文章编号:1001 - 9081(2006)05 - 1198 - 04

基于 Web 的教务管理系统安全方案设计

孙飞显[1],徐明洁[2],杨 进[1],王铁方[1],刘孙俊[1]
(1. 四川大学 计算机学院,四川 成都 610065; 2. 河南教育学院 教务处,河南 郑州 450014)
(sjysfx781@126.com)

摘 要:分析了传统教务管理系统存在的安全问题,提出了基于 Web 的教务管理系统安全设计方案。从网络边界安全、身份鉴别与访问控制、入侵检测、数据加密、服务器安全、灾难备份与恢复等方面对系统进行全方位保护,并给出了整体设计架构。该方案能阻止非法用户的入侵,防止合法用户越权访问;同时,基于身份的加密方案确保数据在使用、存储、传输和处理过程中的机密性、可用性、完整性和不可抵赖性,克服了 PKI 机制公钥管理困难、成本高、效率低等不足。理论分析和实验结果表明,该方法是保证高校教务管理系统安全运行的一种有效解决方案。

关键词:网络安全;PKI/PMI;基于身份加密;教务管理系统
中图分类号: TP393.08 **文献标识码**:A

Design of security solution for Web-based educational administration system

SUN Fei-xian[1], XU Ming-jie[2], YANG Jin[1], WANG Tie-fang[1], LIU Sun-jun[1]
(1. *School of Computer Science, Sichuan University, Chengdu Sichuan* 610065, *China;*
2. *Educational Affairs Office, Henan Institute of Education, Zhengzhou Henan* 450014, *China*)

Abstract: The security problems of traditional educational administration systems(TEAS) were analyzed. In order to improve their security, a novel integrated solution was proposed. In which, network border protection, user identification and access control, intrusion detection, servers' security, and disaster recovery were presented or strengthened. So the invalid users can be held back, and the exceeding access of valid users can be prevented. At the same time, the new method of Identity-Based Encryption(IBE) can ensure the confidentiality, integrality, usability and the undeniable-ness of the data during the processes of storage, transmission, processing, and so on. As a result, the shortages of PKI, such as the difficulty in managing the public keys, high costs, and low performance can be overcome. Theoretical analysis and the experimental results show that it provides a good security solution to the field of MIS.

Key words: network security; PKI/PMI; Identity-Based Encryption (IBE); educational administration system

0 引言

随着高校师生的不断增多以及学分制教务改革的逐步实施,基于 Web 的教务管理系统在学生学籍和成绩管理、网上选课、自动排课、教室安排、教师工作量统计、教材及学费清算等管理工作中的重要作用愈加明显。学生足不出户即可浏览考试成绩、教室安排、选课等信息;教师坐在家中就能上报考试结果;教务人员轻松点击鼠标便可实现宏观管理……。然而,随着网络应用的不断深入,入侵软件、黑客工具随处可见,网站被攻击、网页被篡改、机密被泄漏等恶性事件不断出现,计算机网络与信息安全问题[1,2]日益突出,现有的教务管理系统在安全保障方面的不足也逐渐暴露出来,主要表现有:

1) 缺乏严格的身份认证机制:仅凭户名的口令登录,无法核实学生、教师和教务管理等人员的真实身份,不得不对成绩单等重要数据采取亲笔签名或现场确认等措施,严重影响工作效率;

2) Web 服务器缺乏对页面的鉴别能力,不能区分页面内容是否被篡改;

3) 用户登录信息及学生学籍、成绩等数据在存储、处理、传输等过程中没有经过加密处理,信息容易泄漏;

4) 缺乏用户级别、用户角色划分,或划分不够周密、严格,容易导致越权访问、控制失效等;

5) 缺乏主动的网络安全防御机制:防火墙仅能在一个点上被动防御;

