医疗物联网安全风险及安全控制策略研究

陆向艳　张 超　肖连禹

（广西大学计算机与电子信息学院 南宁 530004）

摘　要　医疗物联网数据和系统的持续运行价值吸引力巨大，逐渐成为网络黑客攻击的重要目标。文中分析了医疗物联网的分层体系结构和各层次面临的安全风险，提出了医疗物联网的安全控制策略。研究旨在提高医疗物联网安全，为保护医疗数据安全和保证医疗系统服务持续性提供参考方案。

关键词： 医疗物联网；安全风险；安全控制策略；安全漏洞；感知层安全

中图分类号　TP393.0

Research on Security Risk and Security Control Strategy of Medical Internet of Things

LU Xiangyan，ZHANG Chao and XIAO Lianyu

（School of Computer and Electronic Information，Guangxi University，Nanning 530004，China）

Abstract　The data and continuous operation of the application of medical Internet of Things are attractive , it has gradually become an important target of network hacking. This paper first analyzes the layered architecture of medical Internet of Things, then analyzes the security risks faced by each layer, and finally puts forward the security control strategy of medical Internet of Things. The purpose of this study are to improve the security of the medical Internet of Things and provide a reference scheme for the protection of medical data and the continuity of medical business.

Key words　Medical Internet of Things，Security risk，Security control strategy，Security vulnerability，Perceptual layer security

0　引言

随着医疗物联网的广泛应用，医疗系统中如血氧传感器、心电图传感器、核磁共振传感器、体温传感器等医疗传感设备越来越多[1]，各种智能诊疗、远程医疗、远程健康检测等医疗应用系统[2]不断被开发和应用。由于医疗物联网中蕴含着丰富的病患隐私数据，因此医院诊疗系统与患者生命健康息息相关，数据和系统持续运行价值吸引力巨大，逐渐成为网络黑客攻击的重要目标[3]。相对于传统网络，医疗物联网中的传感设备、网络、平台和应用类型更加多样和复杂，使医疗物联网面临着巨大的安全挑战。

1　医疗物联网概述

1.1　医疗物联网

医疗物联网[4]是由医疗传感设备、物联网、云平台和医疗应用组成的复杂系统，系统应用医疗传感设备采集医疗数据，通过物联网将医疗数据传输到云平台进行存储，使用医疗应用系统对云平台的医疗数据进行分析处理，从而实现医疗检查、检测、诊断、护理和管理等各项医疗工作的智能化实施。医疗物联网的应用提高了患者的就医效率、医疗实施的精准度，降低了医务人员工作强度，提升了临床医疗服务的质量。

1.2　医疗物联网体系结构

医疗物联网是物联网技术在医疗领域的应用，与其他物联网应用相比，医疗物联网的主要区别是传感设备和应用系统需求是针对医疗领域的。按照功能划分，医疗物联网可以划分为4个层次，如感知层、网络层、平台层和应用层（见图1）。

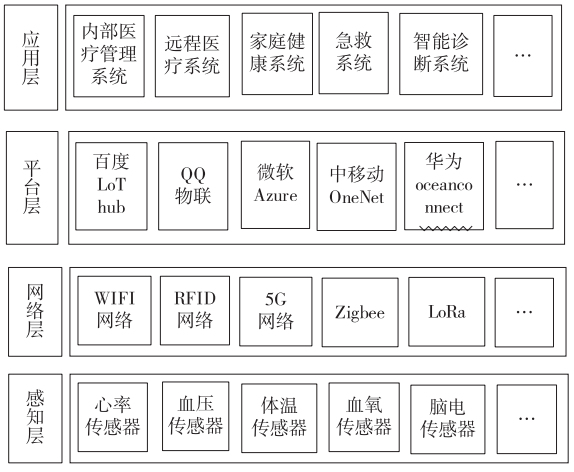

图1　医疗物联网的整体架构

（1）感知层。感知层是医疗物联网的基础，其功能是完成医疗数据的采集，主要由各种不同类型的智能医疗传感

作者简介：陆向艳（1973—），硕士，副教授，研究方向为信息安全。

器、感知协议及所采集的医疗数据组成。(2)网络层。网络层功能是连接物联网设备,实现感知层物理设备的互联和信息共享,主要由移动互联网(WIFI网络、RFID网络、5G网络、Zigbee、LoRa、NB-IoT等)和传统互联网组成。(3)平台层。平台层是医疗物联网的中心枢纽,其功能是实现底层终端设备的管理和监控及为上层提供统一应用接口,平台层一般由大型云平台服务运营商构建,能为医疗机构提供简化的物联网应用服务。(4)应用层。主要由医疗机构各种应用系统(如老年痴呆监护系统、肝癌远程诊断系统等)组成,实现医疗诊断、治疗、监测、护理和管理等各种医疗事务的智能化管理。

