医院移动业务平台中安全模式设计及应用*

徐 骁 李爱勤 陈敏莲 胡外光 胡珊珊

(湖南省儿童医院 长沙 410000)

〔摘要〕 以湖南省儿童医院为例，介绍医院移动业务平台中安全模式设计及应用，包括整体架构、安全接入设备实施方案、安全认证模式策略几方面，为安全部署远程办公、移动应用提供实施思路。

〔关键词〕 移动办公安全；加密通信；数据安全

〔中图分类号〕R-056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673-6036.2017.10.011

Design and Application of the Security Mode for the Mobile Business Platform of Hospital *XU Xiao, LI Ai-qing, CHEN Min-lian, HU Wai-guang, HU Shan-shan, Hunan Children's Hospital Information Center, Changsha 410000, China*

〔**Abstract**〕 Taking Children's Hospital in Hunan Province as an example, the paper introduces the design and application of the security mode for the mobile business platform of hospital from the aspects of the overall structure, implementation plans of security access equipment, security authentication modes and strategies, etc., and provides ideas for safely implementing remote deployment and mobile application.

〔**Keywords**〕 Mobile office security; Encrypted communication; Data security

1 引言

移动化办公是大型三甲医院提升院级管理效率和服务质量的有效手段，利用移动办公产品或者解决方案可以实现跨时间、跨地域、跨各类终端设备的无差别化日常流程事务处理，也能够为医生远程浏览病历资料、化验结果甚至书写患者病历提供操作通道。但是随之而来的安全隐患也日渐凸显，越来越多医疗数据泄露事件曝光以及针对医院核心业务服务器攻击都给医院移动应用安全保障水平提出更高的要求。

2 相关研究情况及移动业务平台设计需求

2.1 相关研究情况

2.1.1 国内医疗行业移动产品应用现状 移动化办公应用设计实施早已普及开展，如邵炜[1]从医院领导管理、员工服务、信息交流 3 个层面出发，对移动办公平台进行模型设计，基于 MVC 开发架构部署了一套医院移动化办公体系，以低成本的方式实现与院内其他业务系统的数据对接、能较好地满足各类不同类型智能终端。周毅[2]为解决原有医院办公自动化系统只限定于局域网的尴尬处境，为智能终端实施部署了基于 Java 开发 B/S 架构的移动办

〔修回日期〕 2017-07-12

〔作者简介〕 徐骁，硕士，发表论文 3 篇。

〔基金项目〕 湖南省科技厅重点研发计划（项目编号：2016JC2020）。

公平台，真正做到了在任何时间、任何地点开展任何业务工作。

2.1.2 针对移动办公安全进行研究 具有较为成熟的体系，大体可以划分为硬件部署解决方案和用户鉴别解决方案。在硬件方面，如徐俊[3]等对移动医疗的信息安全建设内容进行划分指定，分别从硬件安全、数据安全、应用与数据交换安全 3 个方面进行了简述，包含防火墙部署、防病毒网关配置以及漏洞扫描策略制定的硬件安全层面；结合数据安全备份、审计、分级的数据安全设计；最后在应用与数据交换安全层面介绍了一套基于令牌授权、解析管理平台得以实现用户身份认证用以保障移动通信安全。移动安全研究又大体可以分为硬件基础网络设备解决方案和用户身份识别两大主体方向：如刘峰[4]等人为有效隔离医保与医院网络、审计前置机的访问操作、提升整个网络抗攻击能力，采用部署了一套有效认证 + 访问控制的解决方案。通过安全网闸 TCP/IP 阻断医保和医院网络，利用安全网关为多元素认证机制提供硬件支持，终端客户端采用沙箱防护技术提供保护，最终为安全网络边界防护、多层次安全联动防护提供支持。而在身份认证识别方面集中以 CA 认证服务和电子签章为主，如申宝明[5]在其医院多个主要业务系统上，引入 CA 认证服务实现用户身份识别、数字签名、电子签章、时间戳等功能，从而达到权限授权、责任认定、信息保护等目的。李芳[6]等人为保障医疗行为过程中健康数据的不可篡改性和安全性，确保医疗数据的合法性以及对医疗环节责任的精确划分，引入数字认证、签章管理提升了医疗文书的规范性，为药品审方、处方点评提供依据，为医生护士实现自动化签章提高工作效率，强化医疗各环节质量控制、符合医院质量管理更高要求。除技术层面之外，传统隐私保护在我国法律原则在快速发展的移动医疗方面也已经捉襟见肘，在建立移动医疗信息医疗安全的同时，必将会有更加完善的政策和立法不断推出和建立，而认证和签章的引入带来的法律效益也正在日益凸显[7]。