6) 缺乏容灾能力,一旦发生恐怖袭击、火灾等突发事件,系统被毁、关键数据丢失。

文献[3]提出了一种用 PKI 技术解决上述问题的方法,在一定程度上解决了密码传递不可靠、弱口令、密码泄漏和身份验证等问题,但遗憾的是 PKI 技术实现复杂、使用和维护成本高,一般高校难以承受;再说,PKI 技术本身也存在不足之处[4,5]:初次发布证书时,难以验证远程用户的真实身份;冗长难记的私钥保存在用户的计算机中,缺乏安全性;基于 CRL 的证书状态定期发布机制难以确保数字证书的有效性;身份验证过程计算量大,效率低,尤其是交叉认证始终是 PKI 的瓶颈问题。同时,给以信息浏览为主要目的每个学生颁发数字证书,不现实也没有必要。

收稿日期:2005 - 12 - 07 **基金项目**:河南省科技厅科技攻关项目(0424220060);河南省教育厅自然科学基金项目(2003520289)
作者简介:孙飞显(1970 -),男,河南宝丰人,博士研究生,主要研究方向:网络安全、人工免疫; 徐明洁(1968 -),女,硕士,河南新乡人,主要研究方向:计算机网络; 杨进(1980 -),男,四川乐山人,博士研究生,主要研究方向:网络安全、人工免疫; 王铁方(1971 -),男,河北承德人,博士研究生,主要研究方向:网络安全、人工免疫; 刘孙俊(1975 -),男,四川成都人,博士研究生,主要研究方向:网络安全、人工免疫.

本文依据动态网络安全体系结构模型 PPDR 和 PDRR[2],采用基于身份的加密方案[6~9](Identity-Based Encryption, IBE),给出了一种基于 Web 的教务管理系统的安全设计方案(Web-Based Security Educational Administration System,WBSEAS),进行了实验,并与传统的 PKI 安全解决方案进行了对比分析。

1　系统安全

基于 Web 的教务管理系统依托于校园网,其安全性包括校园网的安全和系统自身设计结构的合理性两个方面。前者的实现应包含网络的风险评估、安全策略、保护措施、检测方法、响应机制、备份与灾难恢复等;后者的实现细节参见本文 3.1 节。

1.1　风险评估

依据黑客攻击手段的日益复杂和通用系统不断发现安全漏洞的实际,预先评估和分析网络系统中存在的安全问题就显得十分必要。

传统的网络安全风险评估主要是通过网络扫描技术,通过探测存活设备端口的开放情况和操作系统的版本信息,评估系统的安全隐患,但该方法难以穿透大多数防火墙,评估结果欠准确。针对传统网络风险评估方法不足以及规避 IDS 检测的网络攻击技术,WBSEAS 利用逆向穿透等技术,通过构造模拟攻击的方法,对网络中服务器、路由器、防火墙、交换机等设备的薄弱环节进行评析,并针对存在的安全隐患和它们的危险级别,提供安全建议和改进措施,提醒网络安全管理员及早修补漏洞,最大可能地消除潜在的安全隐患,防范恶意攻击者利用这些安全漏洞入侵系统,提高整个网络的安全性。

1.2　安全策略

安全策略是指在一个特定的环境里,为保证提供一定级别的安全保护所必须遵守的规则,是组织网络安全防御系统的基本依据。网络的安全策略应包括先进的技术、严格的管理、威严的法律法规约束和细致入微的安全教育,本文仅讨论安全技术。

WBSEAS 在网络安全技术方面,从主机、服务器、网络设备、应用程序和数据库安全等方面综合考虑,集防火墙、VPN、身份鉴别与访问控制、主机监控与审计、入侵检测与控制、数据加密、多功能安全服务器、数据备份与灾难恢复等自主技术于一体,构建一个从网络边界到网络内部、从整个网络到单个主机的全方位、多层次、立体化安全保障体系,最大限度地保证系统安全。

1.3　保护措施

安全保护一方面通过划分网络边界,在边界上阻止非法用户入侵;另一方面是通过采取防护、隔离等措施,最终达到保护系统重要数据不丢失、不泄漏、不被篡改等目的。

WBSEAS 的安全保护措施包括网络安全保护和数据访问保护两大方面。网络安全保护是在应用层以下采取的保护措施,包括防火墙、网络活动监视、物理隔离等技术;数据访问保护就是在操作系统、数据存储、数据通讯等方面的安全保护,主要包括数据备份和灾难恢复系统的设计,安全操作系统技术、身份认证与访问控制、病毒检测、数据加密通讯等技术。

