# 在线考试系统的安全性研究

王 琦[1,2]
(1. 南京工程学院 计算机工程系,江苏 南京 211167;
2. 南京大学 计算机系, 江苏 南京 210046)

**摘 要**: 随着教育思想的更新和科学技术的进步,以纸和笔为主要工具的传统考试方式的诸多弊端显露得越来越突出。然而网络考试带来便利的同时也带来了相关的安全问题。为此,提出了一套完整的在线考试系统安全策略,并基于 JSP 平台实现了原型工具 OntoLearner。

**关键词**: 在线考试; 网络安全; 数字签名; 加密
**中图分类号**: TP311 **文献标识码**: A **文章编号**: 1674-7720(2013)04-0001-02

## Approach for the security of online examination system

Wang Qi[1,2]
(1. College of Computer Engineering, Nanjing Institute of Technology, Nanjing 211167, China;
2. College of Computer Science and Technology, Nanjing University, Nanjing 210046, China)

**Abstract**: With the update of the educational ideas and scientific and technological progress, many shortcomings of the traditional test mode using pen and paper as the main tools reveal more and more prominent. However, the convenience of network test also brought related security issues. This paper presents a complete set of online examination system security policy, and implements a prototype tool OntoLearner based on JSP platform.

**Key words**: online examination; network security; digital signature; encryption

目前,基于网络的在线考试系统已经成为现代考试方式的有力补充和发展。相对于传统的笔试,网络在线考试不仅减轻了在组织考试、评卷、成绩统计等方面所花费的人力和物力, 而且突破了时间与空间的限制,节省了资源,提高了评分的客观性、公正性和准确度,大大改善了考试工作的效率[1]。

由于 Web 自身存在的安全性问题,给在线考试的安全和管理带来了潜在的威胁。本文针对基于 Web 环境的在线考试系统进行研究,提出了一套完整的在线考试系统安全设计方案。

针对在线考试系统数据安全性要求较高的特点,在系统中采用了多层次的安全技术来保证考试的安全。

## 1 访问控制

网络考试系统的数据库服务器采用 SQL Server 2005,后台包含了与考试相关的各种数据,包括用户信息、试题信息、组卷方案信息、成绩信息等。除了采用 SQL Server 与 Windows 相结合的方式登录数据库服务器来实现安全性的身份验证方式以外,还根据不同类别用户的功能确定不同的操作对象和操作级别,从源头保证数据操作的安全。通过建立角色,将访问许可集中授予角色, 之后将需要拥有这一许可的用户加到角色中,这些用户即继承角色的访问许可。需要撤销用户的访问许可时,将用户从角色中删除即可[2]。

## 2 数据加密

### 2.1 试题库

试题数据以可读的形式存储在数据库中,高明的入侵者可以采用某种方式进入考试系统窃取或篡改数据。为了防止泄密,试题库需要加密存储。用户编辑输入完试题后,将其加密存储到数据库中,需要更新及查询时,先解密成明文再进行相应操作[3]。

由于非对称加密算法的运行速度比对称加密算法的速度慢很多,当需要加密大量的数据时,建议采用对称加密算法, 以提高加解密速度。本系统采用 3DES(3 Data Encryption Standard)加密, 密钥空间为 $2^{112}$,即用两个密钥对一个分组进行 3 次 DES 加密, 先用第一个密钥加密, 然后用第二个密钥解密, 最后再用第一个密钥加密; 解密时, 首先用第一个密钥解密, 然后用第二个密钥加密, 最后再用第一个密钥解密[4]。

### 2.2 答卷和成绩

学生的答题数据和教师的批改成绩也属于敏感数据,若不加保护则可被轻易的篡改从而无法保证考试的公平与合法。加密后的答卷保存在数据库中,阅卷时教师再解密成明文批阅,批阅后的成绩同样加密保存在数

据库中。加密算法仍选用 3DES。

### 2.3 用户信息

用户的信息档案涉及到个人信息和权限管理，尤其是管理员及教师的资料，这些数据都要加密处理。加密算法也选用 3DES。

## 3 数字签名

在考试系统中采用数字签名技术，主要是为防止恶意篡改考卷及成绩并保证它们的合法性。一是要保证考生的答卷是合法的未经篡改的有效答卷；二是要保证它经过正常的考试过程，考生事后不可否认；三是要保证教师的批改成绩是合法的未经篡改的有效成绩；四是要保证它经过正常的批改过程，教师事后不可否认。

