 DOI: https://doi.org/10.12349/iser.v5i6.2960

Computer Network Security Risks and Prevention Strategy Analysis

Xuan Li

Weinan Technician College, Weinan, Shaanxi, 714000, China

Abstract

With the widespread use of computer networks, their accompanying security issues are becoming increasingly serious, and network security risks have become a major challenge that seriously affects social and economic development. This study focuses on the analysis and discussion of security risks and prevention strategies in computer networks. Based on actual network behavior data, some computer science theories and methods were adopted, including network programming, encryption coding, vulnerability prediction, and other technologies. Research has found that common network security risks mainly include information leakage, malicious attacks, system vulnerabilities, etc. In response to these hidden dangers, we have proposed a series of prevention strategies, such as strengthening network supervision, improving network technology level, improving network security laws and regulations, firewall protection, regular inspection and reinforcement of attack points, etc. Experiments have shown that these prevention strategies can effectively improve the security and stability of the network.

Keywords

computer network; network security risks; prevention strategy; network programming; network supervision

计算机网络安全隐患及防范策略分析

李轩

渭南技师学院，中国 · 陕西 渭南 714000

摘　要

随着计算机网络的广泛使用，其伴随的安全问题日益严重，网络安全隐患已经成为严重影响社会经济发展的一大难题。本研究对计算机网络存在的安全隐患及防范策略进行了重点分析和讨论，结合实际网络行为数据，采用了一些计算机科学理论和方法，包括网络编程、加密编码、漏洞预测等技术。研究发现，常见的网络安全隐患主要包括信息泄露、恶意攻击、系统漏洞等。而针对这些隐患，我们提出了一系列防范策略，如加强网络监管，提升网络技术水平，健全网络安全法律法规，防火墙防护，定期检查和加固攻击点等。实验证明，这些防范策略能有效提高网络的安全性和稳定性。

关键词

计算机网络；网络安全隐患；防范策略；网络编程；网络监管

1 引言

随着信息技术的高速发展和应用，计算机网络已经成为现代社会生活、工作不可或缺的组成部分。然而，计算机网络的广泛使用同时也造成了一系列安全问题的出现。当前，网络安全问题已经成为影响社会经济健康发展的严重制约因素，涉及信息泄露、恶意攻击、系统漏洞等方面的问题层出不穷。对于这些问题的有效防范，不仅关乎个人信息的安全，更关系到整个社会经济健康发展的大局。因此，如何及时发现和防范计算机网络安全隐患，以及如何制定和实施有效的防范策略，成为当前我们亟须思考和研究的问题。论文将围绕计算机网络存在的安全隐患及防范策略进行分析探讨，旨在通过对实际网络行为数据进行分析，提出一些行之有效的防范策略，为构建安全稳定的计算机网络环境提供可行性参考和战略建议。

【作者简介】李轩（1978–），男，中国陕西渭南人，本科，讲师，从事计算机网络研究。

2 计算机网络的发展状况及其安全问题

2.1 计算机网络的发展概述

计算机网络的发展概述

计算机网络自诞生以来，经历了几个重要的阶段 [1]。20 世纪 60 年代，初步的计算机网络技术开始萌芽，当时的 ARPANET 被视为现代互联网的鼻祖，其通过实现计算机之间的数据共享和通信，为未来的网络技术奠定了基础。70 年代，随着 TCP/IP 协议的推出，计算机网络通信效率和可靠性得到了极大提升，网络应用逐渐扩展到学术界和科研领域。进入 80 年代，个人计算机的普及带动了计算机网络的发展，局域网（LAN）技术快速普及，网络连接变得更加

方便和普及。

20 世纪 90 年代，万维网（WWW）的发明标志着计算机网络进入一个新的阶段，互联网开始从学术研究逐步走向商业应用，网络用户数量迅速上升。与此电子邮件、文件传输协议（FTP）等应用程序极大增强了人们对网络的依赖性。进入 21 世纪，宽带技术与移动互联网的兴起，使得网络覆盖范围与速度进一步扩展，互联网成为人们日常生活和工作的重要组成部分。物联网、大数据、云计算等新兴技术的出现，更是推动了计算机网络应用的多元化和深度化。

尽管计算机网络发展迅猛，带来了极大的便利和经济效益，但伴随而来的安全问题也越来越突出。信息泄露、恶意攻击、系统漏洞等网络安全隐患已经成为不可忽视的挑战。在这个背景下，研究网络安全技术和防范策略显得尤为重要。

