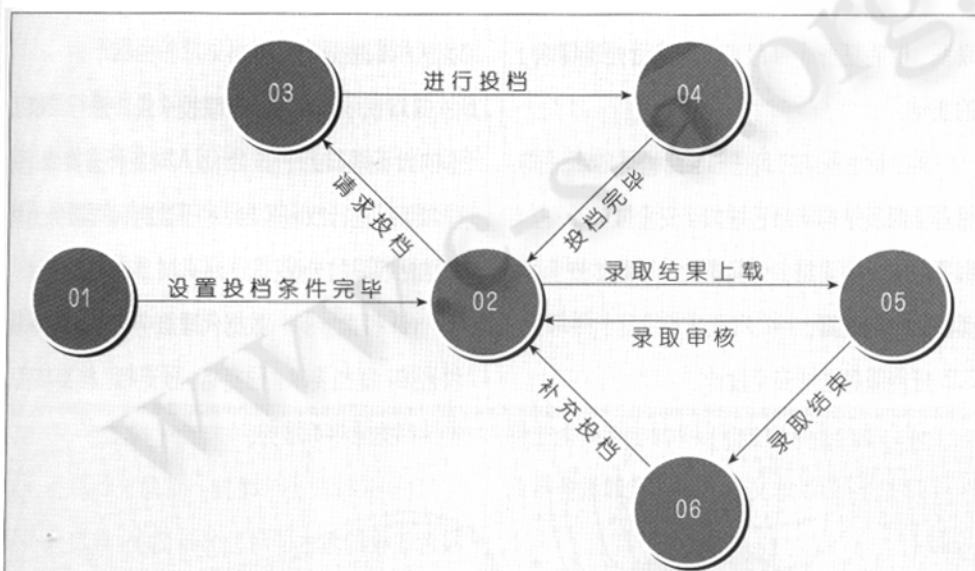


# 高校网上招生系统的安全设计与应用

王明宝 熊焰 陈凯明 (安徽合肥中国科学技术大学计算机系网络研究室 230052)

