# **论信息系统的安全性与保密性设计**

摘要

  2019年3月，我单位联合某高校研发了《程序在线评测比赛考试系统》。系统以程序代码在线提交自动评测功能为核心，分为题库模块、评测机模块、实验作业模块、考试模块、比赛模块、抄袭判定模块、用户管理模块等，支持对接教务平台。在项目中我担任系统架构师，负责架构设计工作。

  本文从网络硬件层、数据层、应用层三个方面，论述了针对该系统的安全性与保密性问题，以及所采用的技术手段和解决方案。网络硬件层设置硬件防火墙，解决病毒木马与外部攻击的隐患；数据层设置数据加密与容灾备份机制，解决数据泄露丢失的隐患；应用层统一采用RBAC授权机制等方案，解决越权操作的隐患，提高了整个系统的抗风险和安全保密能力。最终系统顺利上线，获得了用户的一致好评。

正文

  笔者在一个专为高校建设计算机专业智能教学一体化平台的单位任职，过往成果有《计算机组成原理仿真实验系统》等。2019年3月，我单位联合某大学研发了《程序在线评测比赛考试系统》项目（以下简称为“OJ系统”），以取代原有传统的编程上机考试平台。

  系统以程序代码的在线提交自动评测功能为核心，主要分为题库模块、评测机模块、实验作业模块、考试模块、比赛模块、抄袭判定模块、用户管理模块等。题库模块主要负责试题和测试用例的管理，用户根据试题要求编写程序代码提交到系统，系统将测试用例与程序代码发送给评测机模块，由评测机自动编译、执行、判分，并将结果发送给其他相关模块进行统计；实验作业模块用于在线布置作业，从题库中选取试题，设置截止日期等要求；考试模块用于学生在线考试，按教师预先设置的参数自动从题库随机抽题生成试卷，以及向教务平台上传考试成绩；比赛模块主要用于ACM竞赛的培训；抄袭判定模块用于鉴定代码与他人代码雷同率；用户管理模块负责用户信息的管理。在这个项目中，我担任了系统架构师的职务，主要负责系统的架构设计相关工作。

  OJ系统中存储着学生成绩、学生选课数据、试题数据等大量重要信息，确保系统的安全性与保密性显得尤为重要。系统在安全性与保密性方面主要面临以下问题：网络安全隐患，包括病毒木马、外部攻击等，缺乏主动的网络安全防御机制。数据库安全隐患，例如数据库访问控制不严、敏感数据以明文存储、未制定容灾备份计划等，容易造成系统数据泄露、丢失、篡改。应用安全隐患，包括权限管理混乱、权限设置不够合理等，容易出现人为操作导致数据错误或丢失，威胁到系统的信息安全。

  如果敏感数据不经加密传输，入侵者可通过网络嗅探工具获得用户的账号和口令。在业务逻辑中对用户提交数据的合法性没有判断或过滤不严，攻击者可在事先定义好的查询语句的结尾上注入额外的SQL语句，在管理员不知情的情况下实现非法操作，欺骗服务器执行非授权的任意查询。

  因此，我们在网络硬件层、数据层、应用层三个方面，对提高系统的安全性与保密性，做了充分的设计。通过在网络硬件层设置硬件防火墙，数据层设置数据加密与容灾备份机制，应用层统一采用RBAC授权机制等方案，提高了整个系统的抗风险和安全保密能力。

