中山大学学报（自然科学版）
第40卷 增刊 ACTA SCIENTIARUM NATURALIUM Vol.40 Suppl.
2001年 3月 UNIVERSITATIS SUNYATSENI Mar. 2001

文章编号：0529-6579（2001）S-0130-05

# 校园网应用身份认证系统方案研究*

常晓磊，陈怀楚，王映雪
（清华大学计算机与信息管理中心，北京 100084）

**摘 要：** 描述在校园网络应用中身份认证系统的意义，并探讨一个可行的身份认证系统方案。即由认证服务器、认证接口、安全通道、身份空间和维护平台组成的身份认证系统。

**关键词：** 身份认证；访问控制

**中图分类号：** TP393.18 **文献标识码：** A

随着校园信息化建设的不断深入，校园网络规模不断扩大，网络应用日益丰富，服务范围不断扩大，网络用户的数量和水平大幅提高，网络安全的重要性愈加凸现出来。校园网的安全问题可以分为两个层次，一个是网络整体的安全，另一个是信息的安全。网络整体的安全，主要是防止流量攻击、IP欺骗等影响网络整体运作的破坏行为，本文并不对此展开，我们要讨论的是数据安全层次的问题。

信息安全要求对网络通信的数据加以保护。目前在我们校园网络上最典型的问题是没有统一的身份认证和访问控制机制。校园网中的各应用系统通过各自的一套口令和密码来进行认证和授权。用户访问不同的应用系统时需要提供相应的口令和帐号，为此，用户需要记住多套口令和密码，或在切换到不同的应用系统时重复进行口令验证。因此迫切需要实现全校园网统一的一次认证，即用户只需要输入一次口令和密码就可以访问这些应用。然而实现统一口令认证还只是最为基础的一个要求，更重要的是实现重要应用系统的授权访问控制，即根据用户在校园网络应用中的身份、角色对用户所能使用的操作和数据资源进行权限控制。高校的校园网有自己的特殊性，用户层次和计算机水平比较高，年轻，好奇心强，富于钻研精神、创造性，因此，更有可能威胁网络的安全。实现一个统一的认证系统，针对不同的应用提供不同的安全性，同时构造一个基本的安全框架，为未来的应用提供接口，是建设校园信息高速公路的一个重要环节，也为将来校园网的发展奠定了安全应用的基础。

## 1 身份认证系统的解决方案

校园网应用中的身份认证系统是一个多种技术综合的复杂系统，涉及的技术包括身份认证、访问控制、安全通信、数据库等等重要技术，但在整个系统中如下两方面的技术显得尤为基础与重要，即身份认证技术和访问控制技术。这里我们简要介绍一下。

### 1.1 身份认证技术与访问控制技术

所谓身份认证（authentication），就是判断一个用户是否真是他所声称的身份的处理过

* 收稿日期：2000-11-15；E-mail：ccwyx@mail.tsinghua.edu.cn.

程。最常用的简单身份认证方式是系统通过核对用户输入的用户名和口令，看其是否与系统中存贮的该用户的用户名和口令一致，来判断用户身份是否正确。复杂一些的身份认证方式采用一些复杂的加密算法与协议，需要用户出示更多的信息（如私钥）来证明自己的身份，如 Kerberos 身份认证系统。

身份认证一般与授权控制（authorization）是相互联系的，授权控制是指一旦用户的身份通过认证以后，确定哪些资源该用户可以访问、可以进行何种方式的访问操作等问题。常见的访问控制策略如自主访问控制（Discretionary Access Control，DAC）、强制访问控制（Mandatory Access Control，MAC）和基于角色的访问控制（Role Based Access Control，RBAC）等等。

根据清华大学的实际情况，结合现有的计算机技术，下面我们给出一个校园网应用中身份认证系统的方案。

整个系统包括几大部分（图 1）：认证服务器、认证接口、安全通道（认证协议）、身份空间、维护平台。这种系统中，用户可以两种方式提出认证请求。一种是在客户端通过认证协议直接与认证服务器联系（如图 1 中的安全认证通道 A），或是把这些信息通过一条安全传输通道传输到应用服务器，应用服务器通过认证协议与认证服务器联系（如图 1 中的安全认证通道 B）。

