计算机网络安全技术在系统维护中的应用探析

毛锦

四川机电职业技术学院，四川 攀枝花 617064

DOI: 10.61369/TACS.2025110034

摘　　要： 随着数字化转型进程的加速和网络信息技术的深度应用，计算机网络已成为社会经济发展和日常运行不可或缺的重要支持。与此同时，网络攻击手段呈现出复杂化、隐蔽化和产业化的特点，网络安全威胁已经从单纯地技术风险转变为国家安全、经济稳定和社会秩序的挑战。在此背景下，传统的被动防御与碎片化的网络维护模式已经无法应对新型的安全威胁，这就需要不断优化和完善网络安全技术，构建更加完善的网络维护体系。基于此，本文深入探究计算机网络安全技术在网络维护中的应用，以供参考。

关 键 词： 计算机网络安全；网络维护；技术风险

Application Strategies of Computer Network Security Technology in Network Maintenance

Mao Jin

Sichuan Electromechanical Institute of Vocation and Technology, Panzhihua, Sichuan 617064

Abstract: With the acceleration of digital transformation and the in-depth application of network information technology, computer networks have become an indispensable and important support for social and economic development and daily operations. At the same time, network attack methods have shown the characteristics of complexity, concealment and industrialization, and network security threats have transformed from pure technical risks into challenges to national security, economic stability and social order. In this context, the traditional passive defense and fragmented network maintenance models can no longer cope with new types of security threats, which requires continuous optimization and improvement of network security technologies and the construction of a more complete network maintenance system. Based on this, this paper deeply explores the application of computer network security technology in network maintenance for reference.

Keywords: computer network security; network maintenance; technical risks

前言

网络维护作为保障网络系统正常运行、防范安全风险的关键性工作，其目标不仅在于解决问题和排除故障，更重要的是通过主动防御与实时监控的方式，构建全方位的安全防护体系。计算机网络安全技术的应用，有助于将被动维护转化为主动防护，并从数据传输、储存、访问等多个环节阻断安全威胁，提升网络维护的针对性。因此，深入探究计算机网络安全技术在网络维护中的应用，有助于应对复杂的网络安全形势，保障网络系统的稳定性，促进数字化经济的健康发展。

一、计算机网络安全技术基本原理

计算机网络安全技术作为守护网络系统与信息安全的防护盾，其核心在于通过身份认证、访问控制、数据加密的方式筑牢防线。其中，身份认证是安全验证的第一步，只有确认用户或设备身份信息，系统才会获得准入口令。常见的方式包括以下三种：最基础的是用户名 + 密码的组合，信息匹配得到验证后可以解锁资源；生物识别技术则是通过指纹、虹膜和人脸等个人独一无二的特征进行验证，其安全性相对更高；数字证书和权威机构发的“电子身份证”，使用加密技术也能够保障其身份的可靠性 [1]。

访问控制就像是“权限管家”，它通过设定规则限制谁能访问哪些资源，从而避免其他人员的介入。数据加密则是给信息进行加码，将可读的明文转化为乱码类的密文，防止被偷或是篡改。加密一般分为两种，一种是对称加密，用同一把“钥匙”加密解密，这种操作更加便捷，并且相对简单；非对称的加密则有两把“钥匙”，公钥负责加密，对应的私钥才能够解密，这种模式更加适合远距离的安全传输 [2]。

安全传输专门保障数据在网络中的稳定性，常用的技术包括 SSL、TLS 协议、VPN 和 IPsec 协议。其中，SSL、TLS 协议是

网络传输的安全通道，其具有较强的安全性；VPN 能搭建虚拟的“加密专线”，实现点对点安全传输；IPsec 则在网络底层保护数据，确保所有数据包的安全性。

二、计算机网络安全技术在网络维护中的应用价值

（一）构建主动防御体系，降低安全风险

传统的网络维护主要是在发生网络故障和安全事件之后采取措施，这种情况难以有效规避损失。计算机网络安全技术的应用，能够构建事前预防、事中监控、事后追溯的防御体系。利用防火墙、入侵检测系统等技术，提前阻断非法的访问和恶意供给。利用实时监控技术及时发现网络的异常行为，并发出相应的警报[3]。利用日志分析的方式，在安全事件发生后快速定位攻击的源头和其影响的情况，为后续的处理提供支持。这种主动防御模式有助于降低隐患出现的概率，有效控制安全风险。

（二）保障数据安全完整，维护用户利益

数据是网络信息时代的重要资产，其安全完整与用户的权益和企业的利益息息相关。在网络维护中，数据加密、访问控制等安全技术的应用，能够从多个维度保障数据信息的安全。数据加密技术能够对传输和储存过程中的数据做好加密处理，即便出现数据的窃取也无法进行破解的情况。而访问控制技术则通过身份认证、权限分配的方式，闲置费授权用户对敏感数据的访问，从而避免数据信息的泄漏。这种技术能够保障用户的数据信息安全，从而维护了整个行业的稳定性[4]。

