计算机应用中的网络安全防护研究

王利平
上海俊达汽车装饰有限公司　上海　201402

摘　要：随着信息技术的飞速发展，计算机网络应用已深度融入社会各领域，企业的网络安全占有重要力量，其网络安全风险也随之激增。数据加密技术保障信息传输安全，身份认证与访问控制技术筑牢系统访问防线，网络安全意识培养、风险评估、应急响应及供应链安全管理等策略，从管理层面为网络安全提供支撑。这些防护技术与管理策略相互配合，构建起多层次、全方位的网络安全防护体系，对维护网络空间稳定、保障信息安全具有重要现实意义。

关键词：计算机应用；网络安全；防护

引言

在数字化浪潮席卷全球的当下，计算机网络成为社会运转的关键基础设施，然而网络攻击手段层出不穷，勒索病毒、数据泄露等安全事件频发，严重威胁个人隐私、商业机密、企业利益乃至国家安全。在此背景下，深入研究网络安全防护技术与管理策略迫在眉睫。本文围绕数据加密、身份认证等核心防护技术，以及意识培养、风险评估等管理策略展开探讨，旨在为构建高效、可靠的网络安全防护体系提供理论与实践参考。

1 计算机网络安全概述

计算机网络安全是信息时代的重要议题，它涉及对计算机系统、网络设备及数据信息的保护，以防止未经授权的访问、篡改、破坏或泄露。随着信息技术的飞速发展，网络已渗透到社会生活的各个角落，网络安全问题日益凸显。计算机网络安全涵盖多个层面，物理安全主要关注硬件设备安全防护，涉及服务器、存储设备等，通过环境监控、防灾设计等措施，防止因物理损坏或环境因素导致的服务中断。网络安全聚焦于网络通信安全，通过防火墙、入侵检测系统等手段，抵御外部网络攻击，保障网络传输的保密性、完整性和可用性。系统安全涉及操作系统、数据库管理系统等核心软件的安全配置与维护，采用漏洞扫描、补丁管理等技术，确保系统免受恶意软件、病毒等威胁。应用安全针对具体业务应用，如Web应用、移动应用、API接口等，实施安全防护措施，包括代码审计、安全测试等环节，防止应用层漏洞被利用，造成数据泄露或业务中断。数据安全是计算机网络安全的核心，涉及数据的加密存储、传输及访问控制，采用对称加密、非对称加密等技术，确保数据在生命周期内始终保持机密性、完整性和可用性。随着大数据、云计算等技术的广泛应用，数据安全面临更加复杂的挑战，需要采用先进的数据加密技术、访问控制策略及数据备份恢复机制，事前采取防止措施，以应对潜在的安全风险。计算机网络安全还需要考虑安全管理、安全审计及应急响应等方面，通过建立完善的安全管理体系，实施定期安全审计，制定应急响应预案，确保在发生安全事件时能够迅速响应并恢复。计算机网络安全是复杂系统工程，需要技术、管理等多层面协同实现综合防护。随着网络技术的不断演进和安全威胁的日益多样化，加强网络安全研究与实践，提升网络安全防护能力，已成为保障信息时代社会稳定与经济发展的重要基石。

2 计算机应用中的网络安全防护技术

2.1 数据加密技术

数据加密技术作为保障数据安全的核心手段，通过特定算法将原始数据转换为密文形式，只有掌握对应密钥的授权方才能将其还原为原始数据。在计算机网络环境中，数据在存储和传输过程中面临诸多风险，如被窃取、篡改，数据加密技术则如同为数据披上一层隐形铠甲，有效抵御这些威胁。对称加密算法，如AES（高级加密标准），以其高效快速的加密和解密性能，在处理大规模数据时表现出色，常用于文件加密和数据库字段加密。其加密和解密使用同一密钥，在确保数据快速处理的同时，也对密钥的安全传输和存储提出了更高要求。非对称加密算法，如RSA，采用公钥加密、私钥解密的机制，公钥可公开传播，而私钥由接收方妥善保管，这种方式有效解决了密钥分发的难题，在数字签名和安全通信握手阶段广泛应用。哈希函数加密技术则将数据映射为固定长度的哈希值，常用于验证数据完整性，即便数据出现微小改动，生成的哈希值也会截然不同，能够快速识别数据是否被篡改。在云计算场景中，用户上传至云端的数据经过加密处理，云服务提供商无法直接获取原始数据内容，保障了用户数据的隐私性；在金融交

