医院近源网络攻击风险分析及对策建议*

孟晓阳 杨 巍 张 楠 孙国强

（北京协和医院 北京 100730）

〔摘要〕 **目的/意义** 分析医院面临的近源网络攻击风险，提出对策建议。**方法/过程** 结合实际工作经验，先以近源网络攻击者视角对医院网络架构、现场物理环境、人员行为等方面进行风险分析，再以防守者视角，结合合规要求和技术实践做法，提出对策建议。**结果/结论** 识别出无线局域网破解、有线网络插口暴露、自助机配置不当、投毒与钓鱼、敏感信息泄漏 5 类主要风险，提出加强 Wi－Fi 管理、联网终端准入全覆盖、多部门协作管理自助机设备、内网终端禁用移动存储介质、网络安全教育应与时俱进 5 条防范建议。

〔关键词〕 医院网络安全；网络攻防；渗透测试；近源网络攻击

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2024.09.014

Risk Analysis and Countermeasure Suggestions for Hospital Near－source Cyber－attacks

MENG Xiaoyang, YANG Wei, ZHANG Nan, SUN Guoqiang

Peking Union Medical College Hospital, Beijing 100730, China

〔**Abstract**〕 **Purpose/Significance** To analyze the risks of near－source cyber－attacks faced by hospitals, and to propose countermeasures. **Method/Process** Combined with practical work experience, the risk analysis of hospital network architecture, on－site physical environment, personnel behavior and other aspects is carried out from the perspective of near－source cyber－attacker. Then, from the perspective of defender and in combination with regulatory requirements and technical practices, countermeasures and suggestions are proposed. **Result/Conclusion** 5 main risks are identified, including wireless LAN cracking, exposed wired network sockets, improper configuration of self－service machines, poisoning & phishing, and sensitive information leakage. 5 preventive suggestions are put forward, including strengthening Wi－Fi management, full coverage of network terminal access, multi－department collaboration in self－service device management, disabling mobile storage media on Intranet terminals, and updating cyber－security education.

〔**Keywords**〕 hospital cyber security; cyber－attack/defense; penetration testing; near－source cyber－attack

1 引言

经过多年的网络攻防实战和安全合规性检查，各大医疗卫生机构大多已形成较为完善的网络安全防护体系，特别是针对外部威胁，已在互联网边界部署入侵检测、防火墙、流量溯源、蜜罐等多维度安全设备，攻击者正面突破越来越困难。然而内部区域通常被认为在物理环境上可控，会更多地考虑内部人员使

〔修回日期〕 2024－05－06

〔作者简介〕 孟晓阳，高级工程师，发表论文 20 余篇；通信作者：孙国强。

〔基金项目〕 中国医学科学院医学与健康科技创新工程项目（项目编号：2022－I2M－1－019）。

用方便性因素，安全问题容易被忽视。近源网络攻击是指攻击人员靠近或进入目标单位建筑内部，利用各类无线通信技术、物理接口和智能设备渗透攻击的方法[1]。这种攻击方法在实战中越来越常见，防守方应引起重视。医院中大部分区域是开放的公共场所，每天有大量患者及家属进入，攻击者可以近距离接触连通医院信息系统的终端、有线网口、Wi－Fi。这种场景暴露面大，近源网络攻击更容易得手。针对以上问题，笔者组织并参加过两次针对医院的近源攻击演练。本文旨在基于实践工作经验，全面分析医院普遍存在的近源网络攻击风险，并提出对策建议。