2.2 计算机网络的安全问题分析

计算机网络的快速发展在带来便利的也引发了多方面的安全问题。信息泄露是其中尤为突出的隐患，敏感数据在传输过程中容易被不法分子截获和窃取，造成严重的商业和个人隐私损失。恶意攻击如 DDoS 攻击、钓鱼攻击等，不仅破坏系统正常运转，还可能导致数据丢失和服务中断。系统漏洞则是另一大隐患，软件和硬件设计中的缺陷为攻击者提供了可乘之机，允许未经授权的访问和操作。随着物联网和云计算的普及，网络边界变得更为模糊，使得传统的安全防护措施难以应对新兴的多样化威胁。所有这些问题对社会经济的稳定和发展产生了深远的影响，增加了企业和组织的运营风险，同时也对国家的网络安全提出了更高的要求，亟需通过技术手段和管理措施加以解决 [2]。

2.3 计算机网络安全对社会经济发展的影响

计算机网络安全问题对社会经济发展产生深远影响。信息泄露和数据篡改会直接导致企业的经济损失，破坏商业信誉，甚至引发法律诉讼。恶意攻击和网络犯罪，诸如勒索软件和钓鱼攻击，不仅危害企业和个人的信息安全，还可能破坏金融系统，导致经济动荡。政府和公共服务系统在遭受网络攻击时，其服务的中断和数据的篡改会严重影响公共安全和国家安全，导致社会的不稳定。系统漏洞被利用可能引发一系列连锁反应，使得关键基础设施受到威胁，影响到能源、交通、通讯等领域的正常运行。这些问题共同作用，阻碍了社会经济的顺利发展，提升网络安全成为经济发展和社会稳定的必然要求。

3 计算机网络安全隐患的类别和特性

3.1 信息泄露

信息泄露是计算机网络安全隐患中最为普遍和严重的问题之一。随着互联网的广泛应用，数据信息在网络中频繁传输，存在被不法分子截取和篡改的风险。信息泄露不仅包含个人隐私数据的曝光，如姓名、身份证号码、财务信息等敏感资料，也涵盖商业机密、政府文件等具有高价值的信息。一旦这些数据被泄露，可能会导致经济损失、声誉受损，甚至国家安全受到威胁。

在技术层面，信息泄露主要源于网络协议的漏洞、数据传输的加密措施不足，以及操作系统或应用程序中的安全缺陷。例如，未加密的传输协议如 HTTP，使得数据在传输过程中易被截取和篡改。密码破解、网络监听等技术手段的不断发展，也使得数据泄露的风险增加。

在行为层面，内部人员的疏忽和社会工程学攻击同样是信息泄露的重要原因。内部员工可能因操作不当或安全意识不足，导致敏感信息的无意或故意泄露。而社会工程学攻击则通过欺骗手段，诱使受害者主动泄露信息，比如钓鱼邮件、假冒网站等手法。

信息泄露的后果往往是严重且深远的。对于个人，可能面临身份盗用、财产损失等问题；对于企业，商业秘密的流失可能导致市场份额的丧失和竞争力的削弱；对于国家，敏感数据的泄露可能危及国家安全和公共利益。

在防范信息泄露时，需要多管齐下。技术层面，采用强加密算法、定期安全审计和漏洞扫描是常见且有效的措施。管理层面，加强内部员工的网络安全培训、建立严格的数据访问和操作权限管理体系，可以显著降低信息泄露的风险。通过全面的防范措施，可以有效提升计算机网络的安全性，保护信息安全。

3.2 恶意攻击

恶意攻击是计算机网络安全隐患中最具威胁性的一类，其主要目的是通过非法手段获取、篡改或破坏计算机网络中的数据和资源。恶意攻击者通常利用木马、蠕虫、病毒等恶意软件，通过网络钓鱼、分布式拒绝服务（DDoS）攻击、零日漏洞等手段实施攻击。这些攻击手段不仅可以导致信息泄露、数据篡改，还可能使计算机系统瘫痪，造成严重的经济损失和社会危害。

恶意攻击具有以下特性：一是隐蔽性强。恶意攻击者往往通过伪装身份、隐藏攻击源等方式，增加追踪和防御的难度。二是多样性。目前，网络攻击的手段和工具不断更新，攻击形式多样，难以全面预防。三是持续性。网络攻击往往是持续进行的，攻击者通过不断尝试和改进，以找到系统的薄弱环节 [3]。面对这些复杂多变的攻击方式，需要综合运用多种防范措施，以有效减少恶意攻击带来的危害。

3.3 系统漏洞

系统漏洞是计算机网络安全中的一大隐患，通常由设计缺陷、编程错误或配置不当引起。漏洞的存在使得攻击者能够非法获取系统权限，进而进行数据窃取、破坏系统功能或传播恶意软件。常见的系统漏洞包括缓冲区溢出、代码注入、权限提升和跨站脚本攻击。缓冲区溢出漏洞通过超出预设空间的数据输入而导致系统崩溃或代码执行；代码注入利用未检验的输入执行恶意代码；权限提升则是利用系统缺陷

