基于无线应用协议的医院移动电子商务安全问题与对策

凌科峰 胡珊珊 黄 海

（湖南省儿童医院数据管理部 长沙 410007）

〔摘要〕 介绍基于无线应用协议的医院电子商务工作模式和安全需求，以期为移动电子商务系统提供整体安全架构。从接入终端层、通信层、网关协议层、应用服务层 4 个方面分析医院常见的移动电子商务安全问题，提出医院移动电子商务安全技术方案。

〔关键词〕 医院；终端安全；移动电子商务

〔中图分类号〕 R－056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673－6036.2016.07.011

Security Problems of Hospital Mobile Electronic Commerce Based on the Wireless Application Protocol and the Countermeasures

LING Ke－feng, HU Shan－shan, HUANG Hai, Department of Data Management, Hunan Children's Hospital, Changsha 410007, China

〔**Abstract**〕 The paper introduces the working mode and security requirements of hospital electronic commerce based on the wireless application protocol and aims to provide an overall security framework for the mobile electronic commerce system. It analyzes common security problems of mobile electronic commerce in hospitals from four aspects, namely the access terminal layer, communication layer, gateway protocol layer and application service layer, and proposes the technical solution for the security of hospital mobile electronic commerce.

〔**Keywords**〕 Hospital; Terminal security; Mobile eletronic commerce

1 移动电子商务的定义及其在医院环境下的工作模式与安全架构

1.1 定义及工作模式

移动电子商务是利用移动电话、数据采集和手持计算机等多种无线终端的电子商务方式。它将互联网、移动通信、短距离通信等信息处理技术完美结合，使人们能够随时随地实现线上、线下购物和交易、在线电子支付以及各种交易、商务、金融及相关综合服务活动。移动电子商务在许多领域悄然兴起，特别是在医院，近年来发展很快。基于无线应用协议的医院移动电子商务工作模式，见图 1。

图 1 基于无线应用协议的医院移动电子商务工作模式

在移动端的患者或家属进入一个网址，通过无

〔修回日期〕 2016－05－27

〔作者简介〕 凌科峰，硕士，工程师，发表论文 3 篇。

线网络发送到网关，网关将无线应用协议转换为超文本传输协议和服务器通过互联网传输请求送到医院，经过医院服务器处理后，结果被返回到网下，网关到超文本传输协议数据转换为移动终端的移动电话屏幕，以实现医院移动电子商务交易。在这个过程中，经常会遇到移动端丢失或被盗、拒绝交易、信息披露等问题，严重阻碍了医院移动电子商务的发展。为此对医院移动电子商务系统安全需求。

1.2 安全需求架构

（1）认证患者的身份。通过身份识别与鉴别，可以确认信息发送者和接收者的身份。（2）信息收发不抵赖。发送方和接收方对已发出或已收到的信息不可抵赖。（3）患者完整的信息。数据在传输存储过程中不会受到非法的修改、删除和重放。（4）患者数据的机密。传送过程中的数据确保不被泄露，且通过加密使未被授权的人无法读懂数据。实施这些安全要求，不仅仅是通过一种技术，它是多种技术的组合、多层次的。基于这些结果通过基于无线应用协议的医院移动电子商务模式，提出了医院移动电子商务系统的安全体系结构：网关协议层安全（以常见安全机制为主，如基于 Wireless public key infrarure 的安全机制）；终端接入层安全（以普通手机、智能手机终端安全为主，如 JAVA 版收集、带 OS 的手机）；应用层服务安全（以常见安全应用机制为主，如基于 Wireless public key infrarure 协议的安全）；通信链路层安全（以陆地蜂窝移动通信系统通信安全为主，如 GSM/CDMA/GPRS 等通信网络）。

2 医院移动电子商务存在的安全问题

2.1 网络网关协议层

它是一家医院的移动电子商务服务网关和通信协议的集合，是网关协议层的主要任务。本文讨论了无线应用网关协议，通过它提供接入到增值的应用，是移动终端和应用程序之间的必要协议的转换。在这个过程中由于无线传输层安全和安全套接字层不兼容，医院服务器和无线应用程序之间的数据通信，对无线应用网关的浏览器将在一段时间内以明文的形式存在，使它成为一个安全漏洞。

