

简译版

医疗物联网 (IoMT) 问题

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	IoT Security Meets Healthcare - What You Need to Know		
原文作者	Seema Haji	原文发布日期	2019 年 3 月 13 日
作者简介	Seema Haji 负责 Splunk 公司的产品营销，以及其物联网 (IoT) 和业务分析解决方案。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/iot-security-meets-healthcare-what-you-need-know		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antivy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

医疗物联网 (IoMT) 问题

Seema Haji

2019 年 3 月 13 日

就像智能设备渗透并帮助工业运营和企业一样，物联网 (IoT) 已经在医疗领域占据了一席之地。医疗物联网 (IoMT) ——医疗 IT 网络中的联网设备 and 应用——改变了医疗机构和整个行业的未来战略。它带来了全新的效益，影响诊断、治疗和患者健康管理，同时又能降低成本。本月初，在奥兰多举行的 HIMSS 会议上，与会者全面展示了上述优势。（译者注：HIMSS，Healthcare Information and Management Systems Society，美国医疗信息和管理系统协会。）

但是，IoMT 带来上述优势的同时，也带来了很大的风险。与任何环境一样，更多联网设备意味着更大的攻击面。事实一再证明，IoMT 安全漏洞为医疗机构带来了严峻挑战和重大损失。因此，对于医疗机构来说，IoMT 安全不是可选项，而是必选项。

目前的问题

随着针对医疗机构的网络攻击日益普遍，医疗服务提供商开始受到更严格的审查。2017 年，“魔窟” (WannaCry) 勒索软件造成了重大的损失——医疗机构的管理系统和设备受到感染，医疗服务中断，导致患者面临生命危险。英国国民医疗服务体系 (NHS) 受到的影响最为严重，一度回归到纸笔办公。据报道，此次攻击给 NHS 带来近 1 亿英镑的损失，迫使其取消了 1.9 万次预约。有意思的是，NHS 甚至不是攻击者的直接目标，而只是附带损害。想象一下，如果它是攻击者的直接目标，是被有针对性地、精确攻击的，结果又会如何呢？

这一事件促使医疗设备制造商发布了安全公告。美国食品和药物管理局 (FDA) 也发布了安全建议。但是，这些安全公告和建议只是指南而非法定要求，没有强制性。即使不遵守这些公告和建议，也不会受到任何惩罚。因此，许多制造商并未在合同中添加有关医疗设备安全性的规定。最终，使用这些设备的医疗机构会面临艰难的境地——承受着数据泄露和网络攻击的风险和后果。

老旧设备漏洞

这些安全问题的根源在哪里呢？医疗机构认为，他们的大多数安全问题源于老旧设备的

漏洞而非其运行——这是一个值得商榷的话题。但是，与硬件不同，数字技术确实是日新月异的。如果医疗机构无法及时更新医疗设备的系统和软件，就会面临风险，危害患者的生命安全。

此外，制造商不允许客户对设备进行故障排除或打补丁。如果客户这样做，就会被取消保修。这些设备通常未进行加密，而且使用硬编码的凭证。更糟糕的是，医疗机构的安全控制措施也不到位。

最佳实践很重要

除了与制造商相关的安全问题，医疗机构的失误也会带来风险。根据最新的 KLAS/CHIME 基准报告，安全差距日益扩大、资产的可见性不佳是最严重的问题。

解决 IoMT 安全问题的关键在于制定集中的安全策略，以预测和预防潜在威胁，并在整个运营过程中弥补安全差距。这项工作的核心是部署强大的技术，以便管理所有联网设备的数据、隐私和编排。此外，回归基础的安全措施也很重要——因为我们无法改善已经被攻破的系统。医疗机构应确保 IT 系统全天候运行，保护其免受安全威胁，并将其设置为“可扩展的”，这些问题都不容小觑。

医疗机构该怎么做到这些呢——主要在于有效使用数据。IoMT 设备生成的数据可用于监控、创建基准、为 IT 设置提供更好的支持等。医疗机构更清晰地了解内部 IT 系统的运作，有助于改善患者的治疗效果；关注异常行为有助于防止诈骗；监控 HL7 数据传输则有助于避免计费错误。（译者注：HL7，Health Level 7，标准化的卫生信息传输协议，是医疗领域不同应用之间电子传输的协议，HL7 汇集了不同厂商用来设计应用软件之间界面的标准格式，允许各个医疗机构在异构系统之间进行数据交互。）

诸如 IoMT 这样的新技术，对任何领域来说都是一把双刃剑。但是，安全责任不只在制造商，医疗机构也应该主动管理和保护他们的环境。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：<http://www.avlsec.com>