基于城域网的考试系统中系统安全策略研究

王世伦
(四川师范大学信息技术学院　成都 610068)

摘　要　本文通过对目前网络智能考试系统在安全方面存在问题的研究，综合 VPN 技术、网络访问控制技术、数据加密技术、动态链接库技术等，提出了一套实用的系统安全解决策略。对于开发安全性要求高的 B/S 体系的应用来说，该策略有一定的参考价值和借鉴意义。

关键词　城域网，考试系统，发布，策略

Research on System Secure Policy in Intelligent Exam System Based on Network

WANG Shi-Lun
(College of Information Technology, Sichuan Normal University, Chengdu 610068)

Abstract　This paper focuses on the system secure issues in intelligent exam system over computer network through analysis of the major security threat currently, integrates the advantages of VPN, distance access control methods, data encryption, DLL, etc, and gives a suit of applied solution for system security. It will be referable and valuable for developing some application based B/S system which demands strong security.

Keywords　Exam-system, Security, Policy

1　引言

传统的人工考试组织形式，从考试的准备、组织到实施将耗费大量的人力、物力。采用基于局域网的考试系统，虽然较传统的考试有了很大的进步，但是在考试组织上，需要各个考点的老师先安装考试软件，考试后又需要将结果交给考试组织者判卷，再由考试组织者将成绩返回各个考点，这样就增加了考试的成本。由四川省教育厅和四川师范大学信息技术学院牵头设计实施的城域网考试系统就是为了在城域网中进行计算机类专业考试，并以此为基础推广到其它的考试。学生的考试将在城域网内完成，考试之前各个考点不需要安装任何软件，考试结果直接提交给城域网的服务器，学生可以通过网络，快速知道考试结果。考试组织者也可以迅速得到考试的统计信息。采用城域网考试系统，不仅能准确、客观、公正地反映广大考生对计算机信息技术掌握的程度，而且能最大程度地减轻考试的组织者和管理者的工作量，并节省大量的人力、物力和财力，同时能取得良好的社会效益和经济效益。

城域网考试系统采用浏览器/服务器(Browser/Server, B/S)体系。在 B/S 的系统中，用户可以通过浏览器向分布在网络上的许多服务器发出请求。B/S 结构极大地简化了客户机的工作，客户机上只需安装、配置少量的客户端软件即可。服务器将担负更多的工作，对数据库的访问和应用程序的执行将在服务器上完成。B/S 体系的优点是：系统安装维护简便；数据集中管理；便于分散用户使用，适应互连时代软件的发展趋势。

由于考试要求保密，实现公正、公平，因此城域网考试系统的安全问题成为首要考虑的问题，例如，服务器端如何安全地把考试数据传给客户端，客户端在完成考试后如何把敏感数据安全传回给服务器，如何避免非法用户入侵等。总之，安全系统的设计实施是城域网考试系统的一个关键问题，也是难点所在。

2　系统安全问题概述

在进行系统安全设计时，必须考虑到最恶劣的情况。虽然不可能设计出绝对安全的系统，但系统安全必须避免大灾难以及一般灾难最小化。近年来，加密技术及其应用都得到了极大的发，但安全系统的设计依然是一项棘手的工作。城域网考试系统可能遇到的安全问题包括[1,2]：

(1)关键数据没有被保护。如果不采取任何加密措施即在网络上实施考试，则试题信息、考生的答题信息、系统控制指令等关键数据将直接暴露在整个城域网上，这显然对于考试系统这样的应用来讲是不可思议的。因为这不仅容易造成敏感数据的泄密，还可能让服务器这样的关键设备受到恶意攻击，从而影响考试进程的顺利进行。

(2)密钥管理不安全。常见的问题有：对密钥的使用范围和生存时间不做限制；密钥本身的安全性不够，如密钥构成太简单、密钥长度不够等；密钥的发放途径、措施不安全等。

(3)数据加密算法强度不够所引起的安全问题。在网络考试系统中，考虑到数据实时性的要求，也为了简化配置，很多系统采用自己设计的数据加解密算法，而这些算法一般都没有经过比较严格的安全强度论证。如果数据加密算法强度不够，在有效的考试期间关键数据被破解，也会造成严重后果。

(4)算法或核心程序代码可能被攻击者得到。通过研究我们发现，目前应用的部分网络考试系统，包括一些专门从事网络考试服务的知名公司的系统都直接将数据加密算法或者部分核心的程序代码写在网页文件或其它脚本文件中，这让攻击者可以轻易地获得这些关键代码，当然系统的安全就会

王世伦　副教授，硕士生导师，主要研究方向为计算机网络与数据库。

受到严重威胁。

3 安全系统设计目标

系统设计的使用环境是城域网，其特点是覆盖范围广、用户数量大、网络带宽变化范围大、网络的接入方式复杂等。为了能够在这样的环境下进行大规模的实时考试，必须正确解决如下几个问题：

(1)实时数据交换。从考生试卷的生成(组卷)、试卷加密、答案加密、数据传输、数据解密、答案(包括部分答题过程)上传、考试控制指令的加解密及传送等过程都要求有较好的实时性。考虑到各考点的接入带宽差别较大，所以需要进行传送的数据量应该尽可能地小。

(2)用户访问控制。考虑到城域网环境中用户的复杂性，考试系统应该具备很好的用户访问控制略，最大限度避免用户非法访问和欺骗攻击。本系统在这方面主要采用用户分级访问权限控制来避免用户非法访问；采用用户认证时地址确认机制来降低恶意的欺骗攻击行为。