2 医疗物联网面临的安全风险

医疗物联网包含丰富的医疗隐私信息,这些隐私信息的不当使用将对患者的生活、生命健康等方面造成影响。而基于医疗物联网医护系统的持续性和实时性意义重大,若被黑客攻击造成手术中断等问题,则可能会危及患者生命。

2.1 感知层安全风险

为了采集数据,医疗物联网部署了众多不同的医疗感知设备,这个层次存在设备漏洞、设备暴露、弱口令和私自接入等问题,这些安全问题容易被利用以攻击物理层,从而造成医疗隐私数据泄露、篡改和设备可用性受损,导致医疗事务无法开展等。

2.1.1 设备漏洞

感知层部署着不同厂商、不同类型、不同型号的医疗设备,由于缺乏生产厂商安全人员及设备安全成本等,很多设备在设计上存在安全漏洞,甚至有些老设备没有安全设计。一般情况下,医疗设备使用周期较长,生产厂商补丁更新较慢甚至不再更新,导致漏洞难以修复。设备漏洞可以被黑客利用来进行非授权访问,或植入木马对设备进行长期控制,导致患者医疗数据的机密性、完整性和可用性遭受破坏,对患者隐私数据和生命安全造成严重影响。

2.1.2 设备暴露

大部分医疗感知设备分别安装在不同的物理环境,这些环境缺乏物理访问控制机制,很容易遭受实体攻击,导致信息泄露和篡改或可用性遭受破坏。

2.1.3 设备弱口令

由于使用者安全意识缺乏,终端医疗感知设备往往存在弱口令甚至无密码问题,使得攻击者可以采取暴力破解等方式登录设备,导致数据隐私遭受机密性、完整性破坏或者被植入病毒或木马,引发一系列安全问题。

2.1.4 设备私自接入

由于缺乏相关物理安全管理控制措施及人员缺乏安全意思,感知层设备未经授权接入医疗物联网的情况时有发生,从而使这些设备不受安全管控,成为攻击的突破口,导致医疗物联网遭受入侵和破坏。

2.2 网络层安全风险

医疗物联网网络层负责通信过程,由于物联网网络结构的复杂性,不仅面临传统互联网的所有安全问题,还因无线网络协议的多样性和相对简单性,面临更复杂的安全问题,RFID,wifi,Zigbee等无线网络均存在相当多的安全问题[5]。

(1)RFID网络安全。RFID网络存在嗅探、跟踪、拒绝服务、欺骗、否认、插入、重放、篡改等攻击。(2)wifi网络安全。wifi网络存在未经授权的访问、暴力破解、数据嗅探、病毒和恶意软件攻击。(3)Zigbee网络安全。Zigbee网络存在设备劫持、Zigbee蠕虫、远程代码执行等攻击。(4)明文传输。由于无线物联网设备计算能力和存储能力的限制,无线协议在进行数据传输时往往仅采用简单加密甚至明文传输,传输的数据很容易被窃取、破坏或干扰。

2.3 平台层安全风险

借助云平台,医疗物联网海量的数据可以上传到云端进行存储和分析,所依托的云平台的安全性影响着医疗数据的安全性。平台层安全问题即为云平台的安全问题,主要包括非授权访问、恶意代码攻击、数据库安全、服务器安全和接口安全等。

2.4 应用层安全风险

医疗物联网应用层是各种医疗应用程序,以为不同类型的患者和医疗工作者提供服务,通常是APP或web应用程序。医疗应用可以访问患者的隐私数据,对攻击者而言具有巨大的吸引力,其主要面临的安全问题是非授权访问、非法入侵、身份假冒、网站篡改、病毒入侵、恶意代码攻击、数据泄露、网络钓鱼等。

3 医疗物联网安全控制策略

医疗物联网各层次都有相应的安全风险,从医疗机构角度看,平台层安全由云服务提供商来提供,因此这个层次主要需选择提供可靠安全服务的云服务提供商。而对于其他层次的安全问题需采取以下安全控制策略。

(1)构建医疗感知层设备台账。由于感知层设备是受攻击的重点对象,因此需要构建医疗物联设备台账,了解每台接入设备的基本情况,通过全面的设备资产识别,记录设备类型、型号、安装位置和生产日期、操作系统等信息,建立设备入网、退网、更新机制。(2)定期对医疗感知层设备进行漏洞扫描和物理安全检查。根据医疗物联网设备台账,定期进行设备漏洞扫描,安装漏洞补丁。定期进行设备物理安全检测,消除物理安全隐患。(3)设置高强度设备登录密码及定期更换规范。为了预防暴力破解,应制定高强度设备安全登录密码设置规范,检测并消除设备弱口令,定期更换设备登录密码。(4)建立高强度的数据网络传输加密模式。医疗物联网主要采用无线网络进行数据传输,为保证医疗数据网络传输的安全性,预防网络传输中的数据嗅探、非授权访问、篡改等攻击,需建立安全可靠的高强度数据传

(下转第138页)