2.2 网络终端接入层

终端接入层是终端硬件环境、软件环境以及医院移动电子商务应用的支持。它是终端服务的交互界面。这里的移动终端是智能手机和 JAVA 的手机操作系统，基于移动终端用户，地面通信系统，但在患者移动终端的用户通常具有以下安全问题：（1）患者识别模块卡复制。在患者识别模块卡中的重要信息是被他人非法使用的，伪装成合法用户参与移动电子商务活动，进行欺诈或攻击。（2）患者的移动终端处理能力弱。移动通信终端在交易业务和用户的移动支付，低功耗的硬件资源的发生率低，存储容量和数据传输速度受地理位置限制，速度较慢，存在较大的限制和隐患。（3）患者的移动终端保护能力弱。移动终端用户本身的特点是容易受到木马病毒感染、病毒入侵，移动终端用户的数字证书、机密数据等的破坏、访问等，在未经授权的访问或假交易中发生。

2.3 网络应用服务层

医院移动电子商务服务是应用服务层提供给患者或家属的任务，医院、移动电子商务企业不能被拒绝和认证的特点是需要考虑的安全性。由于不具有不可否认的机制，一旦交易被拒绝的网上交易，则没有已签署的记录作为仲裁的基础，患者的用户名和密码应用服务层认证机制是基于共同的认证机制，但较弱的安全性导致非法窃取患者的帐户和密码伪造患者身份。

2.4 网络通信链路层

通信链路层是指可以用来为医院移动电子商务提供所有服务的各种通信网络。因为在无线电波传播和无线通信网络中的交易数据和敏感信息不受任何时间和地域限制，任何人都可以得到，导致可能的安全问题如下：（1）在医院通信服务网络或主机干扰、网络信息单元重复传输、合法数据不能

及时传递、合法用户不能正常接受网络服务的情况下，拒绝服务攻击。（2）当非法用户拦截一个网络或一个合法的患者用户足够的信息，通过假冒进行欺骗。（3）通过不断截获患者移动终端与网络、基站间交换的信息，非法患者用户可以轻易分析合法患者用户身份。（4）由于非法患者用户对数据进行修改、插入、删除，使数据的完整性受到威胁。

3 基于无线应用的医院移动电子商务安全解决方案

3.1 安全模型

本文从以上 4 个方面详细阐述了目前常见的医院移动电子商务安全问题，需要从整体上解决。建立无线的公开密钥系统，在无线网络环境中使用数字证书和公钥，见图 2。认证中心到医院服务器、无线终端、无线网关的颁发证书，交换证书。而当事人的身份和安全的关键是由第 3 方认证中心或运营商管理，通过其证书制度来保证。

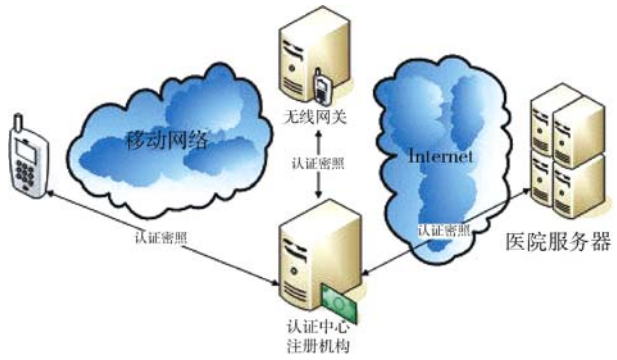

图 2 基于无线公开密钥基础设施的端到端安全模型

3.2 无线网关

医院通过移动用户终端与服务器之间的加密和数字签名技术的使用，以及无线公钥基础设施提供的密钥管理和数字证书服务，以实现端到端的真正安全。医院在移动端和服务器端都设置了相应的程序，这些程序可以对数据进行加密，以消除标准的无线应用协议在安全关的模式。然而，医院应用层安全模型对移动终端增加了额外的负担，建议只对一些关键数据进行加密，以减少无线应用协议网关优化的损失。

3.3 通信传输

医院可以使用无线传输层安全协议，提供通信数据的保密性，同时进行患者身份验证，从而保证医院通信系统的安全性。数据的保密性主要是通过建立一个加密信道来实现的。首先，医患双方交换了信息，对主密钥进行预协商和必要的加密参数，然后使用预主密钥，和一个加密参数计算的主键。最后，在握手验证过程中不受干扰，医患双方使用前的加密算法和共享密钥对通信的实际内容进行加密。无线传输层安全协议识别依赖于证书的实施，目前支持无线传输层安全协议的证书和 X. 509 证书。客户端和服务器存储其数字证书，需要验证和将服务证书发送给客户端，患者客户端验证，客户端证书发送一个消息返回服务器确定对方的身份，在安全的通信过程中完成的。数据完整性是通过使用消息验证码物理地址来实现的。接收器接收数据，首先用私钥解密，然后物理数据源地址运算，连接获得的值与文献报道的实验结果数据进行检查，如果没有可以认为在传输过程中的数据被修改，需重复操作。