需要强调的是,在数据的安全保护方面,为简化 PKI 加密机制中公钥管理困难、成本高、效率低等不足,WBSEAS 采用 IBE 技术,加密浏览器端用户的重要信息。

1.4　检测方法

检测是信息保障技术的核心,是主动防御的根本。针对防火墙不能防范内部网络攻击、无法检查绕过自己的网络数据、无法解决 TCP/IP 协议漏洞、不能阻止内部泄密行为等缺陷,按照主动防御思想,在 WBSEAS 中引入基于硬件设计的高性能入侵检测系统(IDS),提供对内部攻击、外部攻击和错误操作的实时检测,弥补传统被动防御技术的不足。同时,采取 IDS 与防火墙联动技术,自动添加防火墙规则以对付新的攻击;IDS 与交换机联动,使得当 IDS 检测到高风险的入侵行为后,能迅速关闭交换机的相关端口或封堵指定的 IP,达到切断攻击源目的。

1.5　响应机制

响应机制能够对发现的攻击模式、系统弱点和漏洞、病毒、违规行为、泄密等各种威胁,按照事先约定的方式进行报警或控制。

当检测到入侵后,WBSEAS 的实时响应机制根据攻击的性质、强度、持续时间等信息,按照既定的安全策略,及时采取以下防控措施:及时调整安全策略;记录相关信息的日志,并通过控制台消息、E-mail 等发出告警;与防火墙、交换机联动阻断非法连接、限制网络连接、调整网络流量、关闭危险端口、必要时甚至关闭主机等。

1.6　备份与灾难恢复

只有完整地备份重要的数据和系统信息,才能在网络系统的局部或全局遭到毁灭性破坏后快速进行恢复,实现关键业务的持续,提高系统的抗灾能力。

WBSEAS 通过基于 Internet 的跨地域灾难恢复系统,对本地数据中心中的 Web、数据库、邮件及应用程序等服务器进行远程实时数据备份。正常情况下,由本地服务器对外提供服务;当系统遭受火灾、恐怖袭击等灾难时,远程服务器自动对外提供服务,实现服务的转移;本地服务器功能恢复后再继续对外提供服务。从而进一步提高整个系统的可靠性和强壮性。

综上所述,WBSEAS 从网络边界安全、身份鉴别与访问控制、入侵检测、数据加密、备份与灾难恢复等方面进行了全方位的保护,建立了从外到内、功能齐全、具有整体防御和纵身防御能力的动态主动防御机制,为教务系统的正常运行提供强有力的安全保障。

2　IBE 基本原理

IBE 是继 PKI 之后的又一新型公钥加密机制,它借助一个可信的第三方机构私钥生成器(Private Key Generator, PKG),用来生成、保存并传送所有用户的私钥,公钥可选择能表示用户身份的任意字符串(如身份证号、职工编号等)。由于 IBE 不依赖于任何数字证书,有效避免了 PKI 机制中产生、存储、使用和管理证书的麻烦,只用选择比 RSA 小得多的密钥就能取得接近于 RSA 的安全性,成为网络安全中一种成本和复杂度低、易于实施、使用方便的加密和解密方案。同时,

为实现数据在存储、传输过程中的机密性、完整性和不可抵赖性，IBE 还提供了有效的数字签名方案[10,11]。

目前，理论上安全可行的 IBE 方案大致有两种：一种是由 Cocks[8] 提出的基于二次剩余的加密方案，它运用了数论中大整数难以分解因子的基本原理，但该方案产生的密文很长，对传输带宽的要求非常高，一般不易采用；另一种是由 Boneh[6] 和 Baldwin[7] 等人提出的基于椭圆曲线的加密方案，它们使用了超奇异椭圆曲线上的双线性映射，此方案对网络带宽的要求相对较低，实用性比较强。

