统一身份认证平台的设计

沈 斌[1], 史鸣杰[2]

(1. 南京师范大学 信息网络中心, 江苏 南京 210097; 2. 东大金智软件股份有限公司, 江苏 南京 210008)

[摘要] 统一身份认证平台是数字化校园建设的基础, 主要实现用户管理、身份认证、分级权限管理和单点登陆等功能, 以解决校园信息化建设过程中用户定义模糊、用户身份组织零乱、交叉权限管理无法定义和应用系统出口多样性等棘手的问题. 同时给出了校园统一身份认证平台的功能、流程以及接口设计的方法.

[关键词] 数字化校园, 统一身份认证平台, 目录服务, 流程, 接口

[中图分类号] TP393.18, [文献标识码] B, [文章编号] 1672-1292(2004)02-0073-03

随着高校数字化校园建设进程的逐步深入, 校园网内部运行的应用系统也随之增加. 传统上这些应用系统各自拥有一套用户及不同的身份认证方式, 结果造成多套用户共存及用户信息冗余、用户多密码记忆及多点登陆. 这严重影响了用户使用的效率, 并对整个系统的安全带来了极大的隐患.

所以, 在数字化校园建设过程必须通过科学的集中认证技术, 实现应用系统的用户集中管理和统一认证, 彻底改变各自为政、管理松散的用户管理模式; 充分发挥高校内部网络管理维护部门的管理职责; 规范用户操作行为. 要实现集中认证, 必须解决以下 3 个关键问题: 用户资料的集中存储和管理; 用户身份的集中验证; 访问权限的集中控制和管理.

1 统一身份认证系统功能的规划

统一身份认证系统的核心思想是将机构、用户统一存储, 对应用系统统一授权, 规范应用系统的用户认证方式, 从而达到提高整个系统的整体性、可管理性和安全性的效果. 从功能上来看统一身份认证平台有三大逻辑组成部分: 目录服务器、用户身份管理服务和用户身份认证服务.

1.1 目录服务器

目录服务器是整个统一用户认证平台的基础, 必须采用标准的 LDAP 目录服务器产品, 通过 LDAP 目录服务将校内的用户或组织的信息(称为属性)以层次结构、面向对象的数据库的方式加以收集和管理, 对用户信息进行统一管理, 保证了数据一致性和完整性, 为校园各类应用系统提供用户信息的共享和使用.

1.2 用户身份管理服务

用户身份管理服务功能可以采用集中或分布式的工作方式, 对一个中央用户资料数据库进行统一操作. 系统管理员权限可以分派到以组为单位, 访问权限的管理可以下放在各个级别, 理论上可以分无限个下放级别. 必须能实现以下的功能:

(1) 提供自动和管理员确认两种模式的用户注册功能. 系统支持自动根据预定义的策略完成对注册用户的授权, 即自动注册功能; 也支持用户注册后, 由管理员进行确认并进行授权的管理模式.

(2) 提供直观的图形化组织管理界面. 组织管理模块以图形的方式支持管理员完成团体的结构以及团体内部的角色(职务)等相应信息的注册, 提供组织视图和角色视图两种视图:

组织视图主要维护各个组织之间的关系(包括上下级关系、协助关系等), 以及进行组织的增加、删除和修改等工作, 并提供剪切、复制、粘贴以及拖拽等多种方式支持组织机构的快速重组.

角色视图对每个组织内部的角色(职务)数据进行维护管理, 包括角色 ID、角色名称、角色的工作关系以及设置该角色(职务)所需要的权限等.

(3) 提供简单方便的用户管理界面. 用户管理模块负责对校园网用户的数据管理. 和安全相关的用户基本信息由本系统进行维护, 包括对用户数据的增加、修改和删除. 它包含以下两个子模块:

用户基本信息维护子模块: 该子模块完成对用户基本信息的管理和维护.

用户角色设置子模块: 在统一认证平台中, 用

收稿日期: 2003-09-11.
基金项目: 南京师范大学"211"工程二期建设资助项目.
作者简介: 沈斌(1964–), 讲师, 主要从事多媒体及网络技术的研究. E-mail: bshen@njnu.edu.cn

户享有的权限主要由其在组织机构和团体中担任的角色(职务)来确定. 一个用户可以在多个组织中担任职务. 用户角色设置模块完成对用户职务的赋予、剥夺等工作.

(4) 提供严格的分级用户数据访问权限控制, 基于ACI(Access Control Information)机制有效保护用户的资料, 并通过分级管理提高用户管理的效率和质量. 包括: 个人用户只能访问自身基本资料的属性, 不能修改涉及系统的相关属性; 系统管理员可以为某一个组织或部门设置相应的二级管理员(及根据目录树的结构指定授权代理人), 二级管理员也可以为某一个班级或研究室设置相应的三级管理员, 以此类推, 原则上可以提供无限级别的分级管理功能.

(5) 提供基于角色的授权管理模块. 统一身份认证平台授权范围主要是应用系统级的权限, 而对于角色在特定系统中分级权限由各应用系统来确定. 基于这样一个统一的授权入口, 管理员可以完成以下工作: 查询用户在整个校园应用中分类应用系统权限及应用系统中的分级权限; 维护用户总体权限, 对于该用户能够使用的系统, 该模块通过标准的接口直接调用对应子系统的授权管理, 快速完成用户全部的授权管理, 而不需要一个个进入各应用系统本身.

(6) 提供动态规则定义功能. 统一身份认证平台的定位是解决全校所有用户的身份信息的统一管理, 为解决一些非固定人员(临时用户)的管理问题, 系统提供强大的动态规则定义功能. 包括: 命令行批处理机制, 通过编辑一个简单的批处理文件, 通过该文件的手工执行, 批量增加或删除相应的用户; 自动规则机制, 通过定义相应的动态规则以及这些规则的执行时间, 由系统自动在所要求的时间点生成相应的用户, 再在另外一个时间点自动注销这些用户.