易数据传输中，加密技术确保账户信息和交易金额等敏感数据安全抵达目标系统，防止在网络传输过程中被窃取或恶意修改，从而维护金融交易的安全性和可靠性[1]。

2.2 身份认证技术

身份认证技术旨在确认网络中用户或设备的真实身份，是计算机网络安全的第一道防线，只有通过身份验证的主体才能获得相应的访问权限，防止非法用户或设备入侵系统。基于密码的身份认证方式是最常见的形式，用户设置特定的密码，系统通过验证密码的正确性来确认用户身份。密码存在被猜测、窃取的风险，因此衍生出了密码复杂度要求、定期更换密码等增强措施。生物特征认证技术凭借其独特性和难以复制的优势，逐渐成为身份认证的重要发展方向。指纹识别通过扫描用户指纹的纹路特征进行匹配，人脸识别则依据面部的几何结构和特征点进行身份验证，虹膜识别利用人眼虹膜的独特纹理信息，这些生物特征与个体一一对应，具有极高的安全性和准确性，广泛应用于移动设备解锁、门禁系统等场景。双因素认证结合了两种不同类型的认证因素，如密码与动态验证码，或者生物特征与智能卡，即使其中一种认证方式被破解，攻击者仍无法通过另一重验证，极大提升了身份认证的安全性。在企业远程办公场景中，员工需要通过输入密码和接收手机短信验证码双重验证才能登录企业内部系统，防止非法人员冒充员工访问企业敏感数据；在在线支付平台，用户不仅需要输入支付密码，还可能需要进行指纹或刷脸验证，确保交易操作是由本人发起，保障资金安全，避免因身份冒用导致的财产损失。

2.3 访问控制技术

访问控制技术通过制定和实施一系列策略，对网络资源的访问进行精确管理，确保只有合法且具备相应权限的主体能够访问特定资源，防止未授权的访问、使用和修改。自主访问控制（DAC）赋予资源所有者自主决定访问权限的能力，所有者可以根据用户身份和需求，灵活设置其他用户对资源的读、写、执行等权限，这种方式在小型网络环境和个人计算机系统中应用广泛，方便用户对自身资源进行个性化管理。强制访问控制（MAC）则依据主体和客体的安全标签进行访问决策，系统预先定义不同的安全级别，只有主体的安全级别高于或等于客体时，才允许访问，这种严格的控制方式常用于对安全性要求极高的环境，如数据库系统，确保敏感数据只能被特定安全级别的用户访问。基于角色的访问控制（RBAC）将用户划分为不同角色，每个角色被赋予相应的权限集合，用户通过角色获得权限，这种方式简化了权限管理，尤其适用于大型企业网络，当企业人员变动或业务调整时，只需对角色权限进行修改，而无需逐一调整每个用户的权限。在企业文件服务器中，普通员工角色只能读取部分公共文件，部门经理角色可以访问本部门相关的机密文件并进行编辑，而管理员角色则拥有对整个服务器资源的完全控制权限；在电商平台的后台管理系统中，客服人员角色仅能查看和处理客户订单信息，而运营人员角色还具备修改商品信息和设置促销活动的权限，通过精准的访问控制，保障了系统资源的安全性和业务流程的正常运行[2]。

3 计算机应用中的网络安全防护管理策略

3.1 网络安全意识培养

（1）在计算机应用场景中，网络安全意识是用户抵御安全威胁的第一道心理防线。无论是个人或是企业，每一个使用网络的用户都需深刻理解网络安全威胁的多样性，无论是钓鱼邮件中精心设计的虚假链接，还是伪装成正常软件的恶意程序，都可能成为数据泄露和系统入侵的突破口。用户应主动学习网络安全基础知识，掌握识别常见网络攻击手段的方法，提升对潜在风险的敏感度与警觉性。（2）网络安全意识的培养需融入日常使用习惯的塑造。在处理文件时，避免随意打开来源不明的附件和链接，养成从官方渠道下载软件的习惯，防止因软件携带恶意代码而导致系统感染病毒。定期更换复杂密码，不使用简单易猜的组合，同时妥善保管个人账号信息，不轻易向他人透露，从源头上减少账号被盗用的风险。（3）通过模拟网络安全攻击场景进行实践演练，能够有效强化用户的安全意识。在模拟钓鱼攻击的演练中，用户可以直观感受攻击者的欺骗手段，学习如何识别虚假信息；在模拟系统被入侵的场景下，用户能够亲身体验感受到数据泄露的危害，从而更加重视数据备份和安全防护措施，将网络安全意识转化为实际的防护行为。

