API 流量监测技术在医院 DMZ 区的实践与应用

魏 阳 刘卫方 康 蘋

（南昌大学第二附属医院 南昌 330006）

〔摘要〕 **目的/意义** 探索应用程序接口（application programming interface，API）流量监测技术应用于医院内外网缓冲区（demilitarized zone，DMZ）的场景、问题及应对策略，以提升医院数据安全防护能力。**方法/过程** 在医院 DMZ 区部署 API 流量监测系统，镜像获取流量，对已有数据进行预分类分级，定义敏感数据标签，建立 API 资产台账，分析 API 安全漏洞，设计风险场景审计模型，实时监测用户访问行为。**结果/结论** 系统实际监测流量均值近 1G、峰值近 2G，识别接口 80 000 余个、应用 2 000 余个，实现医院 DMZ 区核心业务全流量监测，有效保护了患者隐私数据。

〔关键词〕 API 流量分析；医院 DMZ 区；API 安全漏洞；数据安全

〔中图分类号〕 R－058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673－6036.2025.10.013

Practice and Application of API Traffic Monitoring Technology in the Demilitarized Zone of Hospitals

WEI Yang, LIU Weifang, KANG Pin

The Second Affiliated Hospital of Nanchang University, Nanchang 330006, China

〔**Abstract**〕 **Purpose/Significance** To explore the scenarios, problems and countermeasures of applying application programming interface (API) traffic monitoring technology to the demilitarized zone (DMZ) of hospitals, so as to enhance the hospitals' data security protection capabilities. **Method/Process** The API traffic monitoring system is deployed in the DMZ of the hospital. Traffic is obtained through mirroring. Existing data is pre-classified and graded, sensitive data labels are defined, API asset ledgers are established, API security vulnerabilities are analyzed, risk scenario audit models are designed, and user access behaviors are monitored in real time. **Result/Conclusion** The system actually monitors an average flow of nearly 1G and a peak flow of nearly 2G, identifies over 80 000 API and over 2 000 applications, and achieves full flow monitoring of core business in the hospital's DMZ, and effectively protects patients' privacy data.

〔**Keywords**〕 API traffic analysis; demilitarized zone (DMZ) of hospital; API security vulnerabilities; data security

1 引言

数字化时代医疗行业变革深刻，医院信息系统（hospital information system，HIS）、电子病历（electronic medical record，EMR）系统、影像存储与传输系统（picture archiving and communication sys-

〔修回日期〕 2025－09－30

〔作者简介〕 魏阳，助理工程师，发表论文 2 篇；通信作者：刘卫方。

tem，PACS）等广泛应用[1-2]，提升了医疗服务效率和质量。随着医疗信息化快速发展，三甲医院越来越依赖应用程序接口（application programming interface，API）[3]。通过 API，医院可整合内部资源，优化流程，还能与医保部门、药品供应商等外部机构共享数据、协同工作。

近年来，《数据安全法》《个人信息保护法》等出台，对医疗行业数据保护要求日益严格精细。API 在 HIS 的广泛应用使数据共享和使用更加便捷，但开放性和复杂性使其成为网络攻击的潜在目标[4]。一旦 API 存在安全漏洞或遭受恶意攻击，可能导致患者隐私泄漏、医疗业务中断、服务质量下降，给医院带来巨大经济损失和声誉损害。因此，研究 API 风险监测技术在医院 DMZ 区的应用，对保障医院信息安全和业务连续性至关重要[5]。

2 研究现状

API 是一套定义了软件组件之间如何交互的规则和协议。API 具有灵活且易于集成的特点[6]，允许不同技术平台的不同软件应用共享数据和功能。医院网络架构通常分为内网和外网，DMZ 区位于二者之间，承担内外网数据交互缓冲作用，Web 服务器、邮件服务器、数据库服务器等均部署在此，该区域网络流量中包含有患者身份信息、诊疗记录等敏感数据[7]，见图 1。