2 风险分析

2.1 无线局域网破解

随着移动医疗设备的广泛应用，无线局域网已成为医院不可或缺的基础设施。与有线网络不同，无线网络接入不需要固定的地点和可见的物理线路，更加开放且隐蔽，更易存在潜在的安全风险点。一是 Wi－Fi 常见的加密方式均不安全，有线等效加密（wired equivalent privacy，WEP）存在漏洞协议，只要获取足够多的数据包（一般需要 1 万以上）就可反推出加密信息[1]；Wi－Fi 保护接入（Wi－Fi protected access，WPA）/WPA2 也是可以被监听的，攻击者可以截获正常客户端与无线接入点（access point，AP）之间的握手包，修改后重放，进行密码暴力破解[2]。攻击者还可利用专业设备或软件在医院附近截获无线信号，只需简单的密码破解就可以进入内部网络。二是医院内部员工为了方便连接移动设备，利用办公电脑私自建立 Wi－Fi 热点的情况并不少见，攻击者一旦破解了该热点密码，就拥有了办公机同样的访问权限，直通内网。三是智能手机用户普遍使用的“Wi－Fi 万能钥匙”等软件也可能泄漏个人无线网络密码[3]。这些软件在用户连接网络时会将密码存储在云端，并在其他用户请求连接相同网络时分享该密码。这种密码共享机制可能导致医院内部网络的密码泄漏给外部攻击者。

2.2 有线网络插口暴露

医院建筑内有大量有线网络插口暴露在患者可以接触到的公共区域，如走廊、候诊区等，存在被盗用的风险。在已发生的安全事件中，有攻击者通过拔掉自助机或其他设备的网线，将自己的电脑接入医院内网，进行商业统方等违法操作，造成医院内部数据泄漏。演练过程中，攻击者潜入了一间已结束出诊的诊室，成功避开了院方在公共区域的巡查，并顺利接入有线网络。

2.3 自助机配置不当

为了提升患者就医体验，现代医院普遍配置自助机设备，这些设备涵盖挂号、缴费、检查检验预约、病历打印等多元化业务功能，都要部署在内网环境，访问核心业务系统。由于这些自助机设备均由患者自己操作使用，缺少监管，若配置不当，可能带来网络安全风险。具体而言，如果自助机设备的软件容错能力不足，攻击者可能通过输入异常查询值、高频点击等方式触发系统崩溃；若自助机操作系统未更改默认配置，攻击者可通过在设备边界滑动、三指切换等方式退出至 Windows 界面，执行恶意代码；甚至有些自助机可能因锁具损坏或其他物理安全措施不到位，使攻击者能够轻易打开自助机外壳，插入 U 盘运行木马程序。

2.4 投毒与钓鱼

投毒攻击是一种常见的物理媒介攻击手段，攻击者将含有恶意代码的 U 盘、光盘或其他存储设备故意丢弃在目标区域，诱导用户将其插入电脑。一旦用户执行此操作，恶意代码将自动运行，感染用户的计算机系统，历史上已有类似案例[4]。近年来随着技术进步，攻击者还可能使用更为隐蔽和成本更低的方式传播病毒木马，如二维码等。

Wi－Fi 钓鱼攻击是攻击者通过设置虚假的无线信号，模仿医院可信的无线网络，诱导内部人员连接。一旦用户连接上这些虚假网络，攻击者便可以截获用户的登录凭证、传输数据等信息，或者通过中间人攻击[5]等手段，进一步窃取用户的敏感数据。此外，攻击者还可能开放一些免费的 Wi－Fi 热点，当用户连接并使用这些热点时，攻击者便可轻易截获用户的数据包，窃取信息。

2.5 敏感信息泄漏

社工手段是指攻击者利用社会工程学原理，通过欺骗、诱导等方式收集敏感信息并入侵计算机系统的行为。在攻防实战中，社工手段与技术手段常结合使用。在医院这一特殊环境下，社工手段尤为有效，攻击者可能会利用医院内部的公告栏、海报或其他公开信息收集关键线索，进而推测出内部人员的身份和权限；还可能通过精心设计的骗局，例如冒充计算机维修人员或内部管理人员，与医护人员交互，诱导其泄漏关键账号密码或敏感信息。