（三）保障网络稳定运行，降低维护成本

网络安全事件会导致网络出现瘫痪、系统故障的问题，这也直接影响到网络的平稳运行，还会增加维护的成本。计算机网络安全技术的应用能够减少由于安全事件所引发的故障问题，从而使网络处于一个稳定运行的状态。例如，防病毒技术有助于清除网络中存在的病毒木马，避免其对网络设备和系统产生破坏；流量控制技术则能够合理分配网络，避免恶意流量供给而产生网络拥堵问题。

三、计算机网络安全技术在网络维护中的应用

（一）入侵检测技术的应用

入侵检测技术指的是对计算机中恶意侵入的网络进行全面的检查，一旦在出现问题后可以及时进行有效处理，避免信息的恶意盗取。计算机入侵检测技术的使用，对于用户而言的优势如下：一是在进行系统维护期间使用入侵检测技术，能够让用户充分了解当前系统的整体运行情况，及时拦截病毒，并生成智能的监控体系，如果发生系统被攻击的情况，则可以及时找到出现问题的区域，进而更好地处理和解决问题，并保障计算机的稳定运行；二是入侵检测技术能够对当前网络使用过程中存在的不良行为做好统计和总结，并根据得到的数据信息进行深度分析，依据结论做好预警，对系统信息进行管控；三是这项技术能够对计算机系统做好充分的检测，并在用户操作过程中对不正规的行为做好警告[5]。在此期间，入侵检测技术的使用较为广泛，但也存在着问题，包括漏报以及误报的情况。为了更好地解决此类问题，优化使用的效果，用户还需要注意在信息采集的过程中直接面对危险的数据目标，采取网络衔接模式，保障系统能够与所有端口进行有效衔接。

（二）数据加密技术的应用

数据传输环节的加密技术，是通过加密密钥与算法将原始数据转化为密文，接收方需要匹配对应的解密密钥和算法才能还原信息，在此过程中需要从根本上阻断数据被非法窃取后的解读风险。当前的主流数据传输加密技术可以划分为三类，从而适配不同的安全需求领域。一是节点加密技术。这一技术在数据传输期间会保留报头与路由信息的状态，从而保障传输路径的畅通，加密操作一般集中在网络中间节点。具体来讲，中间节点需要配备专用密码设备与节点进行联动，在接收数据后先解密再重新进行加密，形成加密、解密再加密的节点处理闭环。然而，需要注意的是，在此期间数据传输链路两端的设备要保持同步运行的状态，否则会导致传输中断或数据出现损坏[6]。二是端到端加密技术。此技术在数据发送端与接收端执行加密和解密操作，传输过程中数据始终以密文形式存在，用户无需在传输过程中对数据进行解密处理。和其他的加密方式相比较，端到端的加密不仅其安全等级相对较高，而且能够避免数据丢失问题。三是链路加密技术，这种技术又被称为线路加密技术。这一技术的核心特点是对数据传输的全链路进行全程加密，原始信息在发送前先完成加密，传输到每个节点后需要解密才能继续转发，转发前再次加密，直到抵达接收端最终解密。这种全环节加密的特征，使其成为安全等级最高的传输加密技术，更加适合于高机密文件传输。

（三）防火墙技术的应用

防火墙技术的应用可以从三个方面展开分析。第一，升级防火墙技术，实现智能防护。传统防火墙能够完成基础访问的控制，难以对应 AI 驱动攻击、APT 攻击等新型的威胁。防火墙能够凭借融合防火墙、入侵防御、应用识别等集成优势，成为网络维护的核心防护设备[7]。其应用价值可以从网络策略管控、日志智能监控这两方面进行挖掘，构建主动防御机制。其一，防火墙在网络策划精细化落地中的应用。网络维护中，管理员可以结合业务的需求和安全规范，通过防火墙配置差异化的防卫规则以及权限等级，并实现对网络资源的有效管理。例如，明确限制非工作时段普通员工通过 WEB 访问核心服务器，或禁止外部终端直接链接内网数据库。更加重要的是，部分高级防火墙支持“蜜罐”技术配置，可模拟系统漏洞色好难过程序你攻击的目标，从而使黑客的攻击行为被引导到安全隔离的环境，避免真实系统受损问题，完整捕获攻击行为，为后续的防护提供支持[8]。其二，防火墙在日志全流程中的应用。计算机运用产生的日志数据包括设备状态、访问记录、异常行为等海量信息，人工审核不仅耗费时间、耗费精力，还容易遗漏关键威胁的线索。防火墙可以实现日志数据的自动化采集和全生命周期的监控，从访问前发起规则匹配，完成完整的监控闭环。与此同时，防火墙具备智能数据分析和筛选能力，能够从繁杂的日志中提取高风险的数据，及时拦截非法