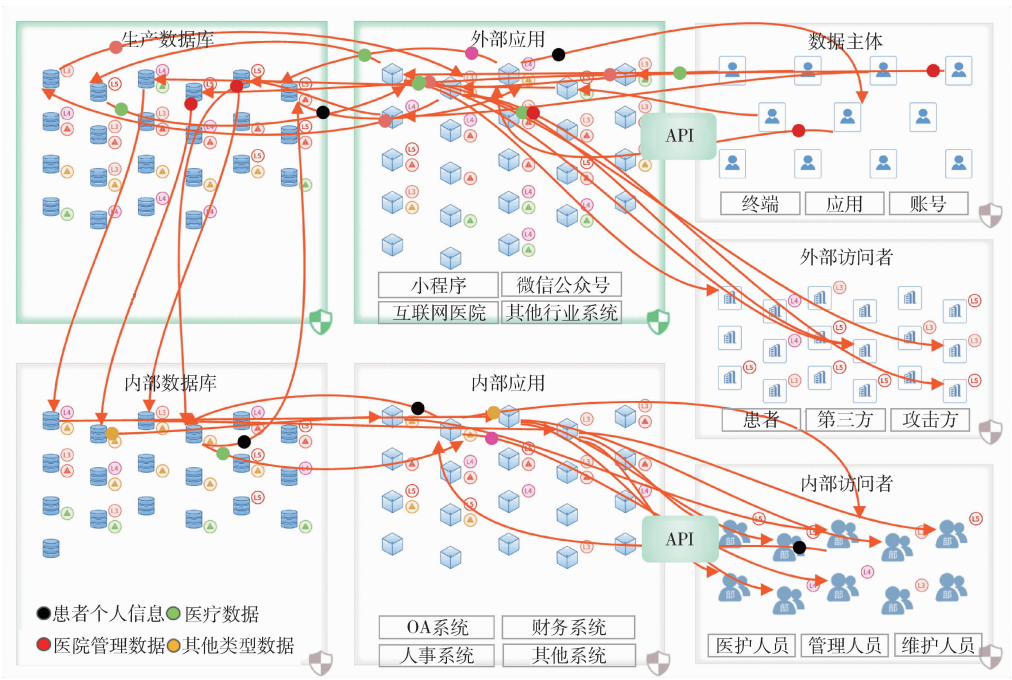

图 1 医院 API 数据链路

医院网络环境下，不同信息系统存储不同数据，如 HIS 存储患者基本信息和挂号、收费等数据，EMR 系统存储病历、诊断结果、治疗方案等，PACS 存储医学影像数据等[8-9]。各系统间数据须共享，例如，患者在互联网医院平台提交问诊请求，通过 API 将请求传至医院 EMR 系统，医生在 EMR 系统回复并开具处方，再经 API 将处方传至药房系统，由药房调配和配送药品。随着远程医疗和互联网医院发展，患者可通过手机 App 或网页端在线预约挂号、咨询医生、获取检验报告等[10]。这些功能均依赖医院 API 接口与内部医疗服务资源、外部互联网平台对接。医院中有大量用于患者监测、诊断和治疗的医疗和物联网设备，如心电监护仪、血糖仪、输液泵、智能病床等[11]。这些设备通过 API 连接 HIS，实现数据实时采集、传输和分析。例如，心电监护仪采集患者心电数据，经 API 传至医院监护系统，医生可实时查看心电图波形，及时发现异常并干预。

HIS 大量使用 API，相关数据安全风险同步增加。近年来，国内外大规模数据泄漏事件频出，API 安全面临巨大挑战[12]。虽然许多医院已部署传统技术手段和安全设备，如漏洞扫描、渗透服务、防火墙等，这些手段依靠已知攻击特征进行模式匹配或针对指定目标测试样本，可解决医院网络环境中的部分威胁。但当前形势下，新型攻击手法层出不穷，传统技术手段在效率、覆盖面、准确率等方面已无法满足数据安全防护需求。在医院 DMZ 区部署 API 流量监测设备，分析内外网双向流量，梳理 API 数据暴露面，识别与外部网络交互的应用和 API，可发现潜在数据安全风险，还能针对互联网 API 攻击、数据窃取行为预警，及时发现并处置潜在风险，对提升医院数据流动防护能力意义重大。

