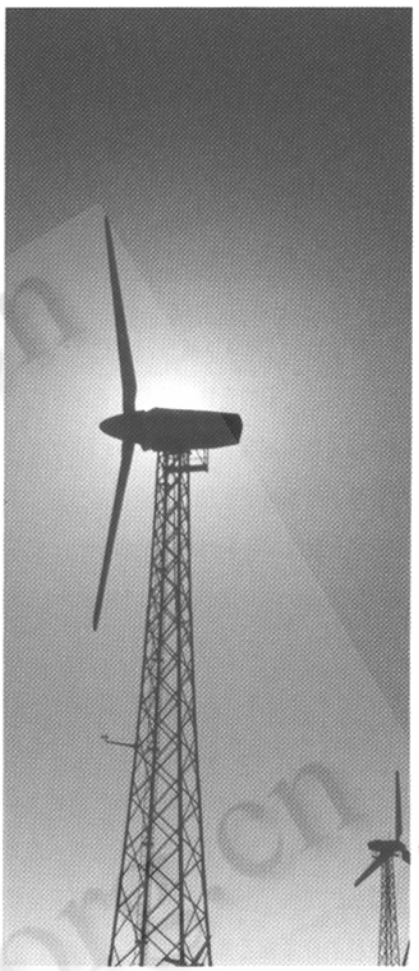
(1) 建立连接；

(2) 绑定到LDAP服务器；

(3) 按表单提交的信息认证并返回结果；

(4) 断开连接。认证由连接对象的authenticate方法来实现，另外还要设定密码过期时间，超过时间必须重新验证，在过期时间内如果要下机可以注销，如果请求要再次验证，这种方式对于在公共机房上机的用户可以防止帐号盗用。

用户管理界面也是通过WEB方式，比如添加一个用户，只需选择添加用户操作项，然后通过表单输入用户的信息，而后台程序实现是在iDS中添加一个Entry,先创建一个包含DN和属性的新Entry，然后引用连接对象add方法来添加，部分代码如下：



```
try{
LDAPEntry newEntry = new LDAPEntry
( dn, attrs );
ldapconn.add( newEntry );
}
```

在管理策略上采用分级管理的方式，将用户分组管理，系统管理员组的用户可以设置服务器超级用户口令，可以添加新的管理员组，管理员组的成员可以添加、删除、修改、复制、对过期或违规用户帐户进行封锁；普通用户只能查询某些信息以及修改自己的部分属性,这种方式减轻了管理员的任务，基本上实现了用户自管理的功能。