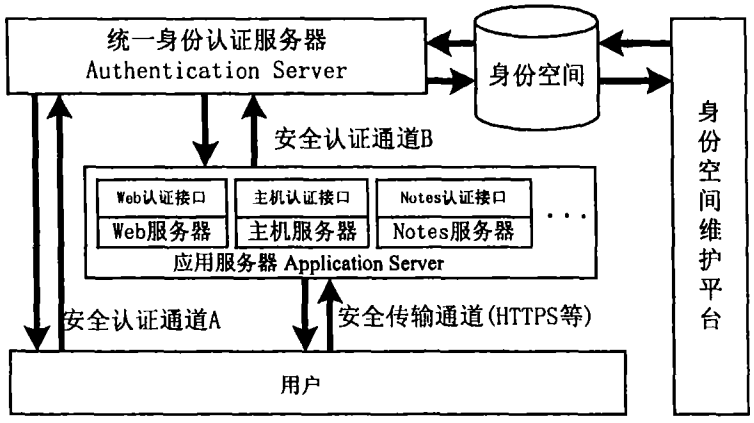


图 1　统一身份认证软件系统结构

### 1.2　认证服务器程序

认证服务器程序的功能是通过安全通道（认证协议），接收认证客户的认证请求，经过与身份空间的数据交换，将认证结果或用户的权限标志返回给认证客户。服务器结构如图 2 描述。

认证系统是各个应用系统的门户，每个用户进入到系统中都需要经过认证这一步骤。因此，认证服务器的性能问题将极大影响各个应用系统的可用性。为了消除认证的性能瓶颈，提高系统的认证响应速度，应考虑如下设计：

（1）采用高性能的服务器，连接到高速网络上，避免网络拥塞。

（2）认证协议采用类似于 RADIUS 协议的方式，通讯数据包使用 UDP 数据包，认证过程的处理采用请求—应答方式，大大简化服务器的处理流程，减少系统资源的消耗，提高

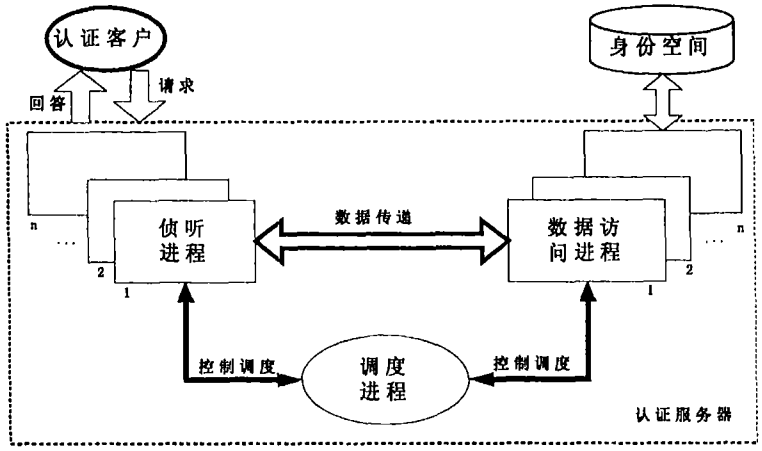


图2 认证服务器结构

系统的响应速度。

(3) 在服务器上对数据库中的用户信息做缓存，并在服务器轻载的时候与数据库进行同步。这样可以减少连接数据库时的资源消耗，能较大幅度提高系统的处理速度。

(4) 采用多服务器并行处理、前端做负载均衡的架构。

### 1.3 安全通道（认证协议）

即认证协议的设计。认证协议是认证客户和认证服务器之间的通信协议，考虑到系统的安全和高效，要求设计的认证算法亦是安全、高效。安全主要有如下三方面的考虑：

(1) 在认证过程中传输的数据不怕被窃听，通过对传输的数据进行加密实现；

(2) 传输中的数据可以防止被篡改，通过对传输的数据进行数字签名实现；

(3) 可以抵抗重放攻击，方法是在认证数据包中打时戳，或在认证过程中使用 Challenge – Response 方法实现。

认证算法采用类似 RADIUS 协议的算法。简单描述如图3。

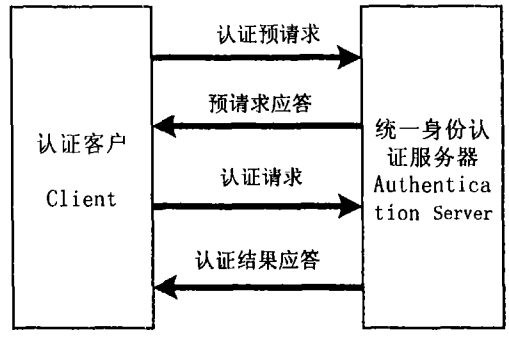


图3 认证算法流程

### 1.4 认证接口

一般来说，现在的应用服务器都有自己的用户认证机制，为了把它们改造成使用统一的身份认证系统，需要使用本系统设计的认证接口模块，以实现与认证服务器通信，完成用户身份认证的功能。由于应用系统多种多样，比如：Web 应用系统、以数据库为核心的

