工程与管理科学
Engineering and Management Science
第 6 卷◆第 07 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

计算机信息管理技术在网络安全中的应用研究

李金泫
海军装备部装备保障大队
DOI：10.12238/ems.v6i7.8201

[摘　要] 本文主要探讨计算机信息管理技术在网络安全中的应用。首先介绍网络安全面临的风险，随后分析计算机信息管理技术在提升网络安全水平中的作用，最后探讨相关信息管理技术在网络安全中的应用。通过这些技术手段，希望能够有效保护网络系统免受各类威胁的侵害，推动信息安全保障能力的提高。
[关键词] 网络安全；计算机信息管理技术；身份认证；数字签名

Research on the Application of Computer Information Management Technology in Network Security

Li Jinlong
Equipment Support Brigade of Naval Equipment Department

[Abstract] This article mainly explores the application of computer information management technology in network security. Firstly, introduce the risks faced by network security, then analyze the role of computer information management technology in improving the level of network security, and finally explore the application of relevant information management technology in network security. Through these technological means, we hope to effectively protect network systems from various threats and promote the improvement of information security capabilities.
[Keywords] network security; Computer information management technology; Identity authentication; digital signature

引言：

随着信息技术的快速发展，网络已经成为人们日常生活和工作中不可或缺的一部分。然而，网络的普及和应用也带来一定安全隐患。网络安全问题的日益严峻性，要求我们采取有效的措施保护信息系统的安全性和稳定性。计算机信息管理技术作为一种重要的技术手段，在此过程中发挥重要作用。

一、网络安全风险概述

随着全球信息化进程的加速推进，网络已经走进了人类社会的方方面面，成为信息交流、商业运作、社会互动的重要载体。然而，网络的普及和便利也带来一系列复杂而严峻的安全威胁和挑战，对个人、组织乃至整个社会的稳定和安全构成严峻考验。网络安全的定义并不仅仅局限于数据、系统的保护，它涉及到通过各种技术手段和管理策略，防止未经授权的访问、使用、修改或破坏网络系统、硬件设备和数据。在当今全球互联网广泛应用的背景下，网络安全问题显得尤为紧迫。主要的网络安全风险包括但不限于黑客攻击、恶意软件、数据泄露、网络钓鱼、勒索软件等。黑客攻击者通过技术手段入侵系统，获取非法访问权限，从而窃取、篡改或破坏数据和系统。恶意软件如病毒、木马和蠕虫则通过各种方式传播，危害用户和组织的系统安全和数据完整性。数据泄露不仅可能源自内部失误或者安全漏洞，还可能是外

部黑客攻击的结果，严重威胁个人隐私和企业机密。

二、计算机信息管理技术应用在网络安全中的意义

计算机信息管理技术作为保障网络安全的重要手段，发挥着重要作用。其应用不仅可以有效防范各类网络攻击和安全威胁，还能够提升信息系统的稳定性、可靠性，从而保护个人、组织和国家的信息安全。首先，计算机信息管理技术通过建立健全的安全管理体系和技术框架，确保信息系统的整体安全。这包括制定和实施严格的访问控制策略，通过身份认证、权限管理和加密技术，限制和管理用户和设备对系统资源的访问权限，防止未经授权的访问和数据泄露。例如，采用多因素身份认证技术可以有效防止密码被盗用或者暴力破解攻击，保护用户账户和个人隐私数据的安全。其次，计算机信息管理技术通过加密技术，确保数据在传输和存储过程中的机密性。数字签名技术利用非对称加密算法，为数据和文件赋予唯一的身份标识，保证数据在传输过程中不被篡改或伪造。加密技术则通过对敏感数据进行加密处理，防止其被非法获取和使用，保护个人隐私和商业机密不受损害。另外，计算机信息管理技术还涉及到对数据备份和恢复的管理和实施。通过定期备份关键数据和系统配置，保障在系统遭受攻击、故障或者灾难性事件时能够快速恢复数据。这不仅可以减少因数据丢失或损坏而造成的经济损失，还可以保证信息系统的持续运行和业务的连续性。此外，网络访问控制技术也是计算机信息管理技术中的重要组成部分。它通过实施网络隔离、流量监控、行为分析和访问审计等措施，有效管理和控制用户和设备对网络资源的访问。通过分析和识别异常访问行为，及时发现和阻止潜在的安全威胁，提升网络系统的安全防护能力。

三、计算机信息管理技术在网络安全中的应用

（一）身份认证技术

在实际应用中，身份认证技术发挥关键作用，涵盖多个关键领域：企业网络安全：许多企业采用基于 LDAP（轻量级目录访问协议）或 Active Directory 的集中式身份认证系统。这些系统管理和验证员工、合作伙伴和客户的身份，确保只有授权的个人可以访问公司的网络和敏感数据。通过密码认证、双因素认证或生物特征认证，企业可以有效地防范内部和外部威胁，维护企业数据的完整性。首先是电子商务平台：在线购物和支付平台依赖于强大的身份认证机制来保护用户的个人信息和财务安全。例如，双因素认证可以确保只有经过验证的用户才能完成交易，防止恶意攻击者利用盗取的账户信息进行欺诈行为。此外，信用卡公司和支付处理器也广泛使用身份认证技术来验证卡主的身份，以减少信用卡诈骗。其次是政府和公共服务：政府部门提供的在线服务通常要求用户进行身份认证，以确保服务的合法性。例如，在线税务申报系统和电子投票系统通过严格的身份验证措施，防止恶意行为和非法访问，保护公民的个人数据和选举结果的安全。最后是医疗保健行业：医院和医疗机构使用身份认证技术来保护医疗记录和患者敏感信息的隐私。只有经过授权的医护人员可以访问和更新患者的电子病历，确保医疗信息的机密性和完整性，同时遵守健康保险可信度法案（HIPAA）等法律法规[1]。

