基于校园网的考试系统双向身份认证方案设计①

游新娥 (娄底职业技术学院 电子信息工程系 湖南 娄底 417000)

摘　要： 在对基于校园网的无纸化考试系统的体系结构及安全需求进行深入分析的基础上，在服务器端与客户端构造了一种基于用户名/口令和数字签名的增强型双向身份认证方案，既保证了考试系统的安全性又满足了其高效性的要求。

关键词： 考试系统；数字签名；身份认证

Design of Bidirectional Identity Authentication of Examination System Based on Campus Network

YOU Xin-E

(Department of Electronic Information Engineering, Loudi Vocational & Technical College, Loudi 417000, China)

Abstract: In this paper, based on the analysis of the system structure and security demand prescribed in the paperless examination system-based campus network, an advanced bidirectional identity authentication in the client and the server is proposed by using username-password and the digital signature solution. It guarantees the security and efficiency of the examination system.

Keywords: examination system; digital signature; identity authentication

1　引言

学校以教学为主，教学就离不开考核。而在传统的考试中，对学生的考核是以笔试为主：教师命题，教务处制卷，学生作答，老师阅卷、评分，统计成绩，分析成绩。显然这种人工考试方式除了需耗费大量的人力物力资源之外，很多性能都比较差。首先，在考试出题阶段，不同的老师出题或多或少的存在差异。其次，在考生参加考试阶段，为避免泄题，在考试前考试部门必须准备数份不同的考卷，一旦泄题，漏题，原有印制考卷就全部作废，还要全部重新印刷。在考试判阅阶段，由于是人工阅卷常常导致阅卷的不客观性[1]。为了使考试更加科学、合理，将教师从繁重的制卷、阅卷工作中解脱出来，开发一个可对考试科目、各科目题库进行有效的管理，能动态地设置考试要求，能随机抽题、自动阅卷，可方便地查询、打印考生成绩，可对考试成绩进行分析研究，使考试能更好地服务教学的无纸化考试系统是具有现实意义的。

目前几乎所有的高等院校都建设好了校园网，为无纸化考试系统的使用与推广提供了有利的条件。但同时，校园网不可避免地存在安全隐患，信息在传输的过程中有可能被第三方获取，在基于校园网的考试系统中，其被第三方获取方法主要有[2]：

(1) 偷听。在这种情况下，信息仍保持原样，但它的保密性却不能保证了。例如，别人有可能获得考试试卷、答案等机密信息。

(2) 篡改。信息在传送的过程中被改变或替换，然后继续发送给正当的接收者。例如，别人可以篡改考生答卷与考试成绩等信息。

(3) 冒名顶替。信息传给了假冒收件人的一方，一个人可以假装成另外一个人。例如：一个人可以在别人不知道的情况下假借他人的名义操作题库。

为了抵御上述安全威胁，我们采取的安全措施必须解决如下的安全问题：用户身份认证、访问控制与授权、保证数据的完整性[3]。可见，身份认证是安全系统中的第一道关卡，用户在访问安全系统之前，必须经过这一关，考试系统的重要性虽不及电子商务，

① 基金项目:2008 年湖南省教育厅科研项目(08D107)
收稿时间:2009-07-17;收到修改稿时间:2009-09-10

但比一般的因特网网站要重要得多。本文在对基于校园网的无纸化考试系统的体系结构及安全需求进行充分的分析后，利用数字签名技术在客户端与服务器端设计了一种简单、实用、快速、可靠的双向身份认证方案，不须第三方机构参与，也无须添加其他的认证设备，具有较好的安全性与易实现性。

2　考试系统设计

2.1 考试系统的逻辑结构

为保证考试的严肃性，防止学生看书、相互抄袭、请人代考等作弊行为，将学生集中在机房进行考试，而在考试过程中需要频繁的和服务器进行数据交互，为避免数据的拥塞，提高服务器的响应速度，在每一个机房设一个考试服务器，让考试客户端和考试服务器处于一个局域网内工作，既解决了数据拥塞的问题，而且把考试环境这个重要的环节置于在局域网内部，大大提高了考试系统的安全可靠性。图 1 描述了考试系统的逻辑结构。