2.2 移动业务平台安全设计需求

由于目前移动业务平台基于沙箱隔离客户端程序，利用远程桌面发布技术得以实现，同时为医院管理层提供办公应用和为医护人员日常工作提供支持。因此其移动安全模式设计应用应该从两个方面进行考虑，一是提供高效数据加密通信通道便于医院领导层进行日常化办公处理，另一方面能够满足不同需求的医护人员进行业务系统的操作，同时防止非法数据拷贝操作。因此架设安全模式应该同时基于基础网络设备和多重身份鉴别的组合模式[4]。

3 移动业务平台安全模式设计

3.1 整体架构

为保证医院移动终端设备访问医院业务系统和办公系统安全稳定，设计架构，见图 1。安全网关、移动终端、安全管理中心 3 部分共同构成移动平台安全接入网关方案。安全管理中心由安全管理中心服务器、安全管理中心控制台组成。通过与内网认证系统结合，为安全网关、USB – KEY 颁发数字证书，再由安全管理中心为安全网关及 USB – KEY 或者安全 SD 卡下发数据加密密钥、安全规则及防护策略，使业务终端与安全网关建立加密隧道以访问业务服务器。架构体系包含多因素身份鉴别是由身份认证和设备认证共同组成。其中，设备认证主要依靠客户端硬件特征提取模块和安全认证网关实现，安装授权过程中对硬件特征进行记录存储至安全认证网关，通过判断是否与该设备的设备证书中硬件特征相符合，用以判断设备合法性。而身份认证则是基于密钥和数字证书进行的双向身份识别认证，其原理是利用存储于安全网关和终端用户的数字证书等，通过反复比对各自生成的随机挑战值从而实现身份的有效性验证。针对医护员工日常工作范围和职责不同，需要为其权限进行较为精细管控，因此通过一整套数字 ID 认证授权管理系统实现其需求，其中包含的 RBAC 管理系统能够很好地基于不同的用户角色实现用户访问控制的管理、配置和维护等工作。

