计算机网络安全防范措施探析

乔祉荀
通化市中心医院　吉林　通化　134000

摘　要：在数字化浪潮席卷下，计算机网络已深度融入社会各领域，成为推动发展的关键力量。本文聚焦计算机网络安全防范措施，以医疗行业为典型场景展开探析。概述了计算机网络安全定义、核心要素与重要性，接着分析医疗网络面临的恶意软件、网络钓鱼等常见威胁。阐述了防火墙、入侵检测与防御等防范技术，最后从构建医疗专用技术防护体系、完善安全管理制度、开展分层安全意识培训及建立应急保障机制等方面，提出针对性防范措施，旨在为医疗行业及类似领域网络安全保障提供参考。

关键词：计算机网络安全；防范技术；防范措施

引言：当前网络安全问题日益凸显，尤其是医疗行业，其网络承载着患者隐私数据与关键诊疗业务，面临的安全威胁具有特殊性与高风险性。一旦遭遇网络攻击，不仅会导致数据泄露，还可能直接影响诊疗服务的连续性与可靠性。深入研究计算机网络安全防范措施，特别是针对医疗行业的有效策略，具有重要的现实意义和紧迫性。

1 计算机网络安全概述

1.1 计算机网络安全定义

在数字化时代，计算机网络已深度融入社会各领域，成为推动经济发展与社会进步的关键力量。计算机网络安全，指的是通过采取必要措施，保护网络系统中的硬件、软件及数据免受偶然或恶意原因导致的破坏、更改、泄露，保障系统连续可靠正常运行，网络服务不中断。这一定义涵盖了网络环境中从物理设备到虚拟数据的全方位保护需求。

1.2 计算机网络安全核心要素

网络安全包含以下三个核心要素：（1）保密性。旨在确保信息仅被授权者访问，防止敏感数据被未授权的个人、组织或程序获取，如个人身份证号、银行卡密码、企业商业机密等信息的泄露将造成严重后果；（2）完整性。要求信息在存储、传输过程中不被未授权地修改、伪造或破坏，保证数据的准确性和一致性，以银行转账数据为例，若交易金额被篡改，将直接损害用户和金融机构的利益；（3）可用性。则强调网络资源在需要时能够被合法用户正常访问和使用，避免因攻击或故障导致服务中断，像电商平台在促销活动期间，若遭遇DDoS攻击导致无法访问，会给企业带来巨大经济损失和声誉损害。

1.3 计算机网络安全重要性

网络安全的重要性主要体现在以下方面：（1）对个人而言，网络安全是保障隐私和财产安全的基础防线。随着移动支付、社交网络的普及，个人信息在网络空间频繁流转，一旦遭遇网络攻击，隐私泄露、财产损失等问题将接踵而至。（2）在企业层面，网络安全是维持正常运营和保持竞争力的关键。企业的核心数据，如客户资源、技术专利、财务信息等，是其生存与发展的命脉。网络安全漏洞可能导致数据被盗取，不仅造成直接经济损失，还可能影响企业信誉，削弱市场竞争力。（3）从国家层面看，网络安全更是国家安全的重要组成部分。关键信息基础设施，如电力、交通、通信等领域的网络系统，若遭受攻击，将严重威胁国家经济秩序、公共安全和社会稳定[1]。

2 计算机网络安全常见威胁

医疗行业网络承载着患者隐私数据与关键诊疗业务，面临的安全威胁具有特殊性与高风险性。以下安全隐患不仅威胁数据安全，更可能直接影响诊疗服务的连续性与可靠性。（1）恶意软件攻击始终是医疗网络的核心威胁。新型病毒通过伪装成医疗软件更新包、学术资料附件等形式，利用医疗设备与终端防护薄弱环节潜入系统，通过修改系统内核长期潜伏。木马程序则常伪装成医疗办公插件，一旦植入便创建隐蔽通信通道，可远程控制设备窃取电子病历、影像数据等敏感信息，甚至将感染设备纳入僵尸网络，威胁整个医疗网络稳定。勒索软件针对医疗数据的加密攻击尤为致命，攻击者利用零日漏洞或钓鱼邮件入侵，对患者诊疗记录进行不可逆加密，并以公开泄露相要挟，迫使机构支付高额赎金，而数据恢复失败可能直接影响患者救治。（2）网络钓鱼与社会工程学攻击对医疗系统危害显著。攻击者通过仿冒医疗期刊官网、医保平台界面，诱使医护人员输入账