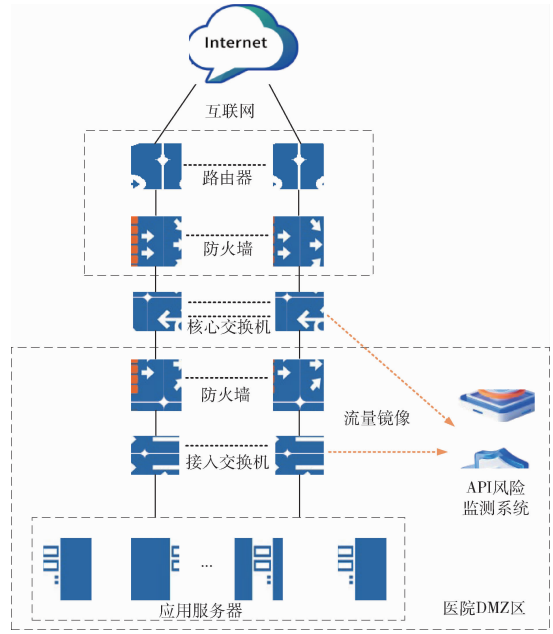

图 2 API 流量监测系统部署结构

3 实施过程

3.1 系统部署

在南昌大学第二附属医院 DMZ 区以旁路模式虚拟化部署 API 流量监测系统。为核心交换机配置端口镜像，将 DMZ 区、关键业务系统流量转发至该监测系统，在不改变网络拓扑、不干扰业务的前提下，实现 API 流量监测与分析，具体部署方式，见图 2。

3.2 API 资产台账

借鉴卫生健康行业数据分类分级标准和电子健康档案数据分类分级相关研究[13-16]，对医院相关数据进行分类分级预定义并标签化，如将患者就诊记录中的诊断信息标记为敏感数据，敏感等级设为最高级。通过监测识别涉及敏感数据的 API，见图 3。

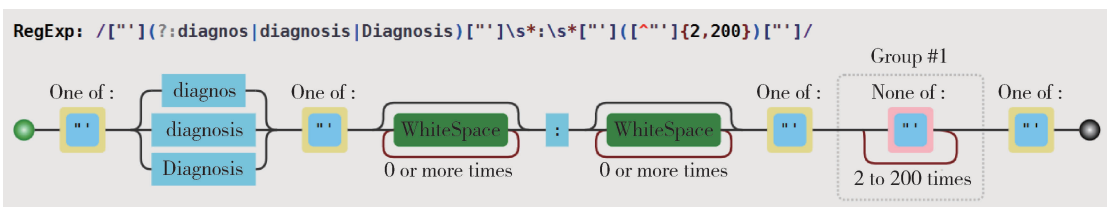

图 3 敏感数据标签匹配表达式

由于 RESTful API 设计规范[6]使用广泛，且医院绝大多数系统采购自第三方，医院网络环境中存在大量类似的 API，路径不同但功能一致，须合并处理。通过 API 流量监测，系统自动合并功能相同的 API，并识别可能须合并的 API，由人工判断是否合并。同时，同一域名下有不同应用也影响 API 资产梳理的准确性，须根据端口号或路径拆分应用。

采取流量丢包补全策略和上下文关联分析手段，自动发现路径并初步形成 API 链接清单；结构化还原网络流量中 API 请求和响应，提取参数配置，分析交互，以识别请求和返回内容中的敏感数据，为每个 API 标注数据标签；持续发现并跟踪 API 活跃状态，分组整合，形成 API 资产清单；最后人工导入应用标签，系统自动整理 API 清单及标签，得到 API 资产台账，见表 1。