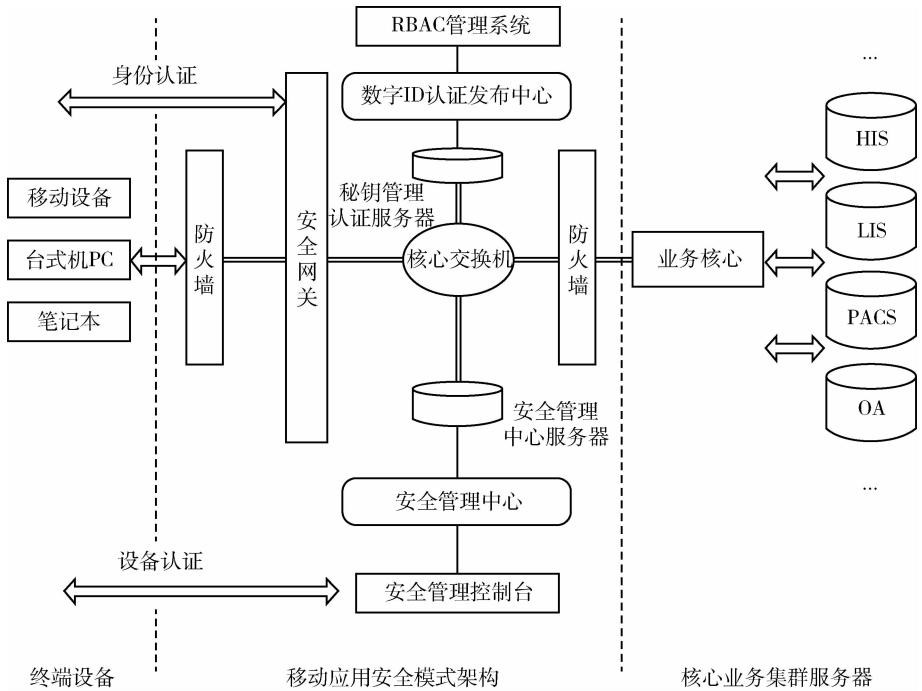

图 1 移动应用安全模式架构设计

3.2 安全接入设备实施方案

安全网关作为用于解决公网用户安全接入内网、网络通信安全保密等一系列问题的网络设备，具有一定通用性。通过在原有网络拓扑上新增加安全网关设备，机密数据在网上进行加密传输确保其安全性，见图 2。配备的安全网关设备同时还需要支持如 LocalDB 认证、第 3 方认证、数据同步、数字证书等多种身份识别方式和衍生功能。同时可以针对资源控制实现动态、静态以及自定义的 ACL、隧道保护以及资源访问监视等功能。依据不同的网络实际情况动态选择接入方式为：旁路接入、虚拟网桥接入或者路由接入等。此外，安全网关设备还需要配备相应的证书加密、隧道加密算法以及内嵌防火墙功能，支持双机热备和自动同步也是其安全性保障的重要功能。湖南省儿童医院目前投入使用的安全网关设备是以以太网作为通信协议，物理接口支持：100Base－T，1000Base－T，1000Base－X，LC 接口、单/多模；SC 接口、单/多模等接口方式，转发速率百兆双向处理达到 80Mbps，千兆下双向处理达到 750Mbps，基本能够满足移动业务平台的通信、安全设计要求。

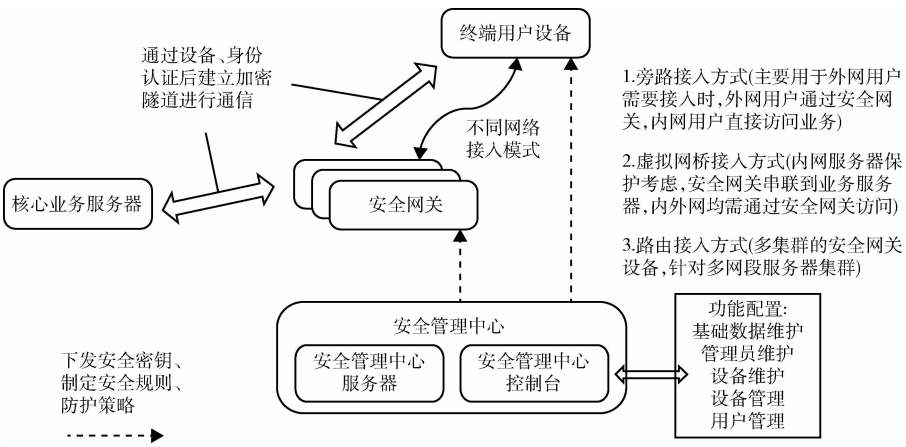

图 2 安全网关工作模式

3.3 安全认证模式策略

3.3.1 *移动安全解决方案认证策略* 由终端设备认证和用户身份认证两个部分组成。其中远程移动终端作为远程接入的源头和发起者，其安全性直接关系到数据传输的安全，乃至内部应用系统的安全。因此本项目移动终端设备接入时需要判断移动终端设备的身份，只有合法注册的设备才可以远程接入。其中设备认证的工作模式即在终端客户端软件中安装硬件设备特征读取模块采集底层硬件信息，安全网关设备将根据所获取的硬件特征信息和该设备的设备证书内容比对，从而验证核实该设备的合法性，一旦验证成功，则可以判断该设备不存在伪造信息，是该系统中注册的合法终端，彻底杜绝不经过注册的非法终端接入内网网络，确保移动终端接入的安全，从源头杜绝威胁。