3 对策建议

3.1 加强 Wi－Fi 管理

首先，医院应严格控制无线网络信号的辐射强度，特别是在室外区域，避免超出医院管理范围。其次，应区分无线网络的用途，对于可访问医院内部系统的无线网络，应特别加强身份验证，例如采用虚拟专用网络（virtual private network，VPN）或零信任认证等安全机制。此外应限制无线网络的使用，保证无线网络通过受控的边界设备接入内网[6]，与有线网络隔离并监测异常流量。对于采用公共密码登录的无线网络，应要求定期更换 Wi－Fi 密码。同时，应严格禁止个人私自连通医院网络建立 Wi－Fi 热点，医院网络安全部门应定期安全检查和审计。

3.2 联网终端准入全覆盖

首先，应能够对非授权设备私自连到内网的行为进行检查或限制[6]，医院应部署终端准入系统，确保在终端联网前能够鉴别身份[7]。其次，对于没有交互界面的联网终端，如摄像头、门禁、IP 电话、手持移动设备（personal digital assistant，PDA）等，应进行 IP/MAC 绑定。再次，可考虑在内网终端区域部署蜜罐系统[8]，主动诱捕发现攻击者。同时，为防止网线被恶意拔出，可选用带有反锁扣的网线头，这样只有使用特殊工具才能拔下网线，增加了非授权访问的难度。最后，应加强后台监控审核，特别是对新接入的设备，要严格审核，确保身份信息准确和配置合规。

3.3 多部门协作管理自助机设备

一是及时维修。对于老旧自助机设备，应及时维修检查，确保外壳不能随意打开。二是软件加固。设置业务程序在最上层运行、全屏显示且不可被退出。对于系统软件进行必要的更新和加固，防范已知安全漏洞。关闭特定版本 Windows 系统的快捷功能，防止攻击者利用这些功能恶意操作。三是加强多部门协作。信息、门诊、保卫、物业和厂商加强沟通与合作，共同制定并执行自助机设备管理规范，一旦在现场发现不穿工装或身份不明的人员维修调试，应立即报告给信息中心核实。

3.4 内网终端禁用移动存储介质

对于可以访问核心业务系统的内网终端，应严格管理导入导出，特别是禁用移动存储介质，减少病毒传播和数据泄漏风险。一是可以通过物理拆除或者物理封堵的方式处理 USB 接口，也可通过终端安全管理软件禁用 USB 存储设备。二是确有 U 盘使用需求的，可考虑建立移动存储介质管理系统防止非法滥用造成信息泄漏[9]。此系统通常自带专用 U 盘，也可采用个人 U 盘格式化处理，确保 U 盘中隐藏分区的数据只能在安装了终端管理系统的主机上读写[10]。

3.5 网络安全教育应与时俱进

网络安全攻击渗透的手段不断翻新，网络安全教育的形式也应同步与时俱进。除了针对全员的安全意识教育，也应包括针对信息技术人员、运维厂商人员的技术培训。形式上除了传统的 PPT 宣讲，也可以采取沙盘推演、参观网络安全展厅、动手实操体验等丰富多样的形式[11]。例如美国 DEFCON 黑客会议上绵羊墙的展示形式[1]，可以让观众参与互动，更令人印象深刻。实践中发现，身边发生的网络安全事件更受关注，对其复盘分析具有很好的警示效果。

4 效果分析

以上近源网络攻击手段在演练实践中攻击方都

有采用，这些新型攻击手段使防守方经历了严峻的考验。通过这次演练，医院提升了应急响应技术能力、排除了潜在的安全风险、加强了部门之间的协作、提高了全员网络安全意识。

演练过程中，医院防守方要迅速识别出攻击手段、分析攻击路径、制定防御策略，并在有限的时间内执行相应的应对措施。这种高强度的实战演练使工程师们能够更加熟练地应对各种网络攻击，提升了应急响应技术能力。

