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-0135-04

一种网上选课系统的安全规划*

徐建勇
（中山大学网络与教育技术中心，广州 510275）

摘 要： 介绍了一种可行的网上选课系统的规划、流程以及所采取的安全技术。

关键词： 网上选课；数据加密；RSA；SSL

中图分类号： TP399 **文献标识码：** A

在互联网应用高速发展的今天，网上选课成为减轻学校教务员负担，方便学生选课，提高选课透明度的必然发展趋势。本文论述了一种目前在大、中院校切实可行的网上选课系统的模式。

1 教务数据库的规划及网上选课服务器平台的选择

1.1 利用原有教务系统数据库中的数据，改造原有教务数据库

如今大多数院校都早已有各自的用以记录学生名册、考试成绩、学校各院系专业等数据的教务数据库。但要进行网上选课，还必须有一个能在网上进行查询的较为稳定的数据库。例如 Oracle、Sybase、Microsoft SQL Server 等大型数据库服务器。而作为中型数据库软件，免费的 Mysql Server 则是一种不错的选择。其他如 FoxBase、SQL Anywhere、Microsoft Access 数据库等则由于稳定性不够，不予考虑。

原教务系统可提供的数据表有 学生名册表、教职工名册表、系所表、专业表、考试成绩表、课程编码表等。

1.2 用于网上选课须创建的表及登录选课系统操作流程

（1）学生密码表（表 1）

保证学生选课记录的可靠性，学生必须输入帐号密码进入选课系统（在这里以学号为帐号），没有帐号的人不能选课。学生在登录界面输入帐号密码后，帐号密码被送到服务器验证，若密码错误，则锁定次数减 1，同时记录登录时间，当锁定次数 < =0 时，把当前时间与登录时间对比，若小于一定的时间（比如半小时）时，无论输入任何密码均不能进入选课系统，即把此帐号锁定半小时。当半小时过后，若输入正确帐号密码，则进入选课系统，并显示密码输错次数，上次成功登录的 IP，以及上次登录的时间，以备察看。当用户成功登录时，除了显示上次的各种登录信息外，还记录当前登录的 IP、登录时间，并分配一随机序号。此随机序号与登录 IP、登录时间一起，用作选课操作的身份识别。因此，一次成功的登录，用户的帐号密码只在网上传输一次，这样可以减低因密码多次传送带来的密码泄露风险。

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

表1 学生密码表结构

字段名	学号	加密密码	随机序号	登录时间	登录IP	提示问题	答案	锁定次数
字段类型	CHAR 8	CHAR 10	Long INT	Datetime	Varchar 20	Varchar 40	Varchar 20	INT

(2) 教师密码表（表2）

教师密码表使教师有权登录选课系统，查看有哪些学生选修他所负责的课程，以及这些学生的资料。

表2 教师密码表结构

字段名	职工号	加密密码	随机序号	登录时间	登录IP	提示问题	答案	锁定次数
字段类型	CHAR 8	CHAR 10	Long INT	Datetime	Varchar 20	Varchar 40	Varchar 20	INT

(3) 公选课表

让学生查询公选课介绍、教师简介、上课时间、地点、考试时间、选课要求等资料。

(4) 选课记录表（表3）

学生选课的记录，作为学生可上某门公选课及参加考试的凭据。

表3 选课记录表结构

字段	学号	课程代码	报名日期	考试成绩	备注	状态
字段类型	CHAR 8	CHAR 14	Datetime	Varchar 6	Varchar 40	CHAR 1

(5) 某课程可选条件表（如年级限制表、专业限制表等）

规范学生选课行为，使学生选课成功率提高。

(6) 预选记录表（结构与选课记录表相同）

当前学期，学生预选课程记录，超过可选人数的课程由这些记录中随机筛选学生，没选中的学生可进入再选阶段。学生选课分四个阶段：浏览可选课程、预选、再选、教务处分派。

1.3 选课服务器平台的选择

以服务器的操作系统而论，Windows NT平台（包括Winnt Server 4.0和Windows 2000 Server）无论稳定性、运行效率和可达到的安全级别都比不上Unix系统和BSD系统。其中以BSD系统的稳定性和效率最高，所以有技术力量的院校应以BSD或Unix系统为首选。而Windows NT平台因为操作、维护简单，进行网页制作开发较简便，因而普遍受到大众院校的欢迎。

若选用BSD或Unix作为操作系统，则应选用PHP或JSP作为服务器端脚本语言。ASP在NT上运行得不错，但不能直接在Unix上运行，即使安装了Chili! soft ASP或者Halcyon公司的iASP［tm］也不能完全避免不兼容情况的产生。据闻，在同一机型上分别用PHP、JSP、ASP语言编写功能相同的Web数据库查询程序，在Unix系统上运行JSP程序的效率比其他操作系统、语言搭配高几十倍。因此，使用FreeBSD操作系统、JSP语言为Web服务器端脚本语言来开发Web网页，是今后网页编程的发展潮流。

若选用Windows NT + ASP作为服务器平台则需要对磁盘目录权限和IIS虚拟目录权限

作仔细地设置，并及时给平台打补丁（NT4.0装 ServicePack 5 或 ServicePack 6，但 ServicePack 6 安装后仍要补新出的漏洞；Windows 2000 要装 ServicePack 1 再补上输入法的补丁）。

2 网上选课相关阶段

学生根据帐号登录系统选课、改选、退选；教师根据帐号进入系统开课、查看选课情况、录入考试成绩。整个选课过程，学生都可随时查询课程信息与选课情况。

2.1 教师开课，教务处审批

进入学期下半段后，由教务处开放公选课录入系统。教师根据帐号登录选课系统，录入他想开的课程，然后等教务处在网上审批（如觉得不保险，可由教师提出书面申请，教务处审批后代为录入课程信息）。经教务处审核符合开课条件的课程，一经上网公布由学生选课，任何人不得随意更改。要销课，必须报系主任和教务处批准。