表 1 API 资产台账（部分）

应用名称	应用	敏感数据标签	路径	API 标签
合理用药	drugs. X. cn	姓名、诊断、生日、用药数量、用药名称、性别、患者登记号、未成年人身份证号	/api/hisUtils/postMethod	单次返回类型多
			/api/phPclPatient/getPatientBaseInfo	单次返回类型多
			/PrecEvaluate/report/PrescOutViewDetail	数据暴露
			/DCStation/submit/checkResultPage	服务调用
医保慢病	mbsb. X. cn	姓名、身份证号码、银行卡号、手机号、性别、公司、地址、未成年人身份证号	/mbapi/WXMedical/GetMedicalUserInfo	数据暴露
			/mbapi/Infomation/GetUserPhone	数据采集
			/WXMedicalReport/IsExistXGPatients	人机访问
			/mbapi/Upload/Attachment/ $（param）	文件上传
影像系统	pacs. X. cn	姓名、患者登记号、身份证号码、电子邮箱、手机号、未成年人身份证号	/VuePatientCenterWebApi/search	服务调用
			/vuepatient/api/v1/patientsV3	数据采集
			/portal/ $（param） /HandleRequest	数据暴露
			/portal/v1/thirdparty/gettoken	URL 重定向
肝纤维检测	liverfiber. X. cn	姓名、体检报告结果、患者登记号、手机号、诊断	/api/UserManager/GetPage	单次返回类型多
			/api/worklist/query	数据暴露
			/restfibroscan/V2/worklistsday	人机访问
招标采购	bid. X. cn	公司、地址、身份证号码、手机号、统一社会信用代码、电子邮箱、银行卡号	/nc/file/down	文件下载
			/nc/file/upload	文件上传
			/nc/bid/template/excel/fill	人机访问
			/nc/template/excel/export	数据暴露

3.3 风险监测与防护

参照开放式 Web 应用程序安全项目（Open Web Application Security Project，OWASP）发布的 API 10 大安全风险，从数据暴露、数据权限、安全规范、高危接口、口令认证等规则维度，识别漏洞和缺陷。结合网络安全领域 50 余项通用漏洞规则，如搜索逻辑调用、硬编码密钥、Web 安全缺陷等，实时监测分析医院网络环境下 API 活动，识别异常行为和恶意风险。

审计账号访问流量，预设告警场景。用户访问特定应用系统且触发风险场景审计规则时，平台自动从网络流量还原业务系统操作账号，包括自动解析提取登录 API 账号，多维度还原用户真实访问情况，如一个 IP 登录多个账号或一个账号在多个 IP 登录。记录数据访问行为，以便数据泄漏事件发生时进行审计回溯。通过回溯可提取被泄漏内容的所有访问记录，再通过集中度分析，聚焦嫌疑人和泄漏路径。

风险防护方面，复现识别出的高危风险，利用抓包工具导出数据流量，通过参数遍历、伪造请求、绕过 token 认证等技术手段进行验证。例如，系统发现某第三方提供的 API 存在高危漏洞，互联网侧无须鉴权即可用常规接口测试工具批量拉取不同患者身份证照片、姓名、性别等敏感信息。对于这类未鉴权访问的 API，检查是否配置横向权限校验，提高可遍历参数的复杂性，避免使用短数字、姓名等易于猜测的参数；保持对接口访问的监控，及时发现通过接口批量遍历数据的风险。从数据泄漏、Web 攻击、账号安全 3 个维度审视 API 攻击行为，记录正常数据访问行为属性，建立 API 行为基准线，对已核实的恶意活动 API 溯源分析，评估漏洞级别和类型，根据风险等级确定修复时间线，快速修复并严格验证，修复后持续监控，从发现到预防，确保整个处理流程闭环。

3.4 风险场景审计

结合医院真实业务设计风险场景审计模型，涵盖风险主体、API 类型、风险周期和风险指标等维度。风险主体可以是员工工号、手机号等账号或终端 IP，支持指定部门和账号专属审计；也可根据实际需要指定具体应用或 API，缩小审计范围，使结果更精准。风险周期一般以时间或次数为单位。风险指标依据业务真实场景设定告警。预设的风险场景审计模型主要分为账号类和 IP 类，其中账号类风

险主要聚焦某账号单次获取高值耗材信息等敏感数据超 100 条、某账号非工作时间频繁访问患者用药数据等场景；IP 类风险主要聚焦某 IP 地址短时间内频繁调用患者健康档案接口、某 IP 多终端异地访问等场景。再结合时间范围、人员职责、敏感数据类型等，通过人工研判行为合理性，必要时溯源和管控风险账号或 IP 地址。