实战演练不仅是对现有安全策略的检验，更是指明了未来安全策略的优化方向。通过演练，医院更加清晰地了解了自身的安全短板和潜在威胁。通过事后对攻击过程复盘，防守人员发现了很多原来忽视的安全风险和系统漏洞。之后逐一整改销项，使医院网络安全建设更加贴近实际场景，更有针对性。

网络攻防演练需要不同部门、不同岗位的人员共同参与和协作。演练过程中，各部门之间实时共享信息、协调资源、共同应对挑战。针对近源网络攻击需要进入物理场所的特点，医院各相关部门分别制定了应对措施，并在实践中不断磨合，完善了部门之间的协同机制，应急处置时效性得到提升。

演练结束后，医院利用演练中的真实素材，在全院范围内进行“网络安全事件就发生在我们身边”的警示教育。医院所有工作人员进一步了解了近源网络攻击这种新型攻击方式，并对网络安全违规行为的危害有了更深入的认识。为医院持续推进网络安全工作奠定良好的基础。

通过以上总结反思和一段时间的安全整改，医院的网络安全防护能力得到显著提升，在第 2 次演练中，院方成功阻断了攻击方的网络攻击行为，达到了预期效果。

5 结语

攻击者从来都是绕过已有的安全措施攻击的[11]。近源网络攻击相较于传统的外部互联网攻击更为隐蔽且难以防范。有攻击者甚至在尝试拿到用户凭证后，将“跳板机”留在目标单位现场，在家远程控制就可以进行后续工作[1]，使防守方排查溯源更加困难。医院掌握着大量高价值医疗数据，且信息化水平参差不齐，极易成为黑客猎取的目标[12]，应引起全社会的重视。医院网络安全从业者应积极了解并掌握最新的攻击手段和技术趋势，从攻击者视角发现防护策略的薄弱环节，持续学习新技术，建立了解安全情报的途径。医院管理部门也应发挥网络安全与信息化领导小组的统筹作用，加强多部门联动，以应对新的网络安全挑战。

作者贡献：孟晓阳负责论文撰写；杨巍、张楠负责相关案例实施、资料收集与整理；孙国强负责论文审核与修订。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 柴坤哲，杨芸菲，王永涛，等. 黑客大揭秘：近源渗透测试［M］. 北京：人民邮电出版社，2020.
2 段越. 使用 kali 进行 WIFI 安全测试［J］. 电脑知识与技术，2019，15（4）：24－26.
3 田延伟，杨松儒，李杰. 无线 WiFi 密钥 App 风险隐患及对策研究［J］. 信息网络安全，2017（7）：80－84.
4 耿家伟. 美国国家安全局对伊朗实施网络战动因及进程分析［D］. 北京：外交学院，2018.
5 赵少飞，吕丽萍，岳剑辉. 浅析中间人攻击的手段及防范措施［J］. 网络安全技术与应用，2023（12）：21－22.
6 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求 GB/T 22239—2019［S］. 北京：中国标准出版社，2019.
7 朱卫国，郑攀. 医院网络安全等级保护（2.0）实施指南［M］. 北京：电子工业出版社，2019.
8 高铭剑，丁炎，王立帅. Wi－Fi 近源攻击捕获方法及装置，设备，介质和程序产品：CN202111297196.1［P］. 2024－02－16.
9 国家卫生健康委员会发布《全国医院信息化建设标准与规范（试行）》：明确医院信息化建设内容和建设要求［J］. 医学信息学杂志，2018，39（4）：94.
10 孟晓阳，孙国强，林泽奇. 医院计算机终端安全防护研究与实践［J］. 中国卫生信息管理杂志，2019，16（1）：13－17.
11 孟晓阳，王辰超，朱卫国. 医院网络安全防护策略实践与探讨［J］. 中国卫生信息管理杂志，2020，17（3）：290－295.
12 孟晓阳，杨巍. 医院数字化转型网络安全应先行［J］. 中国数字医学，2022，17（10）：39－42.