计算机网络安全技术在网络安全维护中的应用

孙雪慧
北京铁路通信信号运维中心　北京　100030

摘　要：在数字化时代，网络已深度融入社会生产生活，而网络安全威胁的频繁出现，使计算机网络安全技术成为维护网络稳定的关键。本文先界定计算机网络安全概念、分析威胁来源，明确技术应用的基础背景；再从技术与管理层面剖析当前技术应用面临的挑战；重点阐述加密、访问控制、防火墙等核心技术在网络安全维护中的具体应用场景与成效；因此，从技术创新、管理机制完善方面提出对策建议。研究旨在为提升网络安全维护水平提供清晰思路，助力构建更安全的网络环境，保障个人与企业的网络权益。

关键词：计算机网络安全技术；网络安全维护；技术应用

引言：社会经济水平的发展，网络已深度嵌入社会各领域，成为推动发展的关键力量。而网络安全威胁如影随形，时刻威胁着个人、企业乃至国家的利益，计算机网络安全技术作为抵御威胁的有力武器，其重要性日益凸显。本文将深入探讨计算机网络安全技术相关概念、威胁来源，剖析其应用面临的挑战，阐述核心应用场景，并提出有效对策建议。

1 计算机网络安全技术概述

1.1 计算机网络安全的概念

计算机网络安全是指通过各类技术与管理措施，保障计算机网络系统中的硬件、软件及数据不受偶然或恶意因素的破坏、更改、泄露，确保网络系统能持续、可靠、正常地运行，为用户提供安全的网络服务。其核心涵盖保密性、完整性、可用性三大要素：保密性要求网络数据仅能被授权用户访问，防止未授权者窃取；完整性确保数据在传输、存储过程中不被篡改，保持原有状态；可用性则保证网络资源与服务在需要时能及时被授权用户正常使用，不受恶意阻断。从范围来看，计算机网络安全既包括局域网、广域网等不同网络环境的安全，也涉及终端设备、服务器、网络设备等硬件安全，以及操作系统、应用软件、数据库等软件安全，是一个覆盖多维度、全层面的安全体系。

1.2 计算机网络安全威胁的来源

计算机网络安全威胁来源多样，主要有外部恶意攻击、内部操作不当、网络环境自身缺陷三类。外部恶意攻击常见，包括黑客攻击、病毒与恶意软件入侵、网络钓鱼等。黑客利用漏洞非法入侵，窃取数据或破坏系统；病毒等通过多种途径传播，感染设备后危害巨大；网络钓鱼诱导用户泄露信息。内部操作不当也易引发问题，部分员工安全意识差，有使用弱密码等行为，少数内部人员还可能恶意窃取数据或破坏系统[1]。此外，网络环境自身有缺陷，如网络协议有漏洞、硬件老化、软件未及时更新补丁等，都可能被攻击者利用，影响网络安全。

2 计算机网络安全技术应用的挑战

2.1 技术层面

在技术层面，计算机网络安全技术应用面临技术更新滞后、技术兼容性差与新兴技术带来新风险三大挑战。随着网络攻击手段不断升级，攻击者的技术水平持续提高，新型攻击方式（如AI驱动的自动化攻击、针对物联网设备的攻击）层出不穷，而部分企业使用的安全技术更新缓慢，仍依赖传统防护手段，难以应对新型威胁。例如，传统防火墙对加密流量中的恶意代码检测能力不足，无法有效阻挡隐藏在加密数据中的攻击。技术兼容性问题也较为突出，不同企业可能采用不同厂商的安全产品（如杀毒软件、入侵检测系统），这些产品之间可能存在协议不兼容、数据无法共享的问题，导致安全防护体系存在漏洞，无法形成统一的防护合力。同时，云计算、大数据、人工智能等新兴技术在推动网络发展的同时，也带来了新的安全风险，如云计算环境中多租户共享资源可能导致数据隔离失效，大数据存储与分析过程中存在数据泄露风险，这些都给计算机网络安全技术的应用带来了新的挑战。

2.2 管理层面

管理层面的挑战主要体现在安全管理制度不完善、人员安全意识薄弱与安全管理资源不足三方面。部分企业虽部署了先进的计算机网络安全技术，但缺乏配套的安全管理制度，如未明确各部门与员工的安全职责、未制定规范的网络操作流程、未建立完善的安全事件应急响应机制等，导致技术无法充分发挥作用。例如，企业虽安装了访问控制技术，但未定期审查用户权限，导致

