**摘要:** 2015年3月，我所在公司承接了一款养老管理信息平台，该系统以养老为主线，其中包括养老档案、照护计划、服务审计、状况跟踪、费用管理等方面的60多个业务功能模块，我在项目中担任系统架构设计师，主要负责整个系统的架构设计。本文以该养老管理信息平台为例，主要论述了针对该系统的安全及保密性问题，我们所采用的技术手段及解决方案。在网络硬件层通过设置硬件防火墙，来保证内部网络安全性；在数据层通过设置数据加密及容灾备份机制，以此保证数据抗突发风险的安全；在应用层统一采用RBAC的授权机制，来保证整个系统认证环节的安全性。事实证明，以上技术方案的实现对整个系统的安全和保密性方面起到了很好的效果，最终项目顺利上线，运行稳定，受到广大用户的一致好评。

目前我国已经进入到老龄化社会，老龄人口逐年增长，按照老龄办提供的数字，预计到2020年中国的老年人口将要达到2.48亿，与之增加的养老消费人均三千元左右，从整个养老产业的规模来看，估算在2025年要增加到五万亿规模，市场前景巨大。随着互联网的迅猛发展，各行各业都在进行着互联网+的尝试，希望搭上这个发展契机。其中，养老领域更迫切需要解决养老专业化程度低，信息化不足，健康照护水平滞后等一系列亟待解决的问题。  
2015年3月，我所在公司承担了全国老龄办及全国几十家养老和医疗机构合作进行的养老管理信息平台的开发工作，我在该项目中担任系统架构设计师，主要负责应用系统的软件架构设计。由于我们公司在医疗行业领域有着丰富的成功经验，同时，近些年在养老领域也成功实施过很多成熟的案例，所以，一期投资方出资3000万，委托我们进行这款综合性养老管理平台的开发工作。该系统以养老为主线，其中包括养老档案，照护计划，服务审计，状况跟踪，费用管理，决策支持等方面的60多个业务功能模块组成，系统功能相当完备。  
经过前期对全国几十家养老机构和相关合作的医疗单位的调研分析，结合原有的经验，对整个系统业务进行详细规划和相关设备的初步选型，即我们内部所说的“两版三端”的方案，机构养老和社区养老两个子系统，同时能够在PC端，PAD端，手机端三端进行呈现和交互。整个养老管理信息平台基于B/A/S模式的分层架构风格设计。同时，结合当前先进的基于租户理念搭建的一个养老云平台（SAAS）。当前信息安全问题严重，而养老云平台是一个养老大型综合管理平台，确保系统的安全性和保密性显得尤为重要，让使用我们平台的每一家机构、社区、老人及相关亲人都能够安心和放心。这样，只有最终得道了用户的信赖，系统的前景才会发展的更好。所以，我在系统的安全性和保密性方面做了充分的设计。  
1、网络硬件层安全方案  
首先，因为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，在这块需要进行合理规划。我们对网络拓扑结构划分为外部网络，内部网络和DMZ三部分。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。在防火墙后，为了加强对病毒入侵的防范，又设置了硬件的防毒墙，实时保证最新的病毒特征库保证有效的病毒工具。为了防止外部客户通过DNS服务直接访问到我们服务器的目标地址，在内部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，更好的保护了应用服务器被攻击的可能性。应用服务器和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，只能通过跳板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  
其次，数据是整个系统平台的核心，其中涉及大量个人隐私数据和重要信息资产，安全不容忽视。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养老档案数据，其中涉及很多个人隐私部分数据，为了防止泄露，我们在存储时进行了加密处理。虽然在处理中损失些性能，但是，提高了数据的安全性和保密性。我们采购商业数据库Oracle作为后台存储，由于其极佳的商业口碑，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，都根据不同角色进行了详细划分，包括对数据库，表，索，记录等的增，删，改，查进行了限制，严格保证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，充分保证数据抗突发风险的安全。  
3、应用层安全方案  
最后，由于我们系统架构采用的是分层架构风格，同时，又是采用“三端”的形式，即手机端，PAD端，还有PC端，所以，在用户认证，接口传输等方面做了充分设计。由于系统涉及到养老机构工作人员，老人及家属等，角色众多，统一采用RBAC的授权机制，既增强系统安全性满足业务需求，同时，减轻由于权限信息维护负担。在登录界面设计上，不仅仅需要提供用户名+口令，同时设置了校验码，而且同时还增加了动态口令，通过短信接收验证码，以此来防止暴露非法破解登录，保证整个系统认证环节的安全性。密码提交和存储过程中，一律通过MD5 +salt加密，即使密码泄露也不会被解密。接口设计是整个系统通信的安全保障，为了防止外部人员恶意调用和窃取信息，我们采用了令牌机制保障每次通讯的安全性，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，然后在后续每次通讯传输过程服务端对token进行校验，充分保障了接口调用的安全。  
整个项目历时10个月开发完成，到目前运行稳定。通过用户一段时间的使用反馈，不论是PC，还是PAD和手机端，在任何环境下使用系统，基本没有信息泄露的情况发生。但是，一些用户反馈，手机登录需要时间较长，查询和保存老人档案信息有时候需要等待，经过分析，登录时间较长，由于登录需要对客户端对用户和密码信息进行客户端加密处理，加密算法耗费了移动端CUP资源，同时在服务端也对数据进行加密处理返回客户端token也消耗了不少时间。老人档案也是由于敏感信息加密的问题，耗费了CPU的处理时间，我们后面通过选择效率更高的加密算法改善了这个问题。  
实践证明，项目能够顺利上线，并运行稳定，使用良好，与系统在安全性和保密性方面设计密不可分。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的过程，我们接下来，还会继续不断完善系统安全方面的设计缺陷和不足，使整个养老平台更加安全好用。