摘要: 本文简述了网上招生过程, 设计了网上招生安全框架以及三层结构网站在网上招生安全方面的应用, 同时提出了确保现场网上招生的顺利进行, 所使用的双备份策略。

关键词: 网上招生 安全 三层结构 双备份



状态说明: 01 初始状态、02 允许投档、03 请求投档、04 正在投档、05 等待审核、06 录取完毕

图 1 院校网上招生状态转换图

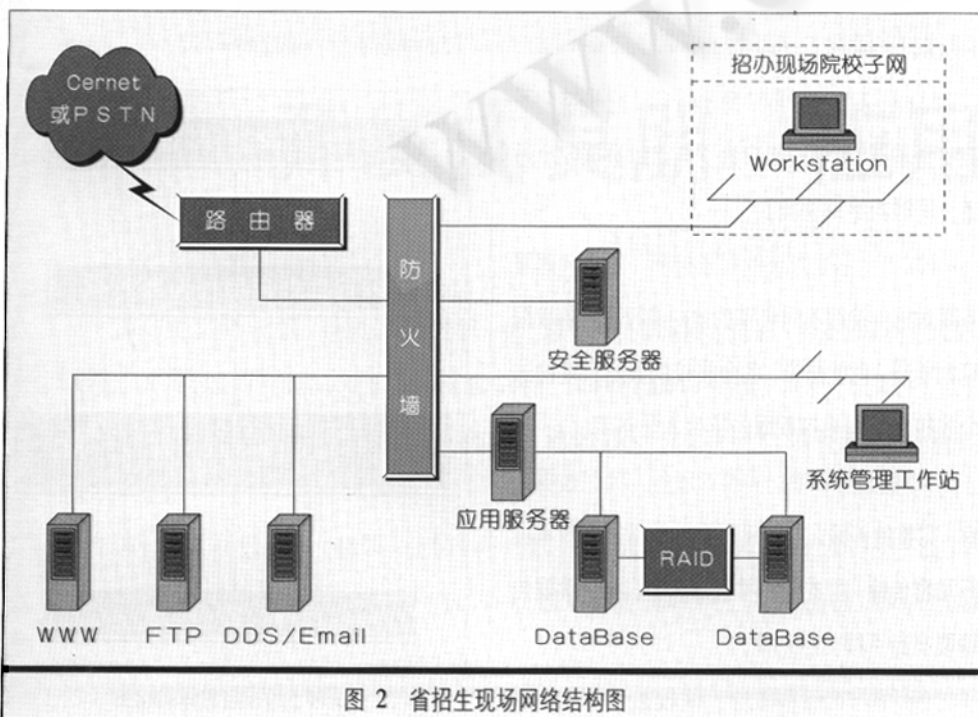


图 2 省招生现场网络结构图

## 1 引言

几年前, 高校招生工作基本上是人工实施, 各个大专院校花费大量的人力、物力到各省招办录检考生, 而各省招办由于考生档案众多, 管理也费时、费力。要求招生信息现代化管理也就成为必然趋势。

随着互联网的飞速发展, 网络在人们的生活中发挥着日益重要的作用。越来越多的人利用网络从事商务、办公、教学、消费等活动。同时, 互联网上存在着黑客、病毒等因素, 网上招生传输的数据是否安全, 也是广大考生关注的问题。基于网上招生关系到广大人民群众切身利益, 影响面广, 意义重大。本文主要针对系统的安全进行设计, 并对现场网上招生顺利实施, 尽可能做到万无一失, 在实践中使用双备份策略。

## 2 概述网上招生系统

### 2.1 简述网上招生系统流程

各招生院校通过 CERNET (中国教育与科研网) 或 PSTN (公用交换电话网) 连接到各省招办的网上录取系统网络, 没有条件的学校可以直接到各省招办设置的招办现场院校子网进行考生录取。

各招生院校设置好投档条件, 然后发出投档请求给省招办录取系统, 省招办录取系统把符合投档条件的学生电子档案发送给高校招办系统, 高校招办进行录取, 并把录取结果上载, 等待省招办审核批准, 一旦审核批准后存档, 录取结束, 请参见图 1

### 2.2 网上招生的拓扑结构图的设计

远程招生院校通过 CERNET 或 PSTN 连接到各省招办网络 (见图 2), 经过防火墙的防黑客、防病毒程序处理后到安全服务器进行用户身份认证, 对合法的用户建立自己的数据安全传输通道, 并对合法的用户进行相应的访问授权、数据签名, 只有合法的用户才能使用应用服务器, 通

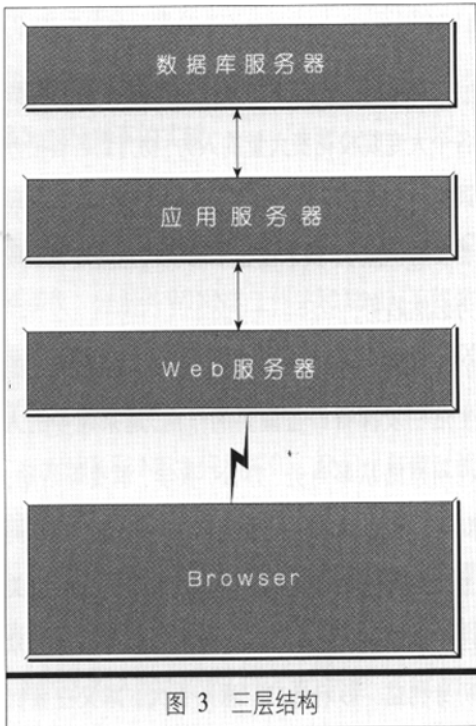


图3 三层结构

过应用服务器提取或修改存取后台数据库服务器中数据,同时应用服务器要处理并发等事件,这样大大减轻了数据库服务器的负担。所有对网络的重要操作都要生成系统日志,供具有某种权限的用户查看。