基于椭圆曲线的 IBE 方案[6]的执行过程分为三个阶段：

1）系统参数初始化

PKG 按如下步骤初始化系统参数：

① 选择一个不少于 1024 比特长的素数 p，且存在大素数 q，使得 $p = 6q - 1$；

② 找出一条满足 WDH(Weil Diffie-Hellman) 安全假设的超奇异椭圆曲线 $y^2 = x^3 + 1$，记为：$E/GF(p)$，其中：p 是该曲线上阶为 q 的一个点，由 p 生成的循环群记为 G；同时，再找出一个双线性映射 $\bar{e}: G \times G \rightarrow GF(p^2)$；

③ 定义 Hash 函数 $H_1: GF(p^2) \rightarrow \{0,1\}^n$，以及一个用于将用户身份 ID 映射到椭圆曲线 $E/GF(p)$ 上阶为 q 的点的函数 $F: \{0,1\}^* \rightarrow E/GF(p)$；

④ 设 $s \in Z_q^*$，将 s 作为主密钥，并公开 $p_{pub} = s \cdot p$。

最后，PKG 将系统参数 $\{p, n, \bar{e}, p, p_{pub}, H_1, F\}$、明文空间 $M = \{0,1\}^n$ 和密文空间 $C = E/GF(p) \times \{0,1\}^n$ 公开，同时秘密保存主密钥 s。

2）用户私钥提取

设 P_{ID} 表示用户的身份 ID 在椭圆曲线 $E/GF(p)$ 上对应的点 $F(ID)$。若身份为 ID 的用户 $User_{ID}$ 通过 PKG 的验证，则将其私钥 $S_{ID} = s \cdot P_{ID}$ 安全送达给 $User_{ID}$。

3）加密／解密

当 A 发送数据 D 给 B 时，A 随机地取 $r \in Z_q^*$，计算密文：$D_{encrypt} = (r \cdot p, D \oplus H_1(g_{ID}^r))$，其中 $g_{ID}^r = \bar{e}(p_{ID}, p_{PUB}) \in GF(p^2)$。设 $D_{encrypt} = (W, V)$，B 收到密文 $D_{encrypt}$ 后，如果 $W \notin E/GF(p)$，则拒绝密文 $D_{encrypt}$，否则用自己的私钥 S_{ID} 按如下方法解密：$V \oplus H_1(\bar{e}(S_{ID}, W)) = D$。加／解密的一致性由下式保证：

$$\begin{aligned}\bar{e}(p_{ID}, p_{PUB})^r &= \bar{e}(r \cdot P_{ID}, s \cdot p) \\ &= \bar{e}(s \cdot P_{ID}, r \cdot p) \\ &= \bar{e}(S_{ID}, r \cdot p)\end{aligned}$$

3 系统设计

3.1 技术架构

传统的基于两层 C/S 架构设计的教务管理系统，尽管能通过网络存取和共享后台数据，但随用户数量的不断增加，暴露出其客户端和服务器端负担过重、维护工作量大、无法远程应用等严重缺陷；纯粹基于 B/S 架构设计的系统方便了广大学生、教师等用户的应用，并大大简化了客户端设计，然而难以开发高度复杂、功能强大的应用子系统，比如排课子系统，同时在安全性和速度方面也存在不足之处。

考虑到教务管理系统的特殊性，WBSEAS 采用 C/S/S 和 B/S/S 相结合的三层／多层架构设计：对安全性和可靠性要求高、交互性强、数据流量大且处理频度高的子系统，采用 C/S/S架构；对地理位置分散、数据流量小、交互速度要求不高的子系统采用 B/S/S 架构，如图 1 所示。

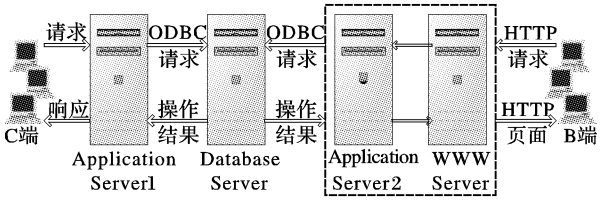

图 1 WBSEAS 技术架构示意图

C/S/S 和 B/S/S 技术架构与传统的 C/S 和 B/S 架构相比，增添的中间层应用服务器呈组件形式，封装了所有的业务规则，便于维护，易于扩展；同时，应用服务器隔离了 C 端用户和 WWW 服务器对数据库服务器的直接访问，进一步提高了系统的安全性。