2.2 学生选课

（1）学生浏览学校公布的公选课课程的详细信息（上课时间、选课要求、考试时间等，需一至两周）。

（2）学生预选，大约须一周。学生上网选课，一周后暂停选课，任课教师和教务处根据选课情况调整某些课程的接受人数，对人数超出范围的课程，由系统自动随机筛选学生。

（3）选不上的学生再选，大约须一周（重复（2）的步骤），已选上的学生一般不予改选。

（4）教务处进行选课后整理。对于选不上的学生和临近毕业但不够学分的学生，教务处酌情分派其上某门公选课。对于不足最低选课人数的课程予以撤消。最后，公布选课学生名单。

2.3 考试结束后，教师录入学生成绩

3 选课系统创建过程中须注意的安全措施

3.1 浏览器端与 Web 服务器端通信的安全保证

如今网上的信息大多数是通过 TCP/IP 协议以明文的形式传送的，因此，未经加密而传送的信息毫无秘密可言。特别是对于仍在使用共享式的集线器 Hub，而不是使用全交换网路的用户来说，数据加密传输特别是帐号密码的加密传输的必不可少的。目前世界上最广泛使用在电子商务上的两种加密算法是数据加密标准 DES（Data Encryption Standard）和公开密钥算法 RSA。DES 算法无论加解密速度和保密强度都比 RSA 算法要高，但存在密钥传送难的问题。而 RSA 算法研制的最初理念与目标是旨在解决 DES 算法秘密密钥的利用公开信道传输分发的难题。而实际结果不但很好地解决了这个难题；还可利用 RSA 来完成对电文的数字签名以抗对电文的否认与抵赖；同时还可以利用数字签名较容易地发现攻击者对电文的非法篡改，以保护数据信息的完整性。因此，一般性的网上商务活动如 B2C 的数据传输大多采用 RSA 加密算法。而且，由于美国政府已解除对加密技术出口的限制，RSA 也对外公开其加密技术，今后 RSA 在网上商务特别是用户身份认证的应用上必将更加成熟、可靠。

在选课系统的服务器端，我们可以设置使用 SSL 协议的虚拟目录（SSL 协议也使用 RSA 算法），用 Https://xxx 的格式浏览需要加密传送信息的网页，使浏览器端到服务器端相互之

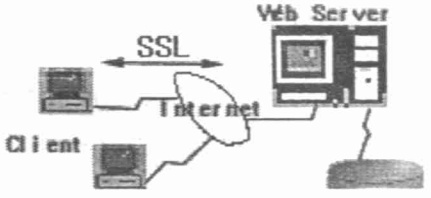
间的数据得以加密传送。Winnt Server 4.0 + IIS4.0 或 windows2000 Server 可进行这样的设置。

3.2 保护好 Web 服务器，严格设置可存取数据库服务器的帐号的权限

由于从 Web 服务器可以对数据库服务器中的表进行存取，所以一定要设置好 Web 各级目录的权限，修复 Web 服务器存在的 bug，以免被人攻破，进而获取数据库帐号，修改数据库记录。另外，用来增添选课记录、修改登录信息、察看课程信息的数据库帐号的权限必须严格设置，除了拥有对有限几个必须存取的表有读或写的权限外，其余权限一律取消。这样即使 Web 服务器被黑客攻破，其对数据库所能造成的危害也比较有限。

3.3 把数据库服务器与外界隔绝，并保证数据有经常备份

要保护好数据库服务器，最简单的方法就是把数据库服务器从物理上与外界隔绝开，只留下与 Web 服务器的连接。可以在 Web 服务器上安装双网卡，把其中一个网卡与数据库服务器直接连接，数据库服务器的 IP 设为内部 IP（如 192.168.*.*）。如果确实需要数据库服务器与网上别的计算机互联，则最好在数据库服务器上安装防火墙。



经常备份数据是一种良好的习惯，它能使你在数据库服务器受攻击或受损的情况下，损失减到最低。

3.4 用户密码的加密存储

数据库加密一般需要实行二级密钥管理。一级密钥为主密钥，二级密钥为工作密钥。主密钥的作用是对二级密钥信息加密生成工作密钥。工作密钥用于对数据库数据的加/解密。在这里，需要保护的敏感数据只有一列，可以直接以学号作为二级密钥信息。

理论上讲，实现了“一次一密”密钥管理的密码是不可破译的，因此如何确保密钥管理系统的安全成为关键问题。本系统中，主密钥保护了工作密钥，工作密钥保护敏感信息，因而整个系统的安全依赖于主密钥的安全。本系统采用 DES 算法，以投币法产生 64 位二进制的主密钥。主密钥经加密并存放于安全区域内，使用时由系统自动获取并解密。

参考文献：

[1] 段素娟，王文钦等编.北京希望电脑公司公司.
[2] 方美琪主编.电子商务概论.清华大学出版社.
[3] http://www.isbase.com/
[4] http://www.drcnet.com.cn/ceb/index.html
[5] http://bj.netfront.com.cn/
[6] Microsoft IIS 4.0 文档

Security Design for Network Elective System

XU Jian-yong *

Abstract: In this paper we deal with some security techniques applied to network elective system and the construction of an elective database.

Keywords: network elective system; data encrypt; RSA; SSL

* Network and Education Technology Center, Zhongshan University, Guangzhou 510275, China