### 3 网上招生系统在三层结构网站的网络安全设计

#### 3.1 三层结构网站

如图3。

三层分别是指Web Server (Web 服务器)、Application Server (应用服务器)和 Database Server (数据库服务器)。这种结构是现在国内外大中型网站日趋流行的结构,它主要指Web 服务器通过应用服务器对数据库服务器进行联系,Web 服务器负责生成动态网页,采集数据,显示数据而不涉及具体的数据库或者表结构。数据库服务器不涉及具体的网页、网站。应用服务器协调Web 服务器与数据库服务器之间的联系,送给Web 服务器的是Web 服务器易于解读的查询结果,送给数据库服务器可直接执行的SQL 语句。数据来源、去向由应用服务器调度,专门模块功能分开,

三层分工明确。

三层结构的优点如下:

(1) 易于实施各种安全措施,应用服务器负责安全调度数据,各层分工明确。

(2) 易于理解,因为各专门模块功能分开,更利于人们理解。

(3) 负载能力高,因为各层分工明确,一个任务由各个部分均衡负担。

(4) 灵活性高,因为各个部分独立性强,数据库服务器与Web 服务器通过应用服务器联系,能胜任各个高级应用,灵活处理需求上的变动。

网上招生系统应用在三层结构网站(见图2),相对于两层结构网站它增加了安全服务器、应用服务器等硬件设施。但换来的是系统的安全性、负载能力的提高。

#### 3.2 应用服务器的安全设计

网上招生系统中应用服务器主要功能是使用代理服务,所以本文称为应用代理服务器见图4。

其中各省招办应用代理服务器设计代理以下服务:

##### 3.2.1 安全代理服务

安全代理服务要实现数据交流的安全,设计时从以下方面进行了考虑:

(1) 网络上远程用户身份认证:它是整个系统安全基石,使合法用户建立自己的数据安全通道,同时拒绝非法用户。

(2) 网上招生系统的权限控制:安全代理服务要对招生院校不同级别的用户进行不同的权限控制管理。也就是说,各个院校的数据只能被这个院校中具有相应权限的招生人员访问。

(3) 数据可靠性、完整性服务:为了数据可靠、完整的传输,安全代理服务器必须对数据进行加密传输,生成密钥并管理密钥,并对数据传输要有断点续传的功能。

(4) 不可抵赖性服务:院校招生信息上载

后不可抵赖,安全代理服务器必须设计有数据签名功能。

(5) 重点事件的审计功能:所有对招生系统的重要操作要有日志功能,供具有某种权限的用户查看。

##### 3.2.2 数据代理服务

数据代理服务是网上招生系统的重要组成部分。需要完成的功能是利用招办的数据给远程院校端提供服务,对远程院校发出招生录取的数据请求进行分析,响应其中合理的请求。设计时从以下方面进行考虑:

(1) 权限服务:对于院校来说,进行录取工作的人可能不止一个,什么人对应什么操作,院校端可以进行权限控制,对于数据代理服务当然还包括权限的分配。

(2) 档案服务:数据代理服务能为院校端提供诸如:提档要求、预提档、预退档、档案核实、特殊档案要求等服务。

(3) 其他服务:诸如:信息统计服务,对报考该校的考生的考分分布情况、地域分布情况等进行分析。特殊录取服务,对于一些特殊的录取,特殊退档也是必要的。交流服务,为远程用户和招办服务人员建立网上信息交流通道。