(3)安全数据传输。城域网环境下站点分布范围广、用户数量大、网络接入方式多样，成分复杂。为了考试能够顺利、可靠进行，必须能够避免数据截获、篡改、重放等攻击方式。本系统有在网络中传送的数据都经过了高强度的安全加密，系统对不符合验证要求的数据直接丢弃。

(4)客户端安全复位能力。这主要包括两个方面的功能：一是考生在答题过程中如遇计算机死机、网络故障、考生误操作等强行退出系统后，系统应该具备保存考生当前状态并能够最大限度自动恢复的能力；二是指某轮考试结束后，客户端应该具备自动安全清空考生答题内容，避免影响下一轮考试的能力。

(5)系统健壮性。为了实现系统安全、可靠、稳定地运行，并能够支持更多的考点以及考生数可以同时在线考试，本系统采用可切换的三层工作模式或二层工作模式。三层工作模式下，系统能够支持更大规模的在线网络考试，系统由中心服务器(L1-Server：负责全局的控制和处理，包括题库管理、组卷、评分、考试结果汇总、分析统计等功能)、考点服务器(L2-Server：由中心服务器控制，负责本考点考题临时存储、考试结果上传、考试监控等功能)、考生客户机(Client：考生通过客户机登录、下载试题、答题等)构成。二层工作模式下，系统由中心服务器与考生客户机两极构成，具有更快的响应速度和控制能力，同时减轻了考点的维护需求。

(6)其它安全策略。客户机使用浏览器与服务器建立联系，不用安装其它第三方软件和试题。除了大大降低考点的维护需求外，也从根本上杜绝了考生在考试过程中窃取考题的可能性；中心服务器和考点服务器上的题库、试卷都是经过加密处理的，它们在客户端由系统自动实时解密，既降低了试题泄密的风险，对操作人员及考生来讲又是透明的。

4 安全系统设计策略

为了保证系统的安全性，系统实施过程中，采用了多种策略：

(1)采用 VPN(virtual Private Network)，保证在专网内的用户才可以考试。VPN 是一种利用公共网络来构建的私人专用网络技术。VPN 系统一般采用建立在网络协议堆栈上的应用层 VPN 技术，在系统的 TDI 层和协议堆栈之间增加安全扩展模块，实现密钥管理、协商、数据加密/解密的过滤驱动程序[3]。通过这种安全扩展方式，不必修改上层的应用程序，所有要通过网络收发的数据包都必须经过该安全驱动程序的过滤。VPN 系统全部采用 CA 认证体制(采用非对称密钥证书体系)，即在企业信息中心 VPN 控制平台建立全省统一的认证授权系统，所有企业客户端都有自己的私有证书、用户名及密码，使接入用户与 VPN 虚拟专网、VPN 网关进行双向身份鉴别，同时客户端支持双因素身份认证。每次用户登录都将有严格的审计日志记录，以便于日后的审计与稽核，同时 VPN 系统增加了用户操作的数字签名，即数据交易的不可抵赖性，其强制认证措施确保了企业内网服务的访问与稽核安全。高强度的数据保密由于数据全部通过互联网进行传输，因此必须进行数据加密与数据完整性保护。VPN 虚拟专网一般提供 128 位以上的对称加密措施，非对称密码算法使用 1024 位，并采用网络协议堆栈上的应用层 VPN 技术，全部采用一次一密体制，数据安全性极高。同时，VPN 虚拟专网采用 MD5 数据摘要算法，用以保护数据传输过程的完整性。VPN 技术虽然构建在 Internet 上，但其高强度的加密措施使得数据传输的安全性大大提高，能够保证外部用户无法窃取数据。

(2)服务器端系统对 IP 地址进行限制，保证只有规定考场客户机在允许的时间才能考试，并阻断所有不用的端口。

(3)服务器端系统在考试即将开始前才生成数据加密密钥。密钥本身也被加密，在传输给客户端后，客户端系统采用专用算法解密并使用，在实际使用时，密钥无法被跟踪。

(4)将关键代码写成 DLL 组件，并采用序号导出的方式，使破解者即使获取到了 DLL，也无法看到有用信息，最大限度保护了加解密算法和其它核心代码的安全。

(5)对关键数据进行二次加密，先用专用加密算法加密，再用 DES 或者 AES(高级加密标准)加密技术进行加密。即便能够获得关键数据，也无法在有效的时间内将其解密。

(6)程序代码和设计方案有专人负责，并签订保密协议，杜绝程序代码和设计的人为泄露。

结束语 网络考试方式在今天已经得到了大量的使用和关注，它具有公正性、方便性、科学性以及易于推广等特性得到了很大程度上的认同。但大量的网络考试系统还停留在局域网阶段，使系统的使用范围受到了很大的限制。另一个方面，开发基于城域网的网络在线考试系统所面临的问题要复杂许多，其中城域网环境下的系统安全问题就是一个核心问题。本文所讨论的考试系统已经投入应用并取得了很好的效果。文中提出了在设计城域网考试系统时在系统安全方面所必须考虑的问题，并给出了一套具体的解决策略，对于开发安全性要求高的 B/S 体系的应用来说，有一定的参考价值和借鉴意义。

参 考 文 献

1 NCNE 考试系统介绍 . http://www.cer.net/article/20040524/3106375.shtml

2 eTesting 网络考试系统简介 . http://www.dotraining.com/dot/netexam.jsp

3 冉先进 . 信息网络安全问题及对策 . 网络安全技术与应用，2004(8)