论网络安全维护中计算机网络安全技术的应用

王文涛
农安县不动产登记中心　吉林　长春　130000

摘　要：网络安全维护通过多元手段，保障网络系统及数据在全生命周期的安全，计算机网络安全技术是防范风险、应对威胁的技术集合，二者相互依存、相互促进。文中阐述了防护型、检测型、响应与恢复型等技术的核心类型与功能，分析了这些技术在网络基础设施、数据、终端、应用等安全维护中的具体应用场景，探讨了技术应用的协同机制与优化路径，为网络安全维护提供了全面的技术应用参考。

关键词：网络安全维护；计算机网络安全技术；防护型技术；检测型技术；数据安全

引言：随着网络技术的快速发展，网络系统及数据面临的安全风险日益多样，网络安全维护成为保障网络环境稳定的关键。计算机网络安全技术作为应对这些风险的核心手段，其发展与应用备受关注。明确网络安全维护与计算机网络安全技术的基础认知，了解技术的类型、功能及应用场景，掌握技术应用的协同机制与优化路径，对提升网络安全维护效果具有重要意义，本文就此展开详细探讨。

1 网络安全维护与计算机网络安全技术的基础认知

1.1 网络安全维护的核心指向

网络安全维护是通过多元手段保障网络系统及数据在全生命周期中的安全状态。网络系统涵盖硬件设备、操作系统、应用程序等多个层级，数据则贯穿运行传输存储等环节。在运行阶段需保障系统指令执行不受干扰，避免因恶意代码注入导致功能异常；传输过程中需确保数据在节点间流转时不被窃取或篡改，维持信息原貌；存储环节则要构建防护机制，防止未授权访问或物理损坏造成数据丢失[1]。潜在风险可能源于外部恶意攻击，如非法侵入系统窃取敏感信息；也可能来自内部操作失误，如权限管理疏漏导致的数据泄露。网络安全维护需提前识别这些风险点，通过规则制定、流程优化、状态监控等方式形成预防体系。面对已发生的威胁，需快速响应并采取阻断、清除等措施遏制影响扩散。长期来看，维护工作还包括安全策略的迭代、人员操作规范的培训，以此维持网络环境的持续稳定。

1.2 计算机网络安全技术的本质属性

计算机网络安全技术是防范网络安全风险应对网络安全威胁的技术集合。技术性体现在其依托计算机科学、密码学、信息论等多学科理论，形成专业技术体系。例如加密技术通过数学算法对数据进行转化，使未授权者无法解读；防火墙技术依据预设规则对网络流量进行过滤，阻隔可疑连接。防御性是技术的核心特征，强调主动构建安全屏障。入侵检测技术通过分析网络行为特征，及时发现异常访问并发出预警；数据备份技术则通过多副本存储为数据恢复提供保障，减少损失。动态性源于网络威胁的持续演变，新型病毒木马、攻击手段不断出现，推动安全技术持续升级。从早期的特征码查杀到如今的人工智能检测，技术始终跟随威胁变化调整防护策略。

1.3 二者的内在关联

计算机网络安全技术是网络安全维护的核心支撑。缺乏技术手段，维护工作只能停留在理论层面。没有加密技术，数据传输的保密性无从谈起；缺少入侵防御系统，网络边界的防护如同虚设。维护目标的实现依赖技术在各个环节的具体应用，从终端防护到云端安全，技术贯穿维护全过程。网络安全维护的需求推动计算机网络安全技术发展。随着物联网、5G等技术普及，网络边界不断扩展，新增的设备接入点带来新型安全隐患，促使零信任架构等技术加速落地。工业控制系统的安全维护需求，推动了针对工业协议的专用防护技术研发。维护过程中遇到的新问题新挑战，成为技术创新的驱动力，而技术进步又为维护工作提供更有效的解决方案，形成循环促进的关系。

2 计算机网络安全技术的核心类型与功能

2.1 防护型技术

防火墙技术在网络出入口对数据流量实施监控和过滤，通过构建逻辑屏障隔离不同网络区域。内部局域网与外部公共网络之间的数据流需经过防火墙检查，符合预设安全规则的数据包被允许通行，不符合规则的则被拦截。这种机制既能阻止外部恶意连接进入内部网络，也能限制内部敏感信息未经授权流出，形成网络边界的第一道防线[2]。不同网络区域如办公网段与核心数据库网