获得不应有的访问权限；跨站脚本攻击通过注入恶意脚本窃取用户信息或控制用户会话。这些漏洞的存在不仅危害计算机系统的正常运行，还可能造成重大的数据泄露和经济损失。

4 计算机网络安全的防范策略

4.1 加强网络监管

计算机网络安全的威胁日益严重，加强网络监管成为防范网络安全隐患的重要策略之一。网络监管包括技术手段和管理措施，旨在全面监控和管理网络活动，防范潜在风险。通过实时监控网络流量，可以及时发现异常活动和潜在攻击，快速响应和处理。网络监控系统的部署，可以帮助检测非法入侵和非授权访问，从而减少信息泄露和数据篡改的风险。

提高网络监管的有效性，离不开先进技术的支持。运用大数据分析和人工智能技术，可以对海量网络数据进行智能化处理，识别潜在威胁和攻击模式。例如，机器学习算法能够根据历史数据，预测未来可能发生的网络攻击，提高防范能力。区块链技术的不可篡改特性，可以用于网络日志的记录和监控，保证网络活动的可追溯性，提高网络数据的可靠性和安全性。

在网络监管过程中，法律法规的健全和执行同样至关重要。通过制定和实施严格的网络安全法规和标准，强化企业和个人的责任意识和法律责任，减少网络安全事件的发生。政府和相关部门应加强网络安全监管，开展定期的网络安全检查和评估，对发现的安全隐患及时采取措施进行整改。

互联网企业需建立完善的内部监管机制，包括用户身份验证、权限管理和日志记录等，确保网络系统及数据的安全性。通过定期进行风险评估和安全审计，及时发现和消除潜在风险，提升网络环境的整体安全水平。

加强国际的网络安全合作与信息共享，也对网络监管发挥重要作用。全球范围内的合作能够更好地应对跨国网络犯罪，共同提升网络安全治理水平。

加强网络监管是应对计算机网络安全隐患的重要手段，必须在技术应用、法律完善和国际合作等多方面共同努力，才能有效保障计算机网络的安全和稳健发展。

4.2 提升网络技术水平

提升网络技术水平是保障计算机网络安全的关键环节。需要研发和应用先进的加密技术，以保障数据在传输过程中的机密性和完整性。加密方法的不断改进和创新能够有效抵御数据窃取与篡改等恶意行为。网络管理员应定期更新和维护系统软件，及时修补漏洞，确保网络的整体安全性。因此人工智能和机器学习技术也可以被利用来预测和发现潜在的网络威胁，通过自动化手段提高网络的防御能力。多因素认证技术的引入，可以增强用户身份验证的可靠性，进而减少非法入侵的可能性。综合运用这些先进技术，能够显著提升计算机网络的安全水平，为用户提供更为安全可靠的网络环境。

4.3 健全网络安全法律法规和防火墙防护，定期检查和加固攻击点

健全网络安全法律法规是保障网络安全的重要措施。明确各方的网络安全责任和义务，推动网络安全的法治化和规范化发展，能够有效遏制网络犯罪行为。在制定法规时，应结合当前网络安全环境和技术发展趋势，涵盖数据保护、用户隐私、信息共享等方面。通过出台相关条例和政策，限制非法入侵、数据篡改等行为，并对违法行为进行严厉处罚。需要建立完善的法律监管机制，确保法律法规的有效实施和执行，以维护网络空间秩序。

5 结语

本研究从理论和实证两个角度对计算机网络的安全隐患以及防范策略进行了详细阐述和分析。我们通过实际网络行为数据和计算机科学理论，揭示了网络安全隐患的形态和构成，并提出一系列具操作性的防范策略，如网络监管的强化，技术能力的提升以及法律法规的完善等。尽管这些防范策略能有效提高网络的安全性和稳定性，实现计算机网络的健康发展，但是在实践操作中，如何将这些策略具体落实到位，还需要我们进一步探索和研究。同时，针对当前日益严重的网络安全问题，个人和企业的网络安全意识的提高以及网络安全教育的普及也是我们需要重视的环节。总的来说，计算机网络安全隐患的防范需要社会共同的参与和努力，每个网民都要有自我保护的意识和能力，法律法规、技术创新以及监管机制都要不断完善，只有这样，我们才能构建一个安全、稳定、健康的网络环境。

参考文献

[1] 马亚燕.计算机网络安全隐患与防范[J].网络安全技术与应用,2021(12).

[2] 李亮超.计算机网络安全隐患及防范策略[J].科技风,2019(4).

[3] 李泳志.计算机网络安全隐患与防范策略研究[J].数字通信世界,2020(2).