C/S 应用系统、Notes 应用系统、自开发的基于 TCP/IP 的应用系统等等。

在此我们以代表应用开发潮流和方向 Web 应用系统为例，描述认证接口。

实现 Web 应用系统的统一认证的简单结构图 4 所示。

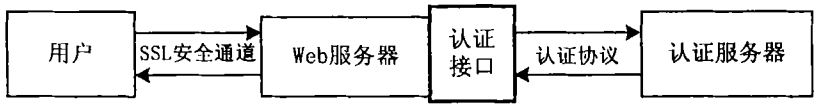


图 4　Web 应用的统一认证方式

用户信息必须经过两次网络上传输，为了保证用户信息的安全，必须保证信息在这两次传输中都安全。

从客户浏览器端传输到 Web 服务器端的信息安全可以使用 SSL 安全传输通道来实现。利用 CA 证书中心，可以很容易在服务器端实现 SSL 传输，保证口令信息的安全。

从 Web 服务器端传输到认证服务器端的信息传输是通过认证协议实现的。可以保证用户的明文口令并不在网络上传输，并可防止假冒，可以保证安全。

位于 Web 服务器的 Web 认证接口模块可以是一个 CGI（或 ISAPI、PHP）的程序，按照认证协议实现，只替换现有的 Web 应用系统自己的用户认证模块即可。

另外，还有 C/S 式数据库应用系统认证接口，Notes 应用系统认证接口，自开发的 TCP/IP 应用系统认证接口等，只需要重新编写用户认证的部分，按照认证协议，利用系统提供的函数调用改写用户认证模块即可。

由于校园网络应用系统多种多样，系统的设计并不能涵盖所有的应用系统。对于未涉及的应用系统，如果也想通过本系统实现统一的身份认证，只需要遵照认证协议与认证服务器通信，即可实现。

### 1.5　身份空间

这一部分是认证系统的核心数据，我们称为身份空间。身份，不仅是指用户身份信息，还包括注册资源信息、应用身份信息、应用访问控制策略等等双向身份认证和授权访问控制的必备信息；空间，而不叫数据库或者其他名称，是因为身份的数字表述可采取很多种方式，而不仅仅是传统的关系数据库，如对象数据库，基于属性名 - 属性值对的注册表文件，或者代表未来应用数据交换格式的 XML。

身份空间共包括用户空间，应用空间，应用接口几个主要部分。

用户空间：包括用户注册的身份信息、个人基本信息、以及其他附加信息等等；

应用空间：包括应用注册的身份信息，该应用的所有合法用户信息，应用功能访问控制信息，应用资源的访问控制信息等等；

应用接口：身份空间不仅包括数据，还应该提供数据操作方法，即用合理的完备指令集合来封装身份空间，实现数据的对外隔离。接口可以提供高级的方法如用户合法性验证，用户个人档案获取，用户访问控制策略获取。或者只提供直接的不加理解的操作，如关系数据库中指定表记录的获取，注册表文件指定路径的键值获取等等，然后由认证服务器进一步的包装后提供给认证客户。

### 1.6　身份空间维护平台

这一部分是用来进行身份空间的维护工作，使用者包括统一身份认证系统管理员，各

个应用系统管理员。包括对用户、应用、访问授权等等信息的维护。比如：新用户新应用的登记注册，应用的访问控制授权等。包括用户信息维护模块，用户信息发布模块，以及应用信息维护和应用信息发布模块等。

通过该身份空间维护平台我们将用户、应用、资源在整个校园网络范围内进行统一的注册、管理、授权。通过预先定义和集中保存访问控制策略，然后根据应用对象选用不同的访问控制策略，减轻了管理负担，加强了资源访问控制的一致性。

网络信息安全体系的建立和完善是一项长期的系统工程，而首要的工作是提供一套身份认证和授权管理的基础设施，然后才是对原有的信息系统进行安全化改造。广大的信息化建设者必须给与足够的重视。

在具体的设计开发工作上，一方面要结合实际，解决校园网的实际问题，满足广大师生的需要，并提供尽可能方便的接口，能够衔接更多的应用系统；另一方面还要注重科研性，探讨各种认证方案并进行比较，设计一种最具有推广价值、安全性又很高的方案，并实现一个功能完善的框架系统。

**参考文献：**

[1] 刘启新，蒋东兴.网络应用统一口令认证系统概要设计.清华大学计算中心，2000(6).
[2] 王映雪.清华大学数字校园建设规划.清华大学计算中心，2000(1).
[3] Orlowski Steve. Electronic Authentication——More Than Just Digital Signatures. Computer Law and Security Report, Vol.16.
[4] JIN Qing-hua, GUO Qing-ping. Authentication in Computer Network. Computer and Communication, Vol.17.
[5] 刘怀宇，李伟琴.浅谈访问控制技术.电子展望与决策，1999(1).
[6] http://www.th-dascom.com.cn

# Research for the Application of Authentication and Authorizaton System in Campus Network

*CHANG Xiao-lei* *, *CHEN Huai-chu*, *WANG Ying-xue*

**Abstract**: This article describes the position and function of authentication and authorization system in campus network, and discusses a practical authentication system's architecture.

**Keywords**: authentication; authorization; access control

* Computer and Information Management Center, Tsinghua University, Beijing 100084, China