段之间，也可通过防火墙进行隔离，降低单一区域安全事件向其他区域蔓延的可能性。加密技术通过对数据进行编码转换，确保数据在传输和存储过程中不被未授权者解读。传输加密可将原始数据转化为乱码形式在网络中传递，只有掌握解密密钥的接收方才能还原信息。存储加密则对数据库文件或本地存储数据进行处理，即便存储介质被盗取，未授权者也无法直接获取有效内容。加密过程依赖复杂算法实现，不同场景可选择对称加密或非对称加密方式，适应不同安全等级需求。访问控制技术依据预设规则对用户或终端访问网络资源进行限制和管理，防止越权访问。系统会对访问主体的身份进行验证，通过密码令牌生物特征等方式确认身份真实性。验证通过后根据主体权限范围，允许其访问特定资源。例如普通员工仅能查看工作所需数据，无法接触核心管理后台。权限分配基于最小必要原则，避免过度授权引发安全风险，同时记录所有访问行为便于追溯。

2.2 检测型技术

入侵检测技术对网络中的异常行为和潜在入侵活动进行监测识别和告警。通过建立正常网络行为基线，持续分析实时流量特征和操作日志。当出现与基线偏离的情况，如短时间内大量连接请求异常数据传输模式，系统会自动标记为可疑活动并发出告警。技术分为基于特征的检测和基于异常的检测两种模式，前者识别已知攻击特征，后者发现新型未知威胁，共同构成动态监测网络。漏洞扫描技术对网络系统设备及应用程序中的安全漏洞进行探测和分析。通过模拟攻击方式向目标发送探测数据包，检查系统是否存在配置错误软件缺陷协议漏洞等问题。扫描范围覆盖操作系统端口服务数据库等多个层面，扫描结果会详细记录漏洞位置危害程度及可能被利用的方式。定期扫描可及时发现新出现的漏洞，为修复工作提供精准指向，减少被攻击的可能性。

2.3 响应与恢复型技术

应急响应技术在网络安全事件发生后采取措施控制事态扩大消除影响。安全事件确认后迅速启动预设响应流程，切断受影响区域与其他部分的连接，阻止攻击横向扩散。同时对事件根源进行排查，清除恶意代码或关闭存在漏洞的服务。响应过程需同步收集事件相关证据，为后续溯源和责任认定提供支持，确保在最短时间内恢复网络基本功能。数据备份与恢复技术对重要数据进行复制存储，并在数据丢失或损坏时进行还原。备份过程可按固定周期执行，也可根据数据更新频率实时进行，备份介质包括本地硬盘异地服务器云存储等多种形式。当遭遇勒索病毒攻击硬件故障或误操作导致数据损坏时，可通过恢复技术将备份数据重新导入系统。恢复操作需验证数据完整性，确保还原后的数据与原始数据一致且可正常使用。

3 计算机网络安全技术在网络安全维护中的具体应用场景

3.1 网络基础设施安全维护

防护型技术在网络设备安全防护中发挥关键作用。路由器作为网络数据转发枢纽，通过防火墙技术设置访问控制列表，过滤不符合规则的数据包，阻止非法访问尝试。交换机则借助端口安全技术限制接入设备数量，绑定合法设备的物理地址，防止未授权设备通过端口接入网络。这些技术形成设备自身的防护屏障，减少被攻击的入口[3]。检测型技术持续监测基础设施运行状态。通过对路由器交换机的CPU使用率内存占用流量波动等指标进行实时采集分析，识别异常状态。当设备出现非预期的配置变更或端口流量突增，系统会发出预警，提示可能存在的恶意攻击或设备故障，为维护人员提供干预依据，保障基础设施稳定运行。

3.2 网络数据安全维护

加密技术在数据传输和存储环节广泛应用。传输过程中采用加密协议对数据进行转化，使数据在公共网络中以不可读形式传递，到达目的地后再通过密钥还原。存储加密则对数据库文件和本地磁盘数据进行处理，即便是存储介质被物理获取，未授权者也无法直接读取内容。访问控制技术对数据访问权限实施精细化管理。根据用户角色和工作需求分配不同的数据访问权限，限定可查看修改删除的范围。每次数据访问都会被记录在日志中，便于追溯异常操作。数据备份与恢复技术为数据完整性提供保障。按照重要程度制定备份策略，定期生成数据副本并存储在安全位置。当数据因意外丢失或损坏时，可通过恢复技术将备份数据还原，最大限度减少数据损失带来的影响。

3.3 网络终端安全维护

防护型技术在终端设备接入网络时执行严格安全验证。终端设备连接网络前，需通过身份认证技术确认设备合法性，检查是否安装必要的安全软件，操作系统是否为最新版本。只有满足安全要求的终端才能获得接入权限，从源头降低风险。检测型技术主动排查终端设备存在的安全隐患。通过定期扫描终端的操作系统漏洞安装的应用软件配置状态，发现可能存在的安全弱点。针对扫描出的问题，如未修复的系统漏洞恶意软件残留，及时发出提示并提供修复建议。应急响应技术在终端遭遇安全问题时快速处理。当终端被检测出感染恶意代