（二）数字签名技术

数字签名技术作为现代网络安全中的组成部分，通过利用公钥密码学原理，能够为数据的完整性、真实性提供了强大的保障。其应用广泛涵盖了电子商务、电子合同、软件分发等多个领域，为信息交换和业务交易的安全性提供关键支持。在电子商务中，数字签名技术被广泛应用于在线交易的安全保障。它确保买卖双方在交易过程中的数据传输的安全性，防止信息的篡改伪造。通过使用数字签名，商家和消费者可以安全地传输和接收敏感信息，如支付信息，而不必担心被第三方恶意攻击者窃取或篡改。在电子合同和法律文件签署方面，数字签名技术为在线签署提供法律效力。通过数字签名，签署者确保签署过程的真实性和不可抵赖性，有效地防止合同内容或签署方身份的伪造。这种技术不仅提高合同签署的效率，也加强合同法律效力的认可，为跨国业务和跨境合作提供便利。在软件分发和更新中，数字签名技术用于验证软件的源头和完整性。软件开发者可以使用数字签名在软件发布之前对其进行签名，而用户则可以使用相应的公钥来验证软件的真实性和完整性[2]。

（三）数据备份技术

随着信息化程度的提升，企业和个人面临着越来越多的

数据安全挑战。数据备份技术以其保护关键数据免受损失和泄露的能力，成为保障数据安全和业务连续性的重要手段。数据备份的核心目标是通过定期将关键数据复制到安全存储介质中，如磁带、硬盘、云存储等，以应对各种潜在的安全威胁和灾难事件。备份策略的制定至关重要，企业通常会根据数据的重要性和更新频率制定不同的备份计划，包括完整备份、增量备份和差异备份等，以平衡数据恢复速度和存储成本之间的关系。在实际应用中，数据备份技术广泛应用于多个关键场景。首先，灾难恢复是其最主要的应用。当网络遭受自然灾害、恶意攻击或硬件故障时，备份技术能够帮助组织快速恢复受影响的系统和数据，减少业务停机时间。其次，面对恶意软件、勒索软件和数据泄露等威胁，及时的数据备份能够有效防止数据被加密、篡改，帮助组织避免支付高额赎金或面临长期数据损失的风险。此外，数据备份技术在长期数据保存和合规性方面也发挥着重要作用。根据法律法规和行业标准，企业需要对重要数据进行长期保存，并保证其完整性。通过有效的备份管理，组织能够满足监管要求，同时确保历史数据在需要时能够快速检索和恢复。在技术实施方面，数据备份技术采用一系列先进的技术手段来增强数据的安全性和效率。例如，数据加密技术可以在备份过程中对数据进行加密，保护备份数据不受未经授权的访问。数据压缩技术则能够减少备份数据的存储空间需求，优化存储资源的利用效率。尽管数据备份技术在提供数据安全保障方面表现出色，但也面临一些挑战和发展趋势。随着数据量的快速增长和多样化，如何有效管理备份数据和优化存储资源成为当前的关键问题[3]。

（四）网络访问控制技术

网络访问控制技术是保障网络安全的重要组成部分，其核心任务是管理和监控网络资源的访问，确保只有经过授权的用户才能够合法地访问特定的网络资源。在实施网络访问控制技术时，首先是身份识别与验证阶段。用户或设备在尝试访问网络资源之前，需要提供有效的身份信息进行识别和验证。常见的身份验证方式包括基于用户名和密码、生物识别技术（如指纹或面部识别）、硬件标识符（如 MAC 地址）等。验证成功后，系统会根据预先设定的访问策略进行授权，确定用户或设备能够访问的资源和服务范围。访问控制技术的关键在于有效的访问策略管理。网络管理员根据安全需求、业务需求和法规合规性要求，制定和实施适当的访问控制策略。这些策略通常包括授权的用户角色、时间段访问限制、特定网络区域的访问权限等。通过精细的策略制定，网络管理员可以在保证安全的同时，最大程度地满足用户的业务需求。网络访问控制技术在多个关键场景中具有重要应用价值。首先，它有效保护关键资产免受未经授权的访问。通过限制和监控用户和设备的访问权限，可以防止恶意活动和数据泄露，保障关键数据和应用程序的安全性。其次，面对内部威胁和外部攻击，网络访问控制技术能够减少安全漏洞的风险，防范恶意行为对网络系统造成的损害。此外，合规性是推动组织实施严格访问控制的重要因素。根据不同的行业法规和隐私法律，组织需要确保访问控制措施符合相关法律法规的要求，防止因合规问题而面临的法律风险和罚款。尽管网络访问控制技术在提供安全访问管理方面表现出色，但也面临着技术挑战和持续发展的需求。随着网络环境的复杂化和用户需求的多样化，如何有效地管理和控制不断增长的网络访问请求，是当前面临的主要挑战[4]。

四、结束语

综上所述，计算机信息管理技术在网络安全中的应用不仅是技术发展的重要方向，也是推动数字经济持续健康发展的关键保障。通过不断深化研究和实践应用，将有望共同迈向一个更加安全、智能的网络安全新时代。

[参考文献]

[1]毛军强.计算机信息管理技术在网络安全中的应用探讨[J].信息与电脑，2023，35（15）：99-102.

[2]白鸥.计算机信息管理技术在维护网络安全中的应用策略探究[J].中文科技期刊数据库（全文版）自然科学，2023（4）：4.

[3]支花明.计算机信息管理技术在医院网络安全中的应用探讨[J].中文科技期刊数据库（全文版）工程技术，2023（10）：11-14.

[4]陶亮.计算机网络技术在电子信息工程中的应用研究[J].智能城市应用，2023，6（11）：56-58.