3.4 应用服务

网上交易行为不能被否认，主要依赖于作为仲裁的基础上签署的记录，客户端和服务器端都需要使用其签名密钥来签名交易信息。具体操作由移动客户端计算数据的物理地址，根据数据格式的应用要求，然后将私钥计算数字签名并发送出去，将服务器端提取的数字签名并存储。而在服务器端使用无线应用协议，开发签名功能组件，该功能将显示文本的签名，要求用户确认，签名数据完成后，签名和数据被发送，客户端根据需要存储签名。

3.5 移动终端

无线身份模块可以在普通手机用户识别模块卡上，集成到无线身份识别模块卡，该卡能防篡改，存储密钥和安全信息，在现有硬件条件下可以快速

完成无线传输层安全协议 3 级加密，签名密钥设备以毫秒为单位，在无线传输层安全协议，主要用于握手时加/解密操作，保证长期无线传输层安全协议会话安全，客户端身份验证和数字签名。

4 结语

随着科技的发展，医院移动电子商务已初具规模，其安全问题也亟待解决。从接入终端层、通信层、网关协议层、应用服务层 4 层分析了医院移动电子商务的安全问题。在此基础上提出了一种基于无线传输层安全协议的医院移动电子商务安全解决方案，可以为医院服务器提供保密、完整、不可否认的识别服务。

参考文献

1 秦成德，王汝林. 移动电子商务［M］. 北京：人民邮电出版社，2012：223 - 227.

2 吴民. 移动医疗的应用［J］. 医学信息学杂志，2012，33（11）：2 - 5.

3 吕晓娟，仇保跃，王晓勇，等. 数字化医院建设热点难点分析［J］. 医学信息学杂志，2013，34（5）：21 - 24.

4 徐洪峰，徐曦，曾杰. 移动电子商务安全问题研究［J］. 计算机技术与发展，2011，21（11）：237.

5 贾末，王永刚，沈韬，等. 医院信息系统性能优化策略探讨［J］. 医学信息学杂志，2014，35（9）：28 - 31.

6 赵长超. WPKI 在移动电子商务中的研究和实现［D］. 济南：山东大学，2011：26 - 29.

7 姚志洪. 跨入移动健康时代［J］. 医学信息学杂志，2014，35（5）：2 - 7，24.

8 郑西川，孙宇，于广军，等. 基于物联网的智慧医疗信息化 10 大关键技术研究［J］. 医学信息学杂志，2013，34（1）：10 - 14.

9 吕福春，陈特放. 基于 WAP 的移动电子商务安全研究［J］. 福建电脑，2011，（12）：15 - 16.

10 张海燕. 移动商务的安全技术研究［D］. 长春：吉林大学，2012：25 - 27.

（上接第 46 页）

5 结语

在未引入安全机制的 PACS 中加入数字水印和数字签名技术能够解决安全性问题。数字水印技术能够保护医学图像数据的完整性，任何人不能对图像进行篡改和替换；水印也由于其透明性，攻击者不易发现其存在，同时也不影响医生对医学图像进行判断；数字签名技术能够同时保障医患双方的利益，发生争端时得到公正的仲裁。虽然数字水印和数字签名技术的引入在一定程度上降低了工作效率，但其提高医学图像保存、传输、显示的安全性，为远程医疗的积极发展提供了较好的保障。

参考文献

1 梁思宇，李继宏. 关于 PACS 与 HIS 的协同问题研究［J］. 中国医院管理，2010，（5）：70 - 71.

2 杨义先，钮心忻. 数字水印理论与技术［M］. 北京：高等教育出版社，2006.

3 J Fridrich，M Golijan，R Du. Distortion - free Data Embedding for Image［C］. Proc. 4th Information Hiding Workshop，Pittsburgh，Pennsylvania，2001：25 - 27.

4 刘瑞祯，谭铁牛. 数字图像水印研究综述［J］. 通信学报，2000，21（8）：40 - 49.

5 顾成喜. 一种改进的数字图像置乱方法［J］. 计算机仿真，2011，28（1）：261 - 264.

6 李子臣，杨义先，吴伟陵. 一类基于数字签名的密钥认证方案［J］. 电子学报，2000，28（4）：1 - 2.

7 郭小涛. 面向医学对象的无损数字水印系统的研究［D］. 上海：上海交通大学，2008.