1.3 用户身份认证服务

通过对角色的定义, 用户身份认证服务允许管理员方便地对各种规模的用户集授权访问或取消访问授权. 提供以下功能:

(1) 提供多种身份认证方式, 支持下列用户认证方式: 用户名/口令认证; 数字证书认证; 卡认证.

(2) 应用资源访问控制. 系统根据用户的角色, 允许使用某些服务或者服务中的一个子集; 提供一个API, 通过它可以定义认证成功/失败后的系统动作, 满足一些特殊的功能要求.

(3) 提供单点登录功能, 实现用户登录一次, 就可以访问所有集成的应用和服务.

2 流程及接口设计

2.1 流程设计

用户管理流程的设计方法如图1所示.

2.2 接口设计

2.2.1 WEB应用的接口

统一身份认证系统需要为多种WEB服务器提供相应的代理接口. 当用户利用浏览器访问受保护的网络资源时, 首先由代理解释该请求, 检查用户所访问的URLs是否属于不受保护的范围, 如果是, 用户马上获得这些资源. 如果不是, 进行下一步检查, 检测用户是否具有合法的数字身份. 如果数字身份得到认证, 请求就会被传递给认证服务器进行身份验证, 认证通过后, 由该代理将登录用户的身份及相关属性传递给相应的应用.

2.2.2 非WEB应用的接口

对于非WEB应用, 系统必须能提供两种统一认证的方式:

(1) 非Web应用通过自动登录服务实现. 自动登录的服务可以获取当前用户访问某个应用所需要的用户标志和口令, 并且以参数的形式传递给一个签名的控件, 控件将直接调用本地的windows登录程序, 完成自动登录的动作.

(2) 用户数据同步的机制. 例如在一卡通的消费系统的前置机上, 部署相应的数据同步服务, 该服务启动时自动以当前系统的管理员角色登录到统一认证平台, 从统一认证平台自动获得需要同步的用户清单及相关属性, 由前置机自主完成用户身份识别.

3 结语

在数字化校园的建设过程中, 统一身份认证平台的建设是一个最为重要的环节, 目前国内尚无成熟的案例. 希望本文中阐述的方法能够对高校的数字化校园建设起到一定的借鉴作用.

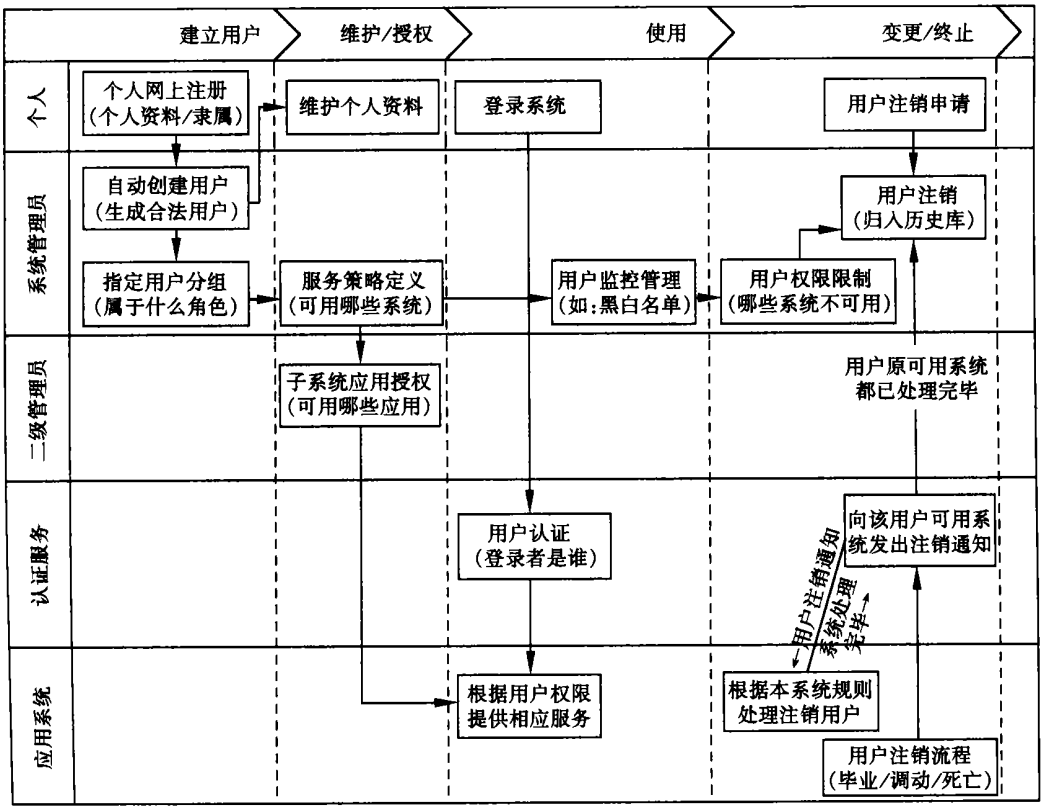

图1　用户管理流程的设计思路

Design of Uniform Identity Authentication Platform

SHEN Bin[1], SHI Mingjie[2]

(1. Information and Network Center, Nanjing Normal University, Nanjing 210097, China;
2. Jiangsu Wiscom Co. Ltd, Nanjing 210008, China)

Abstract: Uniform Identity Authentication Platform is the technique that should be realized first in the course of the realization of E-campus. This paper thoroughly discusses it's function, characteristics and methods of flow design and structural design.

Key words: e-campus, uniform identity authentication platform, directory service, flow, interface

[责任编辑: 严海琳]