以学生数字签名为例。签名的内容是答卷的信息摘要和考生信息。本系统采用 DSA（Digital Signature Algorithm）。DSA 同样属于公钥密码体系，是 Schnorr 和 ElGamal 签名算法的变种，被美国 NIST（美国国家标准局）作为数字签名标准（Digital Signature Standard）。随机种子和初始化参数的选取非常重要，用户根据自身的要求，选择随机种子和初始化参数，可以增加算法的安全性[5]。

## 4 通信的安全性

为保证试卷等数据在传输过程中的安全，确保私有性和保密性，不会被可能使用网络监控软件的窃听者查看到，系统采用 SSL（Security Socket Layer）加密传输[6]。

SSL 是一个用来保证文件安全传输的协议，可以在服务器和客户机之间建立一条安全通道，从而实现在 Internet 中传输保密数据。在 TCP 协议族中，SSL 位于 TCP 层之上、应用层之下。这使它可以独立于应用层，从而使应用层协议（诸如 http）可以直接建立在 SSL 上。SSL 协议由 SSL 记录协议（SSL Record Protocol）和 SSL 握手协议（SSL Handshake Protocol）两部分组成：SSL 记录协议建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持；SSL 握手协议建立在 SSL 记录协议之上，用于在实际的数据传输开始前通信双方进行身份认证（协商加密算法、交换加密密钥等）。

SSL 能实现数据的安全保密传输是指通过 SSL 传输的数据经过服务器与客户机的公开密钥密码体制加密而且密钥是在传输开始时经协商随机产生的。这样即使在传输过程中数据被非法窃取，第三方没有解密密钥也无法获得传输的原始数据或篡改原始数据。

## 5 数据备份策略

定期进行数据备份是减少数据损失的有效手段，能让数据库在遭到破坏（恶意或者误操作）后，及时恢复数据资源。

## 6 其他安全

(1) 屏蔽操作

在学生考试过程中，必须保证一定的操作安全性。有些操作可能是误操作，有些可能是恶意的。学生的考试用机可能存储与考试相关的资料，需要对一些快捷键、鼠标键、菜单命令和 USB 接口进行屏蔽，避免学生获取试题资料。同时，考试系统页面在刷新时会重新生成新的试题，在实现时要加以避免，以免学生通过此方法多次生成试卷。

(2) 二次登陆

在考试中，可能某些考生因成绩不理想而擅自再次登录考试系统、再次做答，系统要记录考生的考试状态，杜绝考生二次登陆。同时系统应定期提取学生的答题情况并存放到服务器的数据库中，以便在死机、误操作、网络故障等原因造成考试意外中断时恢复到之前的状态。

(3) 防火墙技术

防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，有选择地接受外部访问，对内部强化设备监管，控制对服务器与外部网络的访问，在被保护网络和外部网络之间架起一道屏障，以防止发生不可预测的、潜在的破坏性侵入。

本系统采用包过滤技术，限定考试机允许进行的网络访问，并且对考试机的 IP 地址进行限制，使得只有规定范围内的机器才可以进行考试。

由于网络本身的原因，给在线考试的安全和管理带来了潜在的威胁。本文针对在线考试系统数据安全性要求较高的特点，在系统中采用了多层次的安全技术，提出了一套完整的安全策略，并以案例验证了策略方法的可行性和有效性。

## 参考文献

[1] 王海燕.关于网络考试的安全性研究[J].赤峰学院学报（自然科学版），2008,24(1):98-100.

[2] 孙占锋.基于 ASP.NET 的网络考考试系统的用户权限设计与实现[J].电脑知识与技术，2007(11):794-795,797.

[3] 李美满.网络考试系统题库与成绩安全性研究[J].计算机应用，2005,25(S1):133-134,137.

[4] 汪莹. 基于 3DES 加密算法的高校公共课程网络考试系统题库安全性研究[J].网络安全技术与应用,2009(7):78-79.

[5] 颜晶晶，康振华. DSA 数字签名技术及其在 JAVA 中的实现[J].中国现代教育装备，2006(6):72-74.

[6] 张峰岭. 基于 Java2 的身份认证数字签名和 SSL 实现技术[J].现代计算机，2002(4):27-31.

（收稿日期：2012-11-30）

作者简介：

王琦，女，1980 年生，硕士，主要研究方向：网络安全、信息检索及语义 Web 技术。