离职员工仍能访问企业内部网络，造成数据泄露风险。人员安全意识薄弱是另一个关键问题，许多员工对网络安全知识了解不足，存在随意透露账号密码、忽视安全告警、违规处理敏感数据等行为，成为网络安全防护的薄弱环节。此外，部分中小企业面临安全管理资源不足的问题，缺乏专业的网络安全管理人员，无法对安全技术的应用进行有效维护与监控，也难以承担高额的安全技术升级与运维成本，导致网络安全技术应用效果不佳，无法有效应对网络安全威胁[2]。

3 计算机网络安全技术在网络安全维护中的核心应用

3.1 加密技术

加密技术是保障网络数据安全的核心技术之一，通过特定的算法将明文数据转换为密文，防止数据在传输与存储过程中被未授权者窃取或篡改，在网络安全维护中应用广泛。对称加密算法与非对称加密算法是两种主要的加密技术类型。对称加密算法（如AES-256、DES）使用相同的密钥进行加密与解密，加密速度快、效率高，适用于大规模数据加密，在企业内部文件传输、数据库存储中应用较多，例如企业将内部财务数据、客户信息存储在数据库时，采用AES-256算法加密，确保数据即使被非法获取也无法被解读。非对称加密算法（如RSA、ECC）使用公钥与私钥一对不同的密钥，公钥可公开用于加密，私钥由用户自行保管用于解密，安全性更高，适用于跨网络、跨主体的数据传输，如在电子商务交易中，商家与消费者通过RSA算法加密传输支付信息，防止支付数据被拦截与篡改，保障交易安全。

3.2 访问控制技术

访问控制技术通过制定严格的权限规则，限制用户对网络资源的访问，确保只有授权用户能在授权范围内使用资源，是维护网络安全的重要技术手段。基于角色的访问控制（RBAC）与基于属性的访问控制（ABAC）是当前主流的应用模式。基于角色的访问控制根据用户在组织中的岗位角色分配访问权限，不同角色对应不同的资源访问范围，例如企业中，运维人员拥有服务器后台的管理权限，可进行系统配置与维护操作；普通员工仅拥有办公软件、内部文件的访问权限，无法操作核心服务器，这种方式简化了权限管理，避免了权限滥用。基于属性的访问控制则结合用户属性（如部门、职位、所属团队）、资源属性（如数据类型、敏感级别、存储位置）与环境属性（如访问时间、访问设备、网络位置）动态判断用户访问权限，适用于复杂的网络环境，例如政府部门在处理涉密文件时，仅允许特定部门、特定职位的人员在工作时间通过内部办公设备访问，有效保障了涉密数据的安全。

3.3 防火墙技术

防火墙技术作为网络边界防护的关键技术，通过在网络边界设置防护屏障，依据预设的访问控制规则对进出网络的数据包进行过滤与审查，阻挡非法访问与恶意攻击，保障内部网络安全。包过滤防火墙与应用层防火墙（WAF）是两种常见的防火墙类型，在网络安全维护中发挥着不同的作用。包过滤防火墙基于数据包的IP地址、端口号、协议类型等信息进行过滤，可快速判断数据包是否符合规则，例如禁止外部IP地址访问内部网络的22端口（SSH端口）与3389端口（远程桌面端口），防止黑客通过这些端口非法远程登录内部服务器，其特点是速度快、开销小，适用于网络边界的基础防护[3]。应用层防火墙（WAF）则针对Web应用层的攻击（如SQL注入、跨站脚本攻击、文件上传漏洞攻击）进行防护，通过分析HTTP/HTTPS协议流量，识别并拦截恶意请求，例如某电商平台部署应用层防火墙后，成功拦截了大量试图通过SQL注入获取用户订单数据的攻击请求，保障了平台Web应用的安全运行与用户数据安全。

3.4 入侵检测技术

入侵检测技术通过对网络流量、系统日志、用户操作行为等进行实时监测与分析，识别网络中的异常行为与入侵活动，及时发出告警并采取相应措施，在网络安全维护中起到“监控者”与“预警者”的作用，有效弥补了防火墙技术的不足。基于特征的入侵检测与基于异常的入侵检测是两种主要的检测方式。基于特征的入侵检测通过建立已知攻击行为的特征库，将实时监测到的行为与特征库进行比对，若匹配则判定为入侵行为，例如检测到符合勒索病毒传播特征的网络流量时，立即发出告警，这种方式检测准确率高、误报率低，但对未知攻击的检测能力不足。基于异常的入侵检测通过建立正常网络行为的基线模型，当监测到的行为偏离基线模型达到一定程度时，判定为异常行为，可有效检测未知攻击，例如监测到某终端设备突然向外部大量发送敏感数据，偏离了正常的数据传输行为基线，判定为异常并发出告警。目前，多数入侵检测系统结合两种检测方式，在企业网络、政府网络中广泛应用，帮助管理员及时发现并应对入侵活动，减少网络安全事件造成的损失。