码，应急响应流程立即启动，隔离受感染终端与网络的连接，防止恶意代码扩散。同时清除终端中的恶意程序，修复被篡改的系统设置，使终端恢复正常状态。

3.4 网络应用安全维护

入侵检测技术实时监测网络应用遭受的攻击。对网页应用而言，持续分析HTTP请求特征，识别SQL注入跨站脚本等攻击行为。客户端应用则通过监测异常的进程交互和数据传输，发现潜在的攻击尝试。一旦检测到攻击迹象，立即发出告警并采取阻断措施。漏洞扫描技术定期探测应用程序漏洞。针对网页应用的代码逻辑配置参数进行扫描，发现可能被利用的安全缺陷。客户端应用则通过检查软件版本组件依赖，找出已知的漏洞信息。扫描结果为应用开发者提供修复方向，提前消除安全隐患。防护型技术为应用运行环境构建安全屏障。网页应用部署在配备防火墙的服务器上，限制非必要的端口开放和服务运行。客户端应用通过沙箱技术隔离运行环境，防止应用被攻击后影响系统其他部分，保障应用在安全环境中运行。

4 计算机网络安全技术应用的协同机制与优化路径

4.1 技术应用的协同逻辑

不同类型计算机网络安全技术在应用中形成有机配合，构建多层次全方位的安全防护体系。防护型技术作为第一道防线，通过防火墙加密访问控制等手段阻挡大部分常规威胁。检测型技术在防护基础上持续监测，发现突破外层防护的异常行为，如入侵检测技术识别新型攻击模式，漏洞扫描技术找出防护措施未覆盖的薄弱点[4]。响应与恢复型技术则在检测到威胁后迅速行动，应急响应技术遏制攻击扩散，数据备份与恢复技术弥补可能造成的损失。这种配合覆盖威胁预防识别处置恢复全流程，形成闭环防护。例如加密技术保护数据传输安全，入侵检测技术监测传输中的异常流量，应急响应技术在发现攻击时切断连接，三者协同降低数据泄露风险。单一技术难以应对复杂威胁，防护技术无法识别未知漏洞，检测技术缺乏阻断能力，响应技术不能提前预防，只有通过协同让各类技术发挥各自优势，才能提升网络安全维护的整体效果。

4.2 技术应用的优化方向

技术适配性优化需考虑网络环境的具体特征。不同场景对安全技术有不同需求，工业控制系统对实时性要求高，过度复杂的加密技术可能影响系统响应速度；金融领域则需强化加密和访问控制技术，保障交易数据安全。根据网络规模业务类型数据敏感度选择适配的技术组合，避免技术与环境脱节。应用策略优化注重技术部署的合理性。防护技术需平衡安全与易用性，过于严格的访问控制可能影响正常业务开展；检测技术应聚焦关键节点，在核心服务器数据传输通道等重点区域加强监测，避免资源浪费在非关键环节。通过动态调整策略让技术应用与业务流程相融合，在保障安全的同时不阻碍正常运行。更新迭代优化要求技术跟上威胁演变节奏。新型攻击手段不断出现，旧有技术可能逐渐失效。建立技术更新机制，跟踪前沿安全技术发展，及时引入能应对新威胁的解决方案。定期评估现有技术的有效性，淘汰不再适用的技术组件，补充新型防护检测工具，确保技术体系始终保持应对威胁的能力，适应不断变化的网络安全环境。

结束语

计算机网络安全技术在网络安全维护中发挥着不可替代的作用。从基础认知到具体应用，再到协同机制与优化路径，各类技术相互配合，形成全方位的安全防护体系。通过合理应用与持续优化，这些技术能够有效应对不断变化的网络安全威胁，为网络基础设施、数据、终端及应用的安全提供有力保障，推动网络安全维护工作不断完善，适应复杂多变的网络环境。

参考文献

[1]周燕彬.网络安全维护中计算机网络安全技术的应用探讨[J].科技创新与生产力,2023(1):75-77.

[2]于鑫,王婷婷.计算机网络安全技术在网络安全维护中的应用[J].通信电源技术,2024,41(3):167-169.

[3]陈洁.计算机网络安全技术在网络安全维护中的应用分析[J].通信电源技术,2023,40(17):193-195.

[4]柯秀清.计算机网络安全技术在网络安全维护中的应用[J].中国新通信,2023,25(20):65-67.