号密码，从而获取医疗系统访问权限；或通过电话冒充卫健委、医保局工作人员，以数据核查为由套取患者信息。这类攻击利用医疗人员对专业信息的敏感性与信任心理，成功率高且难以防范。（3）黑客入侵直接威胁医疗业务系统安全。攻击者利用医疗系统未修复的系统补丁、弱密码策略等漏洞，通过 SQL 注入、缓冲区溢出等技术手段突破防护，窃取患者身份信息、诊疗数据等核心资产，甚至篡改电子病历，干扰正常诊疗流程。数据泄露不仅会导致患者隐私泄露、机构声誉受损，更可能引发医疗纠纷与法律风险。（4）内部威胁在医疗场景下风险加倍。恶意内部人员凭借合法权限，可轻易导出患者数据或篡改关键诊疗信息；非恶意误操作，如错误配置医疗设备网络参数、使用私人 U 盘传输数据，也可能导致病毒传播或数据丢失[2]。

3 计算机网络安全防范技术

3.1 防火墙技术

防火墙作为网络安全的基础防护设备，通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护。其工作原理基于预先设定的安全规则，对进出网络的数据包进行过滤。包过滤防火墙通过检查数据包的源IP地址、目的IP地址、端口号等信息，决定是否允许数据包通过；状态检测防火墙则在包过滤的基础上，跟踪网络连接的状态，确保只有合法的连接才能通过；应用代理防火墙更进一步，针对特定的应用层协议进行深度检查，对应用数据进行代理转发，能有效防范基于应用层漏洞的攻击。在实际应用中，医院通常会根据自身网络架构和安全需求，部署硬件防火墙、软件防火墙或云防火墙，构建边界防护体系。

3.2 入侵检测与防御系统

入侵检测系统（IDS）主要用于实时监测网络中的异常行为和潜在的入侵活动。它通过收集网络流量、系统日志等数据，运用模式匹配、异常检测等技术手段，对数据进行分析。模式匹配是将收集到的数据与已知的攻击特征库进行比对，一旦发现匹配项，便发出警报；异常检测则是基于正常网络行为建立基线模型，当检测到偏离基线的行为时，判断可能存在入侵并预警。入侵防御系统（IPS）在IDS的基础上，增加了主动防御功能，不仅能检测入侵行为，还能实时阻断攻击流量，通过丢弃恶意数据包、重置连接等方式，将威胁在造成损害前进行处理。

3.3 加密技术

加密技术是保障数据保密性和完整性的核心手段。对称加密算法使用相同的密钥进行加密和解密，如AES、DES等，其加密速度快、效率高，适用于大量数据的加密存储和传输。但对称加密的密钥管理是个难题，密钥的安全分发和存储至关重要。非对称加密采用公钥和私钥配对的方式，公钥用于加密，私钥用于解密，典型算法有RSA、ECC。这种加密方式解决了密钥分发问题，通信双方无需事先共享密钥，可通过公钥进行安全通信。非对称加密的计算复杂度较高，加密速度较慢，常与对称加密结合使用。数字证书则是将公钥与证书持有者的身份信息进行绑定，由可信的证书颁发机构签名，用于验证通信双方的身份真实性，确保加密通信建立在可信的基础上，有效防止中间人攻击[3]。

3.4 虚拟专用网络安全架构

虚拟专用网络（VPN）通过在公用网络上建立专用网络，实现远程用户安全访问企业内部网络资源。VPN利用隧道技术，将数据包封装在另一种协议中进行传输，隐藏原始数据包的内容和来源，保证数据在公网传输的安全性。VPN还采用身份认证和数据加密机制，只有通过认证的用户才能建立连接，传输的数据也会被加密处理。常见的VPN 协议有PPTP、L2TP/IPSec、OpenVPN等，不同协议在安全性、兼容性和性能上各有特点。医院可根据自身需求选择合适的VPN协议和部署方式，如远程办公场景下，员工通过VPN安全接入企业内网，既能访问内部资源，又能保障数据传输安全，避免数据在公网传输过程中被窃取或篡改。

4 计算机网络安全防范措施

4.1 构建医疗专用技术防护体系

医院网络需部署适用于医疗场景的复合型防火墙。在医院外网与内部医疗系统之间，设置支持医疗协议过滤的防火墙，针对医学数字成像和通信、健康信息交换标准等医疗专用协议进行深度检测，阻断利用协议漏洞的攻击，防止非法设备接入医疗影像系统、电子病历系统。在医院信息系统、实验室信息系统等核心业务服务器前部署 WAF，拦截针对医疗业务系统的SQL注入攻击，避免患者诊疗数据被篡改或窃取。

医疗数据安全防护是重中之重。对于存储在医院数据库中的患者病历、检查报告等静态数据，采用AES - 256等高强度对称加密算法加密存储，并定期更新加密密钥。在数据传输方面，无论是院内各科室间的数据交互，还是远程医疗场景下的数据共享，均强制启用SSL/TLS加密通道，并通过数字证书验证接收方身份，确保医疗数据在流转过程中的保密性和完整性。此部署医疗终端安全管理系统，对医院内的医生工作站、护士站终端