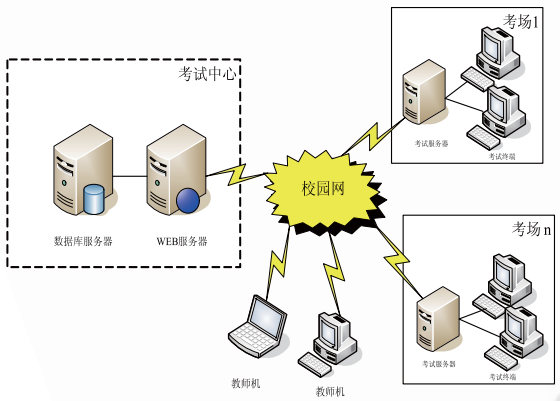

图 1　考试系统逻辑结构图

2.2 考试系统功能模块设计

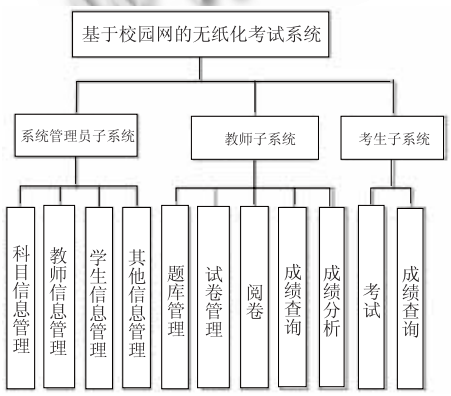

图 2　考试系统功能模块图

通过与多所院校的教学管理人员进行交流、分析、论证后，将考试系统的功能模块设计成如图 2 所示。

此系统的用户有管理员、教师、学生三种。当用户登录时首先选择用户的类型，若是管理员用户或教师用户，则输入用户名与密码，若是考生用户，则输入考号及密码。系统对用户名(或考号)及密码进行检查，只有当二者都正确时才能通过系统的验证进入到指定的导航页面进行相应功能操作。管理员用户的权限主要有科目基本信息管理、教师基本信息管理、考生基本信息管理、及对系部、班级、考试通知等其他信息的管理。教师用户的权限主要有题库管理、制卷、评卷、查询打印成绩、成绩分析等。考生用户权限主要有登陆考试和成绩查询。

3　考试系统的安全性分析

基于校园网的无纸化考试系统采取 B/S 结构，完全实现了客户端的零安装，但所有信息都在校园网中进行传输，给考试系统带来了相关的安全问题，如果这些问题得不到解决，考试这一特殊应用所要求的公正性、客观性将无法保证，考试也就失去了意义。

3.1 考试系统安全需求分析

分析考试系统的安全需求，可概括为如下表所示 6 类安全服务，这些安全服务在基于校园网的网络考试系统中都需要提供[4]。

表 1　网络考试系统一般性安全服务

对等实体认证	客户端和服务器之间相互能够确认合法性
访问控制	不同的用户只能访问不同的页面和数据
数据保密	保证试题信息的秘密性，防止泄密
数据完整性	防止试题、考生答案及成绩被人篡改
信源确认	保证考试的试题来自正确的服务器，考试的答案来自正确的考生
防止否认	防止考生对所做答案的否认，防止教师对所评阅成绩的否认

可用图 3 来描述考试安全系统的逻辑结构。

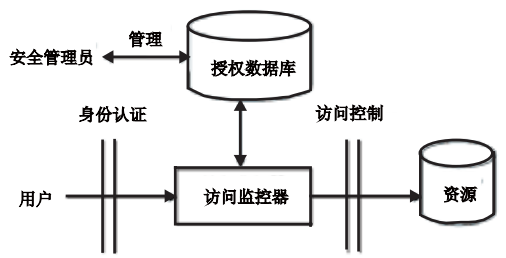

图 3　安全系统的逻辑结构

可见 ，身份认证是安全系统中的第一道关卡，用户在访问安全系统之前，必须经过这一关。考试系统的重要性虽不及电子商务，但比一般的因特网网站要重要得多。故既不宜采用简单的口令认证，也不宜采用设计复杂的认证。

3.2 安全身份认证问题分析

从系统的功能组成来看，考试系统安全身份认证的问题有以下几个方面：

(1) 教师身份认证

教师负责对题库进行更新，负责对学生试卷中的主观题部分进行评阅，故教师与考试中心之间需要进行试题与试卷的提取与提交，并上传考生成绩，因而教师与考试中心服务器之间需进行双向认证。

(2) 考试服务器认证

考试服务器是考试过程中存放试卷、考试资料和考试答案的机器，每次考试前需要从考试中心进行试卷和考试资料的传输，而考试完毕后，也需要往考试中心进行答案的传输。因此需要在考试服务器与考试中心之间进行双向认证。