3.2 安全保障措施

图 2 是 WBSEAS 的拓扑结构，安全保障措施如下：

1）通过防火墙、VPN 划分网络，确保校园网及各部门子网的边界安全。特别地，通过 VPN 可在不同的校区之间建立起基于 Internet，且如同内网一样安全的虚拟专网，拓宽业务空间，节省网络的建设和使用费；

2）集成主机监控、身份鉴别、访问控制、入侵检测、审计、漏洞评估、病毒扫描等技术，对主机和网络活动进行主动、有效监控，阻止非法用户、病毒等恶意入侵，同时实时监控网络流量；

3）使用安全操作系统、安全 Web 服务器，确保网络应用平台安全；

4）使用跨地域的备份与灾难恢复系统，建立基于 Internet 的超常距离数据实时备份和系统备份机制。当本地服务器发生灾难时，远程服务器能够自动切换对外提供服务，使系统具备抗击灾难事件的能力。

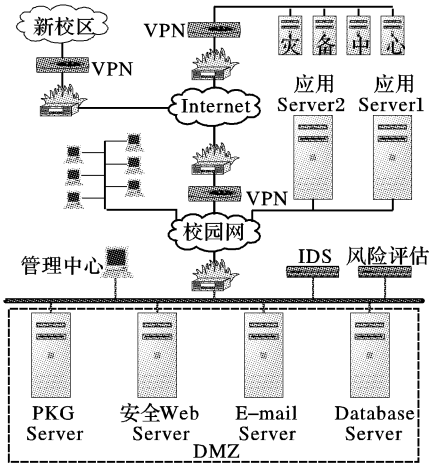

图 2 WBSEAS 拓扑结构

4 实验与分析

为了验证基于 Web 的安全教务管理系统 WBSEAS 的实际效果，我们进行了实验，对系统的功能、性能及安全保障情

况进行了测试,并与传统的教务管理系统[14]、基于 PKI 技术的教务管理系统[3]进行了对比、分析。

4.1　实验环境

我们按照图 2 所示的拓扑结构,在河南教育学院现有教务管理系统的基础上,对 WBSEAS 安全方案进行了验证。同时,在 Linux 操作系统下,基于斯坦福大学计算机科学系安全实验室提供的开源 IBE 程序库[12],用 C 语言编程实现了 IBE 加密方案中系统参数的初始化、私钥获取、加/解密功能以及客户/服务器端应用等;另外为系统编制单独的身份认证程序,协助 PKG 完成用户验证功能。

4.2　结果及对比分析

与传统的教务管理系统 TEAS[14]一样,WBSEAS 能够正确完成学生注册、学籍管理、成绩登录、成绩查询、学生选课、排课、费用清算等各项功能,但在安全性方面进行了改进和加强,如表 1 所示。

表 1　与传统教务管理系统的对比

比较项目名称	TEAS[14]	WBSEAS
教务管理功能	具备	具备
身份验证	一般	严格
访问控制能力	较差	很强
入侵检测与风险评估	不具备	具备
数据加密功能	不具备	具备
页面防篡改功能	不具备	具备
灾难备份与恢复	本地备份	远程备份

部分对比实验数据如表 2 所示。

表 2　对比实验结果

比较项目名称	PKI 方案[3,4]	WBSEAS 方案
证书生成时间/s	> 2	0
私钥生成时间/s	> 1	< 0.5
身份认证时间/ms	> 13	< 10
数字签名速度/(次·s^{-1})	< 180	> 200
平均加密速度/Mbps	< 32	> 50

从实验结果可以看出:WBSEAS 系统工作效率远高于基于 PKI 技术的教务管理系统,良好的实验结果源于采用的公钥机制不一样,表 3 是二者的比较[13]结果。

表 3　PKI 和 IBE 的比较

	PKI 机制	IBE 机制
公钥的形式	数字串	字符串
公钥产生办法	由 CA 产生	用户任意指定
公钥保存方法	与证书绑定	与证书无关
私钥生成时刻	公钥产生时	公钥产生后
公钥的撤销	多用 CRL 实现	一般不存在
运行机制	需 CA/RA/CRL/证书库协作	只需身份验证和 PKG 即可