数据流入。除此之外，防火墙可以长期储存历史操作日志，如果出现黑客入侵的情况，则会及时做好警告并生成标准化日志，当出现攻击行为时，能够根据历史数据快速触发防御措施，从而完善预警机制，大幅提升系统的安全性[9]。

（四）病毒查杀技术的应用

在计算机网络维护期间，病毒查杀技术具有重要的应用价值。计算机在运行的过程中经常会遇到病毒感染的问题，而加强病毒防护软件的安装能够在内部做好对病毒的防御和控制。计算机病毒防护软件可以对计算机中存在的病毒做好识别和处理，根据其情况做好应对，从而保障计算机的安全稳定运行。现阶段，市场上有许多不同类型的病毒防护软件，包括360安全防护软件等。为了提升此类病毒防护软件的使用效果，则需要选择正规的平台来安装，避免计算机的安全性受到威胁；用户也需要定期对软件进行升级和更新，使软件当前的病毒数据库以及相关的系统补丁等较为全面，从而提升计算机网络运行的安全防护能力[10]。

四、制定必不可少的安全防护方案和应对措施

预防数据泄露是信息安全体系的核心目标之一，数据泄露事件一旦发生，会引发法律风险和经济损失。以下是数据泄露后应采取的关键步骤和防护建议：

（一）及时启动应急响应预案、进行取证与系统日志分析并及时通报相关方

确认并隔离泄露源数据泄露的范围、类型。隔离受感染的系统 / 服务器。暂停一切访问权限。组建包括 IT 安全、法务、管理层等在内的跨部门应急小组。明确成员职责。保留所有日志，用于后续调查。根据《网络安全法》《个人信息保护法》等法规，向监管机构和利益相关方报告。及时并尽早发布官方声明，避免隐瞒或模糊处理，以维护公众信任。

（二）系统与数据恢复阶段、加强监控

1. 修复安全漏洞重置凭证与密钥

更新防火墙规则、WAF 策略、IDS/IPS 规则以阻断类似攻击。重置所有可能泄露的账户密码、API 密钥等。启用安全认证作为强制安全措施。

2. 数据恢复与系统重建、加强监控与威胁狩猎

在新环境中重新部署服务。部署 EDR、SIEM 等工具。排查潜伏威胁。采用数据分类与分级保护，进行强身份认证与访问控制，实施差异化保护策略。尤其对管理员、远程访问和高权限账户。定期审查和清理过期权限。

（三）安全防护体系的长期建设

1. 完善安全策略与制度、强化技术防护

根据主流的攻击手段和新技术制定或更新《应急响应预案》、《数据分类分级管理制度》。部署 DLP 系统，对敏感数据进行加密存储与传输。

2. 加强员工安全意识培训、明确第三方风险管理

定期开展防范培训，对供应商、合作伙伴进行安全评估。在协议中明确数据保护责任与违约条款。

“最好的数据泄露应对，就是不让它发生。”通过“快速响应 + 风险把控”的防护机制，筑牢安全底座。

五、结束语

综上所述，网络技术的快速发展给日常生活带来诸多便利。然而，在网络背后隐藏的各类隐患也不容忽视。因此，计算机网络安全技术的应用具有重要的价值。无论是企业还是个人都需要有效做好计算机网络维护工作，利用入侵检测、数据加密、防火墙、病毒查杀等技术入手，避免由于信息被泄露而影响网络安全的问题出现。

参考文献

[1] 侯英杰 . 大数据技术在计算机网络安全中的应用策略 [J]. 通讯世界 ,2024,31(11):34-36.

[2] 夏亦晗 . 计算机网络安全技术在网络安全维护中的应用分析 [J]. 上海轻工业 ,2024,(06):138-140.

[3] 朱意 , 胡雪春 . 计算机网络安全技术在电子商务平台运维中的应用策略研究 [J]. 信息与电脑 (理论版),2024,36(14):124-126.

[4] 李林蔚 . 计算机网络安全技术在系统维护中的应用 [J]. 电子技术 ,2024,53(02):87-89.

[5] 祖晓明 . 数据加密技术在计算机网络通信安全中的应用策略 [J]. 信息记录材料 ,2024,25(02):30-32.

[6] 刘超 . 计算机网络安全技术在广电网络维护中的应用 [J]. 电视技术 ,2024,48(01):164-166.

[7] 薛仓 , 张维航 . 防火墙技术在计算机网络安全中的应用策略 [J]. 中国新通信 ,2023,25(24):110-112.

[8] 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.

[9] 魏涛 . 计算机网络安全技术在网络安全维护中的应用探讨 [J]. 软件 ,2023,44(10):41-43.

[10] 王永范 . 计算机网络安全技术在网络维护中的应用 [J]. 信息系统工程 ,2023,(09):43-46.