(3) 考生身份认证

考生在集中的环境中进行考试，为防止出现假冒的行为，一方面由监考员对考生的有效证件(身份证、学生证)进行检查。另一方面通过考试服务器对考生的用户名及密码进行验证。

4 考试系统双向身份认证方案设计

通过前面的分析，考试系统的安全身份认证主要有教师身份认证、考试服务器认证、考生身份认证，本文以教师身份认证为例来进行分析、设计，考试服务器认证类似于教师身份认证，而考生身份认证主要是通过人工验证与口令认证相结合。

4.1 教师用户登录

在无纸化考试系统中教师用户的身份验证至关重要，因为题库的管理、试卷的制作、主观题的评判都是由任课教师通过校园网登录系统来完成的，如果有非法用户冒充教师将会对系统的题库带来毁灭性的破坏，将会使考试失去科学性、公平性，使成绩失去真实性，鉴于基于用户名/口令的身份认证方式的不足，为了确保系统的安全性，本文在用户名/口令认证的基础上使用数字签名方案在教师客户端与考试中心服务器之间进一步地进行双向身份认证。

当考试中心服务器接收到教师用户的登录请求信息时，按照图 4 所示的过程进行身份验证，具体步骤如下：

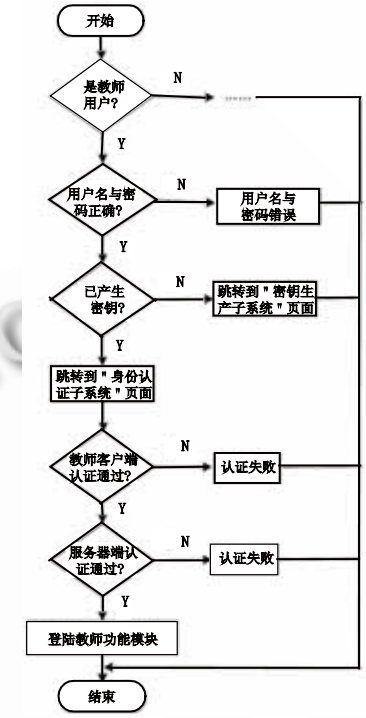

图 4　教师用户身份验证流程图

(1) 判断用户的类型是否为“ 教师 ”，若是则提示“ 教师 ”用户输入用户名与密码；

(2) 查询用户名与密码是否正确,当用户名与密码都正确时，查找该教师用户是否有用于身份认证的密钥对，若没有自动跳转到“ 密钥生产子系统 ”页面，引导用户生成密钥并进行密钥的上传与下载；

(3) 如教师用户已拥有密钥对则跳转到“ 身份认证子系统 ”页面，首先是考试中心服务器对教师客户端进行身份认证，当认证通过时，教师客户端对考试中心服务器进行认证，只有当双方都能确认对方的身份后才能进入教师功能模块对题库及试卷、答卷进行相应的操作。

4.2 双向身份认证方案

4.2.1 方案设计

考虑到在考试系统中安全性与高效性同等重要，根据前面对考试系统的分析，利用数字签名技术，在教师客户端与考试中心服务器之间设计如图 5 所示的双向身份认证方案。

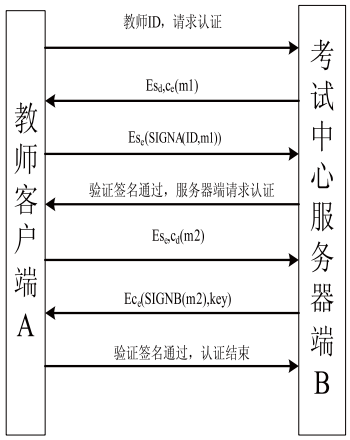

图 5 教师客户端与考试中心服务器端的双向身份认证方案

在图 5 中，S_e,S_d 表示考试中心服务器的公钥和私钥，C_e,C_d 表示教师客户端的公钥和私钥，SIGNA()表示教师客户端的签名，SIGNB()表示考试中心服务器签名。

认证过程说明：

(1) 教师客户端将其 ID 发送给服务器，请求认证；

(2) 考试中心服务器端查表取得教师客户端的公钥，创建一个随机数 m1，使用教师客户端的公钥及考试中心服务器的私钥对 m1 进行加密，将加密的数据发送给教师客户端；

(3) 教师客户端解密，得到 m1,对其 ID 和 m1 进行签名，将签名用考试中心服务器端的公钥进行加密，将加密后的签名发送给考试中心服务器端；

(4) 考试中心服务器端接收到签名后对数字签名进行解密、验证，若验证通过，考试中心服务器端请求教师客户端进行认证；

(5) 教师客户端产生一随机数 m2,利用考试中心服务器端的公钥和教师客户端的私钥对 m2 进行加密，将加密的数据发送给考试中心服务器端；

(6) 考试中心服务器端用私钥对 m2 进行解密，对 m2 进行签名，并产生随机会话密钥，将签名及会话密钥用教师客户端的公钥进行加密，将加密后的数据发送给教师客户端；