3.5 虚拟专用网技术

虚拟专用网（VPN）技术通过在公共网络（如互联网）中构建加密的专用通信隧道，实现远程用户、分支机构与企业内部网络之间的安全数据传输，在远程办公、跨区域企业网络互联中发挥着重要作用，是网络安

全维护的重要技术之一。SSL VPN与IPsec VPN是两种主流的虚拟专用网技术类型，应用场景各有侧重。SSL VPN基于HTTPS协议构建加密隧道，用户无需安装专用客户端，通过浏览器即可接入虚拟专用网，操作简便、灵活性高，适用于远程办公人员访问企业内部网络，例如企业员工在家办公时，通过SSL VPN登录企业OA系统、访问内部文件服务器，数据传输过程全程加密，防止数据被拦截与窃取。IPsec VPN则通过对IP数据包进行加密与认证，实现不同网络之间的安全互联，适用于企业分支机构与总部之间的网络连接，例如某连锁企业在全国多个城市设有分支机构，通过部署IPsec VPN，实现了各分支机构与总部之间的财务数据、业务数据安全传输，确保了企业数据的一致性与安全性。

4 计算机网络安全技术应用的对策与建议

4.1 技术创新

推动技术创新是提升计算机网络安全技术应用效果的核心对策。一方面，需加强对新型网络安全技术的研发投入，针对当前网络安全威胁的新特点与新趋势，研发更先进的安全技术，如基于人工智能的智能防御技术，利用机器学习算法分析海量网络数据，实现对新型攻击行为的自动识别与实时拦截，提升网络安全防护的智能化水平；研发面向物联网、区块链的专用安全技术，解决这些新兴领域的安全漏洞，保障物联网设备与区块链系统的安全运行[4]。另一方面，需促进不同安全技术的融合应用，打破技术壁垒，构建一体化的网络安全防护体系，例如将防火墙技术、入侵检测技术与加密技术结合，形成“边界防护—异常检测—数据加密”的全流程防护机制，提升网络安全防护的整体性与有效性。同时，鼓励企业与科研机构、高校合作，建立产学研协同创新机制，加快安全技术成果的转化与应用，推动计算机网络安全技术不断升级。

4.2 完善管理机制

完善的管理机制是确保计算机网络安全技术有效应用的重要保障。企业与组织需建立健全网络安全管理制度，明确网络安全管理的目标、职责与流程，例如制定《网络安全管理规范》，明确IT部门、业务部门与员工的安全职责，规定网络设备配置、用户权限管理、数据备份与恢复等操作流程；建立网络安全事件应急响应机制，明确安全事件的发现、报告、处置流程，定期开展应急演练，提升应对安全事件的能力。加强对网络安全技术应用的日常管理与监控，安排专业的网络安全管理人员，定期对安全技术的运行状态进行检查与维护，如检查防火墙规则是否有效、入侵检测系统是否正常告警、加密技术是否正常运行等，及时发现并解决技术应用中的问题。同时，建立网络安全绩效考核机制，将网络安全管理成效纳入部门与员工的绩效考核，对在网络安全维护中表现优秀的部门与个人给予奖励，对因管理不当导致安全事件的进行问责，激发全员参与网络安全管理的积极性。

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，从加密技术保障数据安全，到防火墙技术守护网络边界，各类核心技术共同构建了网络安全防护的重要屏障。未来，随着网络技术的不断发展，网络安全威胁将更加复杂多样，计算机网络安全技术也需持续升级与创新。相信在技术、管理协同作用下，计算机网络安全技术将更好地服务于网络安全维护，为个人、企业乃至国家的网络安全保驾护航，推动数字化社会持续健康发展。

参考文献

[1]刘成.计算机网络安全技术在网络安全维护中的应用分析[J].网络安全技术与应用,2022(4):169-170.

[2]王伟.计算机网络安全技术在网络安全维护中的应用研究[J].网络安全技术与应用,2021(1):155-157.

[3]黄雨松.计算机网络安全技术在网络安全维护中的应用研究[J].网络安全技术与应用,2022(7):161-162.

[4]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.