3.2 网络安全风险评估

（1）网络安全风险评估需对计算机系统和网络环境进行全面且深入的分析。要识别网络中的各类资产，包括硬件设备、软件系统、数据资源等，明确其在业务流程中的重要性和价值。针对服务器、数据库等核心资产，评估其可能面临的物理损坏、网络攻击、数据丢失等潜在威胁，以及威胁发生的可能性和影响程度。（2）对网络系统的脆弱性进行细致排查是风险评估的关键环节。利用专业的漏洞扫描工具，检测操作系统、应用程序和网络设备中存在的安全漏洞，如未修复的系统补丁、配置错误的防火墙规则等。分析网络架构设计是否

合理，是否存在单点故障、权限划分不明确等问题，这些脆弱性都可能成为攻击者入侵的切入点。（3）基于资产识别、威胁分析和脆弱性评估的结果，对网络安全风险进行量化评估。采用科学的风险评估模型，综合考虑资产价值、威胁发生概率和脆弱性严重程度，计算出风险等级。对于高风险项，制定详细的风险应对方案，优先采取修复漏洞、加强防护等措施；对于中低风险项，持续监控并适时优化防护策略，确保网络系统在可接受的风险范围内运行[3]。

3.3 应急响应机制构建

（1）构建应急响应机制首先需明确应急响应团队的职责和分工。组建含网络安全专家、系统管理员、数据恢复人员的专业团队，明确各成员具体任务，如专家分析攻击制定防御策略，管理员负责系统恢复，恢复人员专注数据抢救，确保团队高效协作应对安全事件。（2）制定完善的应急响应流程是保障机制有效运行的核心。当安全事件发生时，第一时间进行事件确认和分类，判断是网络攻击、数据泄露还是系统故障等类型。根据事件的严重程度和影响范围，启动相应级别的应急响应预案，采取隔离受感染设备、阻断攻击源等紧急措施，防止事件进一步扩大。深入调查事件原因，收集相关证据，为后续处理和防范提供依据。（3）应急响应机制的有效性需通过定期演练和优化来保障。模拟不同类型的安全事件，如勒索病毒攻击、DDoS攻击等，检验应急响应团队的反应速度和处理能力。在演练过程中，发现流程中的不足之处，及时调整和完善预案，补充应急资源，提升团队成员的实战经验和协同能力，确保在真实安全事件发生时能够快速、有效地进行处置，将损失降到最低。

3.4 供应链安全管理

（1）在计算机应用的供应链安全管理中，对供应商的选择和评估至关重要。引入新供应商时，要全面审查其安全能力与信誉，评估开发中的安全措施，如代码审查机制、安全开发标准遵循情况，并考察其历史有无安全问题导致数据泄露等事件，优先选择安全可靠的合作伙伴。（2）加强对供应链中产品和服务的全生命周期监控是保障安全的关键环节。从产品的设计、开发、生产到交付使用，对每一个环节进行严格把控。在软件开发过程中，通过持续集成和持续交付（CI/CD）流程，定期进行安全测试，及时发现并修复潜在的安全缺陷。在硬件设备生产环节，确保生产环境的物理安全，防止恶意植入硬件后门。在产品交付后，建立反馈机制，及时收集和处理用户反馈的安全问题。（3）建立供应链安全事件的应急处理机制是应对突发状况的必要手段。当发现供应链中存在安全隐患或发生安全事件时，迅速启动应急响应。与供应商紧密协作，共同分析问题根源，制定解决方案。对于存在严重安全问题的产品或服务，及时采取隔离、停用等措施，防止安全风险扩散。总结事件经验教训，优化供应链安全管理策略，提升整体供应链的安全防护水平[4]。

结语

综上所述，计算机应用中的网络安全防护是一项重要而复杂的系统工程，小则影响个体利益，大则危害国家安全。数据加密、身份认证等技术为网络安全构筑技术屏障，网络安全意识培养、风险评估等管理策略则夯实安全管理基础。未来，随着人工智能、物联网、云网联等技术的发展，网络安全威胁将更趋复杂，需持续创新防护技术，完善管理策略，不断提升网络安全防护能力，以应对日益严峻的网络安全挑战。

参考文献

[1]张敏.计算机应用中的网络安全防护研究[J].中国新通信,2024,26(23):41-43.

[2]张志花.计算机应用中的网络安全防护研究[J].电脑编程技巧与维护,2020(8):171-173.

[3]王月红.计算机应用中网络安全防护体系构建研究[J].计算机产品与流通,2023(2):83-85.

[4]赵文杰,谢光敏,罗光明.计算机技术在网络安全防护系统中的应用研究[J].电脑采购,2024(12):31-33.