4 结果与分析

4.1 监测结果分析

在 3 个月实践周期内，系统实际监测流量均值 974 Mbps、峰值 1 861 Mbps，实现对医院 DMZ 区核心业务全流量监测。通过系统自动识别和人工介入结合，识别 API 接口 83 365 个，其中高敏感 991 个（1%）、中敏感 2 736 个（3%）、低敏感 4 014 个（5%）、非敏感 75 624 个（91%）；发现应用 2 158 个，其中高敏感 243 个（11%）、中敏感 178 个（8%）、低敏感 291 个（14%）、非敏感 1 446 个（67%）。涉及敏感数据含密码、手机号、身份证号、疾病诊断、患者登记号、用药数量等信息。监测系统发现的 API 数量庞大，符合医院对外业务数据交互频繁特点。其中，高、中敏感 API 占比小，但高、中敏感应用占比较大。说明多数 API 符合安全标准，但部分应用存在少量高、中风险。

监测系统发现漏洞 1 348 个，其中高危 204 个（15%）、中危 405 个（30%）、低危 739 个（55%），漏洞类型 22 种。高危漏洞主要集中在未鉴权访问、参数可遍历等方面，见表 2。针对漏洞，先定位 API 及应用；召集相关人员组建工作群，分析并复现漏洞；责令系统负责人安排技术人员整改，周期内复测，形成闭环。系统标记并分组展示主要漏洞类型，以便重点跟踪处理，漏洞如已处理则去除标记。

表 2 漏洞情况汇总（示例）

序号	漏洞名称	漏洞等级	漏洞数量（个）	漏洞描述
1	未鉴权访问	高危	121	可查询敏感数据或进行敏感操作的接口可在未鉴权的情况下访问，攻击者不登录即可访问接口，从而获取大量敏感数据或执行敏感操作
2	参数可遍历	高危	83	在接口入参中发现可遍历的参数，攻击者可按照参数的遍历特征，通过脚本进行批量数据拉取
3	明文密码传输	中危	179	在接口请求中发现明文密码传输，攻击者可在传输过程中进行监听或拦截，从而获取用户真实密码
4	返回数据量可修改	中危	134	在接口请求中发现与返回数量相关的查询参数，可通过修改参数，单次获取大量敏感数据
5	鉴权信息在 URL 中	中危	28	在 URL 中发现 Token 或 SessionID 等鉴权信息，URL 中的信息会出现在日志中，也可能通过 referer 发送给第三方，同时 URL 在浏览器页面上也可能被用户看到，导致信息被他人获取
6	登录弱密码	中危	55	在登录接口的请求中存在弱密码，弱密码可能被暴力破解
7	明文密码透出	中危	7	在接口的返回内容中发现明文密码，且密码直接以明文保存在数据库中，服务器不应该以任何形式保存明文密码信息
8	登录认证不合理	中危	2	发现登录接口或其他需要授权的接口使用 URL 参数传递密码，可能导致 URL 中的密码信息在请求日志中泄漏，或者在浏览器页面被他人通过窥视泄漏

4.2 风险审计结果分析

设定业务场景后的 3 个月内，系统识别业务风险 568 条，其中账号类风险 125 条，IP 类风险 443 条。业务风险场景由风险主体、风险周期和风险指标等要素构成，风险指标涵盖返回去重数据量超阈值、操作时间范围不合理、上传下载大量文件等。审计出的风险包含具体案例，如某工号在住院营养服务器系统单次获取去重患者诊断数量 373 条，某 IP 在医学数据智能平台单次获取用药名称 126 条等。结合审计案例与账号所属人员科室职能，判断操作是否越权。综合分析后，针对误报告警，将账号或 IP 加入白名单，以减少后续工作量；针对初判违规告警，先与科室领导沟通，了解是否知晓相关人员告警及操作必要性，如超出职责权限，由保卫处约谈，必要时移交公安部门处理。