1. 网络硬件层安全方案

  网络和硬件是整个系统运行的基础，也是很多外部攻击的主要途径，所以OJ系统在这一方面需要进行严密合理的规划。为解决病毒木马与外部攻击的隐患，我们对网络拓扑结构划分为外部网络、内部网络与DMZ三个部分。在外部网络和内部网络之间设置了硬件防火墙，主要是防止外部的恶意攻击。在防火墙之后，为加强对病毒、木马入侵的防范效果，又设置了硬件的防毒墙，实时保证能够拦截与查杀符合最新特征库的病毒、木马。为防止校外访问者通过DNS服务器直接访问到应用服务器的目标地址，在校内网络中又增加了反向代理服务器，对外只暴露代理服务器的虚拟IP，更好地减小了应用服务器被攻击的可能性。应用服务器与数据库服务器做了物理隔离，内部人员也无法通过IP直接访问，只能通过堡垒机由服务器管理员进行操作，阻断了外界通过内部客户端代理的访问对服务器造成攻击。对于一些核心的FTP服务器、DNS服务器、Web服务器都规划到DMZ中。

2. 数据层安全方案

  数据是整个平台业务运转的核心，其中涉及大量学生成绩、试题数据等重要信息，安全不容忽视。为解决数据泄露、数据丢失的隐患，系统主要从数据存储、数据访问和数据容灾几方面进行了规划。由于系统主要存放的考试题目与学生成绩数据对保密性要求高，为了防止泄露，我们在存储时进行了加密处理。虽然在处理过程中会有性能损失，但也因此提高了数据的安全性与保密性。系统的数据库软件采用Oracle作为后台存储，其公司的商业口碑极佳，对数据存储的安全提供强大保证。为了防止数据信息的泄露，加强了访问权限的限制，在数据库的访问权限上，都根据不同的角色进行了详细划分，包括对数据库、表、索引、记录的增、删、查、改进行了限制，严格禁止非法用户对数据库恶意破坏。同时，在数据库本身，也制定了基于全量、增量、差量的按周备份计划，保证每时每刻的数据都可以及时恢复。在物理存储上也做了本地多机房的容灾备份，充分保证了数据抗突发风险的安全。

3. 应用层安全方案

  由于OJ系统采用MVVM前后端分离架构，通过RESTful风格的WebAPI通讯，所以在用户认证、接口传输等方面做了充分设计。用户认证方面，因系统用户涉及多种类型，如学生、授课教师、课程组、参赛选手、举办方、系统管理员等，统一采用RBAC授权机制，既可增强系统安全性，满足业务需求，也可减轻权限信息维护的负担。在登录界面上，不仅需要提供用户名+口令，同时设置了验证码和动态口令，通过手机或邮箱接收，杜绝非法破解口令登录，保证整个系统认证环节安全。密码提交和存储过程中，一律通过MD5+SHA256+随机SALT哈希加密，即使被拖库也不会泄露密码。接口设计是整个系统通信的安全保障，为防止外部人员恶意调用与窃取信息，使用了https传输协议和令牌机制，保障每次通讯传输安全。即在登录后，通过加密传输的用户信息和时间戳获取到token令牌，在后续每次通讯过程中，服务器端都会校验token，充分保障接口调用安全。在对数据库进行增删查改调用时，统一使用带预处理功能的ORM中间件实现操作，可过滤SQL注入攻击，防止对数据库执行非授权的任意查询。

总结

  系统自2019年10月正式上线后，已运行一年有余，在学校的日常教学考试和竞赛培训中投入使用，截至目前已有3000以上的学生用户、评测了70000条以上的程序代码，获得了单位同事领导和学校教师们的一致好评。在任何情况下使用系统，基本没有信息泄露的情况发生。但在使用过程中一些用户反映，手机端操作编辑题目与保存成绩有时会需要等待，我们分析发现该问题是因为编辑题目信息与保存成绩涉及数据量较大，且手机硬件运行效率比PC低，导致前端加密传输更加耗时，通过优化数据结构、减少数据传输量、选择效率更高的加密算法等方法改善了这个问题。

  实践证明，OJ系统项目能够顺利上线，并且稳定运行，保障了信息安全，与系统在安全性和保密性方面的设计密不可分。系统安全是一个永久的话题，我们对系统安全性的完善是一个持续、迭代的过程，在未来还会不断地完善本系统安全方面的设计，改善缺陷与不足，使整个OJ系统能够更加好用，更有效地服务于高校师生。