3.3.2 *客户端使用者身份合法性验证* 基于密钥、数字证书实现的一种双向验证，通过服务器端配置的密钥管理和数字证书发放系统一并组成实现。终端用户和安全网关之间将通过随机数种子和 CA 中心发布的数字证书已经密钥对在终端用户和安全网关设备之间多次验证比对，最终建立起可信的数字通信隧道，其工作模式，见图 3。

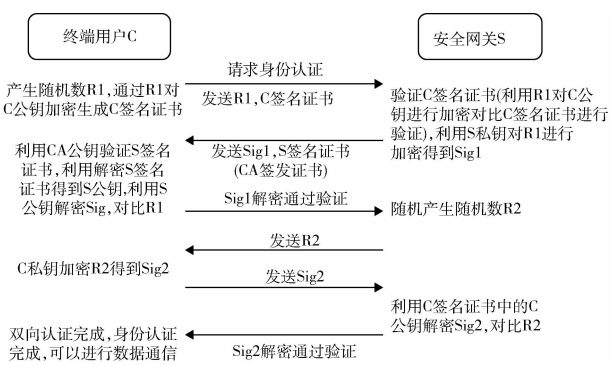

图 3 双向多次握手身份认证模式

3.3.3 *用户身份认证* 认证客户端中使用 TF 卡或是软件方式存储数字证书供用户使用，而在认证服务器上采用 USB Key 和独立密码机组合的方式，由专职密保人员进行管理和使用。在我院的实施实际情况中，移动智能设备上，用户认证采用密钥认证系统提供的用户公钥/证书和私钥完成强双向身份验证；医院外部网络使用 PC 机远程访问内部业务系统时，则采用 USB Key 保存用户公钥完成验证；移动 PAD 设备则采用安全 TF 卡硬件方式和软件方式相结合的方案用以保存用户公私钥。所有用户身份认证过程中使用到的认证设备、公钥证书都是由底层认证库提供的服务完成，其证书的注销、过期、有效性验证都是在底层认证库内容，而对用户是不可见的。

4 结语

以湖南省儿童医院移动办公和远程业务平台部署实施过程中的安全解决方案为实例，对其主要网络安全接入网关部署和多因素组成的用户认证方案进行介绍。该安全设计模式结合目前两大主流移动安全解决方案，为医院移动化终端设备远程访问内部网络提供一个安全可靠的部署、实施方案。利用原有网络架构上增加部署安全网关硬件设备和密钥管理、认证服务器实现多方式的用户身份识别，从而构建起一套可信、高效的移动化办公应用安全实施方案。一方面为提升院内外网络通信安全水平提供一定的实践经验和理论架构，另一方面也是 CA 数字认证、安全网关硬件设备部署、用户身份授权管理平台的综合应用在医疗信息化实际应用，具有一定理论和现实意义。

参考文献

1 邵炜. 医院移动办公应用模型及架构设计［J］. 中国数字医学，2015，10（4）：57－59.
2 周毅. 移动办公平台在我院的应用［J］. 中国医疗设备，2016，31（1）：151－152.
3 徐俊，姚华彦，何萍，等. 移动医疗在医联应用中的信息安全管理［J］. 中国数字医学，2015，10（8）：8－10.
4 刘锋，吴东东，姬晓波，等. 医疗网络与外部网络信息安全交互方案设计［J］. 中国数字医学，2015，10（10）：96－98.
5 申宝明，徐浩，辛海燕，等. 医院信息化中的数字认证设计与实施［J］. 中国医疗设备，2015，30（5）：83－85，32.
6 李芳，王玮. 数字认证与签章在医院电子病历系统的深化应用［J］. 中国数字医学，2016，11（2）：109－110，113.
7 余文清，邓勇. 移动医疗信息安全保护与法律监管机制建构探讨［J］. 中国医院，2016，20（9）：53－56.