4.3 面临的挑战

本研究对医疗健康相关数据进行了分类分级预定义和标签化，以便进行风险计算和存储。但是医疗行业暂无统一、具体的数据分类分级细则[13]，标签无法涵盖所有敏感数据，定级也不一定完全合理。未来应进一步探索医疗行业数据分类分级标准。本研究采用镜像获取流量，可不改变医院原有网络拓扑，对医院业务系统也无干扰。目前大量应用已采用 HTTPS 加密传输，以保障数据安全与用户隐私，取代了早期不安全的 HTTP 明文传输。针对此类应用，须通过负载均衡设备解密，再发送至流量监测设备；而针对在系统层面加密的应用，只能通过在服务器上安装插件的模式获取解密后的流量，暂时无法避免对医院业务系统造成干扰。基于流量的分析多聚焦结构化数据，而医院常用的医疗相关图像、音频和视频等非结构化数据，也存在泄漏风险。非结构化数据监测与保护将成为数据安全领域的研究重点和难点。

5 结语

本研究探索 API 流量监测技术在医院 DMZ 区的应用，总结面临的挑战，并提出应对策略，为医院提升 DMZ 区安全防护能力提供参考。随着技术的发展，医院日益重视信息安全，API 流量监测技术有望在 DMZ 区进一步推广应用，为医院信息化与服务质量的持续改进提供支撑。

作者贡献：魏阳负责资料收集与分析、论文撰写与修订；刘卫方负责提供指导；康蕾负责论文修订。
利益声明：所有作者均声明不存在利益冲突。

参考文献

1 DE MELLO B H, RIGO S J, DA COSTA C A, et al. Semantic interoperability in health records standards: a systematic literature review [J]. Health and technology, 2022, 12 (2): 255 – 272.
2 高竞，李碧辉. 互联互通背景下对医疗数据安全保护的思考 [J]. 中国信息安全，2022 (7)：52 – 54.
3 JANGAM S K, KARRI N, MUNTALA P S R P. Advanced API security techniques and service management [J]. International journal of emerging research in engineering and technology, 2022, 3 (4): 63 – 74.
4 陈润生. 医疗大数据结合大语言模型的应用展望 [J]. 四川大学学报：医学版，2023，54 (5)：855 – 856.
5 WANG J S. Exploring and evaluating the development of an open application programming interface (open API) architecture for the fintech services ecosystem [J]. Business process management journal, 2024, 30 (5): 28.
6 DATLA L S. Optimizing REST API reliability in cloud – based insurance platforms for education and healthcare clients [J]. International journal of artificial intelligence, data science, and machine learning, 2023, 4 (3): 50 – 59.
7 孙保峰，葛晓伟，杨扬，等. 某三级甲等公立医院 API 接口安全监测实践与思考 [J]. 中国数字医学，2024，19 (7)：115 – 120.
8 THERIAULT – LAUZIER P, COBIN D, TASTET O, et al. A Responsible framework for applying artificial intelligence on medical images and signals at the point of care: the PACS – AI platform [J]. Canadian journal of cardiology, 2024, 40 (10): 1828 – 1840.
9 ADAK S. Current risk in the supply chain for the active pharmaceutical ingredients business [J]. Universal journal of pharmacy and pharmacology, 2024, 3 (1): 1 – 5.
10 ANAWADE P A, SHARMA D, GAHANE S. A comprehensive review on exploring the impact of telemedicine on healthcare accessibility [J]. Cureus, 2024, 16 (3): e55996.
11 KUMAR S, SHAW D K. An API security framework for IoT – enabled healthcare system with the application blockchain – based smart contract [J]. SN computer science, 2024, 5 (8): 1044.
12 DIL – NAHLIELI D, BEN – YEHUDA A, SOUROUJON D, et al. Validation of a novel artificial pharmacology intelligence (API) system for the management of patients with polypharmacy [J]. Research in social and administrative pharmacy, 2024, 20 (7): 633 – 639.
13 陈烨，王阳，徐亚兰，等. 电子健康档案数据分类分级研究 [J]. 档案学研究，2024 (3)：119 – 128.
14 王超，张勇. 精细化管理：医疗行业数据分类分级的策略与实践——访西安国际医学中心医院信息管理部基础架构中心负责人张勇 [J]. 信息安全与通信保密，2024 (11)：66 – 70.
15 单博深，左晓栋. 国标《数据安全技术 数据分类分级规则》分析与解读 [J]. 网络安全与数据治理，2024，43 (11)：19 – 22.
16 金涛，王建民. GB/T 39725 – 2020《信息安全技术健康医疗数据安全指南》[J]. 标准生活，2022 (3)：46 – 51.