(7) 教师客户端解密、验证考试中心服务器的签名，并获得会话密钥，认证结束。考试中心服务器端与教师客户端之间使用会话密钥利用对称加密算法进行试题、试卷的保密传输。

4.2.2 安全性分析

(1) 考试中心服务器端的公钥、私钥都存放在考试中心数据库服务器中，而教师客户端的私钥保存在本地磁盘，公钥保存在考试中心数据库服务器中，在加解密及数字签名过程中，私钥无须在网络上进行传输，非法用户无法截获私钥而伪造签名。

(2) 本方案采取用户名/口令及数字签名进行双重身份认证，如果教师客户端不小心将私钥文件外流，但由于非法获取者不知道教师的 ID 及密码仍然无法登录系统。

(3) 如果非法用户截取了签名，但因为签名进行了加密，而非法用户不知道教师客户端或考试中心服务器端的私钥，从而无法解密而获取签名。

(4) 使用随机数进行数字签名，可以有效地防止重放攻击。

5 双向身份认证方案在考试系统中的应用

为了确保服务器端与客户端安全、高效地实现双向身份认证，在本考试系统中设计了“密钥生产子系统”、“身份认证子系统”两个子系统。

5.1 密钥生产子系统的实现

当“教师”用户登录时，系统检查该教师用户是否拥有密钥，若没有则自动进入“密钥生产子系统”页面，提示用户生产密钥，将私钥下载到本地机器保存，将公钥上传到服务器，并下载服务器的公钥。

“密钥生产子系统”页面如下图 6 所示。

图 6 密钥生产子系统页面

5.2 身份认证子系统的实现

当“教师”用户登录，系统检查到该教师用户已拥有密钥时，自动跳转到“身份认证子系统”页面，实现教师客户端与服务器端的双向认证。

图 7 为“身份认证子系统”页面。

图 7 “ 身份认证子系统 ” 页面

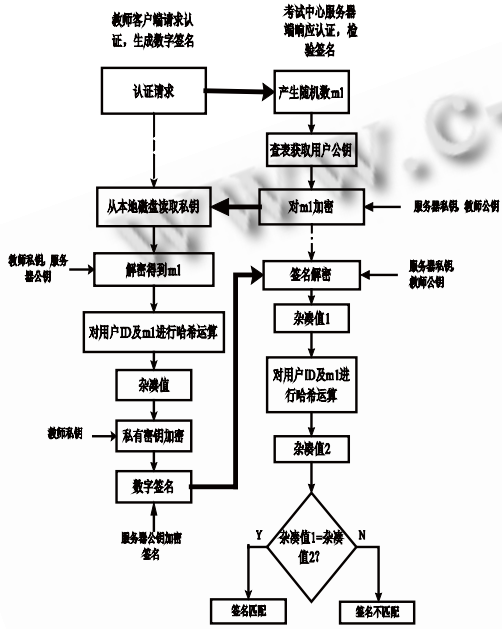

图 8 考试中心服务器认证教师客户端的过程

图 8 说明了通过利用数字签名实现考试中心服务器对教师客户端的认证，而教师客户端对考试中心服务器的认证原理同此。

笔者利用.NET 的安全类设计了所开发的考试系统中的“ 密钥生成子系统 ”与“ 身份认证子系统 ”，并在 C#.NET 平台上进行了实现。

6 结语

本文在考试系统的客户端与服务器端设计了一种简单、实用、快速、可靠的双向身份认证方案。该方案在对用户名和密码进行验证的基础上，通过数字签名来进一步确认用户的身份，不须第三方机构参与，也无须添加其他的认证设备，具有较好的安全性与易实现性，已利用.NET 密码技术在 C#平台上实现了该方案。该双向身份认证方案能方便地移植到其他信息管理系统中，具有很好的应用前景。

参考文献

1 李美满,夏汉铸等.基于 COM 技术的通用考试系统的设计与实现.计算机工程与应用, 2007,43(1):245－248.

2 黎永锋.基于Internet的通用考试系统的身份认证研究与实现 [硕士学位论文].广州:华南理工大学, 2004.

3 先强.基于 WEB 的考试系统安全性研究.计算机安全, 2006,7(1):26－27.

4 朱贵良,宋庆涛,等.基于 Web 模式的网络考试系统安全性研究.计算机工程与应用, 2002,13(8):173－175.