##### 3.2.3 信息查询代理服务

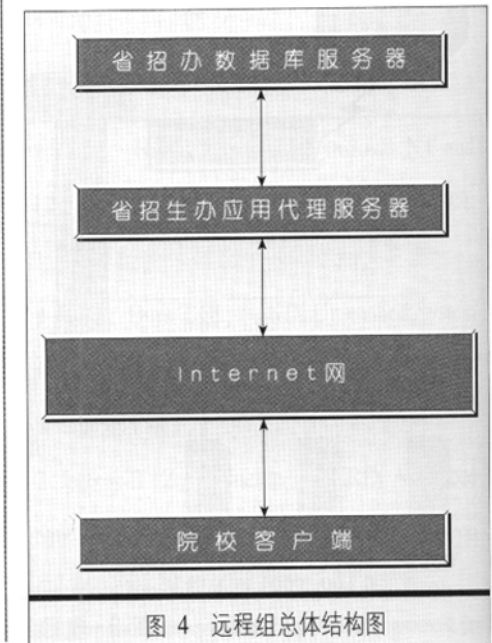


图4 远程组总体结构图

为了实现用户足不出户就能通过 Internet 了解当前招生情况, 为了实现用户的跨平台应用, 设计中采用目前流行的 Web 技术。从数据安全的角度来说, 系统应该保证数据的真实性和敏感数据的保密性, 要能有效的防止恶意的攻击和数据篡改, 信息查询代理服务器要合理分配权限, 实现每种用户只能看到不同程度的数据。

#### 4 双备份策略

##### 4.1 数据库中的数据双备份

由于招生的系统数据库中数据跟广大考生前途息息相关, 此数据非常重要, 所以要对省招办数据库用 RAID 盘进行双机热备份 (见图 2)。用 RAID 盘进行双机热备份, 可以随时恢复有故障的数据库服务器数据, 以避免重要数据丢失。

##### 4.2 现场招生主要设备双备份

由于网上招生时间短暂, 而且传输数据量大, 一旦网络关键设备 (例如路由器、安全服务器等) 崩溃, 系统维护人员没有充足时间重新调试, 最安全也是最简捷方法是在网上招生前把路由器、安全服务器等重要设备进行双备份。也就是说在准备使用前, 调试好两台装有同样安全系统的安全服务器, 两台路由完全相同的路由器等。一旦一个设备崩溃, 另一个设备直接换上, 不会造成招生现场混乱, 这样可保证网上招生实时顺利地进行。

#### 5 结束语

本系统的安全设计已经实施在安徽省网上招生系统的网站上, 并使用效果良好。高校网上招生系统涉及到千家万户, 所以网上招生的安全设

计放在系统的重要位置, 本文提出的一些确保系统的安全设计策略, 是符合这样一个要求安全和负载能力高的系统的。 ■

- 1 网上录取系统总课题组, 全国普通高校招生网上录取系统概要设计, 2001.1.
- 2 信息管理系列编委会 [编], 网络安全管理, 中国人民大学出版社, 2001.
- 3 李雯等, 充分利用网络设备实现网络的多层次安全管理, 计算机应用, 2001.3, 21(3): 61~71.
- 4 王睿, 林海波等, 网络安全与防火墙技术, 清华大学出版社, 2000.10.
- 5 [美] 拉斯·克兰德, 挑战黑客: 网络安全的最终解决方案, 电子工业出版社, 2000.

## 开发的良朋 应用的益友

《电脑开发与应用》月刊

本刊集信息、知识、趣味、可读性于一体, 以计算机实用技术见长, 博采、精选国内外电脑研究、开发与应用的精华, 尤其欢迎网络与通讯、Internet、www、网友、软硬件二次开发、家庭电脑开发、中小学电脑开发等方面的内容, 跟踪报道世界最新技术, 具有前瞻性的预测文章更在欢迎之列!

本刊为大 16 开 (A4)、48 页、定价 4 元/册、全年 48 元之电脑月刊。欢迎订阅, 诚征广告, 全国各地邮局均可订阅, 邮发代号: 22-96 国外代号: M4257 万一邮局漏订, 请与本部联系。

联系地址: 太原市 193 信箱

《电脑开发与应用》编辑部

邮编: 030006

电话: (0351) 7023553-2182

传真: (0351) 7022975

E-mail: Zhuylns.shanx.cetin.net.cn