设备进行统一管控，限制USB接口使用，防止通过移动存储设备传播恶意软件，同时利用数据防泄漏（DLP）功能，禁止未经授权的医疗数据外发。

4.2 完善医疗业务安全管理制度

医院应建立覆盖医疗设备、业务系统、人员权限的全流程管理制度。在医疗设备管理上，对 CT、MRI 等具备网络连接功能的医疗设备进行专项登记，定期检查设备固件版本，及时更新安全补丁；针对老旧且无法升级的设备，通过网络隔离措施限制其访问范围，避免成为攻击跳板。定期梳理医院网络拓扑，明确各医疗业务系统的网络边界，划分不同安全等级的网络区域，如将电子病历系统所在区域设置为高安全等级，仅允许授权设备和人员访问。

人员权限管理需严格遵循医疗业务流程。根据医生、护士、管理人员等不同岗位的职责，分配最小化的系统访问权限，如普通医生仅能查看、修改本人接诊患者的病历，禁止访问其他科室数据。对管理医疗核心系统的超级管理员账户，采用双人双密钥管理机制，涉及系统配置变更、数据删除等操作时，需两人同时验证。建立详细的操作日志审计制度，对医疗数据的调阅、修改、删除等行为进行全程记录，以便在发生数据异常时快速追溯责任。

定期开展针对医疗业务的网络安全风险评估。采用漏洞扫描工具对 医学影像存档与通信系统等系统进行检测，结合人工模拟渗透测试，识别医疗业务系统中存在的安全隐患。针对发现的风险，按照对医疗业务影响程度进行分级，对于可能导致医疗服务中断或患者数据泄露的高风险漏洞，24小时内完成修复；中低风险漏洞则在一周内制定整改方案并跟踪落实。

4.3 开展分层医疗安全意识培训

针对医院不同岗位人员开展差异化的网络安全培训。对于临床医护人员，重点培训医疗数据泄露的危害、常见网络钓鱼邮件的识别方法，如伪装成医疗期刊订阅、学术会议邀请的钓鱼邮件，以及如何正确使用医院信息系统，避免因误操作导致数据丢失或泄露。通过案例讲解，强调在使用移动查房终端、电子病历系统时的安全规范，如离开工位及时锁屏、不使用弱密码等。

医院IT技术人员则需接受深度的医疗网络安全技术培训。内容涵盖医疗系统漏洞修复、医疗设备网络安全防护、医疗数据加密技术应用等专业技能，同时定期组织参与医疗行业网络安全攻防演练，提升其对医疗业务系统安全事件的应急处置能力。对于医院管理人员，培训重点放在网络安全管理策略制定、医疗业务连续性保障方案设计等方面，使其能够从管理层面重视并推动医院网络安全建设。

建立医院网络安全意识考核机制，将安全知识掌握情况纳入医护人员、IT人员的绩效考核。定期开展网络安全知识考试，对考核不通过的人员进行针对性复训，通过常态化的培训与考核，提升全院人员的网络安全防护意识和技能水平。

4.4 建立医疗业务应急保障机制

院需构建完善的医疗业务应急保障机制，确保网络安全事件发生时能快速响应、减少损失。具体如下：制定专门的医疗网络安全应急预案，按事件影响程度划分特别重大、重大等不同等级，明确各等级响应流程，如特别重大事件需10 钟内上报，并立即启用备用医疗系统。定期开展应急演练，模拟勒索软件攻击、DDoS攻击等场景，检验预案可行性，着重验证备用系统切换效率与数据恢复完整性，及时优化流程[4]。建立医疗数据备份与容灾体系，采用全量与增量结合的备份方式，每日本地备份核心医疗数据，并加密传输至异地灾备中心，每周验证备份数据恢复能力，保障医疗业务持续运行。

结束语

计算机网络安全防范是一项长期且艰巨的任务，对于医疗行业而言更是关乎患者生命健康与机构稳定发展的关键。本文通过分析医疗网络面临的常见威胁，探讨了防火墙、加密技术等多种防范技术，并提出了构建医疗专用技术防护体系、完善安全管理制度等一系列防范措施。

参考文献

[1]袁康乐. 计算机网络安全防范措施探析[J]. 信息记录材料,2021,22(11):59-60.

[2]彭鹏. 大数据时代计算机网络安全及防范措施探析[J]. 黑龙江科学,2020,11(16):80-81.

[3]郭威,黄佩洁. 大数据时代的计算机网络安全及防范措施探析[J]. 信息记录材料,2020,21(4):62-63.

[4]董子超. 计算机网络信息安全问题分析及防范措施探究[J]. 科技创新导报,2019,16(2):162,169.