综合分析系统的工作原理和实验结果,可以看到:基于 Web 的教务管理系统安全方案设计中,既允许用户正常浏览公共信息,又禁止对页面的篡改;在学生选课、教师登录成绩、排课等教务管理过程中,用户从登录到数据存取要经过防火墙验证、身份认证、应用程序数据验证、安全连接、加/解密、数字签名等安全过程,既保证了用户身份的真实、唯一,又实现了数据的机密性、完整性和不可抵赖性;同时,WBSEAS 采用基于身份的加密机制取代了基于 PKI 的公钥管理机制,免去了证书产生、存储和撤销等麻烦,又提高了系统的工作效率。

5　结语

本文从网络边界安全、网络活动实施监控、应用平台安全、备份与灾难恢复等方面论述了基于 Web 的安全教务管理系统的设计方案。该方案既能阻止非法用户的入侵及合法用户的越权访问,又能保证重要数据在存储、使用和传输等过程中的机密、完整、可用和不可抵赖性;同时克服了用 PKI 技术解决该系统安全问题时存储和管理公钥困难、系统实现复杂、成本高、效率低等缺陷。WBSEAS 的实现对深化教务改革、进一步完善教学管理模式、提升高校的综合管理水平等,将会起到重大的推动作用。

WBSEAS 的网络安全设计方案具有很强的通用性,对解决电子政务、电子商务等现代网络业务的安全问题亦具有极大的参考价值。

参考文献:

[1] 戴宗坤. 信息安全使用技术[M]. 重庆: 重庆大学出版社, 2005.

[2] 李涛. 网络安全概论[M]. 北京: 电子工业出版社, 2004.

[3] 刘念, 李涛, 赵奎, 等. 基于 PKI 技术的学分制管理系统的安全解决方案[J]. 电子科技大学学报, 2003, 32(4): 440 - 443.

[4] BRANDS S. Rethinking Public Key Infrastructures and Digital Certificates-Building in Privacy [M]. MIT Press, 2000.

[5] ELLISON C, SCHNEIER B. Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure[J]. Computer security Journal, 2000, 16(1): 1 - 7.

[6] BONEH D, FRANKLIN M. Identity-based Encryption from the Weil Pairing[A]. Advance in Cryptology-CRYPTO 2001[C]. LNCS 2139, 2001.213 - 229.

[7] BALDWIN M. Identity Based Encryption from the Tate Pairing to Secure Email Communications[Z]. Master of Engineering Thesis, University of Bristol, 2002.

[8] COCKS C. An Identity-based Encryption Scheme Based on Quadratic Residues[Z]. Cryption and Coding, LNCS 2260, 2001: 360 - 363.

[9] HORWITZ J, LYNN B. Toward Hierarchical Identity-based Encryption[A]. Knudsen L EUROCRYPT 2002[A]. Berlin: Springer Verlag[C], 2002. 466 - 481.

[10] PATERSON KG. ID-based Signatures from Pairings on Elliptic Curves[J]. Electronics Letters, 2003; 38(18): 1025 - 1026.

[11] BONEH D, FRANKLIN M. Short Signatures from Weil Pairing[A]. Boyd C ASIACRYPT 2001[C]. Berlin: SpringerVerlag, 2001.514 - 532.

[12] BONEH D, FRANKLIN M. Stanford IBE Library[DB/OL]. Http://crypto.stanford.edu/ibe/download/ibe-0.7.2.tgz, 2002 - 04.

[13] PATERSON KG, PRICE G. A. Comparison Between Traditional Public Key Infrastructures and Identity-based Cryptography[J]. Information Security Technical Report, 2003, 8(3): 57 - 72.

[14] 陈怀楚. 清华大学学分制综合教务管理系统说明书[Z]. 清华大学计算机中心, 2001.